Xanadu Security Management

Last updated: 06/13/2026

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Please read the ServiceNow Website Terms of Use at www.servicenow.com/terms-of-use.html

Company Headquarters
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

servicenow

Table of Contents

Security Operations **5**

Exploring Security Operations 6

Now Assist for Security Incident Response 11

Exploring Now Assist for Security Incident Response 13

Configuring Now Assist for Security Incident Response 17

Using Now Assist for Security Incident Response to close security incidents 25

Using AI agentic workflows in Now Assist for Security Incident Response 42

Now Assist for Vulnerability Response 51

Exploring Now Assist for Vulnerability Response 53

Configuring Now Assist for Vulnerability Response 55

Using agentic workflows in Now Assist for Vulnerability Response 56

Vulnerability Response AI agent collection for the Assess vulnerability exposure agentic workflow 58

Vulnerability Response AI agent collection for the Analyze vulnerability remediation status agentic workflow 60

Unified Security Exposure Management 62

Explore 64

Implement 121

Integrate 190

Use 205

Reference 263

Vulnerability Response 285

Application Vulnerability Response 1070

Container Vulnerability Response 1268

Configuration Compliance 1341

Vulnerability Response Workspaces 1605

Software Bill of Materials 1789

Enterprise security case management applications 1829

Security Incident Response 1830

Threat Intelligence 3265

Security Posture Control 3509

Explore 3510

Use the workspace 3526

Use mitigation controls 3556

Reference 3578

Cybersecurity Executive Dashboard 3592

Opt-in for benchmark scores 3609

Set targets 3610

Security Simulation and Training Integration for Security Operations 3611

Risk and compliance dashboard for GRC: Metrics 3613

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence Security Center....3622
Explore....3624
Configure....3630
Integrate....3633
Administer....3717
Reference....3776
Use....3787
Data Loss Prevention Incident Response....4001
Explore....4001
Configure....4004
Administer....4005
Manage incidents....4057
Inbound integration....4077
DLP integrations....4080
Security Operations common functionality....4157
Create and define filter groups in Security Operations....4160
Shared data transformation....4161
Security Operations email processing....4164
Security Operations field mapping....4174
Security Operations field value transforms....4178
Security Operations enrichment data mapping....4179
Security Operations user-defined escalation....4182
Create domain-separated property overrides....4183
Create an operating system group....4184
Set up security tag groups and tags....4186
Security annotations....4189
Components installed with Security Support Common....4192
Search Security Operations....4193
Security Operations Integration Reference....4193
Security Operations workflow triggers....4286
Security Operations Orchestration....4288
Security Operations and the ServiceNow Store....4289
Download an application from the ServiceNow Store for the first time....4289
Install a Security Operations integration....4295
Update an application previously downloaded from the ServiceNow Store....4299
Upgrade your instance to the next family release....4300

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations

ServiceNow® Security Operations applications import incident data from your security tools into a structured response engine that uses intelligent workflows, automation, data visualizations, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

Choose one of these tiles to get started.

Security Operations applications and their workspaces



Learn how the Security Operations applications can help you improve your security posture.

Now Assist for Security Incident Response



Learn how Now Assist for Security Incident Response supports ServiceNow® Generative AI (GenAI) skills in the Security Incident Response Workspace and in the Core UI (UI16).

Now Assist for Vulnerability Response



Learn how Now Assist for Vulnerability Response supports ServiceNow® Generative AI (GenAI) skills in the Vulnerability Response Workspace and in the Core UI (UI16).

Unified Security Exposure Management (USEM)



Learn about USEM to transform and manage the security exposure across your digital estate.

Upgrade Vulnerability Response to USEM



Upgrade Vulnerability Response applications to Unified Security Exposure Management.

Enterprise security case management applications



Learn about the applications in Security Incident Response that help you analyze, isolate, and fix critical security incidents as they evolve.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Posture Control applications



Learn about the applications that help you gain insights into your overall security posture.

Cybersecurity Executive Dashboard



Learn how the Cybersecurity Executive Dashboard consolidates data from the various SecOps products into a unified dashboard.

Threat Intelligence Security Center



Learn how the Threat Intelligence Security Center (TISC) platform provides technology solutions for aggregation and management of threat intelligence.

Data Loss Prevention Incident Response



Learn how you can manage sensitive information for your customers and identify and protect your data loss channels.

Security Operations shared applications



Learn about features and modules that provide common functionality across Security Operations.

Security Operations scenarios and examples



Learn more about how to get Security Operations applications from the ServiceNow® Store and scenarios for applications that you can employ while using the products.

Troubleshoot and get help

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring Security Operations

Protect your assets and enterprise environment with ServiceNow Security Operations applications and the power of the ServiceNow AI Platform®. Connect your security and IT teams to help you prioritize and resolve threats based on the impact they pose to your organization.

Security Operations overview

The Security Operations suite of applications helps you protect your assets by improving your overall security posture. For example, by integrating applications such as Unified Security Exposure Management (USEM) Security Incident Response, Vulnerability Response, and Security Posture Control with your existing security tools, your Security Operation Center (SOC) analysts, managers, and IT teams can:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Respond to rapidly evolving cyber and security threats.
- Identify, prioritize, and remediate exposure findings in the Unified Security Exposure Management (USEM) platform that brings together infrastructure, application, container, and configuration exposures into one unified experience.
- View your complete asset inventory.
- Determine your overall security tool coverage.
- Resolve security incidents faster with intelligent workflows and ServiceNow Generative AI skills (GenAI). See Now Assist for Security Incident Response for more information.

Security Operations applications for workflows

The Security Operations applications fall under two broad categories for Security Operations workflows:

- Unified Security Exposure Management (USEM) - Applications and tools that help you anticipate, understand, and close your security exposures. See Unified Security Exposure Management (USEM) for more information about using Security Operations applications in USEM.
- Enterprise security case management - Applications and tools that help you move quickly to respond to critical incidents.

Benefits of the Security Operations applications

View Security Operations applications and data with next-generation user interfaces (workspaces). With workspaces, the security analysts, Security Operation Center (SOC) managers, and remediation specialists in your organization can monitor and manage the following types of workflows from one location:

- The life cycle of security incidents from an initial analysis to containment, eradication, and recovery.
- The security exposures that they care the most about so they can decide strategically which vulnerabilities they send to IT teams to fix.
- Key insights and key use cases for security tool coverage and asset hygiene that report and monitor imported information about your assets.

The two categories of Security Operations applications and the use cases they help you address in your enterprise environment:

- USEM applications - Applications that help you anticipate threats and identify security exposures.
- Enterprise security case management applications - Applications that help you respond to critical security breaches and incidents

USEM applications

Applications that help you anticipate threats and identify security exposures

Application	Description	Users
Security Posture Control	Gain insights into how well security tools are deployed and covering your assets based on an asset inventory	• CISO • Information security analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Applications that help you anticipate threats and identify security exposures (continued)

Application	Description	Users
	and imported data. Service graph connectors and ServiceNow products such as Hardware Asset Management (HAM) and ITOM Discovery are supported for data imports. Audits based on policies help you prioritize the remediation of high-risk combinations such as internet exposure and known vulnerabilities. Create custom policies and insights to monitor the compliance of assets with your internal security tool configuration standards.	• Security operations manager • IT Operations engineer • Service owner (remediation owner persona)
Unified Security Exposure Management (USEM)	View security exposure findings as well as consolidated, multiple exposure findings across all asset types in one unified platform. Monitor and manage all types of security exposures across your organization's attack surface that use imported data from the following applications: • Vulnerability Response • Application Vulnerability Management • Configuration Compliance • Container Vulnerability Response	• Vulnerability managers and analysts • Compliance managers and analysts • Remediation owners • Security champions • Service owners

Enterprise security case management applications

Applications that help you respond to critical security breaches and incidents

Application	Description	Users
Security Incident Response	Simplify the process of identifying critical incidents by applying powerful workflow	• CISO • Information security analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Applications that help you respond to critical security breaches and incidents (continued)

Application	Description	Users
	and automation tools that speed up remediation. Integrate your existing Security Information and Event Manager (SIEM) tools with Security Incident Response and Security Operations applications to import threat data from various sources and automatically create prioritized security incidents.	• Security operations manager • Threat intelligence analyst
Major Security Incident Management	The major security incident management capabilities work with the existing security incident response product capabilities. This includes an ability for a security analyst to escalate a standard security incident to a major security incident, so that the new product capabilities are available to support the remediation process. Track the progress of Major Security Incident (MSI) from discovery to analysis. Propose solutions, promote, and link security incidents, and closure.	• CISO • Information security analyst • Security operations manager • IT Operations engineer • Service owner (remediation owner persona) • General council
Data Loss Prevention Incident Response	The Data Loss Prevention Incident Response (DLP IR) permits you to review and manage the remediation workflow of DLP incidents from multiple sources, such as endpoint, network, email, and cloud. With the DLP application, you can identify, respond, and protect your data loss channels.	• CISO • Information security analyst • Security operations manager
Threat Intelligence	Allows incident response teams to automate threat lookups, searches, and correlation. The integration	• CISO • Information security analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Applications that help you respond to critical security breaches and incidents (continued)

Application	Description	Users
	with MITRE ATT&CK permits you to measure and understand detection and mitigation coverage and assists with threat hunting.	• Security operations manager • Threat intelligence analyst
Threat Intelligence Security Center (TISC)	Aggregate, curate, and manage threat intelligence from multiple sources and conduct threat intelligence case management. Track campaigns, operationalize threat intelligence, and respond to actionable intelligence.	• CISO • Information security analyst • Security operations manager • Threat intelligence analyst

What to explore next

Select a tile to get started with the Security Operations Workspaces.

Security Incident Response Workspace  Learn about the Security Incident Response Workspace	**Security Exposure Management Workspace**  Learn about the Security Exposure Management Workspace	**Security Posture Control Workspace**  Learn about the Security Posture Control Workspace
Vulnerability Assessment Workspace  Learn about the Vulnerability Assessment Workspace	**IT Remediation Workspace**  Learn about the IT Remediation Workspace	**Software Bill of Materials Workspace**  Learn about the Software Bill of Materials Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence Security Center (TISC) Workspace	Data Loss Prevention (DLP) Incident Response Workspace	Major Security Incident Management (MSIM) Workspace
		
Learn about the TISC Workspace	Learn about the DLP Workspace	Learn about the MSIM Workspace

Troubleshoot and get help

ServiceNow Community

ServiceNow Community

Customer Success Center

Impact

Developer

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow University

NowCreate

Best Practices

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://servicenow.com

ServiceNow Store

http://servicenow.com

Support

- https://support.servicenow.com/now
- Known Error Portal

Now Assist for Security Incident Response

Security analysts can use intelligent workflows and ServiceNow generative AI skills to help them resolve security incidents. Security managers can review the context of security incidents and closure notes quickly in a concise, easy-to-read format, view post-incident analysis data,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and see recommended remediation steps with the Now Assist for Security Incident Response application.

Get started

Note: The Now Assist for Security Operations application in the ServiceNow® Store and in your ServiceNow AI Platform instance has changed to the Now Assist for Security Incident Response application starting with version 2.0.1.

Explore	Configure	Use
 Learn about Now Assist for Security Incident Response	 Learn how to configure and activate the skills for Now Assist for Security Incident Response	 Learn how to summarize details and generate closure notes for security incidents with generative AI and Now Assist for Security Incident Response
	Use Security Incident Response AI agent collection  Use the AI agent use cases in Now Assist for Security Incident Response	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important:

- Not all model providers are available for customers with in-country SKUs, and some Now Assist products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some Now Assist products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base . Be sure to check for availability updates in future releases.
- Some Now Assist products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

Troubleshoot and get help

- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

AI limitations

This application uses artificial intelligence (AI) and machine learning, which are rapidly evolving fields of study that generate predictions based on patterns in data. As a result, this application may not always produce accurate, complete, or appropriate information. Further, there is no guarantee that this application has been fully trained or tested for your use case. To mitigate these issues, it is your responsibility to test and evaluate your use of this application for accuracy, harm, and appropriateness for your use case, employ human oversight of output, and refrain from relying solely on AI-generated outputs for decision-making purposes. This is especially important if you choose to deploy this application in areas with consequential impacts such as healthcare, finance, legal, employment, security, or infrastructure. You agree to abide by ServiceNow's AI Acceptable Use Policy, which may be updated by ServiceNow.

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. In addition, this application will collect data from incidents, change requests, problems, and vulnerable items. Customers can opt out of future data collection at any time, as described in the Now Assist Opt-Out page.

For more information see the Now Assist documentation.

Exploring Now Assist for Security Incident Response

Your security analysts can use intelligent workflows and ServiceNow generative AI skills to help them triage, investigate, and close security incidents within the flow of their work with the Now Assist for Security Incident Response application.

Now Assist for Security Incident Response overview

With generative AI skills, your security analysts have the option to:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Summarize security incident details and review the context quickly in a concise, easy-to-read format.
- Generate recommended next steps for a security incident.
- Generate post-incident analysis data.
- Generate closure notes.
- Generate correlation insights
- Generate Security Operation Center (SOC) Performance Analysis

Security analysts can share findings, incident details, and closure notes with other analysts, managers, and key stakeholders.

Now Assist for Security Incident Response users

Users

User	Description
Security analysts and managers	Preview security incident details, see their potential impact, and view the key remediation actions already taken with security incident summaries using generative AI. Summaries and recommended next steps (actions) give analysts and managers a head start with their investigations and help with closing security incidents. Automatically generate a draft of closure notes using generative AI. Closure notes for security incidents are created quickly based on remediation and containment activities, in addition to other relevant details that are related to their closure.

Now Assist for Security Incident Response benefits

Now Assist for Security Incident Response features

Benefit	Feature	Users
Expedite triaging of security incidents with long activity streams by reviewing work notes and contextual information quickly in a concise, easy-to-read format.	Generate summaries for security incidents that include the following information: • Issue • Details • Observations • Key actions taken • Closure details	• Security analysts • Security managers
Automatically generate a draft of closure notes for a security incident when it's ready for closure. Analysts can modify any content that is generated by the AI skill by editing it,	Generate security incident closure notes	• Security analysts • Security managers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Now Assist for Security Incident Response features (continued)

Benefit	Feature	Users
removing it, or adding their own notes before they close the security incident.		
Generate recommended next steps within the workflow upon request to help you close a security incident.	Generate security incident recommended actions	• Security analysts • Security managers
Generate a post-incident analysis that includes a root cause analysis, impact assessment, and lessons learned within the workflow of closing a security incident.	Generate post-incident analysis	• Security analysts • Security managers
Connect current incidents to past events that involve the same affected users, configuration items (CIs), or observables.	Generate correlation insights	• Security analysts • Security managers
Gain insight into how efficiently your security analysts are working with security incidents with an AI agent.	Generate Security Operation Center (SOC) Performance Analysis and get suggestions for improvement from an AI agent. **Note:** You must activate the Security operations metrics analysis skill if you want to use the Analyze security operations metrics agentic workflow. See Configure and activate a skill for Now Assist for Security Incident Response for more information.	Security managers
Learn about the details of a security incident quickly by accessing summaries and closure notes from the Now Assist panel.	Access the generative AI summary and closure notes from the Now Assist panel. Type in requests for more basic information about security incidents in the panel.	• Security analysts • Security managers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Now Assist for Security Incident Response features (continued)

Benefit	Feature	Users
Customize the generative AI skills for summaries and closure notes to suit your needs.	Copy a skill and modify select related table fields, define the availability of the skill, and choose where the skill is displayed.	admin

What to explore next

To learn more about configuring and using Now Assist for Security Incident Response, see:

- Configuring Now Assist for Security Incident Response
- Summarize a security incident with Now Assist for Security Incident Response
- Generate closure notes for a security incident with Now Assist for Security Incident Response
- Generate correlation insights with Now Assist for Security Incident Response
- Generate recommended actions for a security incident with Now Assist for Security Incident Response
- Generate a post-incident analysis for a security incident with Now Assist for Security Incident Response
- Inputs and triggers for Now Assist for Security Incident Response
- Using AI agentic workflows in Now Assist for Security Incident Response

Supporting information for Now Assist for Security Incident Response

Get a quick overview of the important information that is related to the Now Assist for Security Incident Response application.

Supported versions

Version 3.2 of Now Assist for Security Incident Response supports:

- Security Operations UI Components, v1.0.1
- Recommended Actions for Security Operations, v1.0.1
- legacy UI (UI16): Security Incident Response core application, v13.6.5
- Security Incident Response Workspace (SIR Workspace), v1.7.0
- Now Assist for ServiceNow AI Platform® v6.3.0

Version 2.0.1 of Now Assist for Security Incident Response supports:

- legacy UI (UI16): Security Incident Response core application, v13.6.4
- Security Incident Response Workspace (SIR Workspace), v1.7.0
- Now Assist for ServiceNow AI Platform® v6.0.1

Note: The Now Assist for Security Operations application in the ServiceNow® Store and in your ServiceNow AI Platform instance has changed to the Now Assist for Security Incident Response application starting with version 2.0.1.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supported user interfaces

The Now Assist for Security Incident Response includes the generative AI skills listed in the following table.

Now Assist for Security Incident Response supported interfaces and skills

Interface	Features
Security Incident Response	• Security Incident summarization. • Recommended next steps generation for a security incident. • Post incident analysis generation that includes root cause analysis, impact assessment, and lessons learned. • Now Assist panel. • Closure notes generation. • Correlation insights from the Now Assist panel. • Analyze security operations metrics for your remediation teams.
Legacy UI16	• Security Incident summarization • Recommended next steps generation for a security incident. • Post incident analysis generation that includes root cause analysis, impact assessment, and lessons learned. • Now Assist panel. • Closure notes generation. • Correlation insights from the Now Assist panel. • Analyze security operations metrics for your remediation teams.

Configuring Now Assist for Security Incident Response

The Now Assist for Security Incident Response application is supported in the Security Incident Response Workspace and in the legacy Core UI (UI16). You can use the guided setup in the Now Assist Admin console to configure Now Assist for Security Incident Response.

Configuration overview

By sharing data with the ServiceNow® AI development program, you provide relevant data to help improve prediction accuracy, user experience, tailor products to your business needs, and reduce hallucinations for your activated Now Assist skills.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can choose to opt out of a ServiceNow instance from data sharing from the Now Assist Admin console if you don't want to participate. See Opt out of data sharing for Now Assist. Repeat the opt-out process for all instances that use the Now Assist functionality.

Use the Now Assist Admin console to configure Now Assist for Security Incident Response. This console contains everything that you must install the applications and configure the generative AI skills. For additional information, see Configuring Now Assist settings and features.

The following table lists the features and skills that you can access from the Now Assist Admin console.

Now Assist for Security Incident Response features and skills in the Now Assist Admin console

Now Assist Technology product	Security incident skills
Now Assist for Security Incident Response	Security Incident summarization **Note:** The incident summarization supports security incidents in any state other than **Draft**.
	Resolution notes generation.
	Security incident recommended actions The security incident recommended actions skill supports security incidents in any state other than **Closed** and **Cancelled**. **Note:** The AI Search application must be enabled so that the Recommended Actions skill works for security incidents. To verify AI Search is enabled on your instance, navigate to **All** > **AI Search** > **AI Search Status**. Contact support if the page indicates AI Search is not enabled. Correlation insights supports security incidents in all states.
	Post-incident analysis generation
	Analyze security operations metrics for your remediation teams and get suggestions for improvement from an AI agent.

1. Install Now Assist plugins.

   Note: The Now Assist for Security Operations application in the ServiceNow® Store and in your ServiceNow AI Platform instance has changed to the Now Assist for Security Incident Response application starting with version 2.0.1.

   Install the Now Assist for Security Incident Response application (sn_sec_gen_ai).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Configure and activate a skill for Now Assist for Security Incident Response.

   Configure and review the details for a skill. You activate a skill from the Guided Setup.

Using Guided Setup to implement Now Assist for Security Incident Response

Guided Setup provides a sequence of tasks that help you configure Now Assist for Security Incident Response on your ServiceNow instance. To open the Guided Setup for Now Assist for Security Incident Response, navigate to **All** > **Now Assist Admin** > **Skills**.

For more information, see Configure and activate a skill for Now Assist for Security Incident Response.

Configure and activate a skill for Now Assist for Security Incident Response

Configure and review the details for a skill in the Guided Setup. You can activate a skill from the Guided Setup.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Now Assist Admin** > **Skills**.
2. Select **Security Operations** from the list.
   You cannot edit the skills that are included with the application. To edit the default settings, you must make a copy. For more information about customizing a skill, see Customize a Now Assist for Security Incident Response skill.
   These Security Incident Response skills are displayed:
   - Resolution notes generation
   - Security incident summarization
   - Security operations metrics analysis

     Note:

     This skill is activated for use with an AI agent. See Analyze security operations metrics agentic workflow for more information.

   - Correlation insights generation
   - Post incident analysis
   - Security incident recommended actions

     The AI Search application must be enabled so that the Recommended Actions skill works for security incidents. To verify AI Search is enabled on your instance, navigate to **All** > **AI Search** > **AI Search Status**. Contact support if the page indicates AI Search is not enabled.
3. Select **Activate skill** for the skill that you want.

   Note: After you activate a skill, you must deactivate it if you want to edit the configuration settings.

4. Follow the steps to configure and activate a skill using the Guided Setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Some skills do not require all the configuration steps listed below. Select the only tasks that are displayed in the left panel and follow the prompts. After you have completed all the tasks, activate the skill.

5. Select **General Details**.
6. Select **Save and continue** to go to the next step in the Guided Setup.
7. Select **Choose input** to configure the inputs or triggers for the selected skill.

   Some, or all of the following input templates for the skill are listed: **Work In Progress**, **Review**, and **Closed**. The **Work In Progress** template is selected.

   You might prefer to leave these input templates in their default settings until you become familiar with how the skills for Now Assist for Security Incident Response work.

   However, for some of the skills you can modify certain related table fields, test the prompt on a security incident, define the availability of the skill, and choose where the skill is displayed.

   If you choose to modify fields, select only the supported options from the lists provided as part of your input data.

   If you modify the inputs or triggers for a skill, you determine how and when a skill is used. You can't modify a skill's input data source. The data source contains the tables and fields that the skill relies on. However, you can copy a skill and customize it. For more information, see Customize a Now Assist for Security Incident Response skill.
8. **Optional:** If available, select **Customize Prompt** to test the prompt on a security incident record.
9. Select **Save and continue** to go to the next step in the Guided Setup.
10. **Optional:** Choose one of the following options to define availability.

Option	Description
Skill is always available	Skill is always available to users.
Customize skill availability	The skill is available only when certain conditions are met (Default). (Optional) Use the condition builder to set your conditions.

11. Select **Save and continue** to go to the next step in the Guided Setup.
12. Choose **Select display**.

    Select the expand icons ( ) in the sections under Select Display to determine where you'd like the skill to display and who can view it. Skills might have some or all of the following options after you expand a section.

Option	Description
In-product desktop	Select the **Display** toggle so that Now Assist skills with this option are displayed on forms and workspaces.
Now Assist panel	Select the **Display** toggle to display the skill in the Now Assist panel.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Note: If you don't see this option, you must activate the Now Assist panel. For more information, see Turn on the Now The security incident recommended ac tions and post-incident analysis skills are not available from the Now Assist panel.
Conversational experiences	Verify where the skill is displayed and add roles for who can view it. Select **Now Assist Panel** in the Conversation al experiences field to display the skill in the Now Assist panel.

13. Select **Save and continue** to go to the next step.
14. Review your choices and select **Activate** to complete the configuration for the skill.
15. Select **Select back to skills** to return to the Now Assist skills page.

Customize a Now Assist for Security Incident Response skill

Customize some of the input fields of a generative AI skill to suit the requirements of your environment.

Before you begin

Roles required: admin

Procedure

1. Navigate to **All** > **Now Assist Admin** > **Skills**.
2. Select **Security Operations** from the list.
   These Security Incident Response skills are displayed:
   - Resolution notes generation
   - Security incident summarization
   - Security operations metrics analysis

     This skill is activated for use with an AI agent. See Analyze security operations metrics agentic workflow for more information.
   - Correlation insights generation
   - Post incident analysis
   - Security incident recommended actions

     The AI Search application must be enabled so that the Recommended Actions skill works for security incidents. To verify AI Search is enabled on your instance, navigate to **All** > **AI Search** > **AI Search Status**. Contact support if the page indicates AI Search is not enabled.
3. Create a copy of a skill and customize the input fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the more actions icon ( ) on a card.

b. Select **Make a copy**.

c. Confirm your choice in the modal.
The guided setup is displayed.

d. In **General details**, enter a unique name and description for the skill.

e. Proceed to the next step by selecting **Save and continue**.

f. Select **Choose input**.

> **Note:** Some skills do not require all the configuration steps listed below. Select the only tasks that are displayed in the left panel and follow the prompts. After you have completed all the tasks, activate the skill.

Some, or all of the following input templates for the skill are listed: **Work In Progress**, **Review**, and **Closed**. The **Work In Progress** template is selected.

You can configure some of the base input table fields, the conditions, and the related lists for the templates. Select only from the related tables supported on the lists for your input data.

You can’t modify the base input table [sn_si_incident] or add a new data source for your copy of the security incident summarization skill.

g. Continue to modify the editable fields in the templates with filtering conditions.

h. Continue to modify the editable fields in the Work In Progress template with the condition builder and filtering conditions.

i. Select **Save template** to save your changes to a template.

j. Proceed to the next step in the Guided Setup for the Work In Progress template by selecting **Save and continue**.

- **Customize prompt**: Edit the prompt by reordering or removing the predefined sections. You can review and test the prompt on a security incident record for each input template configuration.
- **Define availability**:

Option	Description
Skill is always available	The skill is always available to users.
Customize skill availability	The skill is available only when the conditions are met (Default). Use the condition builder to set your conditions.

- **Select display**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
In-product desktop	Select the **Display** toggle so that Now Assist skills with this option are displayed on forms and workspaces.
Now Assist panel	Select the **Display** toggle to display the skill in the Now Assist panel. **Note:** If you don't see this option, you must activate the Now Assist panel. For more information, see Turn on the Now Assist panel. The security incident recommended actions and post-incident analysis skills are not available from the Now Assist panel.

k. Select **Save and continue** to proceed to the next step in the Guided Setup.

l. Select **Review and Activate** to review your skill and make any additional modifications.

4. Review your choices and select **Activate** to complete the configuration for the skill.
5. Select **Select back to skills** to return to the Now Assist skills page.

Inputs and triggers for Now Assist for Security Incident Response

You can configure some of the inputs or triggers for a generative AI skill. Inputs or triggers permit you to determine how and when a skill is used.

Inputs and triggers

Inputs identify the data used for a skill. Inputs include the table and fields used to generate a security incident summary. A trigger initiates an action. For example, triggers determine when the system generates a summary.

You can modify inputs and triggers, but you can't modify a skill's data source. The data source contains the tables and fields that the skill relies on.

Security incident summarization skill

Inputs for the security incident summarization skill identify the table and fields used when a security incident summary is generated. The following table lists the inputs for the Security Incident summarization skill from the Choose Input page in the Now Assist Admin console.

Input	Description
Data source	Security Incident [sn_si_incident] table.
Input fields	• Short description • Description

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input	Description
	• State • Priority • Work notes • Additional comments
Related Input tables	• Affected CIs - configuration item • Affected Users - Users • Security Incident Response Task - Short description • State - Any state other than **Cancelled**. • Associated Observables - Observable finding is Malicious or Suspicious.

Resolution notes generation skill

Inputs for the Resolution notes generation skill identify the table and fields that are used when the resolution notes are generated for a security incident. The following table lists the inputs for the resolution notes generation skill from the Choose Input page in the Now Assist Admin console.

Input	Description
Data source	Security Incident [sn_si_incident] table.
Input fields	• Short description • Description • Work notes • Additional comments

Security incident recommended actions generation skill

Input	Description
Data source	Security Incident [sn_si_incident] table.

Post incident analysis generation skill

Input	Description
Data source	Security Incident [sn_si_incident] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Correlation insights generation skill

Your correlation insights for a security incident can contain records from the following tables, but you must have permission to access these tables and records.

Input	Description
Data source	Security Incident [sn_si_incident] table. Configuration item [cmdb_ci] table. Incident [incident] table. Change request [change_request] table. Problem [problem] table. Vulnerable item [sn_vul_vulnerable_item] table. Associate observable [sn_ti_observable] table.

Using Now Assist for Security Incident Response to close security incidents

Security analysts can close security incidents quickly from within their flow of work with the generative AI skills supported by Now Assist for Security Incident Response.

Overview of Now Assist for Security Incident Response

With generative AI skills with Now Assist for Security Incident Response, your security analysts have the option to:

- Summarize security incident details and review the context quickly in a concise, easy-to-read format.
- Generate closure (resolution) notes.
- Generate recommended actions for a security incident
- Generate post incident analysis data
- Generate performance metrics for your remediation teams.

  This skill is activated for use with an AI agent. See Analyze security operations metrics agentic workflow for more information.

- Generate correlation insights to speed up incident investigation.

Security managers and analysts can request security incident summaries and closure notes from the following locations:

- Security incident records
- Security Incident Response Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Now Assist panel.

> **Note:** The security incident recommended actions and post-incident analysis skills are not available from the Now Assist panel.

Security managers and analysts can generate recommended next steps and post-incident analysis data from the following locations:

- Security incident records
- Security Incident Response Workspace

Security managers and analysts can create remediation tasks from generated recommended actions only from security incidents in the Security Incident Response Workspace.

1. Summarize a security incident with Now Assist for Security Incident Response

   Generate a summary for a security incident that includes the underlying issue, incident details, related lists data (observables), and key actions already taken.

2. Generate recommended actions for a security incident with Now Assist for Security Incident Response
3. Generate a post-incident analysis for a security incident with Now Assist for Security Incident Response
4. Generate correlation insights with Now Assist for Security Incident Response
5. Generate closure notes for a security incident with Now Assist for Security Incident Response

   Automatically generate the closure notes for a security incident.

6. Request generative AI skills in the Now Assist panel for Now Assist for Security Incident Response

   Generate summaries and closure notes from the Now Assist panel.

   > **Note:** The security incident recommended actions and post-incident analysis skills are not available from the Now Assist panel.

7. Customize a Now Assist for Security Incident Response skill

   Customize the input fields of a skill to suit the requirements of your environment.

Summarize a security incident with Now Assist for Security Incident Response

Understand the context of a security incident with the Security Incident summarization generative AI skill.

Before you begin

You can summarize a security incident in the legacy Core UI (UI16) and in the Security Incident Response Workspace. There must be a minimum of 50 words in the fields that are used for the input data to summarize an incident using generative AI. For more information about the input fields, see Inputs and triggers for Now Assist for Security Incident Response.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the legacy Core UI, navigate to **All** > **Security Incident** > **Incidents** and open a security incident that is assigned to you.
2. Alternatively, navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
3. On the **Overview** tab, select **Summarize**.
   - The generated summary is displayed in a banner at the top of the security incident record in legacy Core UI16.
   - The generated summary is displayed on the **Overview** tab in the Security Incident Response Workspace.
4. **Optional:** Select from the following options after the summary is generated.

   (Optional) Summaries generated by AI might miss key details. You might prefer to review the summary for accuracy and completeness before you proceed.

Option	Description
View details about the summary	Select the information icon (ⓘ) next to the Security Incident summarized by Now Assist.
Save the summary information by adding it to the incident work notes	**a.** Select **Share to work notes**. **b.** Verify the AI-generated content in the modal for accuracy and make any edits. **c.** Select **Save to work notes**.
Expand or collapse the summary	Select the expand icon (⌄) or collapse icon (⌃) next to **Share to work notes** to expand or collapse the summary.
Provide feedback	Select the helpful icon (👍) for positive feed back. Select the not helpful icon (👎) if the summary wasn't helpful. **Note:** Feedback improves the genera tive AI model and can help to improve fu ture versions of this skill.
Copy the summary	Select the copy icon (⧉) to copy the summa ry to the clipboard.

Generate closure notes for a security incident with Now Assist for Security Incident Response

Automatically generate a draft of the closure notes for a security incident when you close it. The draft is editable and will be reviewed prior to closing the security incident, and it can be used or modified as needed. Closure notes provide information about the resolution of a security incident to other analysts, managers, and key stakeholders.

Before you begin

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If the Close code or Close notes fields are already updated for a security incident, Now Assist will not modify these fields, regardless of the incident's current state. To enable Now Assist to update these fields, ensure that both the Close Code and Closure Notes fields are left blank.

Procedure

1. In the legacy Core UI, navigate to **All** > **Security Incident** > **Incidents** and open a security incident that is assigned to you.
2. Alternatively, navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
3. Close the security incident.

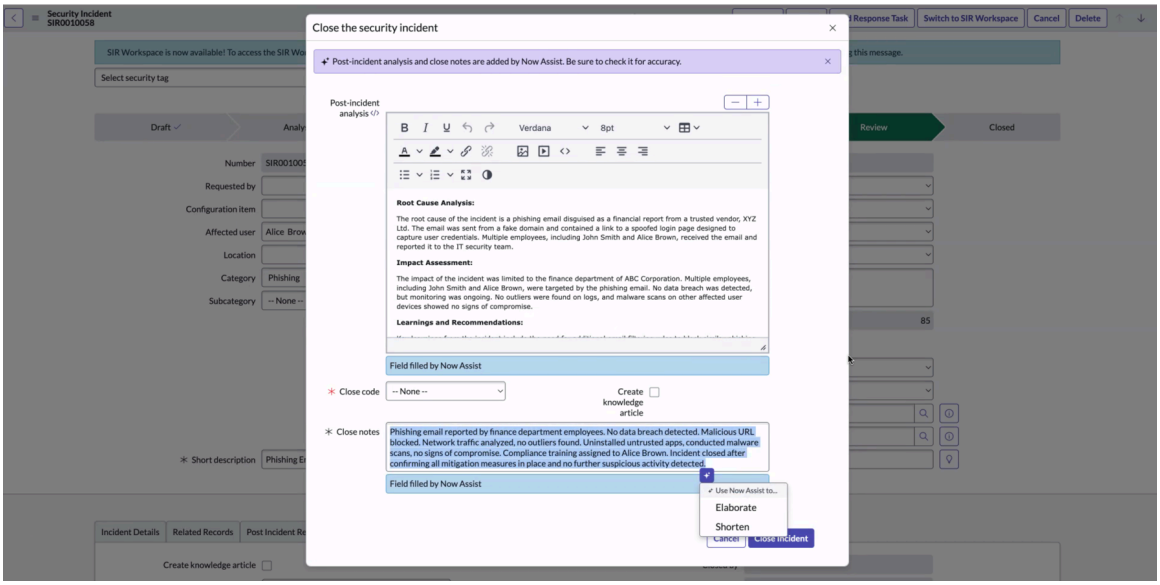
Option	Description
Close the security incident in legacy Core UI16	**a.** Change the **State** field to **Closed**. The stepper modal is displayed. **b.** Review each step and select **Next**. **c.** Select **Provide resolution details**. **d.** Click on the **Close notes** section and use the Now Assist Context Menu (NACM) to generate the resolution notes. The close notes will be auto-generated if no text ex ists, or you can modify the existing text as needed by choosing the required option from NACM. **Note:** You might want to review the generated text and make sure it's ac curate before you close the securi ty incident. Edit the notes or delete them to provide your own. You can al so **Elaborate** or **Shorten** the generat ed text. **e.** Select the required option from the Now As sist Context menu. **Elaborate** will help you to elaborate the text and replaces the se lected resolution text. In case, if you wish to shorten the resolution text you can select **Shorten** option from the Context menu to make the text more concise. **f.** Update the Close code and select **Close in cident**. The resolution summary is displayed in the Resolution Information section on the secu rity incident record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

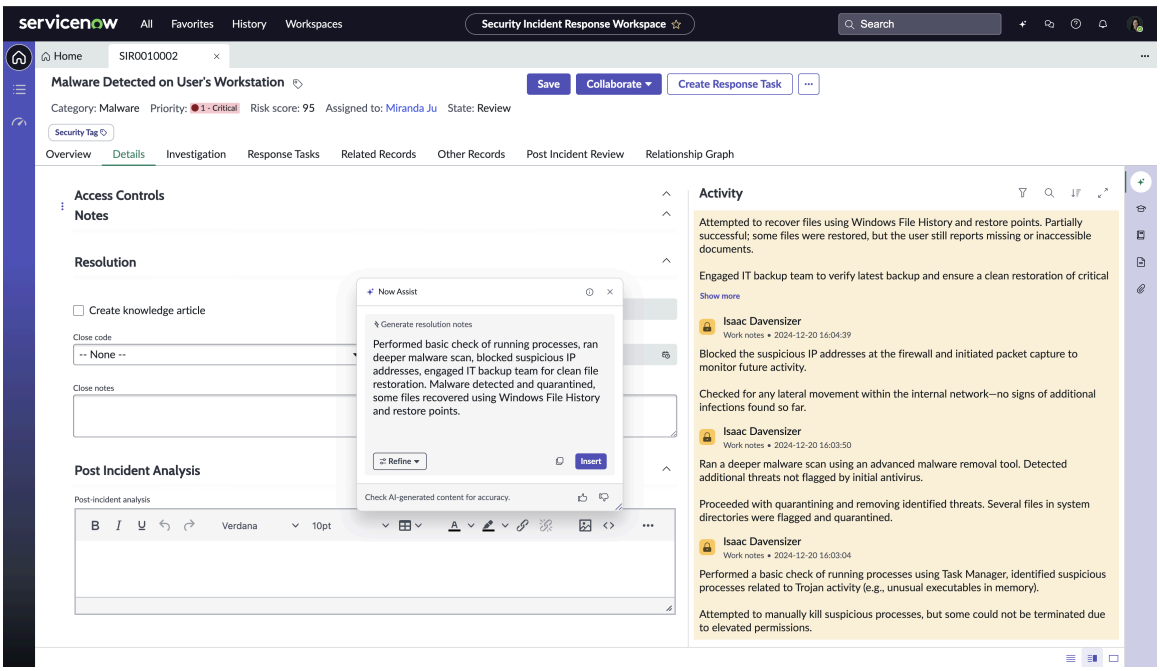
Option	Description
Close the security incident from the Securi ty Incident Response Workspace	**a.** On the **Details** tab of the workspace, change the **State** field to **Closed**. The stepper modal is displayed. **b.** Review each step and select **Next**. **c.** Select **Provide resolution details** **d.** Click on the **Close notes** section and use the Now Assist Context Menu to generate the resolution notes. The close notes will be auto-generated if no text exists, or you can modify the existing text as needed us ing the NowAssist options. **Note:** You might want to review the generated text and make sure it's ac curate before you close the securi ty incident. Edit the notes or delete them to provide your own. You can al so **Elaborate** or **Shorten** the generat ed text. **e.** Select the required option from the Now As sist Context menu. **Elaborate** will help you to elaborate the text and replaces the se lected resolution text. In case, if you wish to shorten the resolution text you can select **Shorten** option from the Context menu to make the text more concise. **f.** Update the Close code and select **Close in cident**. The resolution summary is displayed on the **Details** tab on the security incident record in the workspace. **Note:** Using the Now Assist Context menu, you can directly add or gener ate the resolution notes in the **Close notes** section on the incident record itself, when the incident is in the **Re view** state. For more information, see the screen shot below.

The following screen shot depicts the resolution notes generated for closing the security incident in Core UI16.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

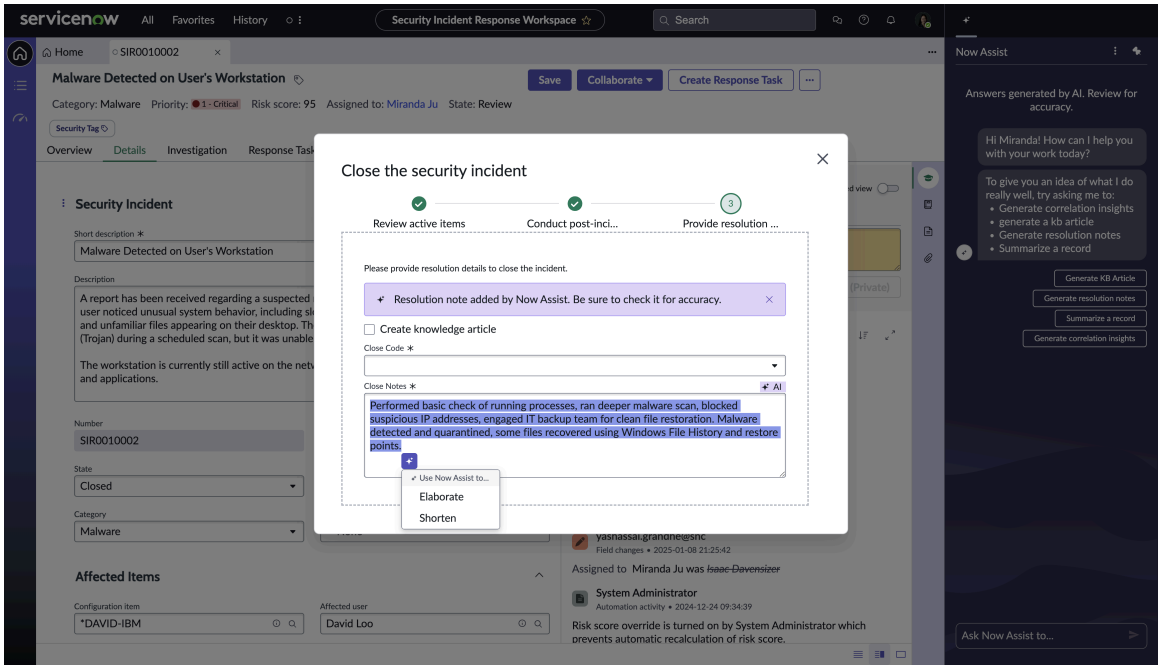


Auto-generated resolution notes from the Security Incident Response Workspace.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Edit the resolution notes generated using the Now Assist context menu on the Security Incident Response workspace.



Generate recommended actions for a security incident with Now Assist for Security Incident Response

Automatically generate the next steps your analysts can take to help them close a security incident in the Security Incident Response Workspace. The recommended steps are based on existing security incidents and knowledge articles.

Before you begin

Recommended next steps work for active security incidents in any states other than **Closed** or **Cancelled**.

The AI Search application must be enabled so that the Recommended Actions skill works for security incidents. To verify AI Search is enabled on your instance, navigate to **All** > **AI Search** > **AI Search Status**. Contact support if the page indicates AI Search is not enabled.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
2. Select the **Recommended Actions** icon (✦) in the contextual sidebar.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Select **Get recommendations**.
4. In the Check AI generated content modal, select **I acknowledge**.
   Generated recommended actions are displayed in cards. Up to four references for the actions are displayed at the top. These references can be any combination of knowledge articles (KB)s or security incidents (SIR#).
5. In a card, choose one.

Option	Description
View details	View the details for this remediation action.
Save to work notes	Review the work notes and have the option to edit them before you save them to the work notes of the security incident.
Select a Reference link	View the security incident or the knowledge article used as the sources for these actions.

6. **Optional:** Select the refresh icon in the Recommended actions panel to regenerate the recommended actions.

   The recommended actions remain cached for one hour. You might choose to refresh the recommended steps if:

   - You believe information related to the security incident has changed since the last time you generated the actions.
   - You leave the page, log out, log back in, and return within one hour to the security incident.

   You must regenerate the actions starting with step 3 to view the them after one hour.

7. Select **Create response task** on a card.
   A new tab opens in the workspace. The **Short description** and the **Description** fields are populated automatically from the details on the recommended action card you selected.
8. Edit the form as needed and the select **Save** to create the response task.
   Until you change the Value on the system property, the two options on any recommended actions you generate remain **View details** and **Create response task**.
9. **Optional:** Create a response task from the recommended actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By default, the workflow provides you with the option to save the recommended actions to work notes from the cards. If you want to have the option to create a response task from an action card instead of saving them to work notes, you must change the Value field for the **SecOps Recommended Action** [sn_sec_ra.card_action_config] system property.

a. As a user with the Security Incident Manager role [sn_si.manager], navigate to sys_properties.LIST.

b. Locate the SecOps Recommended Action [sn_sec_ra.card_action_config] system property and open the record.

c. Change the Value from `share_to_work_notes` to `create_task`.

d. Save the record.

e. Return to the security incident record and refresh the page.
The action cards provide you with the options to **View details** and **Create response task**.

Generate recommended actions in UI16 for a security incident with Now Assist for Security Incident Response

Automatically generate the next steps your analysts can take to help them close a security incident in the UI16 (legacy) view. The recommended steps are based on existing security incidents and knowledge articles.

Before you begin

Generating recommended actions works for active security incidents in any states other than **Closed** or **Cancelled**.

The AI Search application must be enabled so that the Recommended Actions skill works for security incidents. To verify AI Search is enabled on your instance, navigate to **All** > **AI Search** > **AI Search Status**. Contact support if the page indicates AI Search is not enabled.

The recommended actions skill must be activated before you can see the **Recommended actions** button on a security incident.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. In the legacy Core UI, navigate to **All** > **Security Incident** > **Incidents** and open a security incident that is assigned to you.
2. Locate and select **Recommended actions** under the Short description field.
   The recommended actions are listed along with the reference links.

   The recommended actions remain cached for one hour. You can refresh them if you leave the page, log out, log back in, and return within one hour to the security incident.

Generate a post-incident analysis for a security incident with Now Assist for Security Incident Response

Automatically generate a post-incident analysis for a security incident that includes a root cause analysis, impact assessment, and learning and recommendations information.

Before you begin

You must have the post-incident analysis skill activated if you want a post-incident analysis generated automatically by Now Assist for Security Incident Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the Close notes are already populated manually prior to closing the security incident, this content is not over-written by Now Assist for Security Incident Response when analysts set the State field to **Closed**.

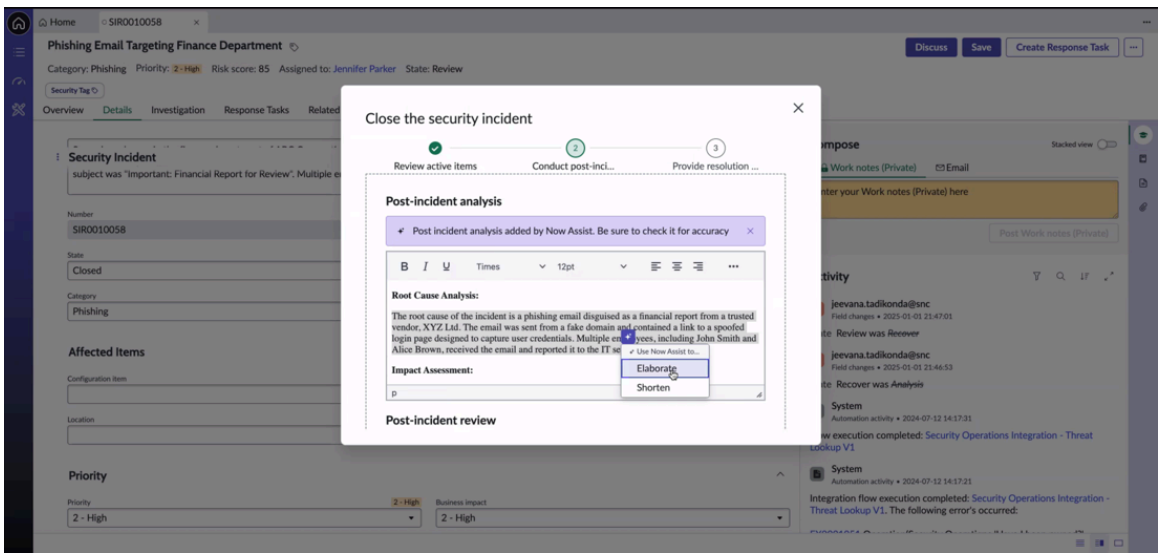
Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
2. On the **Details** tab, select **Closed** in the State field to close the security incident.
   The Close the security incident modal opens.
3. **Optional:** Select **Review active tasks** to review any active remediation tasks that are associated with this incident.
   A new tab opens with record(s) for your review. Use this option to verify that you are ready to close the security incident, because this action cancels any associated workflows and activities and closes the incident on any associated remediation tasks.
4. To generate the post-incident analysis select **Next**.
   The post-incident analysis is displayed in the modal with three sections. Note the Now Assist icon (✦) indicates the content is generated by Now Assist for Security Incident Response.
   - Root Cause Analysis
   - Impact Assessment
   - Learnings and Recommendations

   Note: You can use the Now Assist icon on any of the post-incident analysis options and elaborate or shorten the Root Cause Analysis/Impact Assessment/Learnings and Recommendations and replace the text. **Elaborate** will help you add more information to the existing text. **Shorten** will make the selected text more concise.

   The following screen shot depicts how Now Assist icons are used to elaborate or shorten and replace the desired post-incident analysis text.



5. Review the report to check for accuracy and make any edits required.
6. **Optional:** Select **Take assessment** and **Configure/preview report** to perform the post-incident review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Any edits you make to the post-incident review are preserved for one hour if you leave this page to take the assessment or perform another action. After one hour, you must set the State to **Closed** again on the incident to regenerate the post-incident analysis and close notes.

7. Select **Next** to generate the resolution notes.
   The resolution notes are displayed in the Close Notes field.
8. Select one from the list for the Close Code.
9. Select **Close Incident**.
   The post-incident analysis is saved in the Post incident analysis field on the Details tab and on the Overview tab on security incidents in Security Incident Response Workspace.

Generate a post-incident analysis in UI16 for a security incident with Now Assist for Security Incident Response

Automatically generate a post-incident analysis for a security incident that includes root cause analysis, impact assessment, and learning and recommendations information.

Before you begin

You must have the post-incident analysis skill activated if you want a post-incident analysis generated automatically by Now Assist for Security Incident Response.

If the Close notes are already populated manually prior to closing the security incident, this content is not over-written by Now Assist for Security Incident Response when analysts set the State field to **Closed**.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. In the legacy Core UI, navigate to **All** > **Security Incident** > **Incidents** and open a security incident that is assigned to you.
2. Select **Closed** in the State field to close the security incident.
   The Close the security incident modal opens. The post-incident analysis and close notes are generated and a message prompting you to review them is displayed. Note the Now Assist icon (✨) near the fields that indicates the content is generated by Now Assist for Security Incident Response.
3. Review the report and close notes to check for accuracy and make any edits required.
   Any edits you make are preserved for one hour if you leave this page. After one hour, you must set the State to **Closed** again on the incident to regenerate the post-incident analysis and close notes.
4. Select one from the list for the Close Code.
5. Select **Close Incident**.
   The security incident is displayed.
6. Select the **Post Incident Review** tab to view the analysis data.

   Note: You can use the Now Assist icon on any of the post-incident analysis options and elaborate or shorten the Root Cause Analysis/Impact Assessment/Learnings and Recommendations and replace the text. Elaborate will help you add more information to the existing text. Shorten will make the selected text more concise.

7. Select the **Closure Information** tab to view the close notes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring correlation insights with Now Assist for Security Incident Response

You can generate correlation insights to help you avoid duplicating your investigation into affected users, configuration items, and observables and help you resolve the security incident that you are working on more quickly. You select the criteria from a security incident that you want to base the correlation insights on.

Generating correlation insights from the Security Incident Response Workspace

Starting with version 3.2.1 of Now Assist for Security Incident Response, you can generate and view correlation insights in the Security Incident Response Workspace.

- Generate correlation insights from the **Investigation** tab for a security incident in any state in the Security Incident Response Workspace.
- The agent asks you which CI or Affected user you would you like to correlate the security incident with from the related lists. Previously, if you selected a configuration item (CI) or affected user to base your insights on, the lookup returned the primary affected user or primary CI associated with a security incident.
- You can generate insights for multiple items simultaneously for **Associated Observables**, **Configuration items**, and **Affected Users**.
- Results are displayed in a modeless dialog that you can resize and move.
- Your time range for the lookup of correlation is 30 days.

> **Note:** After you generate an observable associated with a security incident, the insights are stored for that observable until you regenerate it with a different time range. Your insights for your new time range are displayed.

The correlation insights generation skill must be activated before you can see the **Generate correlation insights** option in the Security Incident Response Workspace. For more information, see Configure and activate a skill for Now Assist for Security Incident Response.

Generating correlation insights from the Now Assist panel in the Security Incident Response Workspace and in UI (UI16)

- You can generate correlation insights from a security incident record in any state in the Security Incident Response Workspace or in the legacy UI (UI16).
- By default, correlation insights search for matching records from the last 30 days.
- You can locate and review values for the **Configuration item**, **Affected user**, and **Observables** for correlation insights filters on the **Details** tab in the Security Incident Response workspace, or on the **Configuration Items**, **Affected Users**, and **Observables** related lists in the legacy UI (UI16).
- Your search criteria and results remain displayed in the Now Assist panel until you reset the conversation. To reset your conversation, select the Now Assist reset menu icon () in the panel and select **Reset Conversation**.
- You must have access to the following tables to view these records in the generated correlation insights:
  - Configuration item [cmdb_ci] table.
  - Incident [incident] table.
  - Change request [change_request] table.
  - Problem [problem] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Vulnerable item [sn_vul_vulnerable_item] table.
- Associate observable [sn_ti_observable] table.

- Your results for correlation insights are based on the tables that you have access to. For example, if you want to view vulnerable items (VIT)s in your correlation insights results, you must have the Vulnerability Response application installed and the read access role (sn_vul.read_all).

For the steps to generate correlation insights, see Generate correlation insights with Now Assist for Security Incident Response.

Generate correlation insights from the Security Incident Response Workspace with Now Assist for Security Incident Response

Generate and view correlation insights in the Security Incident Response Workspace to help you connect past events to the security incident you are working on.

Before you begin

Version 3.0 of Now Assist for Security Incident Response supports generating correlation insights from the Security Incident Response Workspace. See Supporting information for Now Assist for Security Incident Response for more information.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
2. Select the **Investigation** tab on the security incident record.
3. Select one or more filters that you want to base your correlation insights on.

   You can select more than one observable.

   - **Associated Observables**: Records that are linked by shared observables that suggest potential ongoing attacks or repeated use of malicious infrastructure. Examples might include IP addresses, URLs, or file hashes.
   - **Configuration items** (CI): Records that have the same CIs to help you identify potential vulnerabilities in specific systems. An example might be users' laptops.
   - **Affected Users**: Past incidents that have the same users to help you see patterns such as frequent phishing attempts or multiple unauthorized access attempts. An example is a specific user's name.

   A list of matching items is displayed.
4. Select the items from the list that you want to generate insights for.
5. Select **Generate Insights**.
   A dialog opens. After a few moments, your correlation insights are displayed. You have the following options from this dialog:

   - Refresh insights ( ) - You can change the items in the list after your initial insights are generated and update your results.
   - Expand ( ) - Resize the dialog and drag it around on the page.

   You have the following options for each correlation insight entry in the dialog.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Change time range** - Select a time range to reload the dialog with matching insights. Your results for this entry are automatically regenerated if you select a new time range. The time range for each entry is displayed next to the insight, for example, `35 . 35 . 35 . 35 . (100 days)`.
- Last generated - The date that the insight was last generated.
- Rate the content - ( ) and ( ).
- Copy - ( ) Copy the insight to the clipboard.
- **Share to work notes** - Edit the content and publish it to the work notes on the security incident.

Correlation insights are stored for observables when you generate them for the first time based on the default lookup period (30 days). These insights are stored until you regenerate insights for the observables with a different lookup period. Modify the 30-day limit for the query by following these steps:

a. As a user with the Security Incident Manager role [sn_si.manager], navigate to sys_properties.LIST.

b. Locate the Correlation lookback period [sn_sec_gen_ai.correlation_lookback_period] system property and open the record.

c. Enter a number in the **Value** field up to 360.

d. Save the record.

e. Return to the security incident record and refresh the page.

f. Generate correlation insights. Your results are based on your new lookup period.

Generate correlation insights with Now Assist for Security Incident Response

Generate correlation insights from the Now Assist panel to help you connect past events to the security incident you are working on. You can use the related information you generate to avoid duplicating your investigation into affected users, configuration items, and observables and help you resolve the incident you are working on more quickly.

Before you begin

The correlation insights generation skill must be activated before you can see the **Generate correlation insights** option in the Now Assist panel.

If you do not see the Now Assist panel, you must activate it. For more information, see Turn on the Now Assist panel.

For more information about correlation insights searches, see Exploring correlation insights with Now Assist for Security Incident Response.

Roles required: sn_si.analyst, sn_si.manager or sn_si.basic

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
2. Alternatively, in the legacy UI (UI16), locate a security incident on the Security Incidents [sn_si_incident] table and open it.
3. Select the Now Assist icon ( ) in the top header to open the Now Assist panel.
4. Select **Generate correlation insights**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Correlation insights are generated if one or more of the following values can be matched. The following filters to base your insights on are displayed in the Now Assist panel. Only the filters that have matches to other security incidents are displayed.

Note: If you do not have a security incident record open, you are prompted to enter the number for a security incident record after you select **Generate correlation insights**.

- **Configuration item** (CI): Records that have the same CI to help you identify potential vulnerabilities in specific systems. An example might be a user's laptop.
- **Affected user**: Past incidents that have the same user to help you see patterns such as frequent phishing attempts or multiple unauthorized access attempts. An example is a specific user's name.
- **Observables**: Records that are linked by shared observables that suggest potential ongoing attacks or repeated use of malicious infrastructure. Examples might include IP addresses, URLs, or file hashes. Note you must enter an exact value for an observable, for example, a complete file hash.

If no matching data exists for any of these filters, none are displayed. You are prompted to add one of these values to the security incident you are working from, save it, and reset your conversation in the panel and try again.

5. To reset your conversation, select the Now Assist reset menu icon () in the panel and select **Reset Conversation**.
6. Select a filter.

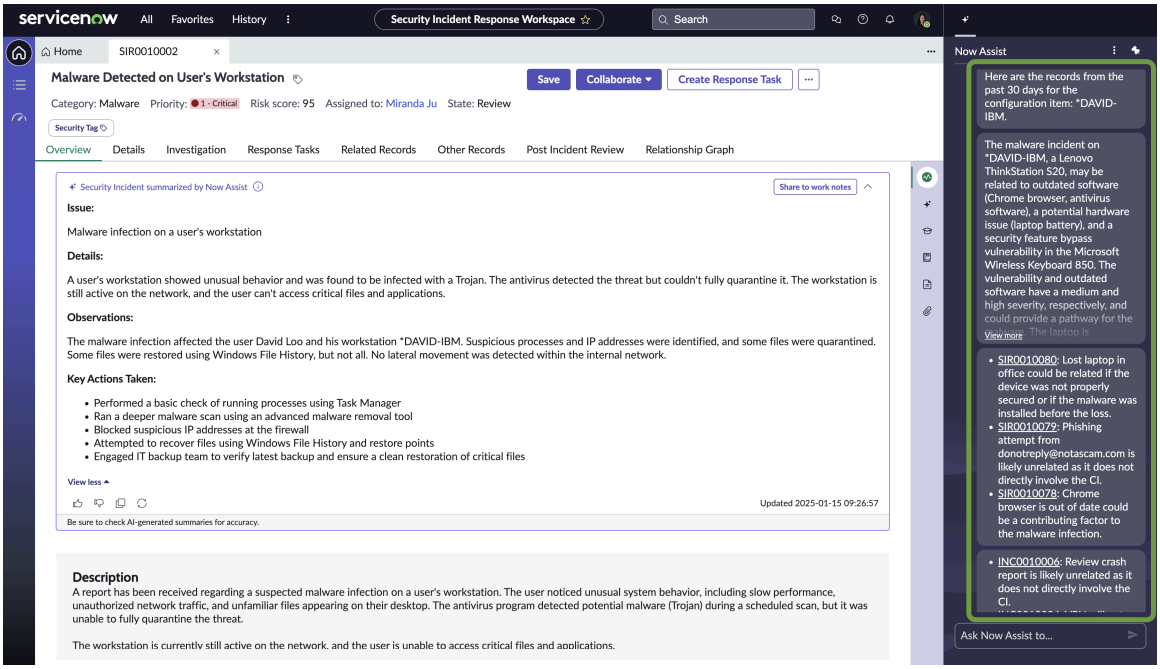
   Matching results are displayed in the Now Assist panel.

   In the following example, **Configuration item** was requested. The search returned a high-level summary and links to records that have a matching configuration item.

   Results are grouped by record type: security incident record (SIR), incident (INC), change request (CHG), problem (PRB), and vulnerable item (VIT).

   - The Affected users filter returns: SIR, INC, and CHG records.
   - The Configuration filter item returns: SIR, INC, CHG, PRB, and VIT records.
   - The Observables filter return SIR records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. **Optional:** To modify the 30-day limit for the query, follow these steps:
   a. As a user with the Security Incident Manager role [sn_si.manager], navigate to sys_properties.LIST.
   b. Locate the Correlation lookback period [sn_sec_gen_ai.correlation_lookback_period] system property and open the record.
   c. Enter a number in the **Value** field up to 360.
   d. Save the record.
   e. Return to the security incident record and refresh the page.

Request generative AI skills in the Now Assist panel for Now Assist for Security Incident Response

Request a security incident summary or closure notes from the Now Assist panel.

Before you begin

See Now Assist panel for how to activate the Now Assist panel.

Roles required: si_analyst, si_manager or sn_si.basic

Procedure

1. Log in to an instance where the Now Assist for Security Incident Response application is installed.
2. In the legacy Core UI, navigate to **All** > **Security Incident** > **Incidents** and open a security incident that is assigned to you.
3. Alternatively, navigate to **All** > **Security Incident** > **Security Incident Response Workspace** and open a security incident that is assigned to you.
4. Select the Now Assist icon (✦) in the top banner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Generate resolution notes	In the Now Assist panel, select **Generate resolution notes**. The closure notes generated in the panel are identical to those generated when you close a security incident from a record. Closure notes for security incidents are created based on any actions taken for remediation and containment, in addition to other relevant details related to their closure. **Note:** You might want to review the generated text and make sure it's accurate before you close the security incident. Edit the notes or delete them to provide your own. See Generate closure notes for a security incident with Now Assist for Security Incident Response for more information.
Summarize a security incident	In the Now Assist panel, select **Summarize a record**. The summary generated in the panel is identical to the one that you generate from a security incident record. Summaries generated by AI might miss key details. You might prefer to review the summary for accuracy and completeness before you proceed. See Summarize a security incident with Now Assist for Security Incident Response for more information.
Generate correlation insights	In the Now Assist panel, select **Generate correlation insights**. Correlation insights from the Now Assist panel to help you connect past events to the security incident you are working on. See Exploring correlation insights with Now Assist for Security Incident Response and Generate correlation insights with Now Assist for Security Incident Response for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using AI agentic workflows in Now Assist for Security Incident Response

Use the Security Incident Response AI agents to complete your tasks autonomously.

Available agentic workflows for AI agents for Security Incident Response

Agentic workflow name	Description	Available AI agents
Close security incident	This agentic workflow helps the security analysts to close a security incident using natural language in the Now Assist panel.	Security incident wrap-up generator
Analyze security operations metrics	This agentic workflow helps a security operations center (SOC) manager analyze their security analysts' performance. Metrics are generated for security incident response (SIR) records for case volume, mean time to assign (MTTA), and mean time to resolve (MTTR).	• Security incident retrieval AI agent • Security metrics analysis AI agent
Security incident resolution	This agentic workflow helps the security analysts to identify a security incident resolution path. This workflow also assist the security analysts to close a security incident using natural language in the Now Assist panel.	• Security incident resolution AI agent • Exchange online integration handling AI agent • Security incident wrap up generator AI agent • Observable analysis AI agent • Security incident activities handling AI agent

Important: By default, all agentic workflows and AI agent records are read-only.

To modify an agentic workflow, you must first Duplicate an agentic workflow, and then proceed with the following steps:

- Activate the workflow.
- Activate all the AI agents within the workflow.
- If required, you can add a trigger to invoke the workflow automatically.

Looking for an AI agent?

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- There might be AI agents installed with the Now Assist application that are not used in agentic workflows. To learn how to see all agents that are available on your instance, see Find AI agents.
- To find agents that might not be installed on your instance, visit the AI Agent Marketplace on the ServiceNow Store.

Activate an agentic workflow for Now Assist for Security Incident Response

You must activate the agentic workflows for Now Assist for Security Incident Response from the AI Agent Studio.

Before you begin

The Now Assist panel must be activated. See Turn on the Now Assist panel for more information.

Role required: aia-admin

Procedure

1. Navigate to **All** > **AI Agent Studio** > **Overview**.
2. Select the card for the agentic workflow that you want to configure and activate.

   If you want to modify an agentic workflow, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicate.

   The Guided setup is displayed. The Describe and connect page is read-only.
3. Select **Continue**.
4. For Define trigger, select **Continue**.

   The Define trigger page is read-only.
5. Select the **Display** toggle for the Select Display page so that the conversation with the AI agent is displayed in the Now Assist panel.
6. Select the arrow icon to expand the section.
   The sn_si.analyst role is displayed. This role is supported for the agentic workflows in the Now Assist for Security Incident Response application.
7. To activate the agentic workflow, select **Save and test**.
   You can now invoke the agentic workflows on-demand.
8. **Optional:** Select **Use case** (agentic workflow) and enter the information you want to test and select **Start test**.

Security Incident Response AI agent collection close security incident use case

The Close security incident use case enables security analysts to close a security incident.

Close security incident use case overview

Using the Close security incident use case, cancel the associated response tasks, generate resolution notes, close notes, close code and post incident analysis (PIA) during a security incident closure and provide feedback and adjust content in natural language from the Now Assist panel.

If you want to modify this use case, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the use case instead.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Agent used in Close security incident use case

The Security incident wrap-up generator expert is used in the Close security incident use case.

Close a security incident

Chat with an AI agent in the Now Assist panel to help you close a security incident.

Before you begin

Role required: sn_si.analyst or sn_si.manager

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace**.
2. Open the security incident that you want to close by using the AI agent.
3. Select the Now Assist () icon.
   The Now Assist panel is displayed.
4. Close the security incident by using one of the following options.

Option	Description
Close a security incident	On the Now Assist panel, ask the agent to close the security incident in natural lan guage by entering `Close this inci dent`, `Close this security inci dent` or `Close the security inci dent: SIR0012345`. **Note:** ○ When you enter `Close this in cident` or `Close this secu rity incident`, the Now Assist panel picks the security incident in context. When you provide a specif ic security incident number, such as `Close the security inci dent: SIR0012345`, the use case takes action for the suggested securi ty incident. ○ You can close any security incident from the Now Assist panel by provid ing the security incident number in your text. ○ When you request a security incident closure, the Close security incident use case cancels the mandatory post incident assessment, flow actions, playbook actions, workflow actions, and response tasks. However, you can close actions manually before ini tiating the security incident closure re quest. The Close security incident use case pro vides content for each of the following fields

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	and asks for your feedback. The use case pop ulates your accepted feedback. After you ac cept the content for a field, the use case pro vides content for the next field. ○ **Post Incident Analysis**: You can accept the suggested content by replying with a posi tive response such as `looks good` or Ok. You can ask the use case to refine the con tent and can also suggest the changes you require. ○ **Close notes**: You can accept the suggest ed content by replying with a positive re sponse such as `looks good` or Ok. You can ask the use case to refine the con tent and can also suggest the changes you require. ○ **Close code**: On the basis of the security incident details, the use case suggests a close code. You can accept the close code or suggest an alternative close code for the security incident. The AI agent closes the security incident. **Note:** When a field is changed, the activity stream appends the words "AI AGENT:" with a description of the up date made by the AI agent. For example, `AI AGENT: Close code is up dated`.
Close a security incident as false positive	On the Now Assist panel, you can ask the AI agent to close the security incident as false positive. For example, `Close this inci dent as false positive` or `close this security incident as false positive`. The use case provides the summary of the se curity incident. To close the security incident, type in positive responses such as `looks good` or Ok. The AI agent closes the security incident. It al so updates the Close notes as `Closed by AI Agent as false positive` and the Close code as **False positive** and cancels all active response tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response AI agent collection Resolve security incident agentic workflow

Chat with an AI agent in the Now Assist panel to help you create a resolution plan for a security incident and to resolve it.

Resolve security incident agentic workflow overview

Use the Resolve security incident agentic workflow to fetch the incident details, fetch the knowledge articles and similar closed security incidents, get a resolution plan, and resolve the security incident.

If you want to modify this agentic workflow, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the agentic workflow instead.

Agents used in the Resolve security incident agentic workflow

The Resolve security incident agentic workflow contains the following agents:

- Security incident resolution AI agent
- Exchange online integration handling AI agent
- Security incident wrap up generator AI agent
- Observable analysis AI agent
- Security incident activities handling AI agent

Resolve a security incident

Chat with an AI agent in the Now Assist panel to resolve an incident.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **All** > **Security Incident** > **Security Incident Response Workspace**.
2. Open the security incident that you want to resolve using the AI agent.
3. Select the Now Assist ( ) icon.
   The Resolve security incident agentic workflow is on-demand. You can enter a query in natural language to resolve a security incident by using this agentic workflow.
4. On the Now Assist panel, ask the agent to resolve the security incident by entering `Resolve this incident`, `Resolve this security incident`, or `Resolve the security incident: SIR0012345`.
   The Now Assist panel provides all the actions that you can perform on the security incident.
5. Select **Resolve security incident**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Resolution Plan for Security Incident

1. Set the incident to Analysis state.
2. Run Threat Look up and observable enrichment on observables.
3. If the observables are not malicious, close the security incident as a false positive, else proceed with next step.
4. If the observables are malicious, send an email to the management informing them about the phishing attack/campaign has occurred.
5. Check with the affected user if they have interacted with the phishing email.
6. Set the incident to Contain state.
7. If the user has interacted with the phishing email, create an incident to immediately reset the password credentials.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The AI agent analyzes the security incident and provides a summary of the incident and its current state. Additionally, by using the incident details, knowledge articles, and similar closed security incidents, the AI agent provides a resolution plan.

6. Enter positive responses such as `looks good` or `Ok` if you agree to the resolution plan. For a positive response, the AI agent investigates each step in the resolution plan and assists the analyst (the user with the sn_si.analyst role) to resolve it. For each step, the AI agent provides feedback and requests for intervention from the analyst. For example, if the AI agent identifies the incident generated for a phishing email, the following agentic workflow occurs:

Agentic workflow for resolving a phishing email incident

Tasks to resolve a security incident	Description
Update the state of security incident	The AI agent updates the state of the security incident. For example, if the state of the security incident is Draft, the AI agent updates it to Analysis.
Run threat lookup and observable enrichment on observable	The AI agent initiates a threat lookup and observable enrichment process. When the analyst confirms with a positive input, the AI agent provides the Observable Analysis and Enrichment summary.
For malicious observables, send email to management	The analyst can ask the AI agent to send a mail to the management. The AI agent provides a draft email and asks for the recipients of the email. **Note:** The analyst can verify the sent email in the **Other Records** tab.
Check with affected user if they interacted with the phishing email	The analyst manually checks with the affected user if they interacted with the phishing email.
If user interacted with the phishing email, reset its password credentials	If the affected user interacted with the phishing email, the analyst can ask the AI agent to create an incident to reset the user password. The AI agent provides a summary for the incident and creates an incident when the analyst approves the summary.
Block the sender/email/URL on the email gateway	The AI agent requests the analyst for blocking for sender/email/URL on the email gateway. The analyst can ask the AI agent to create a response task for blocking sender/email/URL on the email gateway. The AI agent provides the information for the response tasks and creates a response task after the analyst approves it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tasks to resolve a security incident	Description
	Note: The analyst can complete the response task and mark the response task as **Complete** on the **Response Tasks** tab. The analyst confirms to the AI agent that the response task is complete.
Search and delete the phishing email from all user inboxes	The AI agent informs the analyst to delete the phishing email from all user inboxes. The analyst deletes the phishing email and confirms to the AI agent.
Enroll affected user in a mandatory phishing training	If the affected user has interacted with the phishing email, the AI agent informs the analyst to enroll the affected user in the mandatory phishing training.
Perform the audit of the security incident	The AI agent performs the audit of the security incident and provides the summary.
Close the security incident	The AI agent closes the incident. For more information, see Close a security incident.

Security Incident Response AI agent collection for the Analyze security operations metrics agentic workflow

The Analyze security operations metrics agentic workflow helps security operations center managers analyze the performance of their security teams.

The Analyze security operations metrics agentic workflow overview

Security operations center (SOC) managers can analyze metrics for overall case volume, mean time to assign (MTTA), and mean time to resolve (MTTR) on security incident response (SIR) records to give them insight into their security analysts' performance. They can also ask for recommendations for how to improve the metrics.

Agents used in the Analyze security operations metrics agentic workflow

- Security incident retrieval AI agent
- Security metrics analysis AI agent

Analyze security operations metrics agentic workflow

Chat with an AI agent from the Now Assist panel to help you gain insight into how efficiently your security analysts are working with security incidents resolution.

Before you begin

You must activate the Now Assist Security operations metrics analysis skill before you can use the AI agents with the Analyze security operations metrics agentic workflow. For more information, see Configure and activate a skill for Now Assist for Security Incident Response.

Role required: sn_si.manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Select the Now Assist icon (✨) from anywhere in your instance.
   The Now Assist panel is displayed.
2. Select **Analyze Security Operations Metrics** in the Now Assist panel.
3. At the prompt, select **Analyze security incident metrics**.

   The Analyze security operations metrics agentic workflow case is on-demand. You can enter any query in natural language, but you might consider using the prompts described in the following table and steps to become familiar with the metrics data that is available and what you can do with it.

Your request or response	Description
Enter a name for one of your security analyst groups and request metrics, for example: ○ **Analyze security operations metrics for L1 Analyst team.** ○ **Security metrics for L1 Analyst team for the past six months.** ○ **How did the L1 Analyst team perform last month?**	Specify a team by name and indicate a time period.
End the session, or **Stop**.	End the conversation.

   You might prefer to have the Security Incident Response workspace open in another tab so that you can refer to assignment groups, dates, and other information for your prompts.

   Your conversation is saved until you start a new chat. To start a new chat, select the New chat icon (⊞).

   Your request is repeated and displayed in highlighted text with more information.

   After a few moments, you are prompted to provide more information about a specific analyst or an analyst group.

4. Enter an assignment group name, for example, **L1 Analysts team**.
5. At the prompt, enter a time range, for example, **The past six months**.
   The results for mean time to resolve (MTTR), mean time to assign (MTTA), and the total number of security incidents your team handled are displayed. Select the link for more information. A new tab opens with a list in UI16.
6. Expand the **Sources** list and select the **Security Incident List** link.
   A list of security incidents that are assigned to the L1 Analysts group is displayed in a new tab in UI 16. At the top of the list, the date range that you requested (**6 months**) is displayed in the following format: `Opened > = 2024-09-23 > Opened < = 2025-03-23`. You are prompted if you would like to see more detailed analysis for MTTR, MTTA, or case volume.

   From this list, you can select a link to open individual security incidents to review. You can enter a record number from the list in the chat for the AI agent to summarize.

7. Return to the chat and enter your request for a performance metric in natural language, for example, `Yes, dive deeper on MTTR.`
   More information is provided for your request that includes a summary and data organized into sections for fields on the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Category Analysis - Breakdown by category. Examples might include `Unauthorized Access`,`Unpatched Vulnerability`, `False Positive`, and so on.
- Priority Analysis - Breakdown by severity: Critical, High, Moderate.
- Team Analysis - Breakdown of MTTR by team individual members.
- Outlier Analysis - Breakdown of security incidents that have unusually high, low, or other unique values.

8. At the prompt, enter an affirmative response to the request for improvement suggestions. Your suggestions are displayed. Based on the results of the assessment, you might want to look up more information about specific types of security incidents.
9. At the prompt, for example, request in natural language for all the security incidents in the phishing category that are in the state **Analysis**.
10. Select the **View results** link.
    A list of security incidents that match your request is provided in a new tab in UI16.

    From this list, you can open individual incidents and request summaries from the AI agent.
11. **Optional:** Modify system properties for the source fields that are used for metric analysis and the value for the outlier factor.
    - sn_sec_gen_ai.aia_metric_analysis_dimensions - The AI agent breaks analysis down based on the following fields when analyzing MTTR and MTTA metrics: **category**, **priority**, **close_code**, **assigned_to**, **alert_sensor**. Users with the sn_si.manager and sn_si.admin roles can modify this list.
    - sn_sec_gen_ai.aia_metric_analysis_outlier_factor - This property determines the outlier factor for MTTR and MTTA. The default outlier value is 2. By default, a record is an outlier if its MTTR exceeds 2 times the average time that it takes an assignment group to resolve security incidents for the time range that you requested. Users with the sn_si.manager and sn_si.admin roles can modify this value.

Now Assist for Vulnerability Response

Use the Now Assist for Vulnerability Response application to help your vulnerability managers and analysts assess your potential exposure to critical vulnerabilities and gain insight into your Service Level Agreement (SLA) compliance for vulnerable items.

Get started

Explore	Configure	Use
		
Learn about Now Assist for Vulnerability Response	Learn how to configure and activate the agentic workflows for Now Assist for Vulnerability Response	Learn how to use Now Assist for Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



AI agent collection

Get information about the AI agents and agentic workflows for Now Assist for Vulnerability Response

Important:

- Not all model providers are available for customers with in-country SKUs, and some Now Assist products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some Now Assist products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base . Be sure to check for availability updates in future releases.
- Some Now Assist products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

Helpful resources

Some ServiceNow resources that can provide you with helpful information are:

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. In addition, this application will collect the vulnerability data that you import as well as information about the configuration items in your CMDB. Customers can opt out of future data collection at any time, as described in the Now Assist Opt-Out page.

For more information, see the Now Assist documentation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring Now Assist for Vulnerability Response

Get information about how your vulnerability managers and analysts can use AI agents with Now Assist for Vulnerability Response.

Now Assist for Vulnerability Response overview

With AI agents and agentic workflows provided with the Now Assist for Vulnerability Response application, your vulnerability managers and analysts have the option to determine your environment's potential exposure to recent, known vulnerabilities and view how well your remediation targets are in compliance with your Service Level Agreements (SLAs).

Now Assist for Vulnerability Response users

Users

User	Description
Vulnerability managers and analysts	Determine your exposure to vulnerabilities in your environment and their potential impact to your configuration items (CIs) and business services.
Vulnerability managers and analysts	Get insights into how well you're achieving your remediation targets for vulnerabilities according to your Service Level Agreements (SLAs).
Vulnerability managers and analysts	Provide steps for analysts to remediate vulnerable items (VITs) that are assigned to them with watch topics and remediation efforts.

Now Assist for Vulnerability Response benefits

Now Assist for Vulnerability Response benefits

Benefit	Feature	Users
• Identify assets with Common Vulnerabilities and Exposures (CVEs). • Determine the number of active vulnerability items (VITs) that correspond to CVEs. • Identify business services with known vulnerabilities. • Create watch topics for vulnerable item (VIT) remediation based on the information provided. The AI agent can create a Remediation Effort for the active VITs associated with the watch topic.	Assess vulnerability exposure	Vulnerability managers and analysts
Gain insight into the progress of your Service Level Agreement (SLA) compliance summary for the past 30 days. View Groups and Asset Types that missed SLAs to help you track and adjust targets.	Analyze vulnerability remediation status	Vulnerability managers and analysts

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Now Assist for Vulnerability Response benefits (continued)

Benefit	Feature	Users
Retrieve relevant context and details for the vulnerable items assigned to you. Analyze, plan, and create steps for remediation.	Steps for issue resolution	Vulnerability analysts

What to explore next

To learn more about configuring and using Now Assist for Vulnerability Response, see:

- Configuring Now Assist for Vulnerability Response
- Using agentic workflows in Now Assist for Vulnerability Response

Supporting information for Now Assist for Vulnerability Response

Get a quick overview of the important information that is related to the Now Assist for Vulnerability Response application.

Supported versions and required applications

The following applications are required:

Application	Version
Now Assist for Vulnerability Response	1.0.2
Now Assist for platform [sn_genai_platform]	6.3.0
Vulnerability Response Integration with CISA [sn_vul_cisa]	1.5.0
Vulnerability Response [sn_vul]	26.0.13
Vulnerability Response licensing and usage [sn_vul_licensing] (installed with [sn_vul])	2.6
Vulnerability Response Common Workspace [sn_vul_cmn_ws] (installed with [sn_vul])	1.4
Vulnerability Response [sn_vul_cmn] (installed with [sn_vul])	2.11

Supported user interfaces

Now Assist for Vulnerability Response supported interfaces

Interface	Features
Vulnerability Manager Workspace	Vulnerability managers and analysts can assess if your configuration items (CIs) and your business services are exposed to vulnerabilities. Check for any new Cybersecurity and Infrastructure Security Agency (CISA) known exploitable vulnerabilities and assess their potential impact on your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Now Assist for Vulnerability Response supported interfaces (continued)

Interface	Features
	Vulnerability managers and analysts can gain insights into your compliance metrics to understand how effectively your organization is meeting remediation goals for vulnerabilities based on Service Level Agreements (SLAs).
UI6	Links in the responses in theNow Assist panel open new tabs in your browser that expand on the summaries.

Configuring Now Assist for Vulnerability Response

The Now Assist for Vulnerability Response application is supported in the Now Assist panel and available on-demand.

Configuration overview

By sharing data with the ServiceNow® AI development program, you provide relevant data to help improve prediction accuracy, user experience, tailor products to your business needs, and reduce hallucinations for your activated Now Assist skills.

You can choose to opt out of a ServiceNow instance from data sharing from the Now Assist Admin console if you don't want to participate. For more information, see Opt out of data sharing for Now Assist. Repeat the opt-out process for all instances that use the Now Assist functionality.

Use the AI Agent Studio to configure Now Assist for Vulnerability Response.

The Now Assist panel must be activated. For more information, see Turn on the Now Assist panel.

1. Install Now Assist plugins.

   Install the Now Assist for Vulnerability Response application (sn_vr_gen_ai).

   The Now Assist for Vulnerability Response AI agents included with the application are activated by default. You must activate the agentic workflows from the AI Agent Studio to use Now Assist for Vulnerability Response. See Activate an agentic workflow for Now Assist for Vulnerability Response for more information.

2. Activate an agentic workflow for Now Assist for Vulnerability Response

   Configure and activate an agentic workflow from the Guided Setup.

Activate an agentic workflow for Now Assist for Vulnerability Response

You must activate the agentic workflows from the AI Agent Studio. The Now Assist for Vulnerability Response AI agents included with the application and used in the agentic workflows are activated by default.

Before you begin

The Now Assist panel must be activated. See Turn on the Now Assist panel for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: aia-admin

Procedure

1. Navigate to **All** > **AI Agent Studio** > **Overview**.
2. Select the card for the agentic workflow that you want to configure and activate.
   - **Use case Assess vulnerability exposure**
   - **Use case Analyze vulnerability remediation status**

   If you want to modify this agentic workflow, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicate.

   The Guided setup is displayed. The Describe and connect page is read-only.
3. Select **Continue**.
4. For Define trigger, select **Continue**.

   The Define trigger page is read-only.
5. Select the **Display** toggle for the Select Display page so that the conversation with the AI agent is displayed in the Now Assist panel.
6. Select the arrow icon to expand the section.
   The sn_vul.vulnerability_admin and sn_vul.vulnerability_analyst roles are displayed. These roles are supported for the agentic workflows in the Now Assist for Vulnerability Response application.
7. To activate the agentic workflow, select **Save and test**.
   You can now invoke the agentic workflows on-demand.
8. **Optional:** Select **Use case** (agentic workflow) and enter the information you want to test and select **Start test**.

Using agentic workflows in Now Assist for Vulnerability Response

Use the Vulnerability Response AI agents to complete your tasks autonomously.

Available agentic workflows for AI agents for Vulnerability Response

Agentic workflow name	Description	Available AI agents
Assess vulnerability exposure	• Determine if your configuration items (CIs) and business services are exposed to known vulnerabilities. • Determine the potential impact that a specific vulnerability might have throughout your environment. • Check CIs for any new Cybersecurity and Infrastructure Security Agency (CISA) exploitable (zero-day) vulnerabilities.	• CISA vulnerability analysis AI agent • Vulnerability exposure analysis AI agent • Watch topic creation AI agent

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available agentic workflows for AI agents for Vulnerability Response (continued)

Agentic workflow name	Description	Available AI agents
	• Create watch topics in the Vulnerability Manager workspace to remediate vulnerable items.	
Analyze vulnerability remediation status	• Gain insights into your compliance metrics and statistics for how well you're meeting remediation target dates on vulnerable item (VIT) records. • View your monthly VIT record remediation totals and identify missed targets. • Break down remediation data on VITs by **Severity**, **Assignment group**, **Configuration item**, and **Vulnerability** for your monthly Service Level Agreement (SLA) compliance reviews.	Remediation compliance analysis AI Agent

Important: By default, all agentic workflows and AI agent records are read-only.

To modify an agentic workflow, you must first Duplicate an agentic workflow, and then proceed with the following steps:

- Activate the agentic workflow. The Now Assist for Vulnerability Response AI agents included with the application are activated by default.
- If required, you can add a trigger to invoke the agentic workflow automatically.

Looking for an AI agent?

- There might be AI agents installed with the Now Assist application that are not used in agentic workflows. To learn how to see all agents that are available on your instance, see Find AI agents.
- To find agents that might not be installed on your instance, visit the AI Agent Marketplace on the ServiceNow Store.

- Assess vulnerability exposure agentic workflow.

  Chat with an AI agent from the Now Assist panel to help you assess if your configuration items and your business services are exposed to vulnerabilities.

- Analyze vulnerability remediation status agentic workflow.

  Chat with an AI agent from the Now Assist panel to help you gain insights into your compliance metrics for resolving vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response AI agent collection for the Assess vulnerability exposure agentic workflow

The tools and AI agents for the Assess vulnerability exposure agentic workflow.

Agentic workflow overview

The following agentic workflows are included with the Now Assist for Vulnerability Response application:

- Assess vulnerability exposure agentic workflow
- Analyze vulnerability remediation status workflow

If you want to modify this agentic workflow, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the agentic workflow.

Assess vulnerability exposure agentic workflow agentic workflow overview

Use the Assess vulnerability exposure agentic workflow from the Now Assist panel to help you:

- Determine if your configuration items (CIs) and business services are exposed to known vulnerabilities.
- Determine the potential impact a specific vulnerability might have throughout your environment.
- Check CIs for any new Cybersecurity and Infrastructure Security Agency (CISA) exploitable (zero-day) vulnerabilities.
- Create watch topics in the Vulnerability Manager workspace to remediate vulnerable items.
- Adjust content in natural language.

Agents used in the Assess vulnerability exposure agentic workflow

- Vulnerability Response Action Executor
- CISA Known Exploited Vulnerabilities Analyzer
- Vulnerability Exposure Assessment Advisor

Assess vulnerability exposure agentic workflow

Chat with an AI agent from the Now Assist panel to help you assess the potential exposure of your configuration items and your business services to vulnerabilities.

Before you begin

The Now Assist panel must be activated. For more information, see Turn on the Now Assist panel.

Roles required: sn_vul.vulnerability_admin or sn_vul.vulnerability_analyst

Procedure

1. Select the Now Assist icon () from anywhere in your instance.
   The Now Assist panel is displayed.

   The Assess vulnerability exposure agentic workflow is on-demand. You can enter any query in natural language, but you might consider using the prompts described in the following table and steps to start with to become familiar with the vulnerability data that is available and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

what you can do with it. The following steps show you how to request current vulnerability data, create a watch topic based on the returned results, and determine the overall impact a vulnerability might have on your environment.

Your request or response	Description
What are the recent CISA vulnerabilities?	**Recent** in your question refers to new vulnerabilities that have surfaced during the last seven days. Seven days (one week) is the default time period for the agentic workflow. If you want to search for new vulnerabilities for a specific time period other than seven days, type in a request with a value that occurs in the past such as, **What are the recent vulnerabilities for the past 30 days?**
Yes, create a watch topic for the vulnerability CVE-2018-9065.	When asked if you want to create a watch topic, you might prefer to be specific in your response. For example,confirm the request and type in a specific vulnerability in the format: **CVE-2018-9065**.
Can you give me a detailed impact analysis for the CVE-2018-9065 vulnerability?	Potential impact analysis of vulnerabilities is supported only for affected business services and configuration item classes.
Show output for the previous question.	Request the agent to review your previous question if it doesn't give you an answer.
End the session, or **Stop**.	End the conversation.

Your conversation is saved until you start a new chat. If the conversation ends unexpectedly, start a new chat. To start a new chat, select the New chat icon ( ).

2. Enter a request in natural language to see if you're exposed to any recent vulnerabilities, for example, **What are the recent CISA vulnerabilities?**

   Because your entry doesn't specify a range, the agent by default gathers Cybersecurity and Infrastructure Security Agency (CISA) exploitable vulnerability data about your assets and returns information from the last seven days.

   The Common Vulnerabilities and Exposures (CVE) vulnerabilities that impact your assets and have vulnerable items associated with them in your environment are listed.

   You might see that the agent also returns aliases that match CVEs. Aliases are reported if you're using third-party scanners to import your vulnerability data. For example, `CVE-2018-8627 (alias: TEN-119686, TEN-119596) with severity Medium has 4 vulnerable items (VITs)`. This response indicates that the vulnerability was discovered and imported by the Tenable (TEN) scanner product.

3. **Optional:** Select the CISA Known Exploitable Vulnerabilities link for information about all the CVEs that were returned.
   The list opens in a new tab in UI16.

4. Return to the chat and enter a request for the agent to create a watch topic for a CVE at the prompt, for example, **Yes, create a watch topic for the vulnerability CVE-2018-9065.**
   The agent proposes a name for your watch topic and asks for confirmation. You can change the name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Enter **OK**.
6. Select the link to view the watch topic in the Vulnerability Manager workspace and view more details as well as the vulnerable items that are associated with the CVE.
   The list opens in a new tab in UI16. After reviewing the data, you might decide you want more information about the impact the CVE has on your other assets.
7. Return to the Now Assist panel and enter and request the agent for a detailed impact analysis, for example, **Can you give me a detailed impact analysis for the CVE-2018-9065 vulnerability?**
   This request returns information about your configuration items and business services that are affected by this CVE. It provides a criticality breakdown, a list of business services that are impacted, and a list of the classes of affected configuration items. There is also a link for more detailed information.
8. **Optional:** Request an overall vulnerability exposure assessment for a specific business service.
   Information about the business service includes associated vulnerable items, criticality (risk) and the configuration items by class are listed.

Vulnerability Response AI agent collection for the Analyze vulnerability remediation status agentic workflow

The tools and AI agents for the Analyze vulnerability remediation status agentic workflow.

Analyze vulnerability remediation status agentic workflow overview

Use the Analyze vulnerability remediation status agentic workflow from the Now Assist panel to help you:

- Gain insights into your compliance metrics and statistics for how well you're meeting remediation target dates on vulnerable item (VIT) records.
- View your monthly VIT record remediation totals and identify missed targets.
- Break down remediation data on VITs by **Severity**,**Assignment group**, **Configuration item** and **Vulnerability** for your monthly Service Level Agreement (SLA) compliance reviews.

If you want to modify this agentic workflow, you can duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the agentic workflow.

Agent used in the Analyze vulnerability remediation status agentic workflow

The Remediation Compliance Insights Provider is used by the Analyze vulnerability remediation status agentic workflow.

Analyze vulnerability remediation status agentic workflow

Chat with an AI agent from the Now Assist panel to help you gain insights into your monthly remediation compliance metrics for vulnerable items.

Before you begin

The Now Assist panel must be activated. For more information, see Turn on the Now Assist panel.

Roles required: sn_vul.vulnerability_admin or sn_vul.vulnerability_analyst admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Select the Now Assist icon ( ).
   The Now Assist panel is displayed.

   The Analyze vulnerability remediation status agentic workflow is on-demand. You can enter any query in natural language, but you might consider using the prompts described in the following table and steps to familiarize yourself with the available data and what you can do with it.

   These steps give you insights into your compliance metrics for how well your teams meet their monthly remediation target dates for vulnerable item records as reported in your Service Level Agreement (SLA).

Your request or response	Description
What is my compliance for remediation for the month of October 2024?	By default the lookup is based on assignment group. If you do not specify a month, the AI agent looks for the current month and then starts going backwards in time, a month at a time. Alternatively, you might ask the agent for a breakdown by configuration item class or vulnerability. For example, type **What is my compliance for the month of October 2024 for Windows servers?**
Which asset types accounted for the most missed SLAs?	The results are organized based on the data for the month of your original request by asset type.
Which assignment group had the fewest missed Critical SLAs?	Get the assignment group that had the most or least missed SLAs based on the vulnerable item (VIT) severity: `Critical`, `High`, `Medium`, and `Low`. Additionally, you can ask the AI agent to look up missed SLAs by VIT category.
Show output for the previous question.	Request the agent to review your previous question if it doesn't give you an answer.
End the session, or **Stop**.	End the conversation.

   Your conversation is saved until you start a new chat. If the conversation ends unexpectedly, start a new chat. To start a new chat select the new chat icon ( ).

2. Enter a request in natural language to see your remediation metrics for a given month and year, for example, `What is my compliance for remediation for the month of October 2024?`

   The results are organized into sections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Summary - Total records that had SLA remediation targets for the month and year you requested and the percent totals for missed and met target dates.
- Breakdown by severity - Vulnerable items that missed remediation targets are broken down by critical, high, medium, and low severity.
- Breakdown by assignment groups - Percent of the total records with missed targets broken out by assignment groups.
- More information: Remediation Compliance for October 2024 link - View more information about the data. A new tab opens in UI16.

3. You might ask for more specific information about missed SLAs, for example, `Which asset types accounted for the most missed SLAs?`
   The results are organized for the data for the month of your original request by asset type, for example, Windows Server, Database, Linux Server, and so on.
4. You might ask for more specific information about your teams' productivity during that month, for example, `Which assignment group had the fewest missed Critical SLAs?`
   The assignment group is returned that had the least number of `Critical` VITs that missed the SLA.
5. You might compare these results to another month, for example, `How does this data compare with November 2024?`
   The results are organized into sections.
   - Comparison Summary - Total records that had SLA remediation targets for the time period that you first requested (**October 2024**) compared to your latest request (**November 2024**).
   - Breakdown by severity - Vulnerable items that missed remediation targets are broken down by severity: `Critical`, `High`, `Medium`, and `Low`.
   - Observations - Analysis of data and insights into data trends based on the comparison.
   - More information: Remediation Compliance for November 2024 link - View more information about the data used for the comparison. A new tab opens in UI16.

Unified Security Exposure Management (USEM)

Unified Security Exposure Management (USEM) is a comprehensive platform designed to transform how organizations manage security exposure across their digital estate. It consolidates multiple security exposure applications including Vulnerability Response, Configuration Compliance, Application Vulnerability Response, and Container Vulnerability Response into a single, cohesive architecture.

Important: Unified Security Exposure Management (USEM) is a major architectural upgrade to Vulnerability Response applications. If you are currently using Vulnerability Response and upgrading to USEM for the first time, you must use the Migration assistant for Unified Security Exposure Management to ensure a successful upgrade.

For detailed information, refer KB2556844 and Migrating from Vulnerability Response to Unified Security Exposure Management (USEM) before proceeding.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Security Exposure Management (USEM)

Explore



Learn about Unified Security Exposure Management concepts and features.

Configure



Learn to configure Unified Security Exposure Management.

Integrate



Extend Unified Security Exposure Management by integrating with other applications.

Use



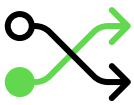
Learn how to monitor, manage, and remediate findings in Unified Security Exposure Management.

Reference



Learn about additional resources in Unified Security Exposure Management.

Upgrade Vulnerability Response to USEM



Upgrade Vulnerability Response applications to Unified Security Exposure Management.

Unified Security Exposure Management (USEM) applications

Vulnerability Response



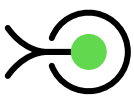
Learn about Vulnerability Response concepts and features.

Application Vulnerability Response



Learn about Application Vulnerability Response concepts and features.

Container Vulnerability Response



Learn about Container Vulnerability Response concepts and features.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Security Exposure Management (USEM) applications (continued)

Configuration Compliance	Vulnerability Response Workspaces	Software Bill of Materials
		
Learn about Configuration Compliance concepts and features.	Learn about the Vulnerability Response Workspaces.	Learn about the Software Bill of Materials concepts and features.

Exploring Unified Security Exposure Management (USEM)

Unified Security Exposure Management (USEM) is a platform that brings together infrastructure, application, container, and configuration exposures into one unified experience.

Unified Security Exposure Management overview

USEM is an evolution of existing Vulnerability Response modules including Application Vulnerability Management, Configuration Compliance and Container Vulnerability Response. It's designed to provide a single, integrated workspace for managing all types of security exposures across an organization's attack surface. Rather than focusing solely on vulnerabilities, USEM consolidates multiple exposure types such as policy violations, misconfigurations across asset types into one unified platform. This approach enables security and IT teams to visualize, prioritize, and remediate risks holistically.

Unified Security Exposure Management users

Users

User	Description
Administrator	Administers and configures the USEM platform and integrated third-party vulnerability tools, ensuring smooth data ingestion and integration health. The role involves setting up workflows, SLAs, notifications, and grouping rules, troubleshooting issues, and maintaining operational efficiency. It also manages role assignments, permissions, and access controls across USEM and connected applications, providing full administrative oversight for exposure management processes.
Vulnerability Analyst/ Manager	Monitors the organization's overall risk posture across integrated environments, ensuring accurate asset discovery and classification for vulnerability correlation. This role serves as an escalation point for remediation teams, assigns remediation tasks based on asset ownership and severity, and organizes vulnerabilities into dynamic remediation tasks to streamline prioritization. Additionally, the role delivers actionable dashboards and reports to track remediation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Users (continued)

User	Description
	progress, highlight critical exposures, and communicate the current risk posture to stakeholders.
Remediation Owner	Drives remediation of assigned exposure findings, submitting exception requests for issues that can't be resolved within defined timeframes, and navigating internal change management processes to implement fixes. The role also involves monitoring assigned workload to track progress and ensure compliance. With permissions to view and update findings and remediation tasks, access all vulnerability entries and solutions, and add internal notes, the Remediation Owner plays a key role in reducing organizational risk exposure.
Approver	Reviews and authorizes requests related to vulnerability and exposure management, including false positive validations, exception deferrals, assignment change approvals, and risk reduction measures. This role ensures governance and compliance by evaluating justification, risk impact, and remediation timelines before granting approval or rejection. Approvers work within a unified approval view, providing timely decisions, maintaining audit trails, and supporting multi-level workflows to keep remediation processes aligned with organizational policies.

Unified Security Exposure Management benefits

Unified Security Exposure Management benefits

Benefit	Feature	Users
Unified workspace: A centralized interface for managing exposures across infrastructure, applications, containers, and configuration compliance.	Security Exposure Management Workspace	Administrators, Vulnerability Analysts, Remediation Owners, and Approvers
Cross-exposure visibility: Provides dashboards and scorecards for monitoring risk posture and remediation progress in real time.	Security Exposure Management Workspace Findings view	Vulnerability Analysts
Streamlined administration: A single console for configuring workflows, SLAs, notifications, and assignment rules across all exposure types	Administration in Unified Security Exposure Management	Administrators
Integration health monitoring: Built-in tools to track and troubleshoot third-party integrations (for example, Qualys, Tenable, Rapid7).	Review Unified Security Exposure Management integrations	Administrators
Role-based experience: Tailored views for personas such as administrators, Vulnerability Analysts, Remediation Owners, and Approvers.	Security Exposure Management Workspace	Administrators, Vulnerability Analysts, Remediation Owners, and Approvers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Security Exposure Management benefits (continued)

Benefit	Feature	Users
AI-powered enhancements: AI generated insights on Findings view dashboards and approval recommendations for approvers.	Now Assist for Vulnerability Response	Security analysts, Governance & Risk teams, Approvers

What to explore next

To learn more about configuring and using Unified Security Exposure Management, see:

- Implementing Unified Security Exposure Management
- Unified Security Exposure Management integrations
- Using Unified Security Exposure Management
- Unified Security Exposure Management reference

Security Exposure Management Workspace

The Security Exposure Management Workspace provides a unified, role-based environment where security teams can investigate exposures, take remediation actions, configure automation, and track risk reduction progress in one place. It centralizes visibility across findings, remediation tasks, approvals, and administration, helping teams collaborate efficiently and respond to risks with clarity and speed.

Security Exposure Management Workspace benefits

The workspace provides multiple views designed for specific workflows, such as prioritizing critical issues, approving exceptions, managing remediation plans, and configuring automation, all in one place, without switching tools or interfaces.

In the workspace, you can:

- Gain real-time visibility into your exposure landscape with dashboards and AI-driven insights
- Act faster and smarter with automated workflows and prioritized remediation
- Ensure compliance through centralized governance and exception management
- Improve collaboration with role-based views tailored to each team's responsibilities

Role-based views ensure that security analysts, remediation owners, vulnerability managers, governance teams, and administrators work with shared awareness and act confidently based on the latest insights.

Workspace views and capabilities

Each view in the Security Exposure Management Workspace is designed for a specific purpose and role, providing targeted functionality to manage security exposures effectively.

View	Key Functions	Primary users	Key Actions
Finding view	Gain a clear, real-time understanding of your exposure landscape through dashboards that surface risks	Security analysts	Explore default or custom dashboards, drill into detailed findings, initiate remediation activities, and use Now Assist

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View	Key Functions	Primary users	Key Actions
	and insight-driven priorities		insights to prioritize critical issues and respond faster
Watch Topics	Continuously track and monitor specific high-priority vulnerability categories that require ongoing attention or strategic focus	Threat analysts, CISOs, Vulnerability managers	Create and refine watch topics, monitor trends and severity changes, evaluate business impact, trigger remediation efforts when thresholds are met
Remediation view	Plan, manage, and track remediation work across teams to ensure timely and effective resolution	Remediation owners, IT operations, security analysts	View assigned tasks, update progress, collaborate with owners, track deadlines
Cloud Exposure view	Gain a unified view to monitor and respond to top cloud risks through multiple lenses, including assets, images, and regulatory standards.	Vulnerability managers, Security analysts	View risk by cloud asset, drill into asset and finding details, and initiate remediation activities.
Approvals	Manage and track all vulnerability and compliance exception approvals in a single, unified workflow with full visibility into request status and urgency	Governance & Risk teams, approvers	Review contextual details for each approval request, take approval actions, view overdue and pending items, access finding details, and record comments or decisions directly
Lists	Access complete lists of findings, remediation tasks, approvals, and exceptions to monitor status, ownership, and progress.	Vulnerability analysts, remediation owners, security managers	Navigate predefined or custom lists, drill into records, create and manage custom lists, monitor status and ownership, and take follow-up actions such as updating records or processing approvals
Administration	Configure and govern Security Exposure Management settings centrally to ensure consistent policies, integrations, and automation across the environment	Admins, Platform owners	Manage integrations, configure rules and automation, set up email notifications and templates, map severity levels, and customize visualization settings

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View	Key Functions	Primary users	Key Actions
			from a unified Admin Console
Approval View	Testing Approval view	Testing Approval view	Testing Approval view

Getting started

Access the Security Exposure Management Workspace by navigating to **Workspaces** > **Security Exposure Management**. Your available views and actions depend on your assigned role.

Next steps

Explore detailed guidance for each Security Exposure Management Workspace view:

Security Exposure Management Workspace Findings view

Security Exposure Management Workspace Watch Topics

Remediation view

Viewing the Cloud Exposure View dashboard

Security Exposure Management Approvals View

Security Exposure Management Workspace List view

Administration in Unified Security Exposure Management

Implementing Unified Security Exposure Management

Administration in Unified Security Exposure Management

The Administration for Security Exposure Management application offers a unified administrative experience across all Unified Security Exposure Management (USEM) applications. It introduces the Admin Console within the Security Exposure Management (SEM) Workspace, allowing administrators to configure Security Exposure Management applications and monitor integrations from a single location.

The Administration Console centralizes configuration and administration for all USEM applications, streamlining the management process and ensuring consistent settings across the environment. The following modules are available within the Admin Console:

- **Integrations**: The Integration status page provides a comprehensive overview of installed third-party applications and their integration runs. Real-time status updates enable administrators to diagnose and resolve issues related to failed integration runs. For more information, see Review Unified Security Exposure Management integrations.
- **Configurations**: Configuring rules automates, organizes, and manages the lifecycle of findings, ensuring scalability, data consistency, and faster response times by reducing manual intervention. For more information, see Configure rules to manage findings.
- **Additional Configuration Options**
  - **Email Notifications**: Set up email notifications to share important updates and activities, such as approval and rejection of false-positive requests. Specify when to send notifications, who receives them, and their content. For more information, see Configure email notifications in Unified Security Exposure Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Email Templates**: Create and manage preconfigured email templates for sending notifications. For more information, see Configure email templates in Unified Security Exposure Management.
- **Severity Mapping**: The Security Exposure Management Workspace severity mapping transforms third-party source severity fields to recognizable fields in Unified Security Exposure Management. For more information, see Severity mapping for Unified Security Exposure Management.
- **Visualization Library**: Configure the Visualization library to select columns for the Findings view page, including available widgets, activation status, and additional details. For more information, see Configure Visualization library.

Related topics

Implementing Unified Security Exposure Management

Visualization library

The Visualization library lists all the widgets that you can use to visualize and categorize findings. It includes a set of default widgets and any custom widgets that you create for organization-specific reporting. You can browse the available widgets, understand the data they use, and add them to dashboards to build tailored security exposure views.

You can use the Visualization library to:

Explore available widgets

Review the complete set of default and custom widgets available for building dashboards.

Understand widget behavior

Review key details such as data sources, grouping, visualization type, and activation status to choose the appropriate widget for your analysis.

Create a custom widget

Build and configure your own widgets to visualize specific metrics or data insights that matter most to your organization.

The following table lists the available widgets, associated tables, and what they display.

Widget name	Findings tables	Description
Deferred findings by reason	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active deferred records grouped by reason.
Findings by assignment group	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records assigned to various assignment groups.
Findings by base image	Container vulnerability	Active records categorized by the type of the image.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Widget name	Findings tables	Description
Findings by CI class	• Infrastructure vulnerability • Application vulnerability • Misconfigurations	Active records categorized by CI classes.
Findings by cloud resource	• Infrastructure vulnerability • Misconfigurations	Active records categorized by various cloud resources.
Findings by remediation status	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records grouped by remediation status.
Findings by risk rating	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records categorized by the risk ratings. • 1: Critical • 2: High • 3: Medium • 4: Low • 5: None
Findings by scan type	Infrastructure vulnerability	Active records grouped by the scan type.
Findings by source	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records grouped by the source.
Findings by state	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records categorized by various states (Open, Under Investigation, Awaiting Implementation, In Review, Resolved, and Deferred).
Findings by technology	Misconfigurations	Active records categorized by technology.
Findings by test group	Misconfigurations	Active records categorized by the test groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Widget name	Findings tables	Description
Findings by Vulnerability	• Infrastructure vulnerability • Application vulnerability • Container vulnerability	Active records categorized by vulnerability.
Findings by Vulnerability Classification	• Infrastructure vulnerability • Application vulnerability • Container vulnerability	Active records categorized by vulnerability classification.
Findings not in remediation task	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records that are and aren't part of the remediation task.
Findings on external-facing assets	• Infrastructure vulnerability • Application vulnerability • Misconfigurations • Container vulnerability	Active records categorized by the asset exposure to internet.
Findings with exploits	• Infrastructure vulnerability • Application vulnerability • Container vulnerability	Active records with and without known exploits.

If your instance uses localization, make sure that the widget titles show up correctly in all supported languages. Default widgets already include translated titles.But if you update a default widget, create a custom widget, or rename a widget, remember to add or update the translation entry. This keeps titles consistent across languages. For steps, see Localize widget titles.

Related topics

- Configure Visualization library
- Create a custom widget
- Visualization widget fields

Viewing the Cloud Exposure View dashboard

The Cloud Exposure View is a module that is supported by Security Exposure Management workspace. Select interactive visualizations and filter aggregated data for your cloud assets by category to view findings for your security exposures. Cloud security teams can monitor and act on all their cloud-related security findings from multiple vendors across their cloud environments from within the workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Locating the Cloud Exposure View

To view the dashboard, navigate to **Workspaces** > **Security Exposure Management** > **Cloud Exposure View**.

Roles required:

- sn_sec_exception.read to view the workspace
- sn_vul_cmn.usem_admin to configure workspace rules
- For vulnerability findings remediation by product:

See Security Exposure Management Workspace Roles

Top-level filters

Locate and organize findings based on the following top-level filters to help you focus your search:

- **Finding type** - View security exposure findings for your cloud service accounts, cloud regions, and cloud resources with this filter.

  Note: Finding types are listed by product. You must install the corresponding applications before you can view the imported data for the following finding types:

  - **Host**Vulnerability Response supports findings for vulnerabilities in virtual machines and servers.
  - **Misconfiguration** Configuration Compliance supports findings for misconfigurations in cloud resource services such as S3 and EC2. Configuration Compliance also supports findings for `Issues`, such as assets that are involved in toxic combinations of vulnerabilities and misconfigurations.
  - **Container** - Container Vulnerability Response supports container vulnerability findings.
- **Source** - View security exposures organized by the third-party scanner product integrations you have installed in your instance.
- **Risk rating** - View security exposures by their criticality (Critical, High, or Medium). Multi-select is supported.

  Note: Select the Settings (gear icon). With **Filters** selected you can include findings with **Low** criticality and no imported criticality (**None**). You might prefer to keep the criticality in its default setting to limit your import and help you focus on your most important findings. If you modify this filter, findings that match your settings are imported with the next daily data import for all your finding types.

Needs attention

Select the totals on the cards to open a list in a new browser tab. View your most critical records organized by the applications that you have installed for the following categories.

- Unassigned findings
- Overdue findings
- Remediation due in 14 days
- Findings in review
- Select the total numbers in the cards to view a list of records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select a card and then select the filters on the new tabs that are displayed to view lists of findings by product: **Host**, **Misconfiguration**, and **Container**.

Cloud Security Overview

- View breakdowns of totals of active findings across cloud resource types that are categorized by provider and severity for the following assets:
  - Compute
  - Network
  - Storage
  - Other - Resources that don't fall under the other categories.
  - Select the total numbers in the cards, a provider icon, or the data visualizations to view corresponding lists of records that display total findings for each asset.
- Select **Base images** or **Other image types** to view the five findings that have the most security exposures (Top) for the following categories:
  - Top base images with active findings
  - Top base images by risk
  - Select the total number in the card.

  Container findings are color-coded for Critical, High, and Medium:
  - Red
  - Orange
  - Yellow

  Select a data visualization graph or a colored pill to view a list of up to 1,000 records.
- Select **Accounts** or **Regions** to view the top five findings that have the most security exposures.

  Findings are grouped by Host, Misconfigurations (Test results), Toxic combinations (Issues), and Container (Container vulnerabilities) and are color-coded for Critical, High, and Medium:
  - Red
  - Orange
  - Yellow

  View records for your least compliant accounts under **Non compliant framework**. If no data is imported, this column remains unpopulated.

  Select a colored pill or **View more** to view a list of up to 1,000 records.
- Select from **Resources** or **Resources - Externally Exposed** to view the top five findings that have the most critical security exposures.

  Findings are grouped by Misconfiguration (Test results) and Toxic combinations (Issues), are and Container findings and are color-coded for Critical, High, and Medium:
  - Red
  - Orange
  - Yellow
- View toxic combinations and assets with the least compliant scores that have the most security exposures due to failed configurations. Both misconfigurations and issues are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

populated on test results in Configuration Compliance. This data is imported by the Understanding the Wiz Vulnerability Response Integration, and this data is not displayed unless Configuration Compliance and the Wiz Vulnerability Response Integration are installed.

Findings with failed test results are color-coded. You can select the date range for the last 7 days or the last 30 days.

- Red
- Orange
- Yellow

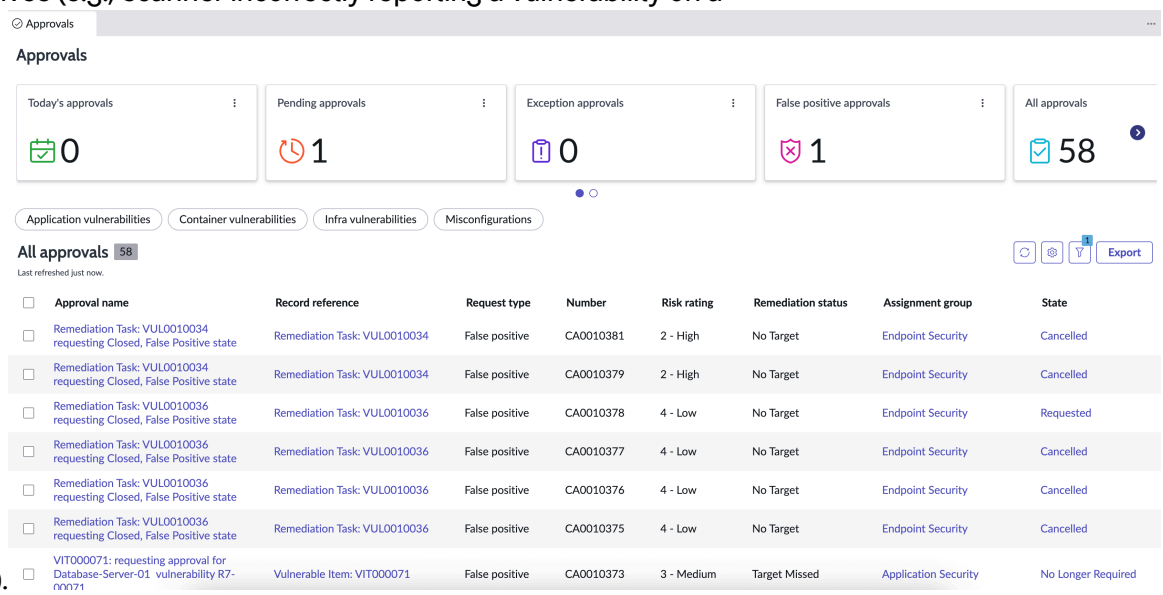
Select **View more** to view a list of up to 1,000 records.

Security Exposure Management Approvals View

The approval process in Security Exposure Management for vulnerability and compliance exceptions is unified to simplify workflows, improve visibility, and streamline actions for Approvers.

The Approvals landing page provides a comprehensive view of all approval requests initiated by remediation owners to view specific requests, with navigation widgets such as:

- **All approvals**: Consolidated list of all approvals, including exception, false positive, risk reduction, and unassignment (e.g., a single view of everything awaiting your approval).
- **Overdue approvals**: Approvals that have crossed their due date (e.g., a risk reduction request that was supposed to be approved yesterday).
- **Pending approvals**: Approvals awaiting action beyond today across all request types.
- **Today's approvals**: Approvals due for action today (e.g., an unassignment request expiring by end of day).
- **Exception approvals**: Approvals specifically for exception requests (e.g., a request to allow delayed patching of a high-risk vulnerability).
- **False positive approvals**: Approvals for requests flagged as false positives (e.g., scanner incorrectly reporting a vulnerability on a host).



Each approval request contains interactive links that provide access to detailed information, including Record Reference for findings, Request Type, Request Number, Risk Rating, Remediation Status, Approval Assignment Group, and Current State. You can also access click-

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

able links to view details related to associated findings. See Configure Approval List and Form View.

When opening a finding record (e.g., VIT, AVIT, CVIT, Test Results), users can view detailed attributes such as state, remediation status, assignment group, information about the finding, relevant detections, change approvals, and requested approvals.

You can defer a finding or remediation task directly from its respective form in the Security Exposure Management workspace. Once submitted, the request is sent for approval. This unification offers:

View the requester, purpose, impacted services, approval levels, and comments all in one place.

Approvers can approve or reject requests directly within the same record. See Reviewing an Approval Request.

Every comment and approval action is recorded and attributed.

All requests including pending, overdue, or completed, are easy to locate and manage in the single view. Links to legacy approval requests are available for items that remain in the old flow during the migration period.

Security Exposure Management Workspace Findings view

The Security Exposure Management Workspace Findings view aggregates the security exposure data and presents it as dashboards containing data visualization widgets.

You can use the Findings view to:

Access default dashboards

Quickly view a preconfigured dashboard that highlights key security exposure metrics.

Create custom dashboards

Tailor dashboards to your specific needs by selecting relevant data visualization widgets.

Drill down into the findings

Use widgets to explore detailed findings and initiate remediation actions directly.

Generate Insights

Act faster with GenAI-powered important actions and insights.

https://player.vimeo.com/video/1144586406?h=35a433da48&badge=0&autopause=0&player_id=0&app_id=58479

The Visualization library offers a rich set of default widgets that fetch from specific findings tables. These widgets help you visualize and categorize findings based on various attributes. In addition to the default widgets, administrators can create custom widgets that meet organization-specific reporting needs. Custom widgets appear in the Visualization library and can be added to dashboards in the same way as the default widgets. For more information, see Visualization library and Configure Visualization library

What to explore next

To learn more about using the Findings view page, see:

- Configure Visualization library
- Create a dashboard in the Findings view page

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation view

The Remediation view in the Security Exposure Management workspace provides remediation owners and vulnerability managers with a consolidated view of remediation tasks, findings (vulnerable items and configuration test results), and assets (configuration items) that are associated with exposure findings.

Locating the Remediation view

Remediation owners and vulnerability managers can view remediation tasks and findings for multiple applications from a single location using filters. The data available on this page can help remediation owners prioritize their work, and vulnerability managers can monitor overall remediation progress for specific types of exposure findings.

Navigate to **Workspaces** > **Security Exposure Management** > **Remediation**. What you can see and do in the view depends on your role and the applications you have installed.

Features of the overview page

Assigned to me

Toggle between findings and remediation tasks that are assigned to you and your groups.

Tabs

View remediation task, finding, or asset records.

Widgets

Select the data visualizations to filter records by remediation tasks, findings, or asset records. These widgets must be activated in the Visualization library to display data on this page.

- Remediation tasks - Filter records by remediation status, state, or risk rating.
- Findings - Filter records by impacted configuration items, by state, risk rating.
- Assets - Filter records by configuration items and their associated security exposures.

Exposure Type

Filter remediation tasks and findings records by the type of security exposure, host findings (VIT), application findings (AVIT), and so on. These records are available based on the applications that you have installed and the roles you have assigned:

- Application Vulnerability Response - AVITs and AVULs.
- Container Vulnerability Response - CVITs and CVUL records.
- Host Vulnerability Response VITs and VUL records.
- Test results Configuration Compliance CTRs and CRG records.

Security Exposure Management Workspace List view

The List view in the Security Exposure Management Workspace permits vulnerability and security managers and analysts to view remediation progress on records, drill down into records, and view the status of their approval requests and exceptions.

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

These lists and links provide you with easy access to records and tasks. It contains two tabs:

- **Lists** tab: Displays the default lists for remediation efforts, remediation tasks, vulnerable items, configuration test results, solutions, exceptions, and libraries.
- **My Lists** tab: Displays any lists that you've renamed from the Lists tab and any lists that you create.

  You can also create your own list to monitor remediation progress. For more information, see Create a customized list of records.

Lists tab

The following table shows the lists available in the Lists tab of the List page:

Tip:

If the *sn_vul_cmn_ws.navigate_to_workspace* system property is set to `true` by an admin, upon selecting the predefined filter links in the Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response and Configuration Compliance modules from the **All** menu, these links open in the List page of the Security Exposure Management Workspace based on your role.

For example, if you select **Assigned to My Groups** by navigating to **All** > **Security Exposure Management** > **Remediation Tasks** > **Assigned to My Groups**, this link is redirected to the Security Exposure Management Workspace. The **Assigned to My Groups** list in the **Remediation Tasks** module opens in the List page of the Security Exposure Management Workspace if you have the vulnerability admin or analyst role. To view the host remediation tasks group the tasks by Record Type.

You can hide the record count on the lists using the *glide.ui.list.seismic.omit.count* system property. For more information on how to turn off/on the record count on a list, see the KBB0010402 KB article.

Lists

List item	Description	Modules	Roles Required
Remediation efforts (REs)	List of **Active** REs and **All** the REs assigned to your assignment groups. Group the remediation efforts by **Record Type** to categorize them by host vulnerable items, application vulnerable	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	items, container vulnerable items and configuration test results.		• sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Impacted Assets	Contains the following lists: • **Assigned to me**: List of impacted assets assigned to you for remediation. • **Assigned to my group**: Impacted assets assigned to your assignment groups for remediation.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)
Remediation tasks	Contains the following lists: • **Active**: List of all the active host, application, container and Test result remediation tasks. • **All**: List of both active and inactive host, application, container and Test result remediation tasks. • **Assigned to me**: List of Remediation tasks assigned to you for remediation. • **Assigned to my group**: Remediation tasks assigned to your assignment	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	groups for remediation. • **Multiple Deferrals**: Lists findings that you've deferred multiple times. Group the remediation tasks by **Record Type** to categorize them by host vulnerable items, application vulnerable items, container vulnerable items and configuration test results. **Note:** The Remediation tasks list includes tasks generated during the Remediation Effort creation in the Security Exposure Management Workspace, as well as those created manually and by remediation task rules and other processes in the classic UI. The Remediation effort column will be empty for any remediation tasks that were not created as part of the Remediation Effort.		
Host Vulnerable items	Contains the following lists	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• **Active**: List of all the active host vulnerable items. • **All**: List of both active and inactive host vulnerable items. • **Assigned to me**: List of host vulnerable items assigned to you for remediation. • **Assigned to my group**: List of host vulnerable items assigned to your assignment groups for remediation.		
Application Vulnerable items	Contains the following lists: • **Active**: List of all the active application vulnerable items. • **All**: List of both active and inactive application vulnerable items. • **Assigned to me**: List of application vulnerable items assigned to you for remediation. • **Assigned to my group**: List of application vulnerable items assigned to your assignment groups for remediation. You can create a new application vulnerable item by selecting the **New** button.	Application Vulnerability Response	sn_vul.app_sec_manager
Container Vulnerable items	Contains the following lists:	Container Vulnerability Response	sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• **Active**: List of all the active container vulnerable items. • **All**: List of both active and inactive container vulnerable items. • **Assigned to me**: List of container vulnerable items assigned to you for remediation. • **Assigned to my group**: List of container vulnerable items assigned to your assignment groups for remediation.		
Configuration Test Results	Contains the following lists: • **Active**: List of all the active test results. • **All**: List of both active and inactive test results. • **Assigned to me**: List of test results assigned to you for remediation. • **Assigned to my group**: List of test results assigned to your assignment groups for remediation.	Configuration Compliance	sn_vulc.admin
Solutions	Contains the following lists: • **All**: Shows all the available solutions which you can use to remediate the host vulnerable items.	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• **Highest Supersedence**: Shows all the solutions which is used to populated Preferred Solutions. • **With Vulnerable items**: Shows the solutions which are being used as Preferred Solution on Vulnerable Items.		
Exceptions	Shows the approval states for all the exception and false positive requests associated with your assignment groups. • **All**: List of the exception, false positive, and unassign approval requests related to VITs, AVITs, and CVITs and their remediation tasks (VUL, AVUL, and CVUL). • **My requests**: List of all the exception, false positive, and unassign approval requests raised by you for host, application, and container vulnerable items and their remediation tasks. • **All (Configuration Compliance)**: List of the exceptions, false positive, and unassign approval requests related test results and remediation tasks (CTR#).	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• **My requests (configuration compliance)**: List of all the exception, false positive, and unassign approval requests raised by you for the test results and their remediation tasks that you are working on. Group the exceptions by **Record type** to categorize them by host vulnerable items, application vulnerable items, container vulnerable items and configuration test results.		
Approvals	**Assigned to me**: Shows the approval requests assigned to you for processing. To process your approvals in the workspace, see Approve or reject requests in the Security Exposure Management Workspace.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Libraries	Consists of the following lists: • **CVEs (NVD)**: List of all the Common Vulnerability and Exposures (CVEs) from Vulnerability	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	Response, Application Vulnerability Response, and Container Vulnerability Response. • **TPEs**: List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs. • **CWEs**: List of all the Common Weakness Enumerations (CWEs) from Vulnerability Response, Application Vulnerability Response, and Container Vulnerability Response. • **Vulnerable Software**: List of all the software vulnerable entries. • **App vulnerabilities**: List of all the third-party application vulnerability entries. • **Test Groups**: List of all the Configuration Compliance test groups. You can view the percentage of CI compliance and test results compliance for a Test Group in the record view. • **Tests**: List of all the tests from Configuration Compliance. You can view the	Configuration Compliance	vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	percentage of test results compliance for a test in the record view. • **Compensating Controls**: List of all the compensating controls which can be used for risk reduction requests. You can add a compensating control by clicking **New**. For more information on how to add a compensating control, see Add a compensating control to the library.		
CMDB	Contains the following lists • **Discovered items**:List of all the discovered items. • **Discovered container images**: List of Container images. These container images provide information on the image ID, Docker image, and the image repository along with the layer information. • **Discovered Applications**: List of all discovered applications, including details such as application name, source, state, integration instance, and more.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
Penetration Test Assessment Requests	Contains the following lists: • **Active**: List of active Penetration Test Assessment Requests. • **All**: List of both active and inactive Penetration Test Assessment Requests • **Assigned to me**: List of Penetration Test Assessment Requests raised by you. • **Assigned to my group**: List of Penetration Test Assessment Requests raised by the users in your assignment groups. For information on how to create a penetration test assessment request, see Create a new penetration testing assessment request.	Application Vulnerability Response	sn_vul.app_sec_manager
Penetration Test Findings	Contains the following lists: • **Active**: List of all the active Penetration Test Findings. • **All**: List of both active and inactive Penetration Test Findings. • **Assigned to me**: List of Penetration Test Findings assigned to you for remediation. • **Assigned to my group**: List of Penetration	Application Vulnerability Response	sn_vul.app_sec_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	Test Findings assigned to your assignment groups for remediation. • **Validation Pending**: List of Penetration Test Findings that are pending validation after remediation. For information on how to create a penetration test findings, see Create penetration test findings based on an assessment questionnaire.		
Patches	**All**: List of all the available patches that can be used to remediation host vulnerable items.	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin
Supporting Data	Contains the following lists: • **Authoritative Sources**: List of authoritative sources that provide summary information which is useful to research the source publications. • **Technologies**: List of technologies that provide the summary information about each authoritative sources and citation (also known, in Qualys, as a framework).	Configuration Compliance	sn_vulc.admin

Related topics

Use the List view in the Security Exposure Management Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Exposure Management Workspace Watch Topics

The Watch topics page in the Security Exposure Management Workspace enables you to create and edit a watch topic. A Watch topic is a set of data visualizations which enables you to monitor a filtered set of records findings (VITs, AVITs, CVITs and CTRs) over time on a dashboard that might be of a particular interest or priority to your organization.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

The data displayed on the data visualizations on the watch topics are dynamically updated as vulnerability data changes upon import. Use the dashboards to monitor the trends, scope, and types of vulnerabilities and your configuration items for the selected watch topic. This information helps you determine how the vulnerabilities in each watch topic impact your environment. The Watch Topics page consists of four modules - Host Vulnerabilities, Container Vulnerabilities, Application Vulnerabilities, Configuration Test Results, and Inactive. For more information on the related items tabs and their visualizations in a watch topic, see Related items list and visualizations in a watch topic.

The following watch topics are provided with the base system in the Host Vulnerabilities module on the Watch Topics page:

- Vulnerabilities on External Facing Assets
- Vulnerabilities with Exploits Available
- Vulnerabilities on Windows Servers
- Vulnerabilities on LINUX Servers
- Critical Overdue Vulnerabilities
- Critical Vulnerabilities not in Remediation Tasks

Note: If a data visualization shows that there are no records for that category, but you can see a list of records when you click the graph icon, check the column with the watch topic name on the list that is displayed. Verify that the value for all the records listed in the column of the watch topic, for example, Internet-facing, is `false`. This value in this example indicates that there are no internet-facing records for this watch topic.

To start the remediation or when a critical need arises for the records that are in a watch topic, you can create a Remediation Effort from a watch topic. For more information, see Create a remediation effort in the Vulnerability Manager Workspace.

Related topics

Related items list and visualizations in a watch topic

Use watch topics in the Vulnerability Manager Workspace

Create a watch topic in the Vulnerability Manager Workspace

Edit or delete a watch topic in the Vulnerability Manager Workspace

Deactivate or activate a watch topic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Exposure Management Workspace Health dashboard

The Vulnerability Response Health dashboard is a tool designed to empower organizations with comprehensive insights into the implementation and usage of their Security Exposure Management applications.

The overall health assessment is determined by aggregating various critical factors across configuration, implementation, integration, performance, data, and process. View the aggregate dashboard for each category for the following applications:

- Vulnerability Response
- Application Vulnerability Response
- Container Vulnerability Response
- Configuration Compliance

Installing the SecOps Vulnerability Response Health Dashboard

To install and configure the SecOps Vulnerability Response Health Dashboard for Vulnerability Response applications in your ServiceNow AI Platform instance, navigate to the ServiceNow® Store and activate the SecOps Health Analytics (sn_sec_analytics) plugin.

Required ServiceNow AI Platform roles

Roles required: sn_sec_analytics.admin, sn_sec_analytics.read

Scheduled job

To view the scheduled job, navigate to **All** > **System Scheduler** > **Scheduled Jobs** > **Collect health dashboard metrics**. The 'Collect health dashboard metrics' scheduled job is run daily at 00:00 hours. It generates the data for the SecOps Vulnerability Response Health dashboard. You can choose to run the scheduled job manually as well.

Accessing the SecOps Vulnerability Response Health Dashboard

To access the SecOps Vulnerability Response Health Dashboard,

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select the **Dashboards** icon.
3. Select **SecOps Vulnerability Response Health Dashboard** from the drop-down list.

Use cases

For examples of how people in your organization would use this dashboard, see these use cases.

User	Dashboard use
Vulnerability admin	Helps you gain an understanding of the health score of the Unified Security Exposure Management applications. It's also helpful to highlight the areas that need improvement. The Vulnerability Response Health Dashboard deals with the implementation and usage

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User	Dashboard use
	health only. It doesn't assist with management of findings.
Support admin	Helps you to identify the performance, customization, and configuration issues using KPIs. Based on the application health, you can perform an extra analysis or provide a recommendation to the users.
Implementation partner	Helps you to evaluate the Unified Security Exposure Management implementation health for configurations, add-ons, customizations, and integrations, and provide improvement recommendations for the users.

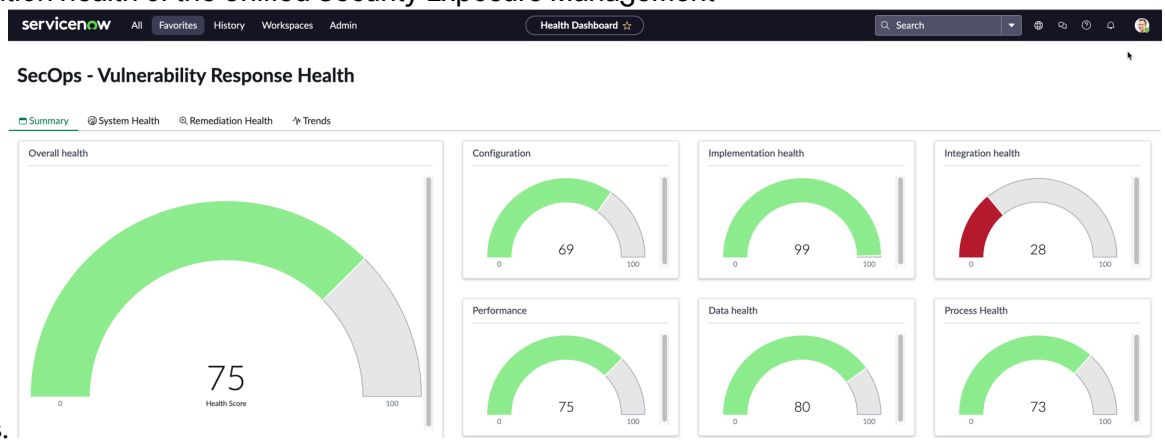
The SecOps Vulnerability Response Health Dashboard tabs

To view the SecOps Vulnerability Response Health dashboard, navigate to **Security Operation Health** > **Vulnerability Response Health**. Each color in the dashboard represents the following:

- Green: Safe
- Yellow: Warning
- Red: Critical

Summary tab

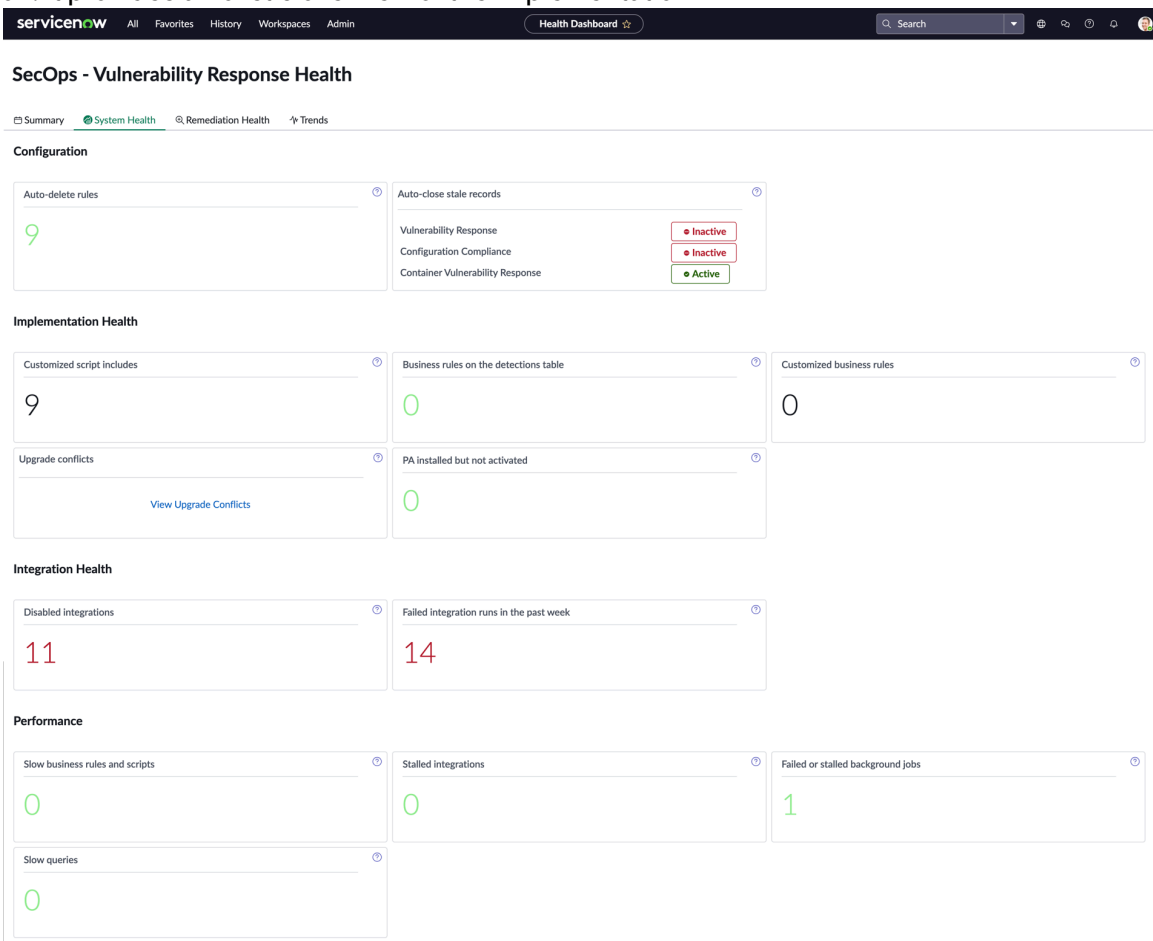
This dashboard communicates the overall health score for the configuration and remediation health of the Unified Security Exposure Management applications.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Health tab

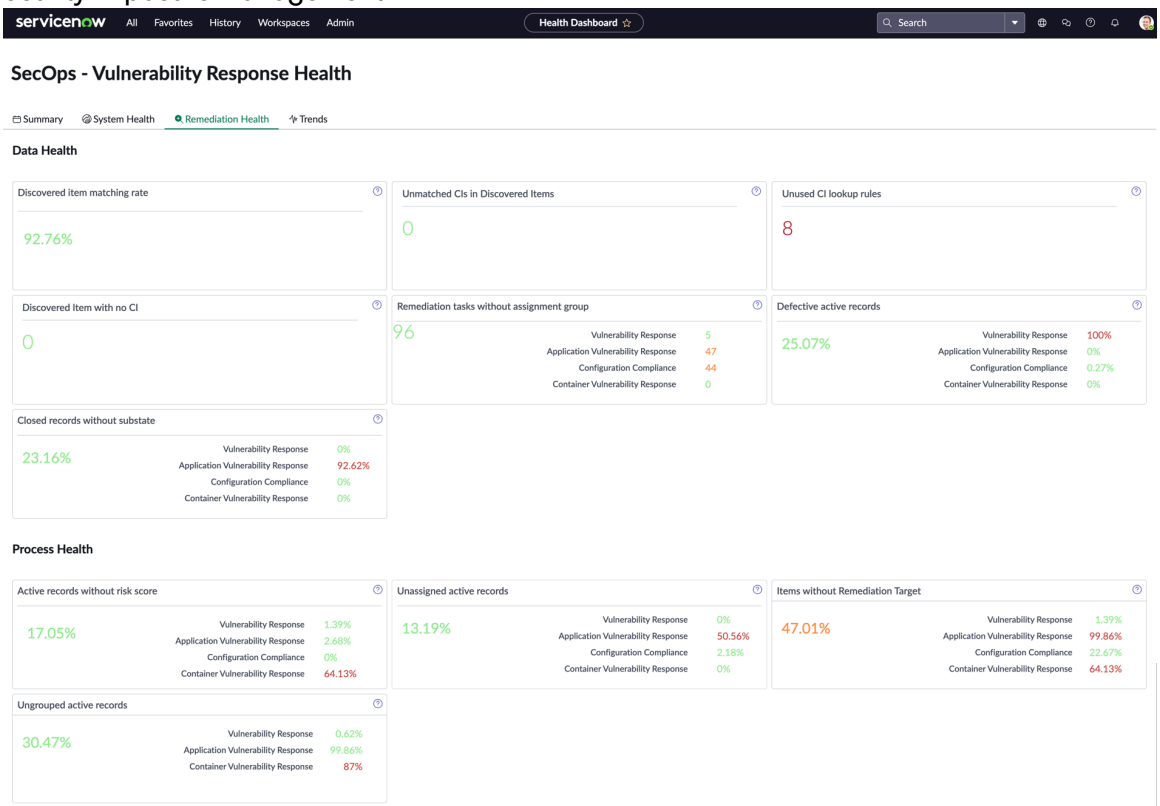
This dashboard displays the configuration and integration health of your implementation. It provides a holistic overview of the implementation performance.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

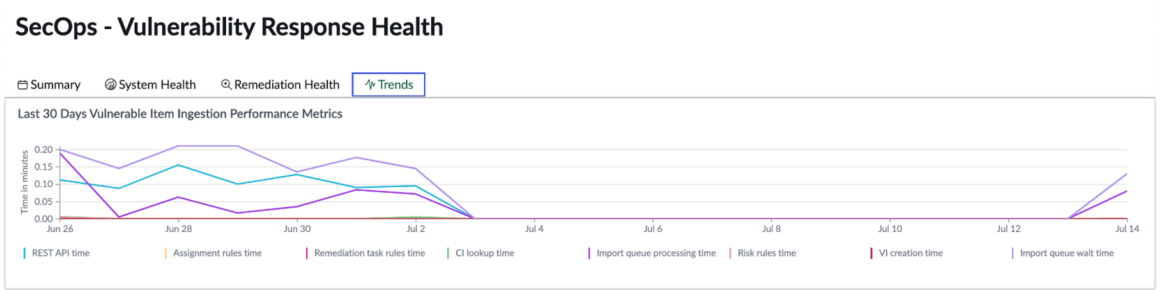
Remediation Health tab

This dashboard displays the data health of the Unified Security Exposure Management applications.



Trends tab

This dashboard displays the trends for the findings ingestion performance metrics for the past 30 days for the Unified Security Exposure Management applications.



Reports

Note: The threshold values are a part of the base system. You can configure the values based on your requirements.

Summary

Title	Description
Overall health	Overall health score for the Unified Security Exposure Management applications. For more information, see the reports for the metrics.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Summary (continued)

Title	Description
Configuration	Overall configuration health of the Unified Security Exposure Management applications.
Implementation health	Overall implementation health of the Unified Security Exposure Management applications.
Integration health	Overall integration health of the Unified Security Exposure Management applications.
Performance	Overall performance health score of the VR applications.
Data health	Overall data health of the Unified Security Exposure Management applications.
Process health	Overall process health score of the Unified Security Exposure Management applications.

System Health

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Configuration				
Auto-delete rules	Displays the number of enabled auto-delete rules.	Review and resolve the inactive auto-delete rules.	3	1
Auto-close stale records	Closes stale detections automatically. For more information, see theClosing stale detections and findings automatically using auto-close rules.	Reduce the volume of stale detections. Enable this option to close the stale detections that aren't closed by the scanners.	3	1
Implementation health				
Customized script includes	Number of 'script includes' customized.	Minimize customized 'script includes' for easier upgrades.	10	12
Business rules on the detections table	Number of customized business rules in the detection table.	Minimize business rules for easier upgrades.	4	8

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Customized business rules	Number of customized business rules before creation of records in the CMDB.	Use the default business rules on records.	5	8
Upgrade conflicts	Conflicts such as business rules and scripts identified on an upgrade.	Review and resolve the upgrade conflicts.	10	15
PA installed but not activated	Indicates if the Performance Analytics dashboard is not enabled.	Activate the PA dashboard.	10	15
Integration health				
Disabled integrations	Number of integrations that have been disabled.	Review and enable the required integrations.	6	9
Failed integration runs in the past week	Number of integration runs that weren't successful in the past week.	Review and resolve the cause of the failed integration runs.	9	12
Performance				
Slow business rules and scripts	Business rules and scripts whose average execution time greater than 10 ms and execution count greater than 10,000.	Review and resolve the slow-running business rules.	10	15
Stalled integrations	Number of integrations that were timed-out before completion.	Review and resolve the cause of the stalled integrations.	10	15
Failed or stalled background jobs	Failed or timed-out background jobs in the past week.	Review and resolve the cause of the failed jobs.	5	10

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Slow queries	Queries whose average execution time is greater than 10 ms and execution count is greater than 10,000.	Review and resolve the slow-running business rules.	10	15

Remediation Health

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Data Health				
Discovered item matching rate	Number of discovered items matched to existing CIs.	Review the health of your CMDB and the CI lookup rules logic.	50	20
Unmatched CIs in discovered items	Discovered items in unmatched state.	Review the health of your CMDB and the CI lookup rules logic.	9	12
Unused CI lookup rules	CI lookup rules that aren't associated with any discovered item.	Change the status of the unused CI lookup rules to inactive.	4	6
Discovered item with no CI	Discovered item with no configuration item.	Review and reapply CI lookup rules.	9	12
Defective active records	Records without a configuration item or vulnerability.	Retire the CIs using the CMDB CI Lifecycle Management option. **Note:** Deleting CIs directly can result in orphan VITs.	40	60

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Remediation tasks without assignment group	Active remediation tasks whose assignment group is yet to be assigned.	Assign remediation tasks to an assignment group and review the existing assignment rules.	40	60
Closed records without substate	Records that are closed without a substate.	Provide information in the Reason field while closing the records.	40	50
Process Health				
Active records without risk score	Active records with a risk score of 0 or with no risk score assigned.	Review and resolve the risk rules.	40	60
Unassigned active records	Records without an assignment group.	Assign a group to the records and review the existing assignment rules.	30	50
Items without Remediation Target	Items without a remediation target date.	Review and resolve the remediation target rules. These rules must include all the records.	30	50
Ungrouped active records	Records that aren't included in a remediation task rule.	Review the remediation task rules.	40	60

Trends

Title	Description
Last 30 days vulnerable item ingestion performance metrics	Average time taken to ingest vulnerable items and process multiple rules in the past 30 days.

Security Exposure Management workflow

Unified Security Exposure Management (USEM) is ServiceNow's next-generation platform that consolidates multiple security exposure applications—Vulnerability Response (VR), Application Vulnerability Response (AVR), Container Vulnerability Response (CVR), and Configuration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Compliance (CC)—into a unified architecture. It provides a single source of truth for security exposure, enabling real-time visibility, streamlined workflows, and automated remediation.

The workflow involves the following steps:

1. **Install and activate USEM applications**: Install the Unified Security Exposure Management plugin from the ServiceNow® Store.This automatically installs dependent apps such as:
   - Security Exposure Management Workspace
   - Administration for Security Exposure Management
   - Risk Scoring
   - Exception Management
   - Remediation Task Management
2. **Access the USEM Workspace**: Navigate to the Security Exposure Management Workspace.
3. **Ingest and correlate data**: USEM supports ingestion from multiple scanners (Qualys, Tenable, Veracode, etc.). It deduplicates and correlates findings across infrastructure, applications, containers, and cloud environments.
4. **Prioritise and remediate**: Use the Risk Scoring module to assign severity based on business impact. Launch remediation tasks directly from findings. Exception management is modularised and unified across all apps.
5. **Monitor and report**: Dashboards provide real-time insights into exposure, remediation progress, and exception trends. Saved filters and watch topics help track critical findings.

Automating prioritization and triaging

Automate prioritization and triaging of findings using rules and severity mapping.

Associating finding with a configuration item using lookup rules

Unified Security Exposure Management uses lookup rules to associate imported third-party exposure findings with configuration items (CIs) in the Configuration Management Database (CMDB). These rules match asset data to existing CIs, enabling accurate remediation.

Findings imported from external scanners such as Qualys, Tenable, and Rapid7 often lack direct CI references. Lookup rules bridge this gap by applying matching logic to map findings to CIs in the CMDB.

Characteristics of lookup rules

- **Domain separation and source specificity**: Lookup rules can be domain-separated and are specific to each source, enabling multiple deployments according to source.
- **Shared across deployments**: Rules are shared across all deployments of a scanner source integration. Any changes or deletions affect all deployments.

How lookup rules work

The lookup rules follow a three-step process.

1. **Initial lookup**: When assets or findings are imported, the system first checks the **Discovered Items** list using third-party IDs. If an asset ID matches, it populates the **Configuration Item** field in the finding record.
2. **Matching process**: If no asset ID match exists, the rules use other asset details to identify the correct CI. You can view mappings in the **Discovered Items** list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. **Placeholder CI creation**: If no match is found, a placeholder CI is created and marked as an Unmatched CI.
   - Matching starts with a vendor ID lookup across source, source_instance, and vendor ID.
   - The rules execute in ascending order and stop when a single CI match is found.
   - If the matched CI is a low-level networking element (for example, `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`, or `cmdb_ci_ip_address`), the parent CI is returned.
4. **Rule execution**: Rules run from lowest to highest priority until a single match is found. If multiple matches occur, only the first is used.

Special considerations

- **Excluding CI classes**: A system property enables excluding certain CI classes from matching. See Ignore CI classes for upgrade information and instructions on setting the property.
- **Parent CI return**: To avoid matching low-level networking elements, the parent CI is returned if the matched CI is a network adapter, Network Interface Cards (NICs), or IP address.

Lookup rules for specific integrations

Each integration plugin includes its own set of rules:

- Qualys: Qualys HOST ID, FQDN, NetBIOS, DNS, IP
- Rapid7: MacAddress, FQDN, HostName, IP
- Tenable.io: FQDN, NETBIOS, HOSTNAME, MacAddress, DNS
- Tenable.sc: MacAddress, FQDN, NETBIOS

> **Note:** Tenable.io lookup rules prioritize and populate the non-empty network interface values (FQDN, IPV4, and MacAddress) over the regular FQDN, IPV4, and MacAddress values for a discovered item. When these network interface values are empty, the regular FQDN, IPV4, and MacAddress values are populated for a discovered item.

Managing Lookup rules

- **Test custom rules**: Test custom or modified lookup rules to avoid performance issues.
- **Deactivate instead of delete**: Deactivate rules rather than deleting them to avoid data loss.

If rules aren't carefully constructed, importing exposure findings data can be taxing on an instance and performance issues with resources can occur. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written lookup rules or modifications to pre-defined **Lookup Rules**. See Steps to help prevent duplicate or orphaned records after running lookup rules for more information on helping prevent duplicate orphan records, deleting data, and cleaning up data.

> **Note:** For information on CI matching, see KB0998706.

Reapplying updated lookup rules

After updating rules, use **Reapply** to rerun them on unmatched or previously matched discovered items. This updates CI information in findings and detections. You can also run lookup rules on specific selected discovered items. For more information, see Reapply lookup rules on selected discovered items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unmatched CIs and unclassed hardware

- **Unmatched CIs**: CIs without a match in the CMDB are listed under Discovered Items with Class set to **Unmatched CI**.

  Note: Each discovered item includes a **Class** field. If a CI is unmatched, this field is set to **Unmatched CI**.

- **Unclassed hardware**: Assets that can't be categorized by lookup rules are referred to as unclassed hardware.

By effectively managing lookup rules, Unified Security Exposure Management can help with identifying accurate ownership and streamlining remediation.

Related topics

Configuring lookup rules

Managing unmatched configuration items (CIs)

When assets are imported, they are automatically matched against existing CIs in your Configuration Management Database (CMDB). Assets that do not find a match are listed as 'Unmatched CIs' under Discovered Items.

Locating unmatched CIs

You can view these unmatched configuration items in the **Security Operations** > **CMDB** > **Discovered Items** module. By default, this list is filtered to show only "unmatched" items. To see all discovered items from an import, simply remove this filter.

Taking action on Unmatched CIs

- **Review Lookup rules:** If you believe an unmatched CI should belong to an existing class within the CMDB, it's recommended to review your lookup rules. This can help ensure proper matching in the future. See Create lookup rule for more information.
- **Consider reclassification:** If a CI doesn't fit an existing class, you may need to reclassify it to ensure accurate CMDB data. See reclassifying the configuration item for more information.

Note: If the Identification and Reconciliation Engine (IRE) is active, the reclassify option for discovered items is not supported.

Related topics

View and reclassify unmatched configuration items

Reconcile unmatched discovered items

Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules

De-duplicating existing configuration items

Managing unclassed hardware

An asset is classified as unclassed hardware when it cannot be matched to an existing configuration item (CI) in the Configuration Management Database (CMDB) using defined lookup rules during import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

How unclassed hardware is created

Unclassed hardware is created during initial import from scanner integrations using the following process:

1. USEM automatically uses host data to search for matches in the CMDB. The lookup rules are used to identify configuration items (CIs) and add them to the finding record to aid in remediation.
2. If no match is found based on the lookup rules, the Identification and Reconciliation engine (IRE) applies its own identification rules defined on the hardware class and all its children.
3. The IRE then creates a new CI under the `cmdb_ci_unclassed_hardware` class.
4. When Discovery finds this asset, instead of reclassifying the existing unclassed hardware, it creates a CI. This is because the identification rule relies on the name of the hardware CI.

The challenge with reclassification and duplication

When Discovery subsequently finds an asset that already exists as unclassed hardware, it often creates a new, classified CI (e.g., a Windows server CI) instead of reclassifying the existing unclassed hardware CI. This happens because:

- **Name Field Discrepancy**: The identification rules heavily rely on the name field of the hardware CI.
- **Inconsistent Naming**: The name used by Unified Security Exposure Management (e.g., FQDN or NetBIOS name) might differ from the name used by Discovery (e.g., just the hostname).
- **Result**: This discrepancy prevents IRE from recognizing the unclassed hardware and the newly discovered asset as the same entity, leading to the creation of a duplicate CI under a new class rather than reclassifying the original.

Note: If the Identification and Reconciliation Engine (IRE) is activated, the option to reclassify items directly from discovered items is not supported.

The following extracts show the IRE payload for creating CI in Unclassed Hardware via Vulnerability Response and Discovery respectively.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
        "name": "asset01.company.com",//from NetBios,
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123"
    }

"settings": {
        "updateWithoutSwitch": true
    }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
        "name": "asset01",
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123",
        "os_domain": "company"
    }
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
"settings": {
        "updateWithoutSwitch": false
    }
```

In this scenario, the existing Unclassed Hardware CI is not reclassified as a Windows Server. Instead, a new CI is created under Windows Server. This is because the identification rule depends on the Hardware CI's name. As you can see from the payloads, the name received from Unified Security Exposure Management matches the FQDN/NETBIOS, whereas the Discovery payload provides only the host name.

Related topics

Reclassify unclassed hardware

Steps to help prevent duplicate or orphaned records after running lookup rules

Take steps to help prevent duplicate or orphan records resulting from matching (configuration items (CIs) within the CMDB.

If rules aren't carefully constructed, importing security exposure data can be taxing on an instance and performance issues with resources can occur. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. Thorough testing and debugging of processing scripts in the rules helps alleviate the potential of issues later in the process.

Avoid duplicate or orphaned records

- Use small subsets of data that are specific to the lookup rule being tested.
  - Set all lookup rules, other than the one being tested, to inactive.
  - Analyze the imported CIs to ensure that you're observing the expected behavior and matching is occurring properly.
- Review matched CIs
  - Examine the count of matched vs unmatched CIs. Ensure that the percentage is acceptable. Don't look at the first page that is likely the first one inserted.
  - Manually search for some CIs.
  - Check to see if there are any naming or field problems (such as searching for a specific domain).

    If it seems appropriate, add additional matching rules.
- Review Unmatched CIs
  - Navigate to the Unmatched CIs table.
  - Group by Configuration Item class.
  - Review any classes that don't look right (certificates, network cards, images).
    - Figure out why didn't they match the correct CI?
    - Should the class be excluded?
    - Should the class be elevated to a related class?
- Review CI states such as **Retired**.
- Remove Test Data

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Once you begin to observe the correct or expected behavior in CI matching, start over.
- Start over by: Deleting the data used for testing: (see the **Deleting data from tables** section)
  - Discovered Items
  - Vulnerable Items
  - Remediation tasks
- Manually rerunning all the CI Matching rules.

For more information on lookup rules and Qualys, see the KB0750656 article.

For more information on lookup rules and Rapid7, see the KB0818096.

Deleting data from tables

Sometimes you have imported data and realize something is wrong. If something is wrong in a development or performance environment, you could reclone from a better environment, but that isn't always an option.

Note: Performing these actions requires ServiceNow expertise.

There are four options for deleting data from tables:

- Using **Delete All Records** on **Table Configuration**.
- Configure the **Table Cleaner** by navigating to **Auto Flushes** (sys_auto_flush.list) and creating a **Auto-flush** record.
- Truncate the gs.truncateTable using a background script.

  Using *truncateTable* requires turning off the record for rollback check box in the background scripts. Otherwise, a copy of the table and related cascade tables are created, take too long, and most likely fail.

  Note: Never use *truncateTable* in a production environment. Consult you Support representative before executing large deletions in production or shared environments.

Categorizing findings and discovered items using classification rules

Classification groups automate the classification of entities or records based on the classification rules defined in the group. The condition for each rule is evaluated in order, and the first matching rule is used.

The Unified Security Exposure Management base system includes the following two classification groups, which classify discovered items and vulnerabilities respectively:

- Technologies Classification
- Discovered Containers Classification
- Configuration Tests Classification
- CWEs Classification
- Test Groups Classification
- Discovered Applications Classification
- Discovered Items Classification
- Vulnerability Entries Classification

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Whenever findings and discovered items are imported, the vulnerability classification rules in the respective groups are executed. Based on the conditions set in the rule, the records are classified into the relevant classification group. You can create, edit, delete, or reapply these rules to an existing vulnerability.

Note:

- For a selected table, there can only be one active classification group.
- Once you create a group, you can't delete it.

Related topics

Configuring classification rules

Prioritizing vulnerabilities and other findings using roll-up calculators

After assessing risk calculators, use the roll-up calculators to configure how the cumulative risk scores are computed for remediation tasks and other higher entities.

The base system includes the following roll-up calculators:

- **Discovered Application Rollup Calculator**: Roll up the risk scores for all application vulnerable items with the same discovered application, to provide an overall risk score for the discovered application.
- **Vulnerability Entry Rollup Calculator**: Roll up the risk scores for all vulnerable items with the same vulnerability entry, to provide an overall risk score for the vulnerability entry.
- **Discovered Item Rollup Calculator**: Roll up the risk scores for all vulnerable items and test results with the same discovered item, to provide an overall risk score for the discovered items.
- **Remediation Task Rollup Calculator**: Roll up the risk scores for all vulnerable items in a remediation task, to provide an overall risk score for the entire group of vulnerable items.
- **Configuration Test Rollup Calculator**: Roll up the risk scores for all test results with the same configuration test, to provide an overall risk score for the configuration test.
- **Discovered Image Rollup Calculator**: Roll up the risk scores for all container vulnerable items with the same discovered container image, to provide an overall risk score for the discovered container images.
- **Remediation Effort Rollup Calculator**: Roll up the risk scores for all the records in a remediation effort, to provide an overall risk score for the entire effort.
- **Container Remediation Task Calculator**: Roll up the risk scores for all container vulnerable items in a remediation task, to provide an overall risk score for the entire group of vulnerable items.
- **Application Remediation Task Calculator**: Roll up the risk scores for all application vulnerable items in a remediation task, to provide an overall risk score for the entire group of vulnerable items.
- **Test Results Remediation Task Calculator**: Roll up the risk scores for all test results in a remediation task, to provide an overall risk score for the entire group of vulnerable items.
- **Organization Risk Score Rollup**: Roll up the risk scores for all vulnerable items and configuration issues in an organization, to provide an overall risk score for the entire organization for unified dashboard.
- *`Patch Update Rollup`*: Rolls up the risk scores for all findings with same patch update, to provide an overall risk score for the patch update.
- *`Remediation Effort Rollup`*: Provides an overall risk score for records within a remediation effort.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring roll-up calculators

When configuring a roll-up calculator, you specify the weight given to each computed value in determining the cumulative risk score. The higher the weight, the more that value influences the rolled-up risk score.

Note: When **All active records** is selected, all deferred findings are included in the rollup calculation for the remediation tasks. Understand the impact on the total calculation before selecting this option.

How roll-up calculators work

Rollup calculators run a scheduled job every 15 minutes to update risk scores and other details for remediation tasks and findings. The risk score is recalculated when:

- Findings risk scores, remediation targets, or statuses change.
- Finding states change (for example, Open, Deferred, Closed).
- Findings are added or removed from a remediation task.

Example: Remediation Rollup Calculator

Vulnerability roll-up calculator example: Consider a remediation task VUL324567, which has the following vulnerable items:

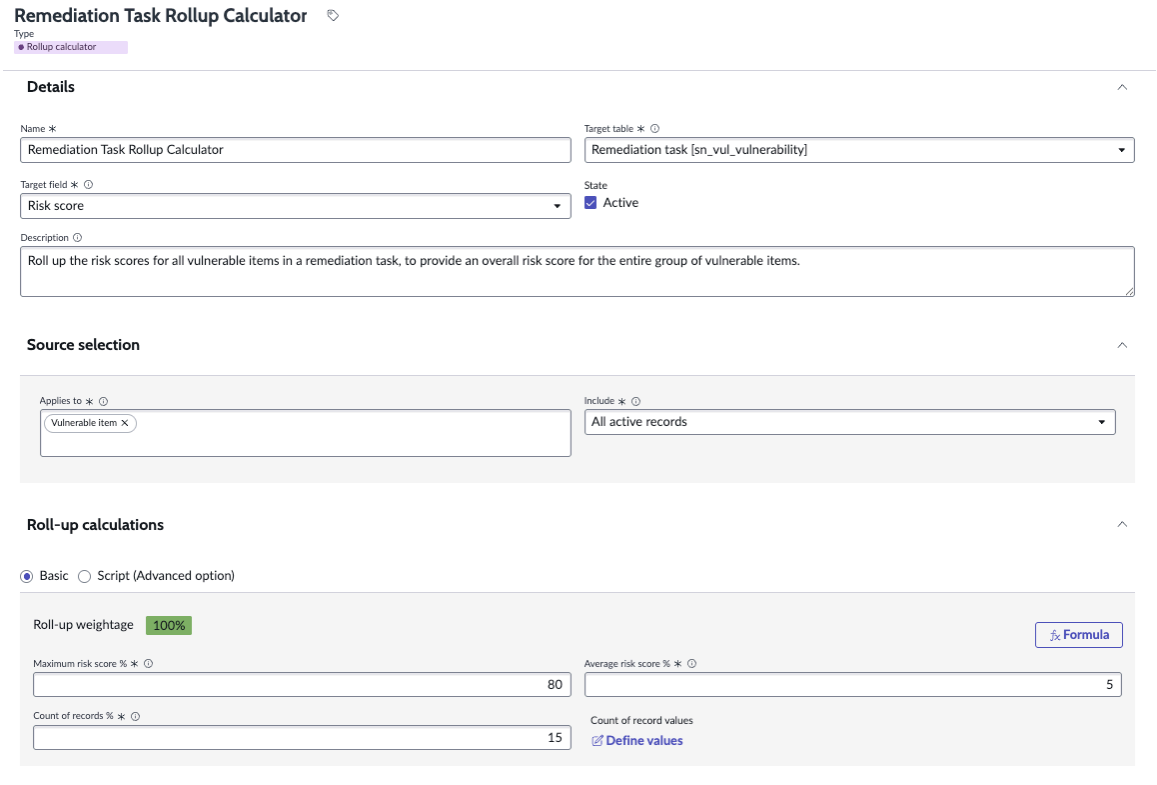
- VIT1001 with a risk score of 30
- VIT1002 with a risk score of 40
- VIT1003 with a risk score of 50

Also, consider the following weights in the vulnerability roll-up calculator:

- Maximum risk score: 80
- Average risk score: 5
- Count of vulnerable items: 15

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability rollup calculator example



In the Vulnerability rollup calculator example, the formula for determining the remediation task **Risk Score** is:

(**Maximum risk score** /100) * 80 + (**Average risk score** /100) * 5 + (factor * 15)

The factor is determined as follows:

VI count	Factor
<10	0.2
10–100	0.4
101–1000	0.6
1001–10000	0.8
> 10000	1

So, for the remediation task, VUL324567:

- The average risk score is 40
- The maximum risk score is 50
- 50 (Maximum risk score)
- The factor is 0.2

The **Risk Score** would be 45 [(50/100) * 80 + (40/100) * 5 + 0.2 * 15 = 40 + 2 + 3 = 45]

Organizational risk score roll-up calculations

The Organization Risk Score Rollup calculator calculates the overall risk score for an organization in the Unified Vulnerability Response Dashboard and Cybersecurity Executive Dashboard. It rolls

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

up the risk scores for host vulnerable items, application vulnerable items, container vulnerable items, and configuration issues.

To calculate the maximum risk score, the highest score among VIT, AVIT, test results, and CVIT is chosen. For example, if VITs have the highest score, that score is considered as the maximum risk score.

Once the counts of VIT, AVIT, CVIT, and test results are obtained, they're added and normalized using a count method. The resulting risk score is then multiplied by the count weight specified in the configuration.

The same process is followed for calculating the average risk score. The risk scores for AVIT, configuration issues, test results, and other scores are summed up, and then divided by the total count to obtain the average risk score. Finally, all the risk scores are added to derive the organization risk score.

Related topics

Configuring roll-up calculator rules

Vulnerability Response Rollup Calculators

After your initial assessment of risk calculators in the Setup Assistant, use the vulnerability rollup calculators to configure how the cumulative risk score is computed for remediation tasks and imported vulnerabilities.

Use the vulnerability rollup calculators to configure how the cumulative risk score is computed for remediation tasks and imported vulnerabilities. The following rollup calculators are shipped with the base system:

- *Remediation Task Rollup*: Rolls up the risk scores for all vulnerable items in a remediation tasks, to provide an overall risk score for the entire group of vulnerable items.
- *Patch Update Rollup*: Rolls up the risk scores for all vulnerable items with same patch update, to provide an overall risk score for the patch update.
- *Organization Risk Score Rollup*: Rolls up the risk scores for all host vulnerable items, application vulnerable items, container vulnerable items and configuration issues in an organization, to provide an overall risk score for the entire organization in unified dashboard.

  Note: Starting with v22.0 of Vulnerability Response, you can configure rollup weights for organizational score. Also, individual roll-up calculators have been removed.

- *Vulnerable Item Rollup*: Rolls up the risk scores for all host vulnerable items in an organization, to contribute to the overall risk score of the entire organization for unified dashboard.
- *Vulnerability Entry Rollup*: Rolls up the risk scores for all vulnerable items with the same vulnerability entry, to provide an overall risk score for the vulnerability entry.
- *Rollup EPSS Scores from NVD to TPEs*: Rolls up the EPSS scores for all vulnerable items/ CVEs listed on the NVD table to existing TPEs, to provide an overall probability of the vulnerability being exploited.
- *Remediation Effort Rollup*: Rolls up the risk scores for all the records in a remediation effort, to provide an overall risk score for the remediation effort.

Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Rollup Calculator**.

Configure the rollup calculator to specify how much weight to give each of those computed values in setting the cumulative risk score. The higher the weight, the more that value is used to determine the rolled up risk score in the vulnerability or remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When **Include deferred** is selected, all deferred vulnerable items are included in the rollup calculation for the remediation tasks. Be sure that you understand the impact on the total calculation before selecting this option.

Rollup calculators run the scheduled job, *Rollup vulnerable item values to vulnerability and groups*, every 15 minutes to pick up changes and roll up the details and risk scores to remediation tasks and vulnerabilities. These scheduled jobs also calculate cumulative values for the number of VIs, maximum risk score, remediation target date, and status for remediation tasks.

Note: Calculated values for vulnerability entries do not include remediation target data.

The risk score is calculated when:

- The risk score, remediation target, remediation status, or vulnerability changes on the vulnerable items.
- The vulnerable item state changes to Open, Deferred, Closed, or changes from Closed or Deferred.
- Vulnerable items are deleted.
- Vulnerable items are added or removed from the remediation task.

Vulnerability rollup calculator example: Consider a remediation task VUL324567, which has the following vulnerable items:

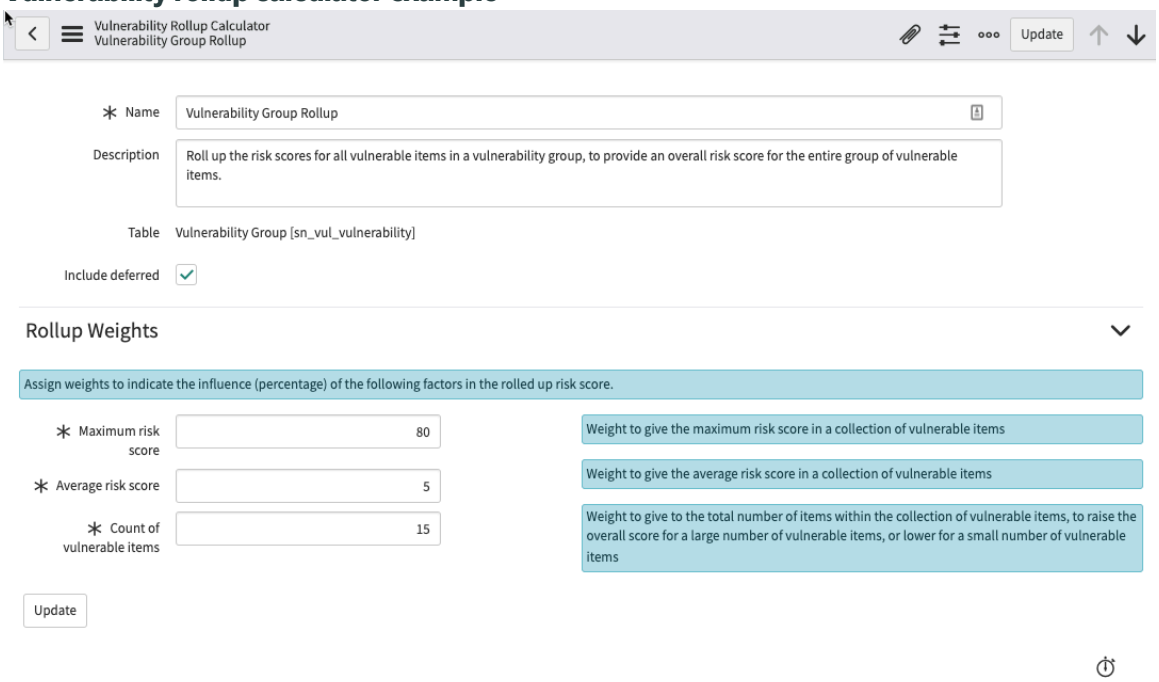
- VIT1001 with risk score of 30
- VIT1002 with risk score of 40
- VIT1003 with risk score of 50

Also, consider the following weights in the vulnerability rollup calculator:

- Maximum risk score: 80
- Average risk score: 5
- Count of vulnerable items: 15

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability rollup calculator example



In the Vulnerability rollup calculator example, the formula for determining the remediation task **Risk Score** is:

(**Maximum risk score**/100) * 80 + (**Average risk score** /100) * 5 + (factor * 15)

The factor is determined as follows:

VI count	Factor
<10	0.2
10-100	0.4
101-1000	0.6
1001-10000	0.8
> 10000	1

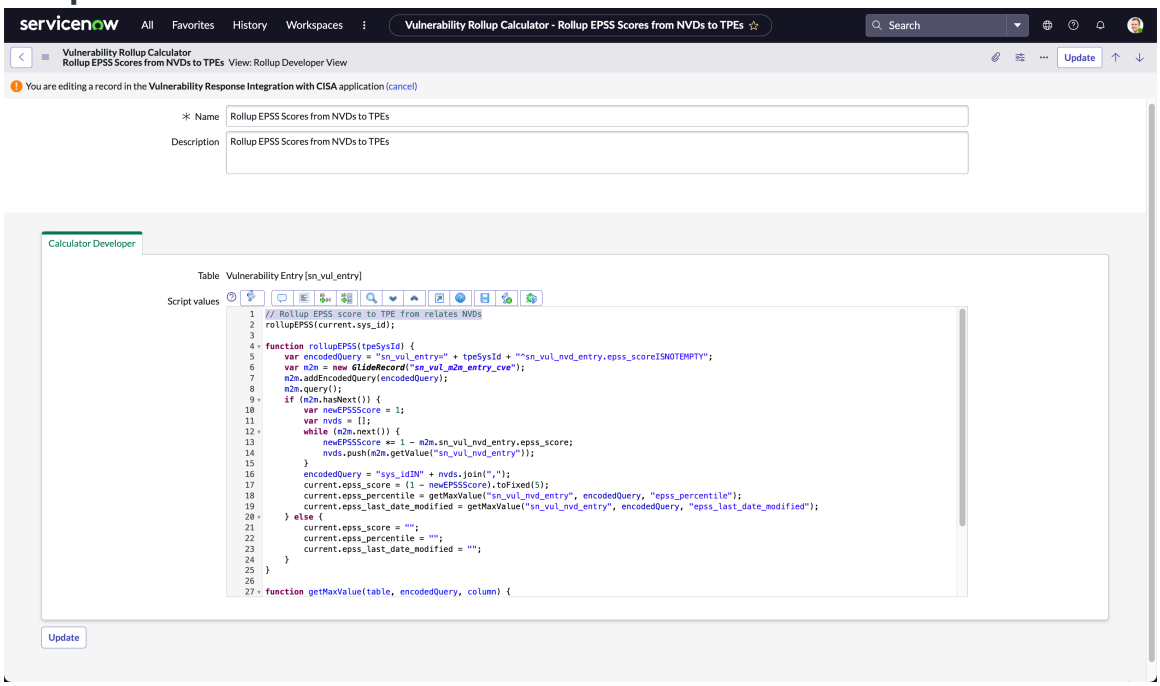
So, for the remediation task, VUL324567:

- Average risk score is 40
- Maximum risk score is 50
- 50 (Maximum risk score)
- Factor is 0.2

The **Risk Score** would be 45 [(50/100) * 80 + (40/100) * 5 + 0.2 * 15 = 40 + 2 + 3 = 45]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rollup EPSS Scores from NVDs to TPEs



EPSS Rollup calculator - Example

For example, consider an organization with 100 vulnerabilities, each with a 5% chance of being exploited. The question of great interest to a network defender might be: what is the probability that at least one of those vulnerabilities will be exploited, and therefore what is my overall threat? The probability of at least one event occurring is simply the complement (opposite) of no events occurring, that is:

```
P(at least one exploited vulnerability) = 1 - P(no
 vulnerabilities are exploited)
```

Where, the probability of no vulnerabilities is the linear product of each vulnerability not being exploited. In this example, since each vulnerability has a 5% chance of being exploited, they each have a 95% chance of not being exploited. And since there are 100 of them, we can write this as:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) =
 1 - P(one vuln not exploited)^100 = 1 - 0.95^100 = 0.994
```

Which says that the probability of at least one of the vulnerabilities being exploited is 99.4%.

Important: To modify the *Rollup EPSS Scores from NVD to TPEs*, you need to switch the Form context menu view to **Rollup Developer View** from the **Default view**.

Assigning findings to remediation teams using assignment rules

Assignment rules automatically assign findings, such as vulnerable items, application vulnerabilities, container vulnerabilities, and configuration test results, to the appropriate groups for remediation. This streamlined triage ensures that tasks are directed to the appropriate teams, and enhances consistency and visibility across security and compliance programs.

In the Security Exposure Management Workspace, you can set up a single assignment rule that applies to all types of findings, including vulnerable items (VITs), application vulnerabilities (AVITs), container vulnerabilities (CVITs), and configuration test results (CTRs). This rule can then be applied to all the findings or a specific combination of findings.

Assignment rules apply when findings are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Created (imported or manually)
- Reopened
- Modified (if rules are manually reapplied)

Assigning vulnerable items automatically

There are three different ways to assign findings using:

- User Group: Assign findings directly to a selected user group.
- User Group Field: Assign any assignment group field available using the cmdb_ci table. Assign based on the assignment group field available using the cmdb_ci table.
- Script: Use a script to define assignment conditions. This option requires coding or advanced ServiceNow® expertise. For more information on how to use the script editor to define complex conditions, see the KB0965240 KB article.

Note: The options for assigning rules using the User group and User group field gets updated based on the tables selected in the **Applies to** field.

Assignment rule evaluation process

When a new or reopened finding is processed, the system evaluates assignment rules in the following order:

1. Ascending order: Rules are processed starting with the lowest execution order.
2. First match: The system applies the first rule that matches the finding.
3. Default group: If no rule matches, the finding is assigned to a default group (if a default rule is configured).
4. Unassigned: If no default rule exists, the finding remains unassigned.

Assigned groups are then used by remediation task rules to determine task ownership and grouping.

Note:

- The default rule should have the highest execution order value to act as a fallback or catch-all.
- Manually assigned findings aren't reevaluated by assignment rules.

Execution order recommendation

You may use the following order to run the rules:

1. High priority rules: Run these rules first for items that require special handling, where the risk is critical, or where findings must be addressed for regulatory compliance.
2. General rules: Run these rules next for items that do not require special handling and where you have a clear understanding of the responsible parties.
3. Default rules: Finally, create a default rule to assign findings to a group that determines the appropriate assignment group. This group can then add additional rules based on their decisions. The default rule should run last.

In the Security Exposure Management Workspace, you can set the execution order of the assignment rules by simply dragging and dropping them to reorder on the Rules list page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Applying assignment rules

Assignment rules are applied to the findings using:

- A scheduled job: The *Run assignment rules* job runs daily to apply the assignment rules on the findings. It's inactive by default. You can configure it to run on a set schedule (daily, weekly, monthly, on demand, and so on) based on the scale of your environment. Depending on how many active findings you have in your environment, remember to set the **Run** field appropriately following the initial run to avoid performance impacts. This job applies to all open findings, excluding those that have been manually assigned.
- The Reapply button: Use the **Reapply** button to reapply updated rules to all open findings. Manually assigned findings are excluded from this process.
- A business rule: The business rule *Link to Remediation Tasks* on the Findings table evaluates all the assignment rules and applies them to the newly created or modified findings. To enable the business rule:
  1. Navigate to **System Definition** > **Business Rules**.
  2. Enable *Link to Remediation Tasks* business rule.
  3. Select the **Active** check box to activate the business rule.

Note: When enabled:

- Findings are automatically regrouped under a relevant remediation task or group. If they can't be grouped under an existing group, a new group is created.
- Manual changes don't trigger regrouping—only rule-driven updates do.
- Remediation tasks themselves aren't deleted. Only findings are removed or regrouped.

When rules are updated, reapplying them ensures that current findings reflect the new logic.

Automating regrouping after assignment group changes

You can automate the regrouping of findings when assignment groups change due to assignment rule reapplication by activating the system property *sn_vul.rerun_task_rules*.

Steps to enable:

1. Navigate to **All** > **System Properties** > **All Properties**.
2. Open *sn_vul.rerun_task_rules* system property.
3. In the **Value** field, set the value to true.

When enabled, findings are unlinked from prior remediation tasks if the rule conditions no longer match.

Assignment impact on remediation tasks

Assignment rules also influence how findings are grouped and managed in remediation tasks. Remediation task rules inherit assignment groups from findings. For example, if findings across multiple CIs are assigned to different groups, remediation tasks may be split accordingly.

If the assignment group of a remediation task is updated:

- All findings within that task, sharing original assignment group, are also updated.
- These findings are marked as manually assigned and excluded from further automatic rule evaluation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Special considerations by finding type

Finding type- assignment rule considerations

Finding type	Notes
Vulnerable items (VITs)	Base system includes an *Assign to CI Support Group* rule. Use order to prioritize critical, general, and fallback rules.
Container vulnerable Items (CVITs)	Only one matching rule applies. Rules ignore non-Open or manually assigned CVITs.
Configuration Test Results (CTRs)	Uses similar logic. Default assignment rule is inactive. Terminology changes as of v14.9 (for example, "Group Rules" → "Remediation Task Rules").

Related topics

Configuring assignment rules

Removing assignments from findings and remediation tasks

You can remove yourself or your group from the **Assigned to** and **Assignment group** fields on findings and remediation tasks if you believe they were incorrectly assigned.

Overview of the workflow

Remediation owners and vulnerability analysts can unassign records using the **Unassign** UI action. This helps route records that are outside their scope to the appropriate owners.

Use case

Use the **Unassign** option when a finding or remediation task is not relevant to your scope or was mistakenly assigned to you or your group.

Unassigning from findings and remediation tasks

You can unassign records in any state except Closed or Resolved, using the **Unassign** button or the More options menu ( ).

Supported Records:

- **Remediation tasks**: When a remediation task is unassigned, all associated findings with the same assignment group are also unassigned.

  Note: Items with a different assignment group than their remediation task are not unassigned, as they are likely manually assigned.

- **Findings**: Records unassigned manually or via UI appear under the **Unassigned** module.

Any records that you update assignments for with the UI action or manually are displayed on the Unassigned module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approval workflow and system properties

By default, unassigning a record triggers an approval workflow if the system property *sn_vul.unassign_vr.approval_required* is set to **true**. This generates an approval request that appears under **My Approvals**. If approved:

- The Assigned to and Assignment group fields are cleared.
- The Assignment type is set to Unassigned.
- The record can be optionally reassigned to a group defined in *sn_vul.default_assignment_group*.
- Notifications are sent to the new group.
- If rejected, the reason appears in the **Notes** tab.

As a vulnerability administrator, you can:

- Disable approvals by setting *sn_vul.unassign_vr.approval_required* to **false**.
- Redirect unassigned records to a specific group by setting its sys_id in *sn_vul.default_assignment_group*.
- Manage notifications using the **Unassign notification user group** if no default group is set.

The Assignment type (Manual, Rule, or Unassigned) helps identify how a record was last assigned. When unassigned, this field is set to Unassigned and is visible on both the record and list views.

Monitoring unassignments with scheduled jobs

A daily *Reassignment count for assignment rules* scheduled job tracks unassigned records to assess assignment rule effectiveness. This job counts:

- Findings reassigned to Unassigned.
- Manually unassigned records.
- System-unassigned records

These counts appear in the Assignment Rules list under the following columns:

- Manual items count
- Unassigned items count

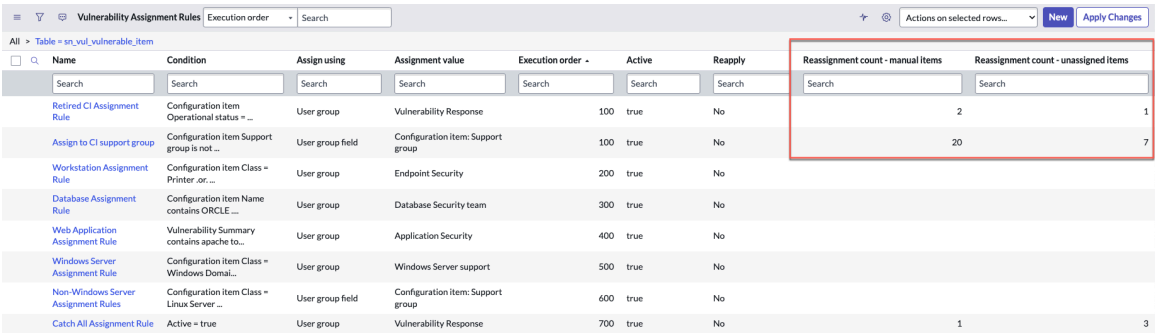
To view reassignment counts:

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Assignment rules** tile.
4. On the **Rules** page, select **Assignment** in the navigation pane.
5. Use the gear icon to add both reassignment columns to the list view.

Each reassigned record retains a reference to its original assignment rule. The list view displays reassignment counts for each assignment rule, helping you identify rules that may need adjustment.

The following example shows reassignment counts for two assignment rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply	Reassignment count - manual items	Reassignment count - unassigned items
Search	Search	Search	Search	Search	Search	Search	Search	Search
Retired CI Assignment Rule	Configuration item Operational status = ...	User group	Vulnerability Response	100	true	No	2	1
Assign to CI support group	Configuration item Support group is not ...	User group field	Configuration item: Support group	100	true	No	20	7
Workstation Assignment Rule	Configuration item Class = Printer ,or ...	User group	Endpoint Security	200	true	No		
Database Assignment Rule	Configuration item Name contains ORCLE	User group	Database Security team	300	true	No		
Web Application Assignment Rule	Vulnerability Summary contains apache to...	User group	Application Security	400	true	No		
Windows Server Assignment Rule	Configuration item Class = Windows Domai...	User group	Windows Server support	500	true	No		
Non-Windows Server Assignment Rules	Configuration item Class = Linux Server ...	User group field	Configuration item: Support group	600	true	No		
Catch All Assignment Rule	Active = true	User group	Vulnerability Response	700	true	No	1	3

Related topics

Remove assignments from findings and remediation tasks

Approve or reject an unassign request

Defining your own service level agreements (SLAs) using remediation target rules

Remediation target rules set the expected time frame for addressing findings, similar to how service level agreements (SLAs) set deadlines for fixing vulnerabilities. You can also send notifications to users and groups when target dates are approaching and when they are past due.

For instance, if an asset contains Payment Card Industry (PCI) data, such as credit card information, the vulnerability must be resolved within 30 days, as per the PCI Data Security Standard (PCI DSS). You can create remediation target rules by specifying:

- **The remediation target**: The deadline by which the vulnerability must be fixed.
- **The reminder target**: The date when reminders should start.
- **The reminder and notification recipients**: Who should be notified if the findings exceed the reminder or remediation target dates without being fixed.
- **The recalculation method**: How the system updates the remediation target (RT) date when a vulnerable item's risk rating changes.

Vulnerability analysts and managers can view the remediation target date in the findings form and list views, provided the findings are not in Deferred, Resolved, or Closed states. Remediation target rules are evaluated during import and re-evaluated if a finding is reopened.

In the findings list view, the remediation target dates are color-coded with dots:

- **Green**: Findings that haven't reached their notification date.
- **Orange**: Findings approaching the remediation target date.
- **Red**: Findings past the remediation target date.

A summary email is sent for each remediation target rule when one or more findings are either approaching their remediation target date or have passed it.

Recalculation of remediation target date

Starting with Unified Security Exposure Management version 30.1.4 and Vulnerability Response version 26.4.4, administrators can configure how the system recalculates the remediation target date when a finding's risk rating changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Under normal conditions, the system calculates the RT date as:

  Remediation Target = **Target from (date)** + **Target (days)**

- When the risk rating changes, the system calculates a new RT date using the formula below. The selected recalculation method determines whether this new date replaces the existing RT date.

  Recalculated RT date = **Field change time** + **Target (days)**

  Field change time captures when the risk rating changed. Target (days) uses SLA of new risk rating.

The following options define how the system applies the recalculated RT date when a risk rating changes:

Recalculation method	Description
Default calculation	Retains the existing RT date. The recalculated date isn't applied.
Recalculate from risk change date	Updates the Remediation Target date to: Field change time + Target (days) based on the new risk rating.
Recalculate from risk change date and always set to earliest target date	Compares the existing RT date with Field change time + Target (days) and applies the earlier date.
Recalculate from risk change date and set to earliest target date only when risk rating increases	If the risk increases: Compares the existing RT date and the recalculated RT date and applies the earliest date. If the risk decreases: Applies Field change time + Target (days) without comparison.

For configuration steps, see Recalculate a remediation target date.

Deactivating or deleting remediation target rules

- **Deactivating a rule**: When a rule is deactivated, the current remediation target dates for the findings it was applied to are cleared. If a finding meets the criteria of any active rule, that rule is applied; otherwise, the finding has no target date and its status is set to "No Target."
- **Deleting a rule**: When a rule is deleted, the remediation target date and related fields on closed, deferred, or resolved findings are preserved. For non-closed findings, these fields are cleared, and any dependent rules are reapplied.

Remediation target rule scenario

When multiple remediation target rules apply to the same findings, the most restrictive rule is used.

Remediation targets are calculated from the **Target from (date)**. The default value remains **Last opened date**.

For example, if a finding meets the conditions for two remediation target rules:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scenario: Finding last opened on 03/01/2018 at 10:00:00.

- Rule 1: Last opened on 03/07/2018; remediation target is 15 days since it was last opened; calculated remediation target date is 03/16/2018 10:00:00.
- Rule 2: Last opened on 03/10/2018; remediation target is 10 days since it was last opened; calculated remediation target date is 03/11/2018 10:00:00.

In this scenario, Rule 2 applies to the finding because it has the more restrictive date (10 days since the item was first identified, compared to 15 days).

Note: Remediation targets are calculated from the "Last Opened" date plus the specified number of days (measured in 24-hour increments).

About the Evaluate remediation targets scheduled job

Evaluate remediation targets job runs once daily at 4:00:00.

It processes all active rules, starting with those that have the earliest remediation target dates. The job evaluates findings that:

- Aren't in a Closed, Deferred, or Resolved state.
- Have no remediation target date.
- Have a remediation target date later than the date specified in the rule.

If a finding lacks a remediation target date, the job adds one. If a rule results in an earlier date than the one in the record, the job updates the existing target date. It also updates the **Remediation target** and **Remediation status** fields in the findings form.

Once the job runs, any applicable notifications are sent. The job clears the remediation fields on the finding and stops sending notifications.

Note: The *sn_sec_cmn.evaluate_targetmissed_records* property, enabled by default, helps prevent the *Remediation Target Rules* scheduled job from evaluating missed findings.

Reapplying remediation target rules

When you modify a remediation target rule, use the **Reapply** button on the Remediation target rules list page to rerun the changed rules on all active Open findings, excluding those in the Closed, Deferred, or Resolved states. Depending on the number of findings, this process may take some time.

Note:

- If the *Evaluate remediation targets* job is running, you can’t initiate a reapply process. However, if a reapply process is already running and the scheduled job is triggered, they run in parallel.
- As a vulnerability admin or analyst, you can obtain the latest remediation target date for selected findings in the Security Exposure Management Workspace. This method is more efficient than running the remediation target rules for all findings in the classic UI, which can be time-consuming. For more information, see Re-evaluate the remediation properties of the records in the Security Exposure Management Workspace.

Related topics

Configuring remediation target rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deferring findings automatically without manual intervention using exception rules

Exception rules for Security Exposure Management Workspace enable you to automate the deferral process for findings. Request an exception for the findings that can't be remediated or deferred immediately, by identifying the impacted vulnerabilities, configuration items (CIs), or VIs. Defer the matching findings based on the rule when the system identifies them by automating the finding deferral process.

Using exception rules in your organization

Use exception rules to automatically defer new and existing findings for a specific period if they match the approved rule condition. Automation minimizes the risk of missing service level agreements and makes it easier to manage multiple items, because you are eliminating manual intervention.

Deferral rules support ordering, that is, the rule with the highest priority is run first. When a high-priority rule is applied on a finding, no subsequent rules are applied on it again even if the condition matches the Finding.

The life cycle of an exception rule is as follows:

- Creating an exception rule
- Approving an exception rule request
- Activating an exception rule
- Deferring an exception rule
- Expiry of an exception rule

Creating an exception rule

You can create an exception rule to automatically defer the findings that match the defined conditions for the specified period. After you create an exception rule, submit it for approval.

Approving an exception rule request

Approving an exception rule request is a two-level process. If only the first-level approver is present, the exception rule can be assessed and approved by a single approval. However, if there's no first-level approver, an exception rule approval can't be approved. See Approve an exception rule request for more information.

Note: The Change Approval (CA) is now also created during exception rule submission. This enhancement ensures consistency across exception workflows and improves traceability.

After an exception rule request is approved, you can perform the following actions:

- Cancel
- Delete

Activating an exception rule

Starting from the "Valid from" date, the exception rule runs on all the findings that are created and also on the ones that are moved from the Closed to the Open state.

Note: If you enable the Execute on existing data option, a scheduled job runs once on the existing data on the "Valid from" date.

Deferring an exception rule

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can defer findings that match the conditions defined in this exception rule, up to the "Deferred until" date that is defined for the rule. On this date, the remediation task that you created for the exception rule is closed and all the findings in this group move back to the Open state.

Expiry of an exception rule

After the exception rule expires, it no longer runs on new or reopened findings.

Related topics

Configuring an exception rule

Grouping multiple findings as remediation tasks for easy processing using remediation task rules

Remediation tasks help vulnerability analysts and remediation teams manage findings in bulk. By configuring remediation task rules, you can automatically group findings into remediation tasks, eliminating the need for manual task creation and streamlining remediation efforts.

Remediation task rules define how findings are grouped into tasks. A default rule based on vulnerability is included in the system, but rules can also use other attributes such as:

- Vulnerability severity or summary
- Configuration item (CI) or product model
- Assignment group
- Risk score
- Technology or attack vector

You can define up to six "Group by" criteria and apply multiple conditions. Once a match is found, the system either adds the finding to an existing Open remediation task or creates a new one. These rules apply to newly created findings or the ones updated with attributes that impact task assignment: Task rules can be reapplied to update groupings as needed. Rules are evaluated after CI matching, risk calculation, and assignment.

Note: Excessive rules may impact performance. Ensure that rules are optimized to avoid duplication and inefficiency.

#

How remediation task rules work

When a new finding is created, imported, or reopened, the system evaluates it against the defined remediation task rules. For each rule where the condition matches, the system pulls the relevant data from the "Group by" selections and builds a group name. If a matching open remediation task exists, the finding is added to it. Otherwise, a new task is created. By default, remediation task rules use the assignment group set by the assignment rules on the finding. The assignment of these remediation tasks is controlled by the assignment rules. When a task rule is deleted, you have the option to delete all open tasks created by that rule.

Managing remediation task rules

Remediation rules: Use the **Reapply** button on the rule form to rerun the rule on all open remediation tasks it created. The reapplication process deletes and recreates tasks based on the updated rule.

Deleting rules: When deleting a rule, you may also delete the open tasks created by it. Tasks not in the Open state remain unaffected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Creating and managing remediation tasks

Remediation tasks can be created in the following ways:

- Automatically using remediation task rules (recommended for efficiency).
- Manually in the IT Remediation Workspace. For more information, see Create a remediation task manually in the IT Remediation Workspace.

State synchronization

- **Rolldown**: When a remediation task state changes (for example, from Open to Under Investigation, this change is pushed to all associated findings.)
- **Rollup**: When all associated findings share a common terminal state (for example, Deferred, Closed - Fixed), their state rolls up to the remediation task. Rollup jobs run at scheduled intervals (for example, every 15 minutes).

Assignment management

Assignment groups and assignees from remediation tasks are rolled down to associated findings unless those findings already have different assignments. This roll down helps standardize ownership across all related records.

Related topics

Configuring remediation task rules

Closing stale detections and findings automatically using auto-close rules

Auto-close rules automatically close stale detections and findings based on predefined criteria. These rules ensure that redundant or unwanted findings are marked as closed, helping to maintain an accurate and up-to-date record of the organization's security posture. By automating this process, the rules reduce manual effort and enable teams to focus on active and critical vulnerabilities.

Auto-close rules can be set up to close stale detections and findings based on factors such as:

- The status of the vulnerability (for example, marked as resolved or mitigated)
- The age of the finding (for example, findings older than a certain number of days)
- Specific conditions or thresholds (for example, a certain number of consecutive scans without the vulnerability being detected)

Auto-close rules are crucial for managing stale detections and findings. When a finding is matched with the filter criteria, the auto-close rule can automatically close the associated record. This helps in maintaining a clean and accurate record of the security status, ensuring that teams can focus on new and critical exposure findings. By automating this process, organizations can improve the efficiency and accuracy of their exposure management practices.

Related topics

Configuring auto-close rules

Deleting stale findings automatically using auto-delete rules

Auto-delete rules automatically remove findings from the system based on predefined criteria. These rules help manage the life-cycle of vulnerabilities by ensuring that resolved or outdated findings are removed, reducing clutter and maintaining a clean, up-to-date database. This automation streamlines the vulnerability management process and ensures that teams focus on current and relevant issues.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Over time, a significant number of closed records can accumulate in the Findings tables in your ServiceNow instance. Many of these records may have been closed for more than 365 days but haven't been removed. Using auto-delete rules can help you remove these older, closed records. Running these rules not only significantly reduces the number of records in the Findings tables but also helps maintain high performance.

By default, auto-delete rules target records that have been closed for 365 days. However, the first run might attempt to purge too many records in a single transaction, which can be problematic in larger environments. To avoid this issue, you may stagger the deletion process. For example, you could start by deleting records that are older than 450 days. Once that run is complete, you can gradually work your way down in smaller increments. For example, delete records older than 425, 400, 375 days until you have reduced the number of records older than 365 days.

Related topics

Configuring auto-delete rules

Controlling the ingestion volume with automatic exclusion

Exclusion rules provide a way to filter or exclude detections from getting converted into VITs during the ingestion process in Vulnerability Response.

These rules can be set up to handle various scenarios such as:

- Excluding vulnerabilities with low severity or risk that don't require immediate remediation.
- Improving the remediation process by prioritizing the most critical VITs for action.
- Reducing the processing time during data import by excluding a percentage of detections from VITs conversion.

During the process of ingesting data, there are distinct approaches for handling new and existing detections.

- For new detections:
  - If a new detection doesn't meet the conditions of an exclusion rule, a detection is created with the VITs.
  - If a new detection meets the conditions of an exclusion rule, the rule gets associated with the detection, but a finding isn't created. Populate the matching Exclusion Rule reference on the Detection record. The Exclusion rule column is populated with Exclusion Rule reference on the Detection record accordingly.
- For existing detections:
  - If the detection doesn't meet the conditions of any exclusion rule, it proceeds with the normal workflow.
  - If an existing detection matches the conditions of an exclusion rule, the finding associated with that detection stays in its current state but the rule gets associated with the detection. The state of the finding is governed by the value defined in the *sn_vul.close_vit_with_excluded_detections* property. By default, the value in this property is set to False. If the value is set to False, then the detections under a finding get excluded and the state of the VITs stays in its current state. However, if the value is set to True, the following scenarios may occur:
    - If every detection under a finding is excluded, the finding's status is updated to Closed Excluded.
    - If one detection is marked as Closed while the remaining are excluded, the finding is designated as Closed Fixed.
    - If the finding has open detections, then the finding remains Open.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Configuring exclusion rules

Severity mapping for Unified Security Exposure Management

Severity mapping is a critical feature that enables organizations to standardize and normalize the severity levels of findings detected across different sources. This process involves mapping the severity levels from various scanners and sources to a common severity scale used within Unified Security Exposure Management.

Severity Mapping

Note: Business rules run in the background to evaluate the priority for Qualys data and perform the corresponding mapping to the **Priority** field. Therefore, the business rule is responsible for handling the mapping of Qualys data.

Field	Description
Normalised_Severity	Calculates the severity values received from the scanner.
Source_severity	• Data from the severity_score table is mapped to the source_severity table during the execution of the **Rapid7 Vulnerability Integration- API.** • Data from the SEVERITY_LEVEL is mapped to the source_severity table during the execution of the **Qualys Knowledge Base Integration**. • Data for risk_factor table is mapped to source_severity during the execution of the **Tenable.io Plugin Integration**. • Data for riskFactor table is mapped to source_severity during the execution of the **Tenable.io Plugin Integration**. • Data from severity table is mapped to source_severity during the execution of the **Microsoft TVM Vulnerability(CVE) Integration**. .

Related topics

Configure a severity map in the Security Exposure Management Workspace

Implementing Unified Security Exposure Management

This section guides you through the entire process of implementing Unified Security Exposure Management (USEM) on your ServiceNow AI Platform instance. It provides detailed instructions on how to download the application from the ServiceNow Store, install it, and configure it to optimize your security workflows.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Installation overview

This section provides information on the initial setup of USEM, whether you're a new user or upgrading from an older version of Vulnerability Response (VR).

- Install Unified Security Exposure Management

  For new deployments starting with version 30.0 of Vulnerability Response and other related applications, follow these steps to install USEM for the first time.

- Migrate to Unified Security Exposure Management (USEM) from Vulnerability Response

  If you are upgrading from a version prior to 30.0 of Vulnerability Response and other related applications, refer to these instructions to successfully migrate to USEM.

Configuration overview

Once you install USEM, you must configure rules, email notifications, dashboards and so on to automate and streamline your exposure management.

1. Configure rules to manage findings

   Automate the prioritization and triaging of security exposure findings using configurable rules.

2. Configure email notifications in Unified Security Exposure Management

   Set up email notifications to share critical information about important updates and activities, such as the approval or rejection of false-positive requests.

3. Configure email templates in Unified Security Exposure Management

   Create and manage preconfigured email templates for consistent and efficient communication.

4. Configure Visualization library

   Customize the Findings view page by selecting the columns and widgets you want to display, and manage their activation status and conditions.

5. Configure Exception Management for Security Exposure Management

   Manage requests for exceptions and review, approve, or reject exceptions for findings or remediation tasks.

Migrate to Unified Security Exposure Management (USEM) from Vulnerability Response

Use the Migration assistant for Unified Security Exposure Management tool to migrate to the Unified Security Exposure Management (USEM) platform for a smooth and secure transition.

Before you begin

Role required: Admin

Ensure that you:

- Run the migration in a sub-production instance before attempting to use it in production.
- Install the Unified Security Exposure Management application from the store.
- Upgrade to USEM using the Migration assistant for Unified Security Exposure Management tool if you are migrating from a version below 30.0.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The Migration assistant for Unified Security Exposure Management tool provides a guided user interface and helps with preparation, conflict resolution, post-migration verification, and more. It verifies that all records and integrations are correctly updated.

The Migration assistant for Unified Security Exposure Management tool is included with the Unified Security Exposure Management application. Install the Unified Security Exposure Management application [sn_vul_usem_common] before you install v30.x of any of the other Vulnerability Response applications.

The Unified Security Exposure Management application [sn_vul_usem_common] is available in the ServiceNow® Store.

See the Migration Guidance to Unified Security Exposure Management Knowledge Base article for more details about the migration.

Procedure

1. **Accessing the**Migration assistant for Unified Security Exposure Management tool: Navigate to **All** > **Vulnerability Response** > **Administration** > **Migration assistant for Unified Security Exposure Management**.
2. **Preparation**: Review the customizations that may have to be resolved after upgrading to USEM.
3. **Migration**:
   a. Review the ordered list of applications to upgrade in the Migration assistant for Unified Security Exposure Management.
   b. Upgrade applications in the order displayed (core applications first, then integrated applications).

      Note: Follow the upgrade order strictly to avoid dependency issues.

   c. Confirm all applications display the status `Completed`.
   d. Verify all post-upgrade scheduled jobs are completed (status shows `upgrading job, running` until jobs are finished).

      Note: You can't proceed until all upgrades are complete.

4. **Optional: Resolve conflicts**: Address any upgrade conflicts found.
5. **Complete migration**:

   The post-migration step restores the turned off items and validates the results.

   a. Navigate to the post-migration page of the Migration assistant for Unified Security Exposure Management.
   b. Select **Enable all** to restore integrations and jobs.
   c. Review the summary showing the number of integrations restored, scheduled jobs re-enabled, and migration rules successfully migrated.
6. **Verify completion**:
   a. Run sample Vulnerability Response jobs or check integration connectivity to verify instance functionality.
   b. Review any unresolved upgrade conflicts.
   c. Review the list of re-enabled integrations and jobs

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Review the number of successfully migrated VR migration rules

e. Review any unresolved upgrade conflicts (if applicable)
Your instance is ready to operate with USEM. You're redirected to the lookup rule page.

Result
The migration to Unified Security Exposure Management is complete. All integrations and jobs are re-activated, migration rules are successfully migrated, and the instance is ready for use.

Installing Security Exposure Management Workspace applications

The required applications for the Security Exposure Management Workspace are available from the ServiceNow Store.

1. See Exploring the ServiceNow Store for more information about applications, integrations, and products in the ServiceNow® Store.
2. See Migration upgrade prerequisites and Migration upgrade reference information for more information about setup requirements for the USEM migration.
3. See Download and activate applications for a list of the required applications and installation steps for the Security Exposure Management Workspace.
4. See Security Exposure Management Workspace Components for roles and tables that are installed with the applications.

Migration upgrade prerequisites

Before you install the required applications for Security Exposure Management Workspace, review the following information and setup tasks.

Unified Security Exposure Management overview

Unified Security Exposure Management (USEM) introduces a unified foundation across all Vulnerability Response and Security Exposure Management applications. The new architecture consolidates data models, streamlines feature sets, and enhances performance and scalability. However, migrating to USEM is a significant upgrade that requires careful planning, validation, and change management.

Security Exposure Management supports the following applications:

- Vulnerability Response (infrastructure)
- Application Vulnerability Response
- Container Vulnerability Response
- Configuration Compliance

Prerequisites and notes for upgrade

- You cannot use Operational Technology Vulnerability Response (OT VR) in the same instance with Unified Security Exposure Management.
- You are aware of the significant data model changes and user experience updates outlined in this document.
- Perform the upgrade in a non-critical, non-production instance first and validate the migrated data and any customizations.
- Rollback is not possible once an instance is upgraded to USEM.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You must deactivate all third-party integrations and ensure that no integration runs are underway before upgrade.

  To deactivate scheduled jobs and scheduled jobs within integration-specific scopes:

  1. Navigate to the Third Party Integration [sn_sec_int_integration] table.
  2. Open an integration record.
  3. Locate the integration instances related list and open a record.
  4. Clear the Active flag and save (Update) the record.
- You must deactivate the scheduled jobs and scheduled jobs within integration-specific scopes for the Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance applications. For a list of scheduled jobs you must deactivate, see Migration upgrade reference information.

  To deactivate scheduled jobs:

  1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
  2. Open a record.
  3. Clear the Active flag and save (Update) the record.

After you have completed the deactivation of scheduled jobs and third-party integrations, upgrade plugins in sequential order to migrate to USEM. See Download and activate applications for more information.

1. Vulnerability Response (This will upgrade all the dependent plugins shown in the flow chart)
2. Configuration Compliance
3. Container Vulnerability Response
4. Upgrade each of the third-party integrations you are using, one at a time.

Install Unified Security Exposure Management

Before you run the Unified Security Exposure Management application in your ServiceNow AI Platform instance, you must get entitlement and download the application from the ServiceNow Store, install it on your ServiceNow AI Platform instance, and complete a few installation steps in Setup Assistant.

Before you begin

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

- Verify that you have the required ServiceNow roles assigned for your instance.
- The admin role is required for installation and assigning roles.

Important: Unified Security Exposure Management (USEM) is a major architectural upgrade to Vulnerability Response applications. If you are currently using Vulnerability Response and upgrading to USEM for the first time, you must use the Migration assistant for Unified Security Exposure Management to ensure a successful upgrade.

For detailed information, refer KB2556844 and Migrating from Vulnerability Response to Unified Security Exposure Management (USEM) before proceeding.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To get entitlement and download the Unified Security Exposure Management core application, navigate to the ServiceNow Store.
2. In the upper right of the page, click **Log In**.
3. In the dialog that is displayed, enter your Now Support credentials and click **Login**.
4. On the page that is displayed, if not selected, click the **ServiceNow Products** tab.
5. To view the associated applications that you are eligible for with the Unified Security Exposure Management application, on the product list page, click the **Unified Security Exposure Management** product.
   The Eligible tab lists all the applications you are eligible for if you opt-in. For more information on an application, click a link.
6. To get the Unified Security Exposure Management application, click **Opt-in**.
7. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.
   A message is displayed that indicates you have successfully opted-in for the application. With the ServiceNow Products tab selected and displayed, a green check mark replaces the plus sign to the right of the Unified Security Exposure Management application.After you have accepted the terms and conditions and managed entitlements for any of the applications on the **ServiceNow Products** tab, on the Products List page, you can click the plus sign (+) to get entitlement and opt-in for the other applications on this page with a single click.
8. Skip to step 10 to install the application on your ServiceNow AI Platform instance.
9. **Optional:** Alternatively, to manage your entitlement for the Unified Security Exposure Management application on other ServiceNow AI Platform instances, follow these steps.

   a. If the Manage Entitlement button is not displayed, click the Unified Security Exposure Management application on the Product List to display it.

   b. With the Eligible tab selected, click **Manage Entitlement**.

   c. In the Manage Entitlements for USEM dialog that is displayed, choose one.

   d. Click **OK** or **Cancel** to continue.
      You are ready to activate plugins and install the application on your ServiceNow AI Platform instance(s).

10. Log in to the ServiceNow AI Platform instance that you want to install the Unified Security Exposure Management application on.
11. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
12. From the applications listed, locate the Unified Security Exposure Management application, select a version from the choice list, and click **Install**.
    The Application installation dialog is displayed. Any dependencies that will be installed are displayed.
13. **Optional:** If you want demo data, select the Load demo data check box and click **Install**.

    Note: If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Workaround to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This installation may take some time. A message is displayed in the Install dialog after the application is successfully installed.

14. Click **Close**.
15. After installation is successfully completed, navigate to **Workspaces** > **Security Exposure Management**.
16. Select **Administration**
17. Follow the instructions on the forms in each section.

Download and activate applications

Download the required Security Exposure Management Workspace applications from the ServiceNow® Store into your ServiceNow AI Platform® and activate them to upgrade.

Before you begin

- Download core products and applications.
  - A product contains one or more applications. For example, Vulnerability Response is a product.
  - An application is a standalone piece of code that implements a collection of features.
  - A plugin is a set of customizations that extends the functionality of the ServiceNow AI Platform® and any apps already installed on your instance. Some plugins are pre-activated in your instance, while others might need to be activated manually by you or by ServiceNow® personnel.
- Some applications have dependencies that you must download and install separately.

For more information about downloading and activating applications see Download an application from the ServiceNow Store for the first time.

Note: If you're downloading applications to sub-production or development instances, it's not necessary to get entitlements.

Role required: admin for download, installation, and activation of all applications.

Procedure

1. Click the link provided to you in the email you received to access the required applications in the ServiceNow Store.
   Select the **Dependencies** link to view the dependencies for an application on the application's listing page in the ServiceNow Store.
2. After you have downloaded the applications into your ServiceNow AI Platform, navigate to **All** > **System Applications** > **All Available Applications** > **All**.
3. To activate the applications you downloaded along with any of their dependencies and plugins in the order listed in the following table, locate the cards for the applications and select **Install**.

   Any dependency applications are typically installed automatically along with an application and are displayed in the Application installation dialog. However, if you are prompted to install dependency plugins during the installation, follow the prompts provided.

   A dialog is displayed after an application is successfully activated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application name	App id and version	Description
Vulnerability Response dependencies	com.snc.vul_dep	Installs all the dependent plugins required to support the Vulnerability Response application.
Security Integration Framework	sn_sec_int	Common functionality for Security Operations integrations. Dependency for Vulnerability Response.
Security Support Common	sn_sec_cmn	Provides the necessary functionality to support Security Operations applications, includingVulnerability Response. This application supports integrations, email processing, filter groups, security tags, workflows, and so on.
Security Support Orchestration	sn_sec_cmn_orch	Dependency for the Vulnerability Response application.
Vulnerability Response Common	sn_vul_cmn	Enables core functionality used by Vulnerability Response applications.
Risk Scoring for Security Exposure Management	app-sec-calculator	Calculate and roll-up risk scores across all Security Exposure Management applications.
Administration for Security Exposure Management	app-sec-workflow	Manage configuration for all Security Exposure Management applications from a centralized admin console.
Remediation for Security Exposure Management	app-sec-rem	Group and manage findings into Remediation Tasks across all Security Exposure Management applications.
Vulnerability Response Common Workspace	sn_vul_cmn_ws	Vulnerability Response Common Workspace is a framework that supports and provides common resources for the Vulnerability Response Workspaces.
Security Exposure Management	app-vul-uasm	Manage security exposure across your organization from within a single workspace for all personas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application name	App id and version	Description
Exception Management for Unified Security Exposure Management	app-sec-exception	Align approvers and security and remediation teams to efficiently manage exceptions and false positives through configurable approval workflows.
Vulnerability Response	sn_vul	Connects the workflow and automation capabilities of the ServiceNow AI Platform with imported vulnerability scan data from leading vendors.
Configuration Compliance dependencies	com.snc.vulc_dep	Plugin that provides dependencies for the Configuration Compliance application.
Configuration Compliance	com.snc.vulc	Exposes configuration-related security vulnerabilities.
Vulnerability Response and Configuration Compliance for Containers	sn_vul_container	Imports vulnerability scan data from leading container security vendors.

Security Exposure Management Workspace Roles

Security Exposure Management Workspace Roles

List of roles installed with Security Exposure Management, defining user permissions and access for Security Exposure Management-related tasks.

Application	Role title	Description	Contains roles
Vulnerability Response Common	sn_vul_cmn.usem_admin	Configures rules, integrations, and related settings for Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance.	• sn_vul.vulnerability_admin • sn_vul.app_sec_manager • sn_vul_container.vulnerability_admin • sn_vulc.admin
Administration for Security Exposure Management	sn_sec_wf.read_admin_rules	Read access to administration rules.	• sn_sec_calculator.read • sn_vul_cmn_ws.read_admin_rules • sn_vul_cmn.read_auto_close_rules
Administration for Security Exposure Management	sn_sec_wf.manage_admin_rules	Create, read, update, and delete administration rules.	• sn_vul_cmn.manage_auto_close_rule • sn_sec_wf.read_admin_rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Role title	Description	Contains roles
			• sn_vul_cmn_ws.write_admin_rules • sn_sec_calculator.admin
Exception Management for Unified Security Exposure Management	sn_sec_exception.approver	Approve or reject exception requests, false positive requests, and exception rules.	sn_sec_exception.read
Exception Management for Unified Security Exposure Management	sn_sec_exception.read	Read access to exception management configuration and exception rules.	None.
Exception Management for Unified Security Exposure Management	sn_sec_exception.admin	Create, read, update, and delete exception management configuration and exception rules.	sn_sec_exception.read
Risk Scoring for Security Exposure Management	sn_sec_calculator.read	Read access to records in the `sn_sec_calculator` scope.	None.
Risk Scoring for Security Exposure Management	sn_sec_calculator.admin	Create, read, update, and delete records in the `sn_sec_calculator` scope.	sn_sec_calculator.read

Access control lists (ACLs) for administration rules

You can either view or modify the administration rules based on the roles assigned to you.

New roles for administration rules

The following two new roles have been introduced to manage administration rules within the Security Exposure Management Workspace:

- sn_sec_wf.read_admin_rules: Enables you to view all the administration rules.
- sn_sec_wf.manage_admin_rules: Enables you to perform all CRUD (Create, Read, Update, Delete) operations on administration rules.

Personas with read access to administration rules

The following personas can read administration rules:

- sn_vul.vulnerability_analyst
- sn_vul_container.vulnerability_analyst
- sn_vulc.auditor
- sn_vulc.vulnerability_analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Personas with create, update, and delete permissions

The following personas can create, update, and delete admin rules, provided they have access to the corresponding findings table:

Persona accessible tables

Persona	Accessible Findings table
sn_vul.app_sec_manager	Application Vulnerable Item
sn_vul. vulnerability_admin	Vulnerable Item
sn_vulc.admin	Test Result
sn_vul_container.vulnerability_admin	Container Vulnerable Item
sn_vul_cmn.usem_admin	Vulnerable Item, Application Vulnerable Item, Test Result, Container Vulnerable Item

Note: You can only modify the rules if you have create, update, and delete permissions and access to the corresponding findings table.

Additional considerations for other rule types regarding create, update, and delete access:

- **Lookup and Exclusion rules**: Access to create, update, or delete these rules is determined by the persona's permissions for the rule table itself, as they don't have an associated findings table.
- **Auto-delete rules**: Only users with the admin role can create, update, or delete these rules.
- **Classification rules**: Personas can manage these rules if they have access to the specific table defined within the classification group.
- **Rollup Calculator rules**: Personas who have access to the corresponding target table can manage these rules.

Security Exposure Management Workspace personas and granular roles

Before you can successfully remediate vulnerabilities with the Security Exposure Management Workspace plugin, you must assign personas and roles to your users and groups in Setup Assistant.

One of the first configuration steps required for the Security Exposure Management Workspace plugin is to assign roles to users and groups. Roles define what users and groups can see and do in Security Exposure Management Workspace, Performance Analytics for Vulnerability Response, and all third party integrations with Security Exposure Management Workspace.

You assign persona roles to existing users and groups in Setup Assistant. See Assign the Vulnerability Response persona roles using Setup Assistant.

Note:

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

However, for more control over what users and groups can do and see in the Security Exposure Management Workspace plugin at the task level, you may prefer using granular roles. For more information, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you have already assigned roles using Setup Assistant and you want to manage granular role assignments for all users and groups from the User Administration module, see Manage persona and granular roles for Vulnerability Response for more information.

Persona roles and granular roles starting

Key terms.

Role

Roles define what users and groups can see and do in the Security Exposure Management Workspace plugin.

Group

A set of users who share certain roles and a common purpose.

Persona role

A pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

Inherited roles

A term that describes roles that users automatically acquire when they are assigned other roles. For example, any users or groups assigned with the sn_vul.remediation_owner persona role also inherit the sn_vul.read_assigned,sn_vul.write_assigned granular roles.

Access control list (ACL)

Access control lists restrict access to data by requiring users to pass a set of requirements before they can interact with it.

Starting from Vulnerability Response v16.5, to protect reports from being exposed, set the **All report_view ACLs** as *`active=true`*. This ACL ensures that the protected data is only available to authorized users.

You assign groups and users to persona roles in Setup Assistant.

Note: In Setup Assistant, the system admin role (admin) is required for the tasks in the first section, assigning roles and installing integrations. After you assign persona roles in Setup Assistant and install integrations, you may prefer to assign a user or group with the sn_vul.vulnerability_admin role to finish any remaining tasks in Setup Assistant and to manage the Vulnerability Response application.

The following table lists Vulnerability Response persona roles installed with the application.

Persona roles for Vulnerability Response	Description
Assign sn_vul.vulnerability_admin - Vulnerability Admin to users or groups.	Users with this role have complete access to the Vulnerability Response (VR) application and its records. Users with this role configure all VR applications and rules and install third party integrations.
Assign sn_vul.vulnerability_analyst - Vulnerability Analyst to users and groups.	Users and groups with this role view and update all records for VI remediation.

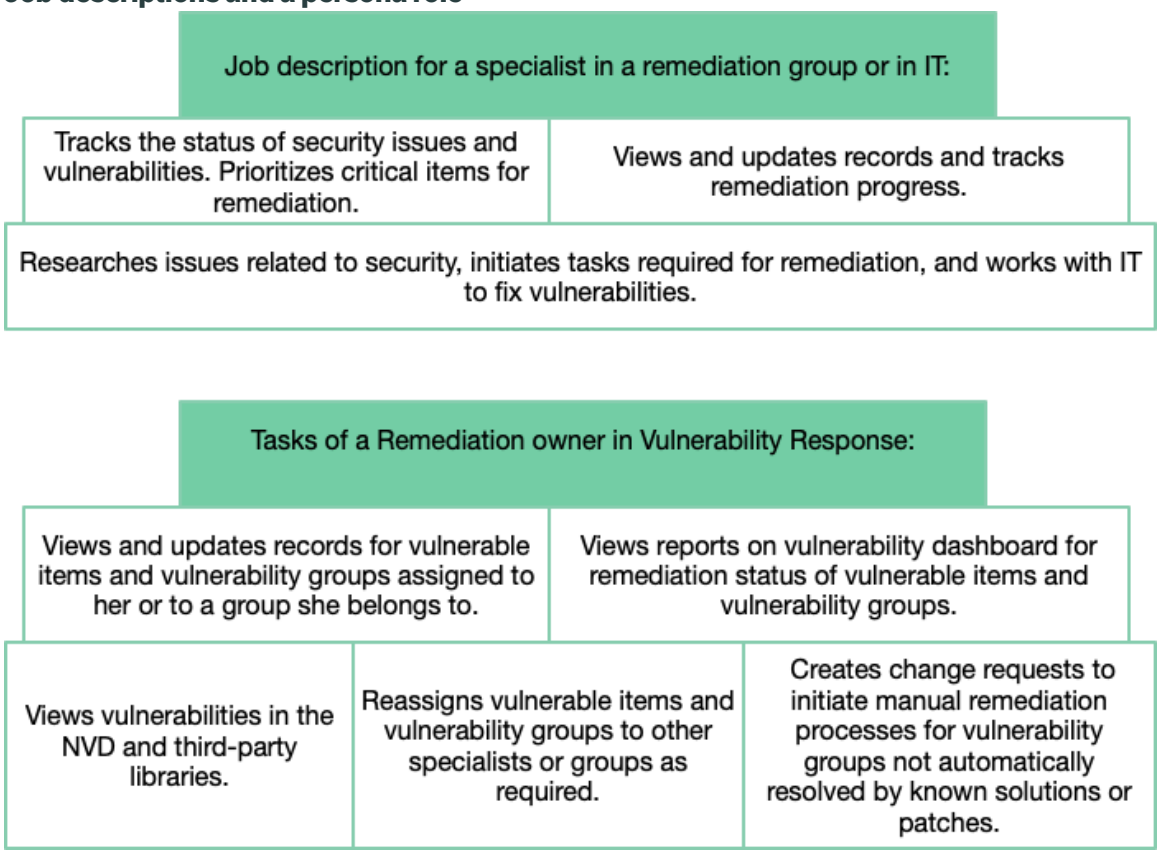
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Persona roles for Vulnerability Response	Description
Assign sn_vul.remediation_owner - Remediation Owner to users and groups.	Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to. Groups or users with this role view and update the records assigned to them or to a group they belong to.
Assign sn_vul.ci_manager to users and groups.	Users and groups with this role manage reclassification of unmatched configuration items (CIs) that are not found in the Configuration Management Database (CMDB).
Assign read access to specific areas in the application by task.	For example, assign sn_vul.read_all so a user can view all VR records. For read access to view remediation task rules, assign sn_vul.read_group_rules. Users and groups with this role do not update records.

Granular roles and persona roles

One way to think about persona roles is to consider how their descriptions may relate to job descriptions for various IT or vulnerability remediation positions in your organization. The following figure illustrates a possible job description for a remediation specialist in IT, and how the tasks associated with this job relate to the tasks of a remediation owner persona role in the Vulnerability Response application.

Job descriptions and a persona role



Both the job description and the remediation owner persona role could be defined as a series of remediation tasks. In the preceding image, a job description and a persona role in green blocks sit atop the tasks that describe them. In this example, some of the typical job requirements for a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

specialist in a remediation group correspond directly to the tasks that make up the remediation owner persona in Vulnerability Response: Review and update records, track the remediation status of vulnerabilities, prioritize items for remediation, and apply fixes and patches with IT.

Sometimes, however, the jobs in your organization may not directly correspond to the tasks that make up one of the five persona roles in the Vulnerability Response application. For various reasons, such as protecting sensitive data, or complying with regulations, you must limit the broad access some of the persona roles provide to your users and groups. Or, conversely, you are required to provide users and groups with more access so they can perform their jobs. Using granular roles, you can easily customize roles and control the access users and groups have to Vulnerability Response, Performance Analytics for Vulnerability Response, and third party integrations.

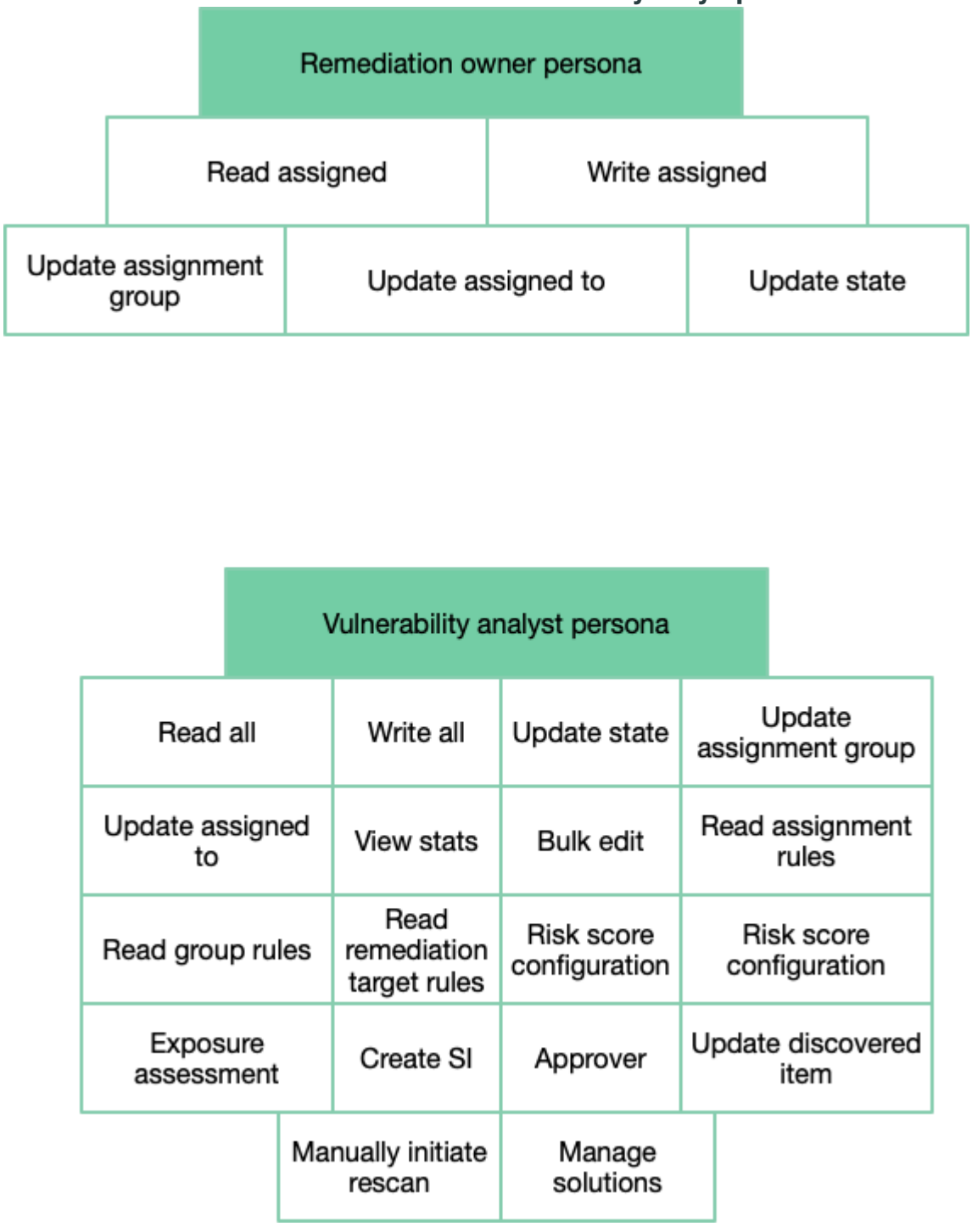
The granular roles define the tasks

The names for the granular roles in Vulnerability Response usually describe what users can do and see in the Vulnerability Response application. For example, in the previous image, users and groups with the Remediation owner persona assigned have the sn_vul.read_assigned and sn_vul.write_assigned granular roles. These granular roles permit users or groups to view and update vulnerable items and remediation task records that are assigned to them. To view descriptions of specific granular roles, as a user with the system admin role, navigate to **User Administration** > **Roles** and locate the role that you want. Roles that are automatically inherited when a role is assigned are listed. Also, when a role depends on other role assignments, any required roles are also listed.

In the following image, the granular roles of both the remediation owner persona role and the vulnerability analyst persona are illustrated. Note that the remediation owner persona does not include the read_all and write_all permissions of the vulnerability analyst persona. The granular roles, read_all and write_all, are required before users and groups can read and edit all of the vulnerable item and remediation task records. To customize these roles, simply add or remove granular roles to expand or limit access.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Granular roles and the remediation owner and vulnerability analyst personas



If you want your users and groups to have more access than the persona roles permit, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles.

Note: To assign and edit granular roles in the User Administration module, the system admin role is required.

Granular roles in the User Administration module

For an example of how to manage granular roles for a user or group, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To assign persona roles, see Assign the Vulnerability Response persona roles using Setup Assistant.

Assign the Vulnerability Response persona roles using Setup Assistant

Assign the Vulnerability Response persona roles to groups or users with Setup Assistant.

Before you begin

If you have already assigned persona roles in Vulnerability Response using Setup Assistant and you want more information about editing and managing your granular roles and role assignments in the User Administration module, see Manage persona and granular roles for Vulnerability Response.

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner roles available in previous versions of Vulnerability Response has not changed.

However, for more control over what users and groups can do and see in the Vulnerability Response application at the task level, you may prefer using persona and granular roles.

If you have not already assigned the sn_vul.vulnerability_admin persona role using Setup Assistant, follow the steps below to assign it. Once assigned, the vulnerability administrator with this persona role has permission to complete the Setup Assistant tasks after the first section, and manage rules and third-party integrations in the Vulnerability Response application.

For an overview about persona roles and granular roles, see Vulnerability Response personas and granular roles.

If you are an upgrade customer, use the following table as a reference.

Prior to v10.3	Starting with v10.3
If you assigned sn_vul.admin	You may prefer to assign sn_vul.vulnerability_admin - Vulnerability Admin to users or groups. Users with this role have complete access to the Vulnerability Response (VR) application and its records. Users with this role configure all VR applications and rules and install third-party integrations.
If you assigned sn_vulnerability_write for users and groups.	You may prefer to assign sn_vul.vulnerability_analyst - Vulnerability Analyst to users and groups. Users and groups with this role view and update all records for VI remediation.
If you assigned sn_vul.remediation_owner	You may prefer to assign sn_vul.remediation_owner - Remediation Owner to users and groups. Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to. Groups or users with this role

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prior to v10.3	Starting with v10.3
	view and update the records assigned to them or to a group they belong to.
If you assigned sn_vul.admin for management of unmatched configuration items (CI)s	You may prefer to assign sn_vul.ci- CI Manager to users and groups. Users and groups with this role manage unmatched configuration items (CIs) not found in the Configuration Management Database (CMDB). Groups or users with this role update discovered items.
If you assigned sn_vul.admin for deferrals and exception approvals.	You may prefer to assign sn_vul.exception_approver - Exception Approver to users and groups. Users and groups with this role approve exceptions, deferrals, and closures of remediation tasks and vulnerable items. Starting from v20.0, the granular role, sn_vul.read_all, has been removed for this role so that you can access the vulnerable items and remediation tasks assigned to you and your group instead of all the vulnerable items and remediation tasks.
If you assigned sn_vul.vulnerability_read to provide visibility into vulnerability management.	You may prefer to assign read access to specific areas in the application by task. For example, assign sn_vul.read_all so a user can view all VR records. For read access to view remediation task rules, assign sn_vul.read_group_rules. Users and groups with this role do not update records.

To view the granular roles a user or groups with a persona role inherits by default, navigate to **All** > **User Administration** > **Roles**. Locate the role you want, and click it to open the record. The Contains Roles tab lists all the granular roles of the persona role as well as any inherited roles.

You may prefer to verify that you have all your required users and groups created before you assign roles in Setup Assistant. Alternatively, to add new users and groups from inside Setup Assistant, click the **User Administration module** link in the form shown in the following figure.

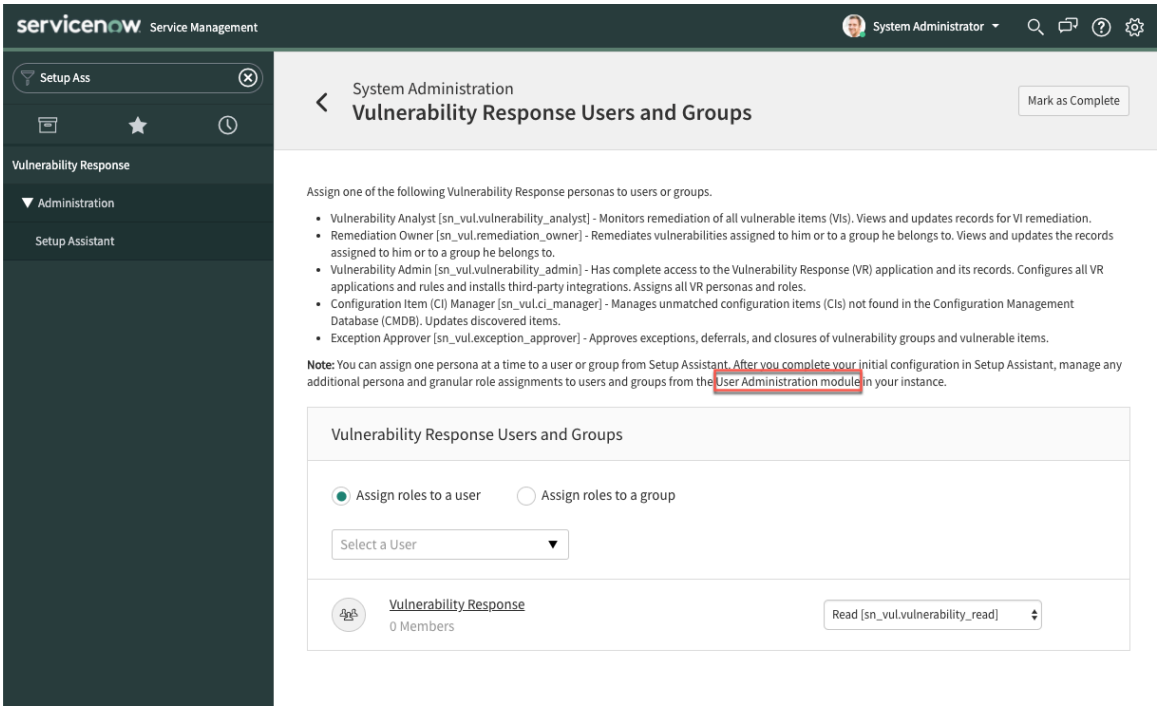
For the following example, to limit access to the Vulnerability Response application, this example shows how to assign a user with the vulnerability admin persona. Usually, you may prefer to assign persona roles other than sn_vul.vulnerability_admin to groups.

Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration Setup Assistant**.
   The Setup Assistant page is displayed.
2. Click Vulnerability Response User and Groups.
   The System Administration Vulnerability Response Users and Groups page is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. With Assign roles to a user selected, choose an existing user from the list.

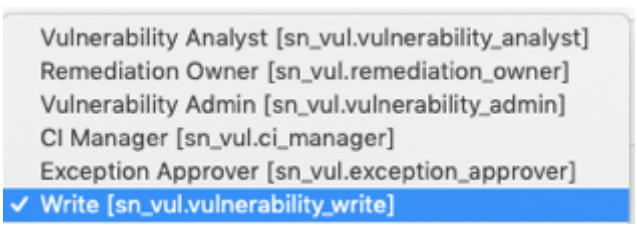
   You can only assign a user or a group with one persona role.

   On the right of the form, after you select a user or group, the default persona, Remediation owner [sn_vul.remediation_owner] is assigned by default and remains displayed in the list until you change it.

   Note: If you are upgrading to a newer version of Vulnerability Response and you previously assigned the sn_vul.vulnerability_read or sn_vul.vulnerability_write role to a user or group prior to the upgrade, it is displayed along with the new persona roles, as shown in the following figure.

   If you are an upgrade customer, you can keep using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

   Note that for existing users or a groups currently assigned with the sn_vul.vulnerability_read or sn_vul.vulnerability_write roles, these roles are displayed along with the persona roles in the list. Once you assign a persona role, the old role is no longer available going forward. For example, as shown in following figure, the Write [sn_vul.vulnerability_write] role is no longer displayed as an option for this user or group after it is assigned one of the persona roles.

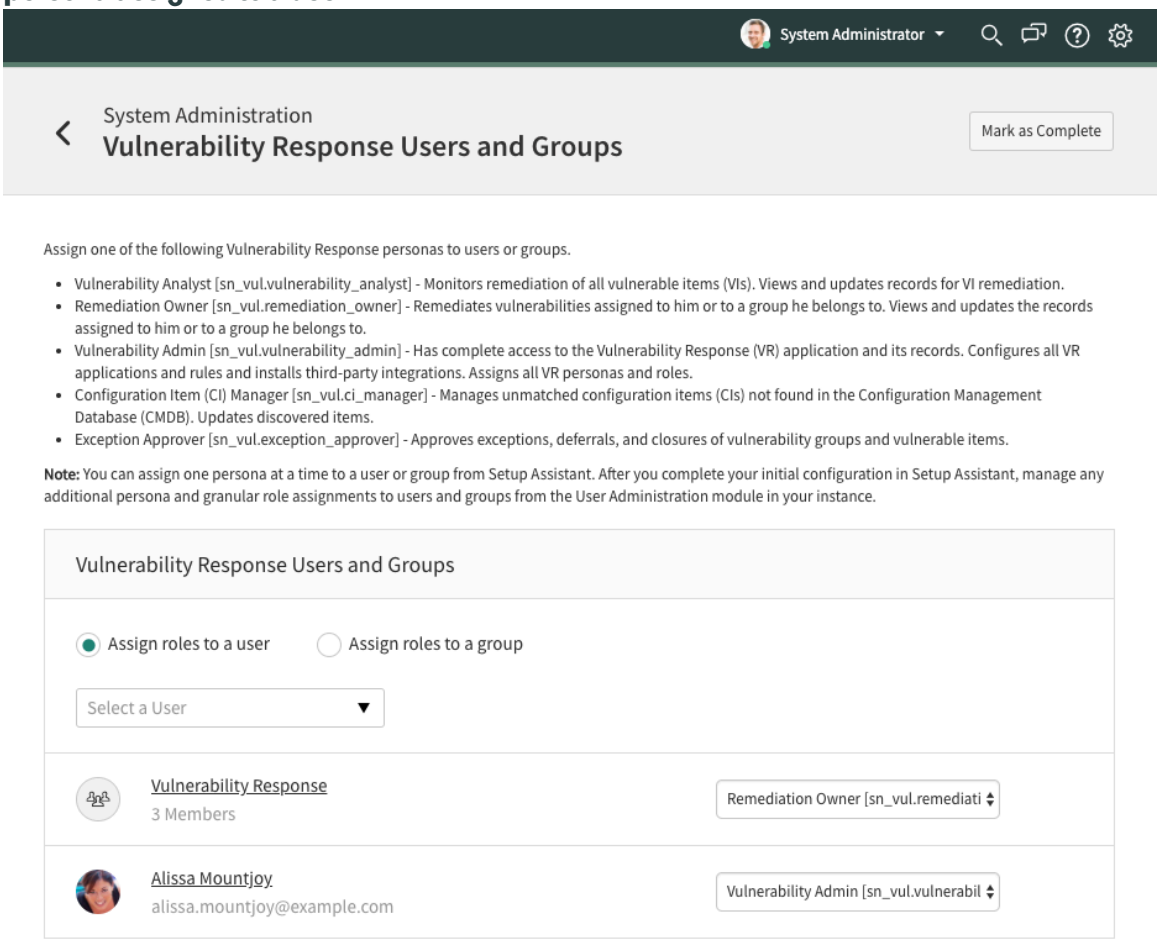


4. From the list on the right of the form, select **Vulnerability Admin [sn_vul.vulnerability_admin]**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A message is displayed that indicates the user or group is successfully assigned with the persona.

Remediation Owner persona assigned to a group, and Vulnerability admin persona assigned to a user



5. Using the descriptions of the persona roles listed above, continue to assign any users and groups to the remaining persona roles: Remediation Owner, Vulnerability Analyst, CI Manager, and Exception Approver.
   You have successfully completed assigning persona roles to users and groups using Setup Assistant.
6. **Optional:** To edit the users in a group from Setup Assistant, follow these steps.

   a. With the group displayed on the form, click the name of the group you want to edit.
   The Group record is displayed.

   b. With the Group Members tab selected, click **Edit**.
   The Edit Members form is displayed

   c. Use the slushbucket to select or remove users.

   d. Click **Save** to save your changes and return to the Group record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Click **Update** to return to Setup Assistant.

f. On the Setup Assistant page, click **Vulnerability Response Users and Groups** to continue with your configuration in Setup Assistant.

What to do next

As system admin, continue with the configuration of Vulnerability Response in Setup Assistant. Note that after the first section is completed, you can have a user you assigned with the vulnerability admin persona role complete the tasks in Setup Assistant. For more information about managing granular roles and examples, see Manage persona and granular roles for Vulnerability Response.

Manage persona and granular roles for Vulnerability Response

After you complete your initial assignment of persona roles using Setup Assistant, manage additional granular role assignments to users or groups from the User Administration module in your instance.

Before you begin

If you have not already completed your initial set up and configuration for Vulnerability Response using Setup Assistant, or assigned persona roles to users and groups, navigate to **Vulnerability Response** > **Administration** > **Setup Assistant**. See Assign the Vulnerability Response persona roles using Setup Assistant.

For key terms and an overview of persona roles, see Vulnerability Response personas and granular roles.

A persona role is pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

If you want your users and groups to have more access than one of the roles permits, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles. Also, you can build custom roles to suit your needs.

Role required: admin

Procedure

1. To manage granular roles for users and groups, choose one to continue.

Option	Description
Edit the granular roles for a user or group	Assign or remove granular roles for users or groups, or edit granular roles so that only se lect users within a group have expanded or limited permissions. An example follows the table.
Create a new role	Create a new role using one or more granular roles from the library for a specific job title, or to fulfill a specific requirement.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	An example follows the table.

The names for the granular roles in Vulnerability Response usually describe what users can do and see. To view descriptions of specific granular roles, navigate to **All** > **User Administration** > **Roles** and locate the role that you want. Role description, roles that are automatically inherited when a role is assigned, and any roles that depend on other roles are also listed.

2. To assign or remove a granular role for a user or a group, follow these steps.
   As an example, assume you want to assign an IT manager with a role that permits this manager to view records but not update or edit them. To view records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for all third party integrations, you assign this user with the sn_vul.read_all granular role.

   a. Navigate to **All** > **User Administration** > **Users**.

   b. Locate the user, and, in the Name column, click the record to open it.
   The user's record is displayed.

   c. If not selected, select the Roles tab.
   The roles currently assigned to the user are displayed.

   d. Click **Edit**.
   The Edit members form is displayed.

   e. In the Collection field of the slushbucket, enter the name of the role if you know it, or, enter `*sn_vul` to view only the granular roles available for Vulnerability Response.

   f. Locate and move sn_vul.read_all to the Roles List.

   > **Note:** Use the same process to remove specific granular roles from users in the slushbucket by moving the role from the Roles list to the Collection list.

   g. Click **Save**.
   The user record is displayed with the new granular role.

   h. Click **Update** to save your changes and return to the Users list.
   You have provided a user with permission to read but not update records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for third party integrations.

3. To edit a group so that only specific members have expanded access with more granular roles, follow these steps.
   As example, assume you want to permit certain users in the Remediation Owner (sn_vul.remediation_owner) group to create vulnerable items manually, but you don't want to expand that permission to all users in the group. The permission to create vulnerable items manually is granted by the sn_vul.create_vulnerable_items granular role. To grant this permission to only select users from this group, follow these steps.

   a. Navigate to **All** > **User Administration** > **Groups**.

   b. Locate the Remediation Owner group, and, in the Name column, click the group to open the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The group record is displayed.

c. If not selected, select the Group Members tab.
The current members of the group are displayed.

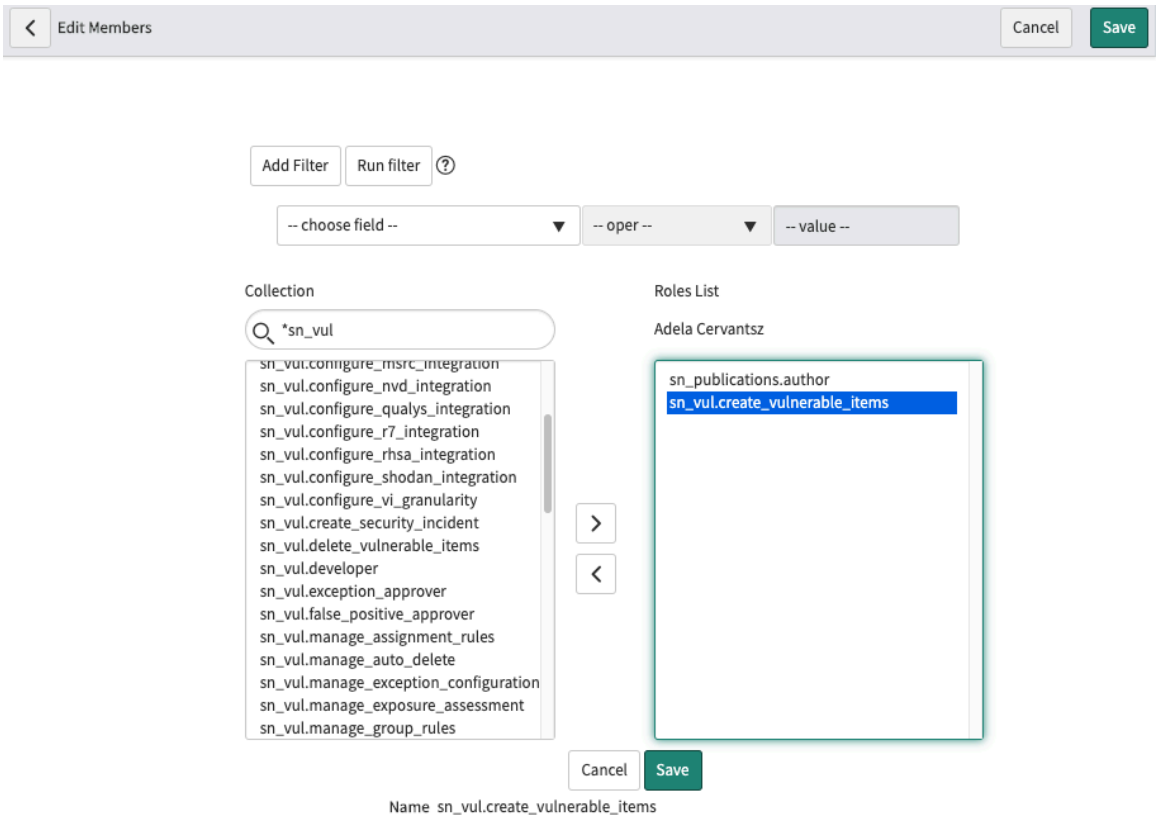
d. Click a name from the list you want to assign the granular role to and open the record.

e. On the record, scroll to the Roles tab and select it.
The roles assigned to the user are displayed.

f. Click **Edit**.
The Edit members form is displayed.

g. In the Collection field, enter the name of the role if you know it, or, enter `*sn_vul` to view all the granular roles available for Vulnerability Response.

h. Locate and move sn_vul.create_vulnerable_items to the Roles List.



i. Click **Save**.
The user record is displayed with the new granular role.

j. Click the back arrow to return to view the users in the record for the Remediation Owner group

k. Click names from the list you want to assign this granular role to, open their records, and use the slushbucket to assign the role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

l. After you complete your edits, Click **Update** to save your changes and return to the groups list.
You have provided some users in the Remediation Owner (sn_vul.remediation_owner) group permission to create vulnerable items manually.

4. To create a new role using only granular roles you select, follow these steps.
For this example, assume you want to create role for a compliance auditor. This role works closely with Governance, Risk, and Compliance (GRC), and the job requires the following permissions and tasks within Vulnerability Response:
   - Manages remediation deadlines for vulnerable items and vulnerability groups
   - Approves exception requests for extending deadlines or deferring remediation
   - Manages the clean up of older vulnerable items with auto-delete
   - Define risk scores
   - Reads all records in Vulnerability Response but is not permitted to edit them.

   a. Navigate to **All** > **User Administration** > **Roles**.

   b. In the Roles list, click **New**.

   c. In the Role record, fill out the fields.

   Create a name, select the application that contains this record, and enter a short description for your new role. For more information about the other fields on the form, see Create a role

   Note: When creating a name for your new role, you may prefer to use a name that is easily recognized in the roles list and describes the functionality of the role. For this example, you may prefer a title such as, Compliance Auditor - GRC-VR.

   d. Click **Submit**.
   The Roles list is displayed.

   e. Locate your new role and click it to open the record.

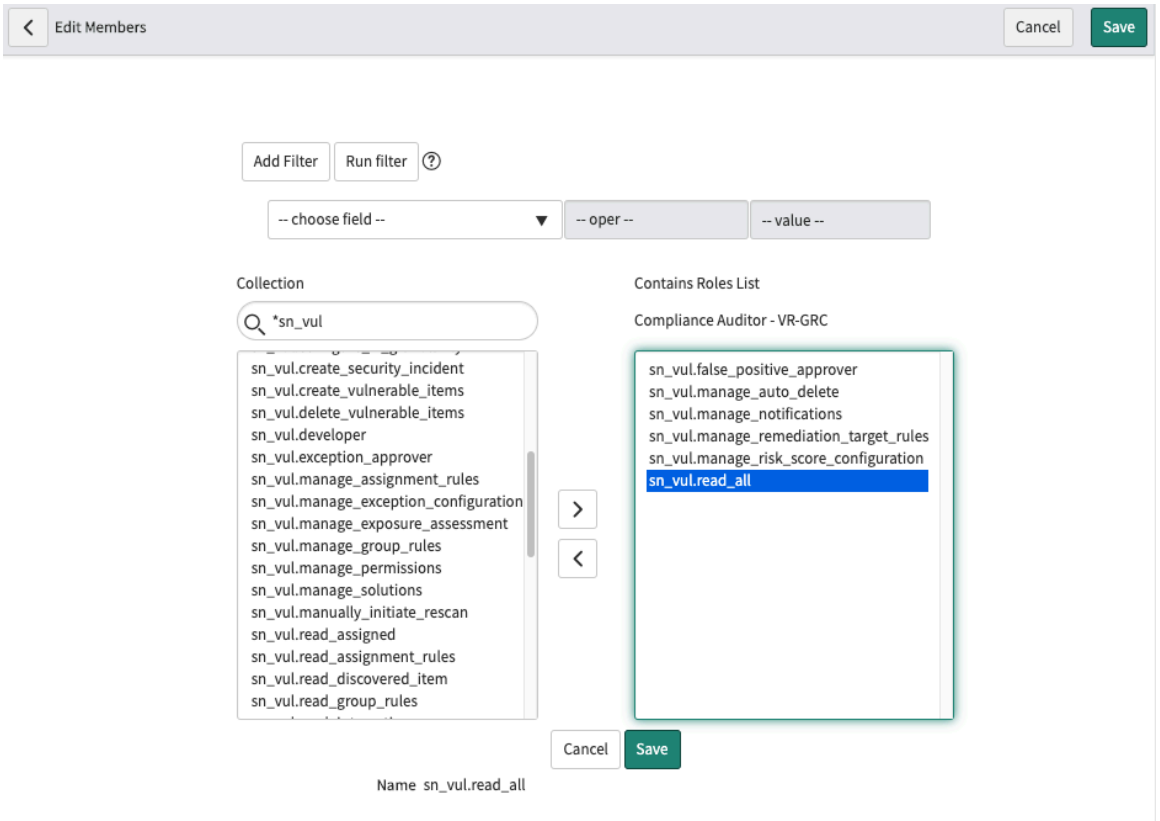
   f. Click **Edit**.
   The Edit Members form is displayed.

   g. Use the slushbucket to add granular roles to your new role.

   For this example, the required roles for this new role are displayed in the right column in the following figure.

   To display only the granular roles for Vulnerability Response, in the Collection field, enter `*sn_vul`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



h. Click **Save**.
The record for your new role is displayed. Starting with the Contains Roles tab, continue editing the role as required.

i. Click **Update** to save your changes.
Your new role is displayed on the Roles list.

Configure rules to manage findings

By configuring rules, you can automate, organize, and manage the lifecycle of findings. The rules help ensure scalability, data consistency, and faster response times by reducing manual intervention across large volumes of vulnerability data.

Configuring lookup rules

By configuring lookup rules, you can map security exposure data to the correct configuration items (CIs) in the CMDB. This mapping is a critical function because associating exposure findings with the right assets is essential for proper risk assessment, assignment, and remediation workflows.

Related topics

Associating finding with a configuration item using lookup rules

Create lookup rule

Create lookup rules to automatically and accurately associate incoming exposure findings data with the correct configuration items (CIs) in the Configuration Management Database (CMDB) This is essential for enabling the rest of the vulnerability management process to function correctly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Creating lookup rules requires advanced ServiceNow and Unified Security Exposure Management (USEM) expertise. Rather than modifying one of the existing lookup rules, consider copying it and modifying the copy. When you are satisfied that the new rule does what you want, deactivate the original.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Procedure
1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Look-up rules** tile.
4. On the Rules page, select **Look-up** in the navigation pane.
5. Select **New**.
6. On the form, fill in the fields.

Look-up rule form

Field	Description
Details	
Name	Name of the rule.
Lookup method	Method used for matching. Choices are: ○ **Script**: Pre-built (IP address, DNS name, and so on) or custom script. ○ **Field matching**: Search on table or field in the CMDB.
Type	Type used with the Script **Lookup method**.
Order	Order of precedence for the rule. Rules with the lowest order are evaluated first.
Active	Check box for whether the rule is active or disabled.
Source	Source used as input to this rule.
Source field	Source field used as input to this rule. Select any field, but it is treated as a string value.
Description	Description of the new look-up rule.
Lookup target	Lookup approach you want to follow. Select from: ○ Configuration item ○ Product model
If condition is met	
Condition	Condition based on which the lookup rule is applied. This condition depends on the attribute from the third-party scanner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

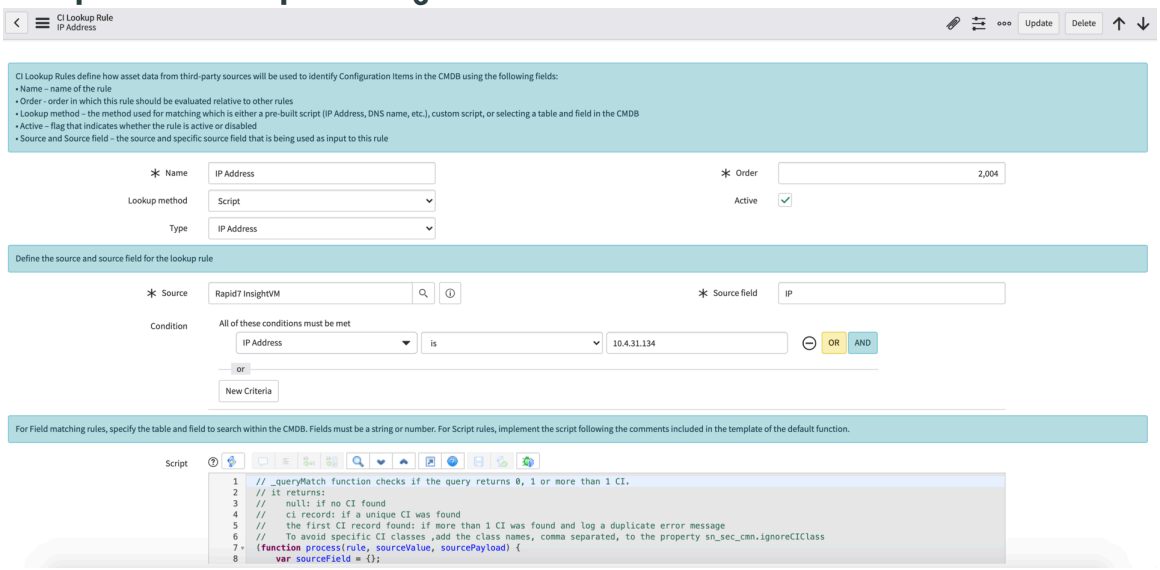
Field	Description
	Note: The asset attribute is a part of the payload. It is received from the third-party scanner. See the Discovered Items table for payload examples.
Then set this value	
Lookup method	Method used for matching. Choices are: ○ Script: Pre-built (IP address, DNS name, and so on) or custom script. ○ Field matching: Search on table or field in the CMDB.
Search on CI table	Table to search within the CMDB. Used with field matching **Lookup Method**.
Search on product table	If you choose the Product model Lookup target, the default value is Application Model.
Search on CI field	Field that contains information that can be used to locate a CI. Used with the field matching **Lookup method**. This field may be on the CI record, or on a related record, such as a network adapter.
Search on product model field	If you choose the Product model Lookup target, the default value is Name.
Type	Type used with the Script Lookup method.
Script	Editable sample script, based on the **Type**, is shown. Implement the custom script following the comments included in the template of the default function. **Note:** The process function has three parameters: *`rule`*, *`sourceValue`*, and *`sourcePayload`*

7. Select **Save**.

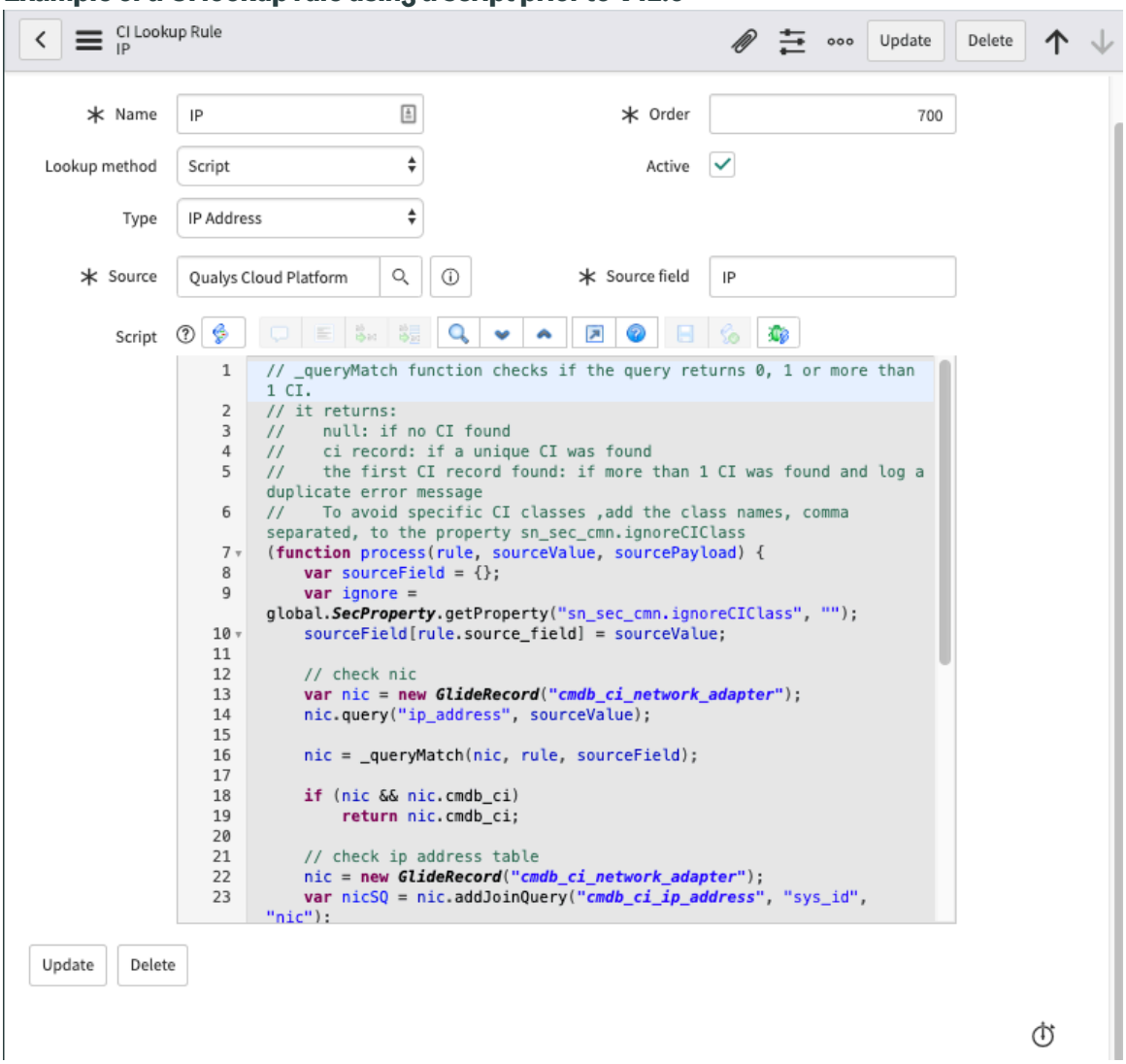
For more implementation information for lookup rules see, Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example of a CI lookup rule using a condition builder for V12.0



Example of a CI lookup rule using a script prior to V12.0



Related topics

Vulnerability Response vulnerable item form fields

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ignore CI classes

To ignore some configuration item (CI) classes, for example Load Balancer [cmdb_ci_lb], when running CI Lookup Rules, set the **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*] system property.

Before you begin

Role required: admin

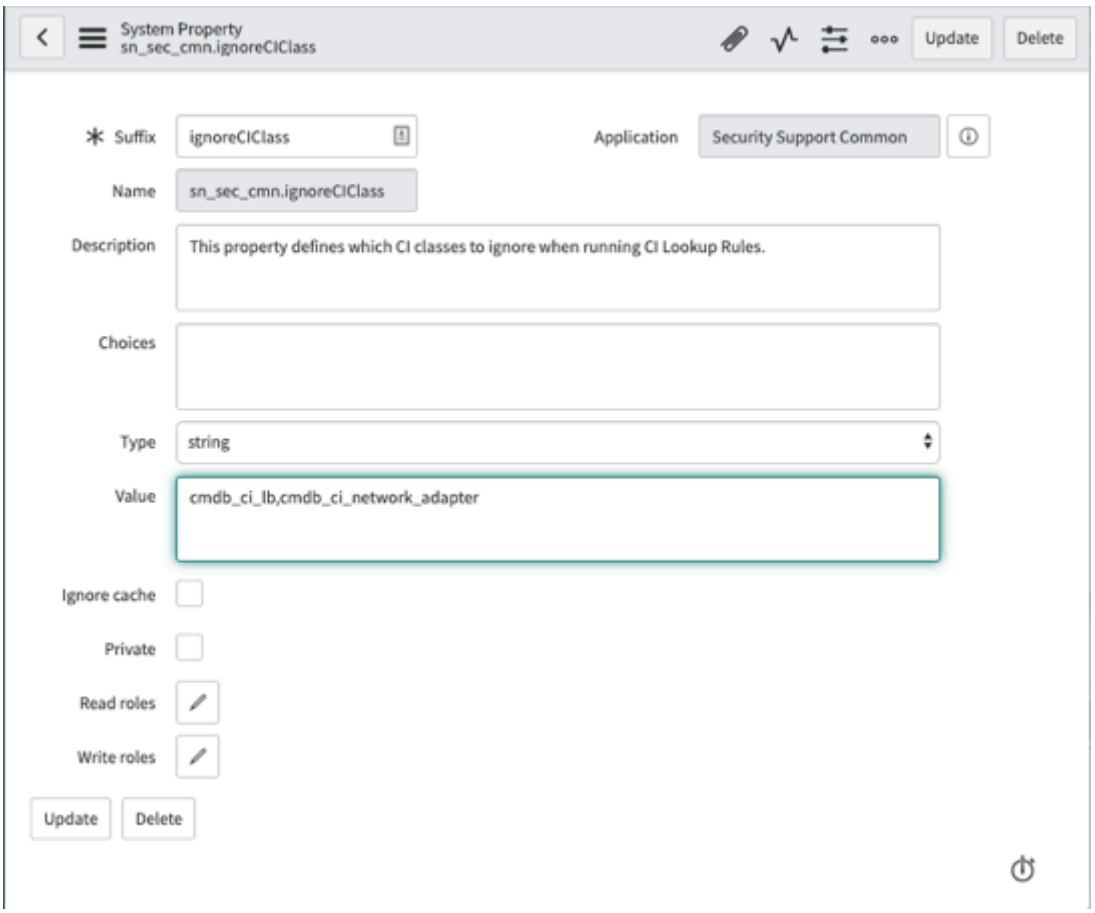
Note:

The **ignoreCIClass** system property is available starting with Vulnerability Response v9.0. However, the property functionality is not available upon upgrade from any previous version.

If you have upgraded from any Security Operations application, prior to version 9.0, see KB0788209 for instructions on how to enable this functionality.

Procedure

1. Enter `sys_properties.list` in the left navigation bar.
2. Click **Enter**.
3. In the **Search** menu, under **Name** enter `sn_sec_cmn.ignoreCIClass`.
4. In the **Value** text box, enter the CI classes to exclude in a comma-separated list.



5. Click **Update**.
   This list is used by CI Lookup Rules during the next import. Vulnerable items created during import are not associated to a CI of any type listed in the **Value** field of the `sn_sec_cmn.ignoreCIClass` system property.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reapply lookup rules on selected discovered items

Reapply the lookup rules on selected discovered items from the discovered item list view select actions. If the configuration item (CI) changes after you reapply the rules, the discovered items are updated with the new CI and impacted detections. Vulnerable items are also updated.

Before you begin

Roles required: admin

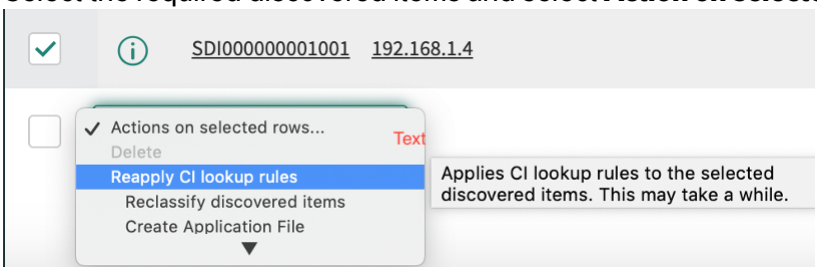
About this task

For more information, see CI changes for discovered items.

For more information on the concepts of CI matching and the CMDB, discovered item lookup, rule-based identification, see the CI matching in Vulnerability Response [KB0998706] article in the HI Knowledge Base.

Procedure

1. Navigate to **All** > **Security operations** > **CMDB** > **Discovered Items**.
2. Select the required discovered items and select **Action on selected rows**.



3. From the list, select **Reapply CI lookup rules**.

   Note: You can skip the reapplication of lookup rules on discovered items with the substate 'CI Decommissioned' by enabling the system property *sn_sec_cmn.skipItemsWithCIDecommissioned*.

   The rules are reapplied on these discovered items.

4. Select **View status** in the message.

   The status displays on the background job form.

   Note: In the **Notes** field, the `Discovered items could not be process due to exception` attribute with a non-zero value indicates that there's an error or exception while reapplying a look-up rule. Check the system logs for more details.

5. Reapply only applies to items scanned within the last 90 days based on the **last_scan_date, last_comp_scan_date, non_infra_last_scan_date, non_infra_last_comp_scan_date** column.

   Added ci_lifecycle_status_source (scope = sn_sec_cmn) system property for configuring CI lifecycle status columns (for example, Install Status, Operational Status). You can configure additional columns for retiring CIs.

   Columns are added to the background job list view:

   - Elapsed Time(ms): The time required for processing the background job.
   - Items Processed: The number of items processed until now.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Total Items to be Processed: The total number of items remaining to be processed.
- Time Until Completion(ms): The time remaining until the background job is processed. These columns provide visibility into job progress. These columns are available for each form view for you to add according to requirement.

Configuring classification rules

By configuring classification rules, you can ensure consistent categorization and processing of vulnerabilities, discovered items and other finding related entities based on key attributes. This helps the system route findings to the correct tables, apply the appropriate grouping, assignment, and remediation rules, enhance reporting accuracy, and determine which business logic to use (such as prioritization and remediation targets).

Configuration of classification rules includes the following steps.

Related topics

Categorizing findings and discovered items using classification rules

Create and edit a classification group

Create groups so that the underlying rules of this group can classify the entities or records in a specified table based on the conditions. The rules can be used to select any field in the corresponding table.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Review** on the **Classification rules** tile.
3. On the Rules page, select **Classification** in the navigation pane.
4. Select **New**.
5. On the form, fill in the fields.

New classification group form

Field	Description
Details	
Name	Name of the new classification group.
Table	Table based on which the rules are executed. **Note:** The base system includes classification groups for discovered items and vulnerability entries.
Active	Option to activate the group.
Description	Description of the new classification group.

6. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create or edit classification rules

Create rules to classify entities or records in the specified table into choice of classifications for use in downstream process or rules. .

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Classification rules** tile.
4. On the Rules page, select **Classification** in the navigation pane.
5. Select a classification group.
6. Select **New rule** and fill in the fields on the form:

Classification rule form

Field	Description
Details	
Name	Name of the new classification rule.
Active	Option to activate the rule.
Classification group	Classification group for which the rule is being created. This field is auto-populated.
Description	Description of the new classification rule.
If this condition is met	
Condition type	Type of condition for the rule. Choices are as follows: ○ **Filter**: Basic filter conditions for determining whether to use the rule or not. ○ **Filter group**: Set of multiple conditions that are used together. The rule is evaluated based on the conditions defined in the filter group. ○ **Script**: Scripted condition used to determine when to apply this rule. This field appears only when the **Advanced view** option is selected.
Condition	Condition for the rule. Define conditions based on the column selected on the required vulnerability entry column. You can add multiple conditions to refine the rule. This field appears only when **Filter** is selected from the **Condition type** field. **Note:** When defining multiple conditions or templates, you can select only from a parent and a child table. You can't select from two or more child tables.
Filter group	Group of filters. The group is defined when a set of conditions is used repeatedly in multiple places. Select the lookup using the list icon ( ) to select the filter group. For more information, see Create and define filter groups in Security Operations. This field appears only when **Filter group** is selected from the **Condition type** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Script	Script that is evaluated to determine when to apply this rule. You can write your code and set the response as either true or false. This field appears only when **Script** is selected from the **Condition type** field
Set these values	
Classification	Classification of the rule. The list includes the following options: ○ Platform ○ Application ○ Service ○ Business Application Alternatively, you can enter your own classification that is not in the list.
Classification type	Type of classification. This field shows the filtered list of classification types based on your selected value for the **Classification** field.
Value type	Type of the value that is assigned by using this rule. Choices are as follows: ○ **Template**: Select a template. You can use a required template. ○ **Script**: Select a pre-existing script, or write your own custom script. This field appears only when the **Advanced view** option is selected.
Field	Option to select another field for the rule apart from the **Classification** and **Classification type** fields. Select a combination of fields and values that you want to set when the rule is evaluated.
Script value	Script to set values on the current record. This field defines what values to set on the fields in vulnerability entries. This field appears only when **Script** is selected from the **Value type** field.

7. Select **Save**.

Reapply a classification rule to existing records in the table

Rerun all active rules on all the findings when you modify a classification rule. You can also update existing vulnerabilities by applying the new classification rules.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Classification rules** tile.
4. On the Rules page, select **Classification** in the navigation.
5. Select the classification group or rule you want to reapply.
6. Select **Reapply**.

Deactivate or delete a classification rule

Deactivate or delete a classification rule if it is no longer needed or relevant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: See Access control lists (ACLs) for administration rules

About this task
When a classification rule is deactivated or deleted, the data that was populated in the **Classification** and **Classification_type** fields by that deleted rule remains in their respective tables.

If you want to clear this data, create a rule with empty values in the **Classification** and **Classification_type** fields and reapply the group. Once this new rule is reapplied, the changes are reflected on all the records that this rule is applicable for, based on the conditions of the rule.

If a classification rule is deleted or deactivated, it's no longer applied to the specified table and the data in the **Classification** and **Classification_type** fields get cleared.

Procedure
1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Classification rules** tile.
4. On the Rules page, select **Classification** in the navigation.
5. Select the rule that you want to delete.
6. In the classification rules form, select the ellipses next to the **Update** button.
7. Select **Delete**.

> **Note:** If you don't click this button, the rule continues to reside in the system. Findings referenced by the rule continue to reference them.

Configuring roll-up calculator rules

Configure roll-up calculator rules to compute the cumulative risk score for remediation tasks and imported vulnerabilities.

Related topics
Prioritizing vulnerabilities and other findings using roll-up calculators

Create or edit roll-up calculator rules

Create rules to roll-up risk scores on imported findings and remediation tasks.

Before you begin
Role required: See Access control lists (ACLs) for administration rules

Procedure
1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Roll-up calculator rules** tile.
4. On the Rules page, select **Roll-up calculator** in the navigation pane.
5. Select **New** and fill in the fields on the form:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roll-up calculator rule form

Field	Description
Details	
Name	Name of the rule.
Target table	Name of the table from which the risk score must be rolled-up.
Target field	Name of the field from the table that must be considered for risk roll-up.
Active	Indicates whether the rule is active.
Description	Description of the rule.
Source selection	
Applies to	The finding table to which the risk score roll-up applies to. The **Applies to** field is dependent on the selected target table, and its options are updated accordingly. For instance, choosing the Container remediation task [sn_vul_container_vulnerability] limits the **Applies to** field options to Container vulnerable item. This dynamic update ensures that only relevant options are available based on the target table selected.
Include	Defines the conditions for roll-up on the finding table.
Roll-up calculations	
Basic	Assign weightage to specify the relative impact of each of the following factors on the rolled-up risk score: ○ **Maximum risk score**: Maximum risk score of the findings considered. ○ **Average score**: Aggregate of the risk scores of all the findings. ○ **Count of records**: Number of findings. A larger number of findings increases the overall score, while a smaller number lowers it.
Script (Advanced option)	The scripting feature is an advanced feature to build a custom script that should return the risk score, which is an integer value ranging from 0 to 100.

6. Select **Save**.

Configuring assignment rules

By configuring assignment rules, you can automate the process of routing findings to the appropriate teams or individuals. By defining assignment criteria based on vulnerability attributes or affected assets, you can ensure timely and accurate ownership for remediation efforts.

Assignment rules help streamline vulnerability management by automatically assigning ownership to the correct team, reducing manual triage and accelerating response times.

In the Security Exposure Management Workspace, you can set up a single assignment rule that applies to all types of findings, including vulnerable items (VITs), application vulnerabilities (AVITs), container vulnerabilities (CVITs), and configuration test results (CTRs). This rule can then be applied to all the findings or a specific combination of findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration of assignment rules includes the following steps.

Related topics

Assigning findings to remediation teams using assignment rules

Create or edit assignment rules

Create rules to assign findings automatically based on specific filter conditions. These rules apply to items as they're imported or manually created.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

About this task

The base system includes one default vulnerability assignment rule, *`Assign to CI support group`*, which assigns findings to the same assignment group as the CI support group. You can modify this rule using filter conditions or create a rule. With assignment rules, you define the conditions for assignment and the order in which they're executed. Once a finding matches a rule condition, the assignment process stops.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Assignment rules** tile.
4. On the Rules page, select **Assignment** in the navigation pane.
5. Select **New** and fill in the fields on the form:

Assignment Rule form

Field	Description
Details	
Name	Name of the assignment rule.
Applies to	Finding types the assignment rule applies to.
Active	Indicates whether the assignment rule is active.
Description	Description of the assignment rule.
If this condition is met	
Condition fields	Conditions that must be met.
New condition set	Adds more condition filter fields to choose from.
Then set this value	
Assign using	To automate the assignment of groups created based on this rule, choose one of the options available. ○ User group: Select a user group from the lookup table. ○ User group field: Select a user group field from the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Script: Create or edit a script. **Note:** Creating or editing a script requires ServiceNow expertise.

6. Select **Save**.
   New or updated rules are evaluated on the next import.
7. To edit the rule, select the rule and update the details as required.

Reapply assignment rules

Reapply assignment rules to rerun assignment logic on existing findings or groups after they've already been created.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

About this task

Reapplying assignment rules is useful when:

- Assignment rules are updated or newly created.
- Findings were previously unassigned or incorrectly assigned.
- You must reassign ownership based on updated business logic or CI ownership changes.

Note: You can reapply assignment rules for deferred items and manually assigned items basis system properties:**(sn_sec_wf.enable_deferred_item_reassignment**, **sn_sec_wf.enable_manually_assigned_item_reassignment**, that are set to false by default. Now, reassign items through the Re-evaluate action in the list view.

Normally, assignment rules are applied only once, when a finding is first created. If rules are changed or added later, existing findings don't automatically update their assignment. Reapplying the rules enables you to bring all vulnerability findings into alignment with current rule logic. To reapply all vulnerability assignment rules, activate the *`Reapply all vulnerability assignment rules`* scheduled job. Set the **Run** field appropriately to prevent performance impacts, especially after the initial run.

Note: To reapply rules to a specific subset of findings, use the 'Evaluate rules' feature. This approach ensures efficient rule re-evaluation for targeted findings.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Assignment rules** tile.
4. On the Rules page, select **Assignment** in the navigation.
5. In the **Filter by** list, select the finding type for which you want to reapply the rules.

   Note: To reapply the rule to all the finding types, select **All**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Reapply**.

Note:

- Use the **Reapply** button on the Assignment Rules form if you haven't run the scheduled job.
- Reapplication overwrites existing assignment values based on the first matching rule.
- Reapplication does not regroup the findings.
- Test the rule logic thoroughly before applying it in bulk.

Delete assignment rules

Delete assignment rules after careful consideration of potential impacts on the assignment logic and operational workflows.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

About this task

When you delete an assignment rule:

- It's removed from the rule table.
- It doesn't affect already-assigned records. Deletion helps prevent the rule from applying to new or updated records going forward.
- Rules are evaluated in order. If a rule is deleted, the system evaluates the next matching rule.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Assignment rules** tile.
4. On the Rules page, select **Assignment** in the navigation.
5. Select the rule that you want to delete.
6. In the assignment rules form, select the ellipses next to the **Update** button.
7. Select **Delete**.

Remove assignments from findings and remediation tasks

Clear the **Assigned to** and **Assignment group** fields on vulnerable item records in the Vulnerability Response, Application Vulnerability Response, and Container Vulnerability Response applications.

Before you begin

Roles required:

- sn_vul.remediation_owner or sn_vul.vulnerability_analyst for vulnerable items (VITs) and remediation tasks (VULs).
- sn_vul.app_sec_manager for Application Vulnerability Response vulnerable items (AVITs) and remediation tasks (AVULs).
- sn_vul_container.remediation_owner or sn_vul_container.vulnerability_analyst for container vulnerable items (CVITs) and remediation tasks (CVULs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The **Unassign** UI action is supported in both the classic environment and the workspaces for the following records in any state other than Closed or Resolved:

- Remediation tasks (VULs, AVULs, and CVULs). If a remediation task is updated with this feature, the **Assigned to** and **Assignment group** fields on all of its associated VITs that have the same assignment group are also cleared.
- Vulnerable items (VITs).
- Application vulnerable items (AVITs).
- Container vulnerable items (CVITs).

Important: You can unassign host vulnerable items in bulk in the Vulnerability Manager Workspace. For more information, see Using bulk edit in the Vulnerability Manager Workspace.

Procedure

1. In either the classic environment, or in the IT Remediation Owner Workspace, navigate to a vulnerable item (VIT) record that is assigned to you that is in any state other than Closed or Resolved.
2. To clear the **Assigned to** and **Assignment group** fields in the classic view, at the top of the record, select **Unassign**.
3. Alternatively, navigate to a vulnerable item (VIT, AVIT, or CVIT) record in the IT Remediation workspace that is assigned to you or your groups and click **Unassign** in the More options menu () to clear the assignment fields.
4. For remediation task records in the workspace that are assigned to you or your groups, open a record select **Unassign** in the More options menu () to clear the assignment fields.
5. In the Unassign dialog for both vulnerable items and remediation tasks, provide work notes and select **Submit**.
   The state change approval request is submitted for approval.

   Note: For remediation tasks, you are notified that the **Assigned to** and **Assignment group** fields on all of a remediation task's associated VITs are also cleared.

   After the request to clear the fields is approved for a remediation task, all the **Assigned to** and **Assignment group** fields on its vulnerable items that have the same assignment group are also unassigned. If any vulnerable item has a different assignment group than its associated remediation task, it is not unassigned. In most cases these vulnerable items have been manually assigned.

6. View the following information:
   - The work notes that you provided is displayed in the Notes section.
   - On the **State Change Approval** tab, the state change approval record displays with the In Review state, which helps to track the approval workflow.
   - On the **Requested Approvals** tab, your request for the removal of you or your assignment group is displayed in the Requested state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result

The request is approved by using a default, one-level approval workflow. For more information, see Approve or reject an unassign request.

- If your request is approved, the state change approval record and the requested approval record transition to the Approved state. You and your groups are removed from the **Assigned to** and **Assignment group** fields. `Unassigned` is displayed in the **Assignment type** field, and the remediation task and VITs are displayed in the list of the Unassigned module for each product.

  Notifications that records are unassigned are sent automatically to vulnerability managers or analysts in the Unassign notification group. To configure the approval flag, notifications, and default assignment group, see Remove assignments from findings and remediation tasks.

- If your request is rejected, the state of the change approval record and requested approval record transition to the Rejected state.

Note: As a vulnerability administrator, you can set the *`sn_vul.unassign_vr.approval_required`* system property to **false** to disable the approval process.

What to do next

Navigate to the Unassigned modules for the Vulnerability Response and Application Vulnerability Response Container Vulnerability Response applications, monitor any unassigned records for items that might fall under your scope, and reassign them to yourself.

Configuring remediation target rules

By configuring remediation target rules, you can set the expected time frame for addressing findings, similar to how service level agreements (SLAs) set deadlines for fixing vulnerabilities.

The base system ships with three remediation target rules that are applicable only for application vulnerable items:

- **Critical Risk Rating Rule**: A remediation target with a 1-Critical risk rating, a remediation target of 15 days, and a reminder of 7 days before the target date.
- **Less Critical Risk Rating Rule**: A remediation target with either a 2-High or 3-Medium risk rating a remediation target of 30 days, and a reminder of 7 days before the target date.
- **Medium-High RIsk Rating Rule**: A remediation target with a 4-Low risk rating a remediation target of 45 days, and a reminder of 7 days before the target date.

These rules are inactive by default. If you choose to edit one, rather than create a new one, remember to check the Active box before saving.

Related topics

Defining your own service level agreements (SLAs) using remediation target rules

Create or edit remediation target rules

Create remediation target rules to ensure the timely remediation of high-risk vulnerabilities by setting up a remediation target rule at the findings level.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Remediation target rules** tile.
4. On the Rules page, select **Remediation target** in the navigation pane.
5. Select **New**.
6. On the remediation target rule form, enter the required details.
   For a full description of each field, see Remediation target rule fields.
7. Select **Save**.

   This rule goes into effect during the next run of the scheduled job, *`Evaluate remediation targets`* or when using the **Reapply** button on the Remediation target rules list view. The same is true when an existing rule is updated.

Related topics

Create or edit remediation target rules

Recalculate a remediation target date

Examples of recalculating a remediation target date

Recalculate a remediation target date

The remediation target (RT) date defines when a finding must be remediated. Recalculation verifies that RT dates stay accurate and reflect the latest risk rating updates. When a finding's risk rating changes, the system can recalculate RT dates using the most recent update date, helping maintain accurate SLAs and avoid outdated or overdue target dates.

Before you begin

Note: By default, recalculation applies only to findings that aren't overdue. To include overdue findings in the recalculation, enable the *`sn_sec_cmn.evaluate_targetmissed_records`* system property.

Role required: admin

Procedure

1. Navigate to **Security Exposure Management** > **Administration** > **Remediation Target Rules**.
2. Open an existing rule to make updates.

   If you need to create a new rule, select **New**.

   For instructions, see Create or edit a Vulnerability Response remediation target rule.
3. Choose how the system should recalculate the remediation target (RT) date when the risk rating changes.
   - In Workspace, this option appears in the Recalculate target date section
   - In Classic view, use the **Target recalculation method** field.

Choice	Description
Default calculation	Retains the existing RT date. The recalculated date isn't applied.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Choice	Description
Recalculate from risk change date	Updates the Remediation Target date to: Field change time + Target (days) based on the new risk rating.
Recalculate from risk change date and al ways set to earliest target date	Compares the existing RT date with Field change time + Target (days) and applies the earlier date.
Recalculate from risk change date and set to earliest target date only when risk rating increases	If the risk increases: Compares the existing RT date and the recalculated RT date and ap plies the earliest date. If the risk decreases: Applies Field change time + Target (days) without comparison.

4. Select **Save**.

What to do next

For more information on remediation target rules, see:

- Vulnerability Response remediation target rules
- Create or edit a Vulnerability Response remediation target rule
- Examples of recalculating a remediation target date

Examples of recalculating a remediation target date

The following examples show how the system recalculates the remediation target date based on different rule selections and risk rating changes.

Note: By default, SLAs define the remediation window for each risk level:

- Low risk: 30 days
- Medium risk: 15 days
- High risk: 10 days

Target from (date)	Field change time	Initial risk (Target (days)) → New risk (Target (days))	Existing RT date	Recalculated RT date	What happens
Default calculation					
Feb 1	Feb 10	Medium (15 days) → High (10 days)	Feb 16 (retained)	Feb 20	The recalculated RT date isn't applied. The system keeps the original RT date: Target from (date) + Target (days) → Feb 1 + 15 = Feb 16.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Target from (date)	Field change time	Initial risk (Target (days)) → New risk (Target (days))	Existing RT date	Recalculated RT date	What happens
Recalculate from risk change date					
Feb 1	Feb 10	Medium (15 days) → High (10 days)	Feb 16	Feb 20 (applied)	Uses the recalculation formula: Field change time + Target (days) → Feb 10 + 10 = Feb 20.
Recalculate from risk change date and always set to earliest target date					
Feb 1	Feb 10	Medium (15 days) → Low (30 days)	Feb 16 (applied)	Mar 12	Compares the existing RT date (Feb 16) with the recalculated date (Feb 10 + 30 = Mar 12) and selects the earliest date → Feb 16.
Recalculate from risk change date and set to earliest target date only when risk rating increases					
Feb 1	Feb 10	Low (30 days) → High (10 days)	Mar 3	Feb 20 (applied)	Because the risk increased, the system compares the existing RT date (Mar 3) with the recalculated date (Feb 20) and applies the earlier date → Feb 20.
Feb 1	Feb 10	High (10 days) → Low (30 days)	Feb 11	Mar 12 (applied)	Because the risk decreased, no comparison is performed. The system sets RT date to: Field change time + Target (days) → Feb 10 + 30 = Mar 12.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Re-evaluate the remediation properties of the records in the Security Exposure Management Workspace

Evaluate the assignments, remediation target date, remediation tasks, exceptions, and risk score for a set of records (VITs, AVITs, CVITs or TRs) in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

Previously, applying rules to all records was necessary to obtain the latest assignments, remediation target dates, risk scores, and remediation tasks, which was time-consuming. Now, you can selectively evaluate and update these properties for specific records, reducing processing time. This update also allows for refining the remediation process based on the updated properties. Furthermore, evaluating exception rules for selected records is now possible, streamlining the process.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable Items
   - Application Vulnerable Items
   - Container Vulnerable Items
   - Configuration Test Results
3. **Optional:** Select the check box of the desired records to updated only the selected records by selecting the Selected items option in the modal.
4. Select the **Re-evaluate** button.
5. In the Re-evaluate update remediation properties modal, select the properties that you want to update for the selected records.

Field	Description
Record selection	○ **Selected items**: Updates the selected records only. ○ **All items**: Updates all the records in the list.
Assignments	Updates the assignments in the **Assignment Group** field according to the latest Assign ment Rules.
Risk score	Updates the risk score in the **Risk score** field as per the latest Risk Score Rules.
Remediation tasks	Updates the remediation tasks according to the latest Remediation task rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Exceptions	Updates the deferral status of the records according to the latest Exception rules. For more information on how the deferral status of the records is updated, see Re-evaluating the exceptions for selected records in the Security Exposure Management Workspace.
Remediation target date	Updates the Remediation target date according to the latest Remediation Target Rules.

Note: When you select a property, its dependent properties are selected automatically.

6. Select **Apply**.

Result
The properties are updated for the selected records. You can check the **Work notes** of the records for the previous and latest values of the updated remediation properties.

Configuring an exception rule

You can request an exception for findings that can't be remediated or deferred immediately. By automating the finding deferral process, you can defer the matching findings based on the rule when the system identifies them.

Related topics

Deferring findings automatically without manual intervention using exception rules

Create an exception rule

Create a rule to automatically request an exception for a specific condition for a group findings, such as a rule with a condition that is based on the vulnerability severity of these findings. With this rule, you can defer new and existing findings automatically if they match the approved rule condition.

Before you begin
Role required: See Access control lists (ACLs) for administration rules

About this task
The rule is applied from the "Valid from" until the "Valid to" date. The remediation task (VUL) is created when the rule is approved. The grouping method for this VUL is known as exception rules. The VUL is created in the Deferred state. You can't close, reopen, or delete this VUL. New and reopened VIs are deferred and added to this VUL from the "Valid from" date until the group expires on the "Valid to" date.

Note:

Email notifications are sent at every stage of the exception rule work flow. These emails provide the status and other details of a request. For example, when an exception rule is requested, the requester receives an email that confirms that the request is submitted.

Note: If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Exception rules** tile.
4. On the Exception Rule new record page, click **New** to create a rule.
5. On the form, fill in the fields.

Exception Rule form

Field	Description
Name	Name of the exception rule.
Valid from	Date from which this rule is active to defer the Findings.
Valid to	Date from which the remediation task stops accepting new Findings.
Reason	Reason to create this exception rule.
Assignment group	Group that the remediation task that was created for tracking the deferred Findings is assigned to.
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.
Condition	Filter condition for the Findings that can be defined while processing the Findings.
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run.
Workflow stage	Current approval status of the exception rule.
State	State of the exception rule.
Execution order	Unique order for each exception rule.
Deferred until	Date until when the VULs and Findings are deferred. On this date, the created VUL is closed, all the Findings move out of the group, and group rules are reapplied.

6. Add the assignment group when you are creating the rule.
7. Submit the form for approval.
   The status of the request changes to In review. Until you submit the exception rule, it remains in the Draft state.

Approve an exception rule request

Assess exception rule requests from users so that you can approve or reject these requests.

Before you begin

Role required: sn_vul.exception_approver

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Exception approver level 1 user group members can approve the level 1 exception rule requests. Similarly, exception approver level 2 user group members can approve the level 2 exception rule requests. Both the user groups inherit the exception approver role by default.

Note:

If you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Exception rules** tile.
4. Select a request from your queue.
5. Approve or reject the request with and explain why you approved or rejected the request.

Activating an exception rule

A rule is activated on its "Valid from" date. After activation, it automates the exception process for findings.

The exception rule follows this life cycle:

1. The new findings that you create or reopen, and that meet the specified condition, are deferred. If you enable the Execute on existing data option when you run the exception rule for the first time, all the active and non-deferred findings that match the exception rule condition are moved to the newly created remediation task (RT) and its state is changed to Deferred.
2. If a newly created finding matches the exception rule condition, it is moved to the deferred RT that is associated with the rule and the group rule is not run on it.
3. On the "Valid from" date, existing findings are added if you enable the Execute on existing data option.
4. The RT stops accepting new findings when the rule expires on the "Valid to" date. The RT remains in existence until the "Deferred until" date.
5. The exception rule expires on the "Valid to" date.

Reopen an exception rule

Reopen an exception rule that has been rejected, but you want to resubmit. Reopening the rule moves it to the Draft state.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

You can then update and resubmit the rule for approval.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Review** on the **Exception rules** tile.
4. Find the rule that you want to reopen and click **Reopen**.
5. Update the form and resubmit it for approval.

Update an approved exception rule

Cancel an approved rule to be able to update it. For example, before you can modify any dates or add a condition to an approved rule, you must cancel it so that the remediation task finding is deleted, and the findings move to the Open state.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Group rules are reapplied to these findings. Submit the rule after making the changes so that it goes through the approval process once again.

Procedure
1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Exception rules** tile.
4. Open the exception rule that you want to cancel and click **Cancel**.
5. In the Cancel Rule dialog box, click **Cancel rule**.
   The rule moves back to the Draft state and the associated VUL is deleted. The related Findings are reopened, and group rules are applied to the individual Findings.

Delete an exception rule

Delete an exception rule that is not required anymore. For example, you can delete a rule if you don't want to defer a finding during ingestion.

Before you begin
Role required: See Access control lists (ACLs) for administration rules

About this task
Deleting a rule cancels the associated remediation task (VUL). The related findings are reopened, and group rules are applied to the individual findings.

Procedure
1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Exception rules** tile.
4. Open the exception rule that you want to delete and click **Delete**.
5. In the Delete Rule dialog box, click **Delete rule** to delete the selected rule.
   The associated remediation task is also deleted. The related findings are reopened, and group rules are applied to the individual findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define fields and weights for the risk rule for Unified Security Exposure Management risk calculators

Customize risk rule parameters and weights to generate risk scores that reflect your organization's specific finding and asset data. By selecting relevant fields for the risk rule, you can create an effective risk scoring framework that meets your organization's unique needs.

Before you begin

Additionally, you can use attributes in the configuration_item [cmdb_ci] in the Configuration Management Database (CMDB) to help you create logic for your Unified Security Exposure Management risk calculators. If, for example, you determine that CIs that are external-facing in your organization are more vulnerable and might require immediate remediation, you can assign attributes such as *Internet Facing* for these CIs. This attribute, and others, are listed in the Common Service Data Model release notes for the Orlando family release. For current information and guidance on the CMDB, see the following topics:

- Common Service Data Model conceptual model
- CMDB schema model

Role required: sn_vul.manage_risk_score_configuration

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Calculators**.
2. On the Vulnerability Calculators page, select **Default Risk Calculator**.
3. Navigate to **Vulnerability Calculator page** > **Vulnerability Calculator Rules tab** > **Default Risk Rule**.
4. **Optional:** In the Risk Calculator Criteria section of the Vulnerability Risk Rule page, set the weight for each criterion according to its importance in the overall risk score calculation.
5. To deactivate the rule, you must clear the **Active** check box.
6. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
7. On the form, fill in the fields.

Risk rule field form

Field	Description
Choose reference table	Table that you use to define the risk score weightage. You can select one of these options: ○ **Vulnerable Item**: Add fields that are directly dot-walkable from the vulnerable item (VI). ○ **Vulnerable Item - Configuration Item**: Add dot-walkable fields that are part of the base table extensions, such as the Hardware table. These fields aren't part of the base table (cmdb_ci). ○ **Vulnerable Item - Vulnerability**: Add dot-walkable fields that are part of the tables that extend the base table, for example, third party Entry. These fields aren't part of the Vulnerability Entry base table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Vulnerable Item Reference Table**: Add fields that are a part of the Related tables (m2m) or tables that have a reference to the vulnerable item. These fields aren't directly dot-walkable from the VI. ○ **Configuration Item Reference Table**: Add fields that are a part of the Related tables (m2m) of cmdb_ci or tables that have a reference to cmdb_ci. These fields aren't directly dot-walkable from the VI. ○ **Vulnerability Reference Table**: Add fields that are a part of the Related tables (m2m) of sn_vul_entry or tables that have a reference to sn_vul_entry. These fields aren't directly dot-walkable from the VI. ○ **Custom Conditions**: Use this option to assign weights to the rule by evaluating the condition. For example, the internet-facing filter determines if a configuration item (CI) is external or internal.
Table	Field that appears only when one of the following options is selected from the Choose reference table: ○ **Vulnerable Item -> Configuration Item** ○ **Vulnerable Item -> Vulnerability** ○ **Vulnerable Item Reference Table** ○ **Configuration Item Reference Table** ○ **Vulnerability Reference Table**
Field	Field to be used for risk score calculation for this rule.
Aggregation	Field that appears only when a reference table is selected from the Choose reference table. Select the minimum or maximum value to be considered for calculations when Field is selected from the Related tables (m2m).
Weight	Weightage of this field within the risk rule. The value must be an integer from 0 through 100.
Define Value Weightage	Component to assign weights to each field value. For numeric fields, field values can be defined as a range (for example, 1–5). The weights must be integer between 0–100. **Note:** This field doesn't appear if the Custom Conditions option is selected from the Choose reference table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Condition table	Field that appears only when Custom conditions are selected from the Choose reference table. Select a condition from the list.
Field name	Field that appears only when Custom conditions are selected from the Choose reference table. Enter a name for the risk criteria.
Condition	Field that appears only when Custom conditions are selected from the Choose reference table. Preview the items in this table that match the defined conditions.

8. Select **Submit**.
9. In the Rule page, activate and reapply the rule to reevaluate the risk score on the active vulnerable items.

Note: Starting with version 23.0 of Vulnerability Response, in case of:

- **Default Risk Calculator** rule: Whenever the risk score on a vulnerable item (VIT) changes, the following details are documented in the Notes section of the VIT:
  - Calculator group name
  - Calculator name
  - Field values that have a weightage greater than 1 and their risk score contribution.
  - Final risk score
- **Vulnerability Severity** risk rule: Whenever the risk score is updated on a VIT, the **Notes** section is updated with the following details:
  - Calculator group name
  - Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, select any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If **Template** is selected, the risk score is updated according to the specified condition in the rule. If **Script** is selected, you can either add or update the existing script.

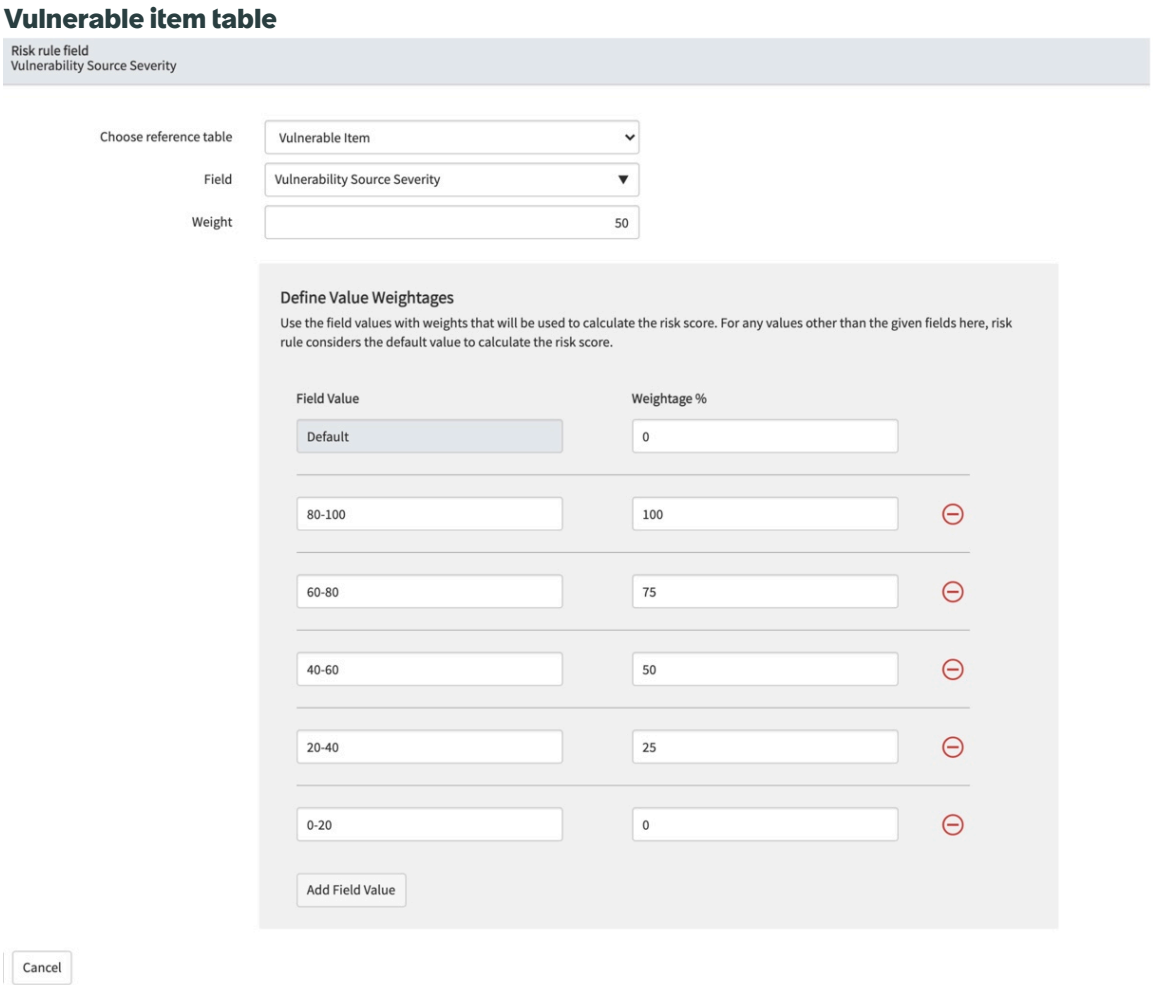
Example:
Example 1: Add a source severity as a criterion for a risk rule.

Use case: Third-party vendors, like Qualys and Tenable, provide their own scores. These scores are populated in the **Source Severity** field on the sn_vul_entry table. Use this field for risk score calculations. To use this score to compute the risk score, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Vulnerable item**.
5. From the Field list, select **Vulnerability.Source Severity**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
7. In the Define Value Weightage section, add field values, and assign a weight to them.



8. Select **Submit**.

Example 2: Add a business criticality as a criterion for a risk rule.

Use case: Let's assume your organization has many business services. The configuration item (CI) LINUX-SF-6381 is being used by the following services:

Criticality of the business services

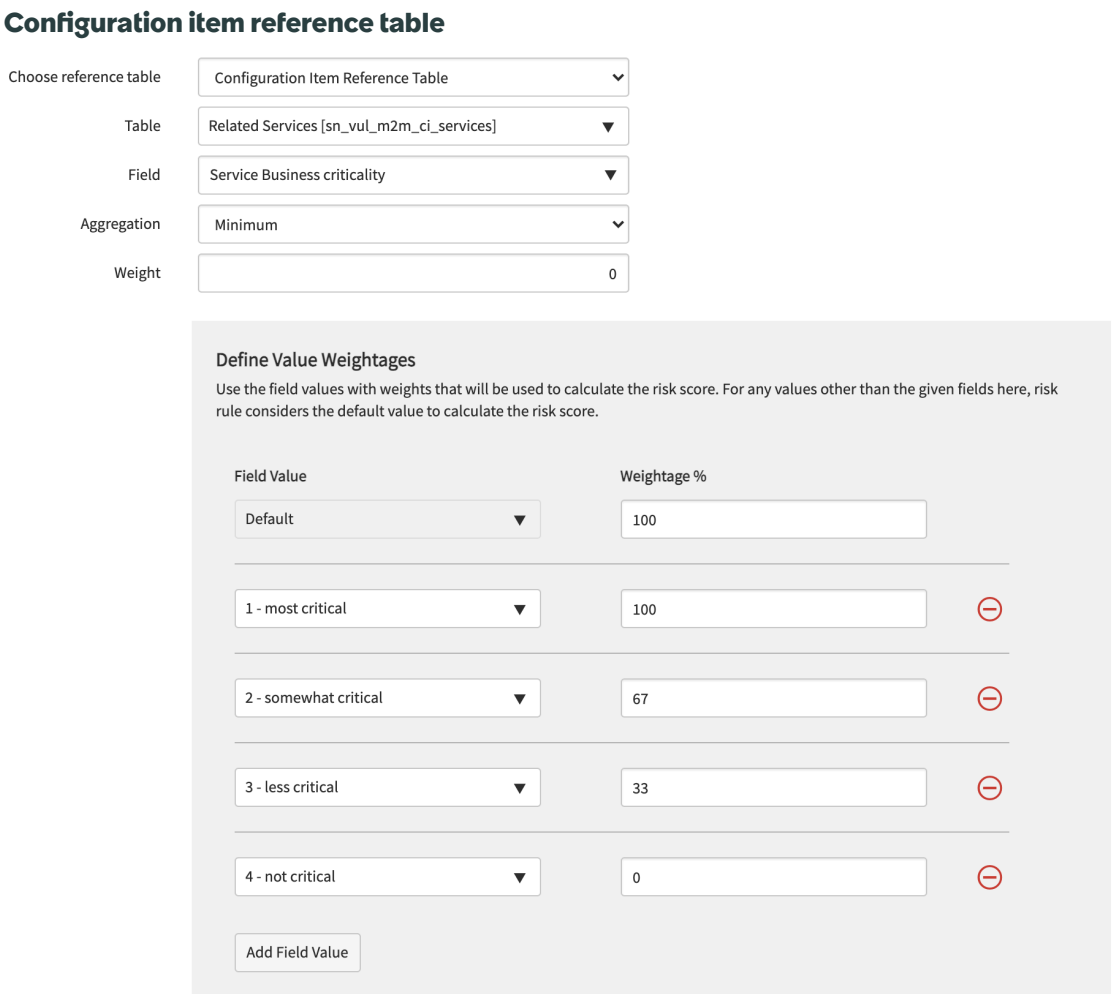
Business service	Criticality
Cloud Management	1 - Most critical
E-Commerce	2 - Somewhat critical
Client services	3 - Less critical
Travel and Expense	4 - Not critical

The mapping between the CI and services is stored in the Related Services [sn_vul_m2m_ci_services] table. When a vulnerability is found in the asset LINUX-SF-6381, a vulnerable item (VI) is created. You can use the value of the business criticality from the affected

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

services to compute the risk score for this VI. To use the criticality value of these services to compute the risk score, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Configuration Item Reference Table**.
5. From the Table list, select **Related Services [sn_vul_m2m_ci_services]**.
6. From the Field list, select **Service.Business criticality**.
7. In the **Aggregation** field, select **Minimum** to retrieve the most critical service for this use case (**1- Most critical** value) or Maximum to retrieve the least critical service for this use case (**4 – Not critical** value) for this use case.
8. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
9. In the Define Value Weightages section, add field values, and assign a weight to them.



10. Select **Submit**.

Example 3: Add a conditional criterion to the risk calculator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

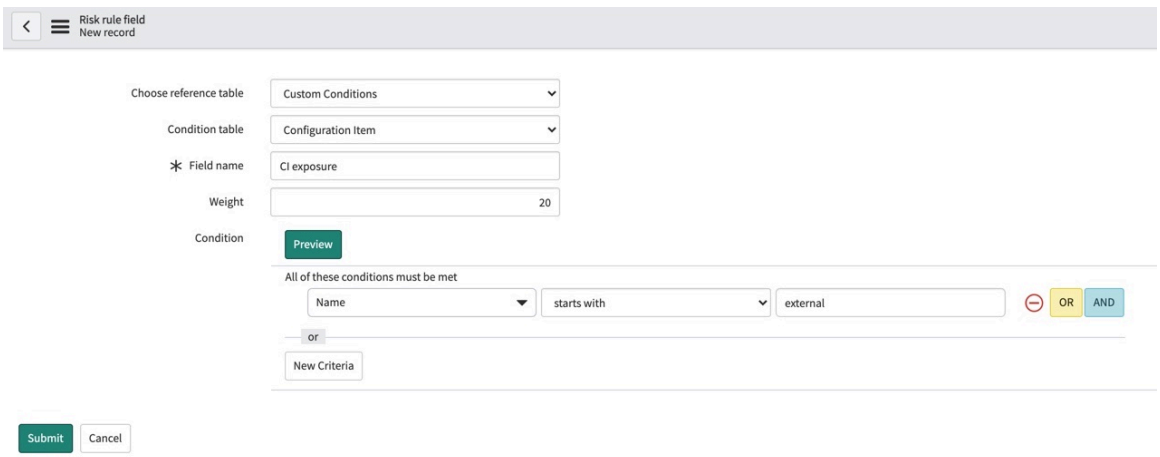
Let's assume that an organization has multiple configuration items (CIs), of which only a few can be accessed by an external user. You can add risk score weightages for these outward-facing CIs.

Note: You can identify these CIs by their name. The names start with 'external'.

To add a conditional criterion to the risk rule, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Custom conditions**.
5. From the Condition table list, select **Configuration item**.
6. In the **Field name** field, enter the name **CI Exposure**.
7. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
8. In the **Condition** field, select **Name** > **starts with** and enter the value **external**.

Custom conditions for the new risk rule



9. Select **Submit**.

Note: Adding conditional criteria to your risk rule might degrade performance.

Related topics

- Vulnerability Response calculators and vulnerability calculator rules
- Create a Vulnerability Response calculator
- Filtering within Vulnerability Response

Configuring remediation task rules

By configuring remediation task rules, you can automatically group findings based on filter conditions.

In the Security Exposure Management Workspace, you can set up a single assignment rule that applies to all types of findings, including vulnerable items (VITs), application vulnerabilities (AVITs), container vulnerabilities (CVITs), and configuration test results (CTRs). This rule can then be applied to all the findings or a specific combination of findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Grouping multiple findings as remediation tasks for easy processing using remediation task rules

Create remediation task rules

Create remediation task rules to automatically group findings based on filter conditions. These rules automatically group findings as they're imported or manually created. Use the filter to limit the findings grouped by this rule, such as selecting all findings with exploits.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

About this task

The base system ships with one remediation task rule, **Vulnerability**, which groups vulnerable items by vulnerability and assignment group (from Assignment rules). You can reapply the rules from the form or list view. For some sample entries, see Vulnerability Response remediation task rule examples.

This rule can be modified by using filter conditions and Group by choices. By default, remediation tasks use Assignment Rules, when available, as part of their filter criteria.

Note: If no assignment rules exist, you can select a group using the User group field.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Remediation task rules** tile.
4. On the Rules page, select **Remediation task** in the navigation pane.
5. Select **New** and fill in the fields on the form:

Remediation task rule form

Field	Description
Details	
Name	Name of the remediation task rule.
Applies to	Tables the remediation task rule applies to.
Active	Indicates whether the remediation task rule is active.
Description	Description of the remediation task rule.
If this condition is met	
Case sensitive	Determines whether a condition is case sensitive or not. **Note:** The default value is case insensitive.
Condition fields	Conditions that must be met. By default, searches in the condition builder on task rule records and forms aren't case-sensitive (the Case sensitive check box is inactive). If needed, you

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	can enable case-sensitive searches by selecting the Case sensitive check box on the relevant task records and forms.
New condition set	Adds more condition filter fields to choose from.
Group by	
Group findings from	The table the rule uses to group the findings. Choices are: ○ Finding [sn_vul_vulnerable_item] ○ Finding > Configuration Item [cmdb_ci] ○ Finding > Vulnerability **Note:** ○ The **Group findings from** field updates based on the number of tables selected in the **Applies to** field. If one table is chosen, it shows the corresponding item. If multiple tables are chosen, it displays Findings. ○ You can add up to six grouping criteria.
Using field	Field on the table that the rule uses to group findings.
Assignment	
Assign remediation tasks by	When automatically assigning remediation tasks, the Assignment choice is used in addition to the Group By choices to group the findings. New tasks are created, as needed, to ensure that each finding is placed in a task with a matching assignment group set. To automate the assignment of tasks created based on this rule, choose one of the options available. ○ Group by field: If you selected any user group field from the Using field values in the Group by section, they appear in the drop-down menu. ○ User Group: Use the lookup list to select a static user group.

6. Select **Save**.

Configuring auto-close rules

By configuring auto-close rules, you can automate the process of closing stale detections and findings associated with retired configuration items (CIs).

The base system provides the following auto-close rules:

- **Assets last scanned**: Detections associated with assets that haven't been scanned within the last 90 days are transitioned to Stale state.
- **Detections last found**: Detections that haven't been found within the last 90 days. If you activate Detections last found record, then this feature requires a successful integration run of Rapid7 Comprehensive Vulnerable Item Integrations and Microsoft TVM Machine Vulnerabilities Integration (Full import) within the last seven days.

Configuration of auto-delete rules includes the following steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Closing stale detections and findings automatically using auto-close rules

Create or edit auto-close rules

Create rules to close stale detections and findings associated with retired CIs automatically.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Auto-close rules** tile.
4. On the Rules page, select **Auto-close** in the navigation pane.
5. Select **New** and fill in the fields on the form:

Auto-close rule form

Field	Description
Details	
Name	Name of the rule.
Table	Name of the finding type for which the rule is being applied. **Note:** For vulnerable items (VITs), rules are applied to detections first, and then applied to the VITs, rather than being directly applied to the VITs.
Description	Description of the rule.
Active	Indicates whether the rule is active.
If this condition is met	
Condition fields	Filter conditions defining the records in the Findings and Remediation Task tables to which the rules apply.
New condition set	Adds more condition filter fields to choose from.
Then do this	
Close findings automatically	
Ignored deferred items	If selected, any findings or detections that are mapped to the **In-review** or **Deferred** states are ignored and not closed. If you clear this option, any findings or detections that match your criteria are closed.

6. Select **Save**.

The *`Auto-Close Stale Detections`* scheduled job runs daily. It identifies detections based on the specified conditions and transitions the matching ones to the **Stale** state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The job handles the following scenarios:

- If all the detections within a VIT are marked as stale, the VIT is closed with the sub-state set as "Stale".
- If there is at least one detection that remains open within a VIT, while others are in the Stale status, the VIT remains open.
- In cases where there are detections with both "Closed" and "Stale" statuses within a VIT, the VIT is closed with the sub-state set as "Fixed".

When you upgrade to the latest version of Unified Security Exposure Management, the conditions set in your auto-close rules also get updated accordingly. Additionally, if the rules are associated with different domains, the rules are created specifically within those domains.

Configuring auto-delete rules

By configuring auto-delete rules, you can automate the process of deleting older findings and remediation tasks.

The base system provides two preconfigured auto-delete rules that automatically remove closed records and any related records. One rule targets findings, and the other targets remediation tasks. These rules are inactive by default, so you must activate them manually before they can delete any records. You can use the two preconfigured rules or create your own to suit your specific needs.

Configuration of auto-delete rules includes the following steps.

Related topics

Deleting stale findings automatically using auto-delete rules

Create or edit auto-delete rules

Create rules to delete findings and remediation tasks automatically based on specific filter conditions. These rules help remove older records from the Findings and Remediation Task tables.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Auto delete rules** tile.
4. On the Rules page, select **Auto delete** in the navigation pane.
5. Select **New** and fill in the fields on the form:

Auto-delete rule form

Field	Description
Details	
Tablename	Name of the table for which the rule is being applied.
Matchfield	Field for which the system monitors the duration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Age in seconds	Age of the vulnerability record to be deleted. For both findings and remediation task rules, the age is 365 days. This age is displayed in seconds.
Active	Indicates whether the rule is active.
Cascade delete	Option to delete all matching records, plus any records referring to them. If this option isn't selected, only matching records are deleted, but not the records that refer to them.
Conditions	
Condition fields	Filter conditions defining the records in the Findings and Remediation Task tables to which the rules apply.
New condition set	Adds more condition filter fields to choose from.

6. Select **Set conditions**.
7. Select the conditions.
8. Select **Set**.
9. Select **Save**.
   Once the rule is activated, the hourly platform function, **Auto flush** deletes those records from the table for which the rule is activated.

   If your environment contains millions of records that match your delete criteria, it's advisable to consult with ServiceNow Customer Support before enabling the auto-delete rules. They can assist you in deleting records through a phased process to ensure smooth and efficient data management.

Configuring exclusion rules

By configuring exclusion rules, you can filter or exclude detections from being converted into vulnerable items (VITs) during ingestion. This filtering helps streamline vulnerability management by reducing noise and prioritizing critical issues.

Execution order behavior

The execution order defines the priority in which exclusion rules are processed. Rules with a lower execution order value are evaluated first.

1. Default execution order for new rules

   When you create an exclusion rule, the system automatically assigns an execution order to maintain spacing and avoid conflicts.

   System behavior:

   - The first rule created: Execution order = 1000
   - Subsequent rules: Execution order = (highest existing execution order) + 1000

2. Updating execution order via drag

   In the Security Exposure Management Workspace, you can reorder exclusion rules using drag in the list view. When rules are repositioned, execution order values are recalculated automatically based on their new position.

   System behavior:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Between two rules: New execution order = (Order of previous rule + Order of next rule) ÷ 2
- Moved to the top of the list: New execution order = (Execution order of current top rule) ÷ 2
- Moved to the bottom of the list: New execution order = (Execution order of current bottom rule + 1000)

Related topics

Controlling the ingestion volume with automatic exclusion

Create or edit exclusion rules

Create a rule to filter or exclude detections from getting converted into vulnerable items (VITs) during ingestion.

Before you begin

Role required: admin

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Select **Review** on the **Exclusion rules** tile.
4. On the Rules page, select **Exclusion** in the navigation pane.
5. Select **New** and fill in the fields on the form:

Exclusion form

Field	Description
Details	
Name	Name of the exclusion rule.
Active	Option to activate the exclusion rule.
Execution order	Unique order for each exclusion rule.
Description	Description of the exclusion rule.
If this condition is met	
Condition	Filter conditions for the detections that can be defined while processing them.

6. Select **Save**.
   Once an exclusion rule is created, it takes effect on detections starting from the subsequent ingestion.
7. To edit, select the rule name and update the required fields and select **Update**.

Approve or reject an unassign request

Approve requests for the removal of findings from an assignment group or an individual user in the Security Exposure Management Workspace.

Before you begin

Role required: For unassign approvals, one approver is required in the Approver – Level 1 group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.unassign_approver for AVITs and VITs
- sn_vul_container.unassign_approver for CVITs

About this task

By default, an approval configuration is provided and an unassign approval group is created. Users of the Unassign Approver - Level 1 group can approve the request. This group contains an unassign approver role, sn_vul.unassign_approver, by default. You can modify or create a new group and update the approval configuration. To configure an approval rule, select any of the following approval rule in the Approval Rules module and navigate to the approval configuration on the **Approval Configurations** tab:

- *`Vulnerable item field change request`* for a vulnerable item.
- *`Vulnerability field change request`* for a remediation task.
- *`Application vulnerability field change request`* for an application vulnerable item (AVIT).
- *`Approval for container management`* for a container vulnerable item (CVIT).

For more information on approval rules and configurations, see Approval workflow configurations for unassign request.

Important: You can approve or reject requests in the Vulnerability Manager Workspace. .

Procedure

1. Navigate to **All** > **Vulnerability Response** > **My Approvals** for VITs and AVITs.
   Alternatively, navigate to **All** > **Container Vulnerability Response** > **My Approvals** for CVITs.
2. Select a request from your queue.
3. Approve or reject the request by adding the appropriate comments.

Approval workflow configurations for unassign request

You can design the approval workflow for the removal of assignments from vulnerable items (VIs, VITs), remediation tasks, application vulnerable items (AVITs), and container vulnerable items (CVITs) for you and your group.

VIT, remediation task, AVIT, and CVIT have a default approval rule each. Each approval rule has a default approval configuration. Each approval configuration has a default approver level. The approval rules for VITs, remediation task, AVIT, and CVIT are enabled by default. As an admin, you can perform the following actions by navigating to **All** > **Vulnerability Response** > **My Approvals** > **Approval Rules** and selecting the appropriate approval rule.

- enable or disable an approval rule.
- create and update an approval configuration.
- define conditions for vulnerable items and remediation tasks for which the approval rules apply.
- create and update multiple approver levels.

The following table shows the default approval rules, approval configurations, and approver levels for a VIT, remediation task, AVIT, and CVIT which are shipped with the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Default approval rules, approval configurations, and approver levels

Type	Approval Rule	Approval configuration	Approver levels
VIT or VI	Vulnerable item field change request	Vulnerable item field change request	Level-1 Unassign Request for VI
Remediation task	Vulnerability Group field change request	Vulnerability field change request	Level 1 - Unassign Request for VG
AVIT	Application vulnerable item field change request	Application vulnerability field change request	Unassign app vulnerability item
CVIT	Approval for container management	Default Configuration Unassign CVIT	CVIT unassign approval level - 1

For more information on how to approve unassign requests, see Approve or reject an unassign request in Vulnerability Response.

Configure Exception Management for Security Exposure Management

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to a finding or remediation task (RT) that cannot be remediated according to the policy.

Before you begin

Limit the duration of an exception requested and add a questionnaire to the exception or false positive request using the Security Exposure Management workspace. You can also request an exception using the GRC: Policy and Compliance Management integration.

Role required: sn_vul_exception.admin

About this task

If Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

It’s useful for the exception approver to understand the reason for requesting the exception.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **Administration** > **Exception Management** > **Review** > **Basic configuration**.
2. You can select any one of the apps **Vulnerability Response Exception Management**, **Application Vulnerability Response Exception Management**, **Container Vulnerability Response Exception Management**, **Configure Compliance Exception Management**.
3. On the Exception Management Configuration page, select how you want to manage an exception by selecting an option from the **Manage exceptions using** list.
   You can select either **Security Exposure Management** or GRC: Policy and Compliance Management. You must activate the GRC plugin to use GRC: Policy and Compliance Management to request an exception. Changing the configuration doesn’t impact the existing data.
4. If you selected the settings for any of the apps, enter the following information:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Settings for Exception Management form

Field	Description
Exception management ownership	This is a read-only field if GRC plugin is not installed.
Questionnaire for exception request	Displays the questionnaire selected by you to request an exception. The **Exception Questionnaire** is displayed by default. You can also select questionnaire from the drop-down list.
Questionnaire for compensating control	Displays the questionnaire that a remediation owner must answer for risk reduction requests. You can set questionnaire for risk reduction requests. The **Compensating Control Questionnaire** is selected by default. You can also select questionnaire from the drop-down list. (This option is not available for CC Exception Management).
Maximum Duration for exception (days)	Add the maximum number of days for which an exception can be requested.
Questionnaire to mark false positive	Displays the questionnaire selected by you to mark as false positive. The questionnaire for false positive request is displayed by default. You can also select questionnaire from the drop-down list.

5. If you selected the GRC: Policy and Compliance Management option, enter the following information:

Settings for Exception Management form

Field	Description
Questionnaire to mark false positive	Displays the questionnaire selected by you to mark as false positive. The questionnaire for false positive request is displayed by default.

6. To configure **Conditional questionnaires** based on conditions for exception and false-positive requests:

   a. In the Exception Management Conditional Questionnaires section, select **New**.

   b. In the New conditional questionnaire form, fill in the fields and select **Save**.
   The created questionnaire appears in the VR Questionnaire Configuration section of the Settings for VR Exception Management form.

   For example, if you want to configure questionnaire for false-positive requests for critical vulnerable items, then select the **False positive for vulnerable items** approval rule, provide the condition as `Risk rating is 1 - Critical` and select the desired questionnaire in the Questionnaire configuration form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select **Design New Questionnaire** to design new assessment questionnaires using the templates present in the Assessment Workspace.
8. Select **Save**.

Request an exception using GRC: Policy and Compliance Management

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Vulnerability Response.

Before you begin

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Role required: sn_vul.remediation_owner

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management** > **findings** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.
2. On the selected form, click **Request Exception**.
3. On the form, fill in the fields.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you are requesting an exception for.
Control objective	Control objectives that are associated with the policy you selected. If a policy is not selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date cannot be in the past.
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid cannot exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click **Submit**.
   For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance optional setup.

Specify the duration of an exception requested for a remediation task

Use system properties to limit the duration for which an exception is requested for a remediation task. Remediation of the remediation task is deferred for the specified period.

Before you begin
Role required: sn_vulc.admin

About this task
The `sn_vulc.exception_max_request_days` property is used to specify the maximum number of days for which an exception for a remediation task can be requested. The default value is 365 days.

Note: You can use the `sn_vulc.exception_approval_required` property to disable the exception approval work flow for the remediation task if it is not required. By default, this property is enabled and its value is `true`.

Procedure

1. Navigate to **All** > **System Properties** > **All Properties**.
2. On the System Properties page, search for `sn_vulc.exception_max_request_days`.
3. Click on the property name to open the System Property record.
4. To be able to edit this record, ensure that Configuration Compliance is selected as the current application.
5. Enter a positive **Value** and click **Update**.
   The record is updated and saved.

Configure email notifications in Unified Security Exposure Management

Set up email notifications to share useful information about important updates and activities such as approval and rejection of false-positive requests. Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin
Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Under **Others**, select **Review** on the **Notifications** tile.
4. Select **New**.

   For detailed instructions on creating email notifications, see Create an email notification.

Result
When a recipient clicks the links in an email notification, the links open in the Security Exposure Management Workspace or IT Remediation Workspace based on their role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Links open in the Security Exposure Management Workspace for the users with the roles, sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin.
- Links open in the IT Remediation Workspace for the users with the role, sn_vul.remediation_owner.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Configure email templates in Unified Security Exposure Management

Create and manage preconfigured email templates for sending notifications.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Under **Others**, select **Review** on the **Email templates** tile.
4. Select **New**.
5. Fill in the form fields.

Field	Description
Name	Enter a unique name for the template.
Table	Select the name of the table involved. For example, **Change Request** `[change_request]`.
Email layout	Select a predefined layout.
Subject	Enter a subject line that explains the purpose of the email. Select the appropriate variables for the subject line from the fields available on the selected table. Place the cursor where you want the variable to appear, and select the field name in the **Select variables** column. For example: `${sys_class_name} ${number} with ${risk} risk has been assigned to you.`
Message HTML	Enter the content of the email template message. You can use the HTML editor toolbar to format the HTML, and you can include variables from the **Select variables** column. Variables map to column names available from the notification table, its parent tables, and reference tables. Use variables to include values from a record in the table such as an incident short description or comments and work notes. Notes:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ When a template is applied to a notification, the contents of this field are used when you select **HTML and plain text** or **HTML** in the **Content Type** field in the Email Notification form. ○ You cannot use HTML code to control the appearance of the contents in the `${comments}` variable. ○ If you want to include a link to the record that triggered the notification, see Enable links to records.
Message Text	Enter the notification message to send in plain text. **Note:** When a template is applied to a notification, the contents of this field are used when you select **HTML and plain text** or **Text** in the **Content Type** field in the Email Notification form.
SMS alternate	Create a different message to be delivered to an SMS device. Enter a brief message, showing the most important information only. If this message field is blank, the contents of the **Message Text** field are used for the SMS message. **Note:** The message in this field is used when the message is sent to a device configured as SMS.

For detailed instructions for creating email templates, see Construct an email message with a template.

6. Select **Save**.

Configure a severity map in the Security Exposure Management Workspace

Security Exposure Management Workspace severity mapping transforms third-party source severity fields to recognizable fields in Unified Security Exposure Management.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

About this task

Security Exposure Management Workspace ships with National Vulnerability Database (NVD) to normalized ServiceNow severity mapping. ServiceNow third-party integrations such as the Qualys Vulnerability Integration provide severity mappings on installation. These maps can be adjusted by changing the fields in existing maps.

Creating or editing a severity map is intended only for customized or non-standard third-party mappings in your environment.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select **Administration** in the navigation pane.
3. Under **Others**, select **Review** on the **Normalized Severity Mapping** tile.
4. Select **New**.
5. Fill in the fields on the form, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field mapping

Field	Description
Source	The name of the source for the severity mapping.
Target value	The target severity value. Choices are: ○ 1- Critical ○ 2 - High ○ 3 - Medium ○ 4 - Low ○ 5 - None
Source value	The source severity value.

6. Repeat Step 5 for each source severity level.
7. Select **Save**.
8. To edit the severity mapping for an integration, select the integration and update the values in the **Source Value** and **Target Value** fields.

Configure Visualization library

The Visualization library lists the available widgets for the Findings view page and their additional details, such as, the current activation status, additional conditions, and other columns. Configure the visualization library to select the columns you want to view.

Before you begin

Role required: See Access control lists (ACLs) for administration rules

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. In the navigation pane, select **Administration**.
3. Under **Others**, in the **Visualization library** tile, select **Review**.
4. In *Visualization library*, select the **List Actions** icon, and then select **Edit columns**.
5. Select the required columns from the **Available columns** pane, and select **OK**.

Visualization widget columns

Field	Description
Active	Indicates whether the widget is available to add to a filter. The widgets are active by default. Users with the sn_sec_wf.manage_admin_rules role can deactivate the widgets by setting the value of *Active* to `False`.
Additional condition	Additional conditions added to the widget.
Class	The class that the record belongs to.
Created	The date when the record was created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created by	The user who created the record.
Findings table	The tables the widgets to fetch data.The widgets can fetch data from one or more of the following tables: ○ Infrastructure vulnerability ○ Application vulnerability ○ Misconfigurations ○ Container vulnerability
Framework	The framework that the record applies to.
Group by	The column on the findings table which provides the score for the widgets or categorizes the data.
Tags	The tags assigned to the record during import
Updated	The date when the discovered Item record was updated.
Updated by	The user who updated the data.
Updates	The updates to the record.
Visualization group	The visualization group under which the widget is displayed in the carousel.
Visualization type	The visual format to represent the filtered data.
Widget name	The name of the widget.

Create a custom widget

Create a custom widget in the Security exposure management (SEM) workspace to visualize findings data that meets your organization's reporting needs. This feature enables administrators to extend the default widgets in the visualization library by adding new widgets that reflect organization-specific risk and exposure metrics.

Before you begin

- Check that the visualization group limit set by the system property *sn_sec_sem.vizGroupLimit* (default = 10 widgets in a group) isn't exceeded before adding a new widget.
- Verify that the *Group by* value you plan to use doesn't exist in another widget. The **Group by** field must be unique.

Role required: admin

Procedure

1. Navigate to **Security Exposure Management** > **Administration** > **Visualization library**.
2. Select **New**.
3. On the new Visualization widget form, enter the required details.
   For a full description of each field, see Visualization widget fields.
4. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The widget is now saved to the **Visualization Library** and can be used when creating or editing dashboards.

Note:
- You can create or update widgets in the **Findings view**, but not in the **Remediation overview** page. Widgets in the **Remediation overview** are predefined and cannot be created or edited. You can only change their display order or activate or deactivate them.
- Only the widgets marked *Active* = *true* appear in the dashboard creation view.

Update a widget

Update a widget in the Visualization Library to modify its configuration or presentation. You can update attributes to refine how data appears in Findings dashboards and ensure that the visualizations stay relevant to your reporting needs.

Before you begin
Role required: admin

Procedure
1. Navigate to **Security Exposure Management** > **Administration** > **Visualization library**.
2. Open the widget record to update.
3. Update any of the editable fields.
   - For default widgets (User created = false), you can only:
     - Change **Display order**, or
     - Set **Active** to true or false
   - For custom widgets (User created = true), you can edit all the fields.
4. Select **Update** to save change.

Result
The widget is updated in the Visualization Library and can be used when creating or editing dashboards.

Note:
- You can create or update widgets in the Findings view, but not in the Remediation overview page. Widgets in the Remediation overview are predefined and can't be created or edited. You can only change their display order or activate or deactivate them.
- Only the widgets marked **Active** = *true* appear for selection while creating a dashboard in the finding view.

Localize widget titles

Update the widget title in the Messages [sys_ui_message_list] table whenever you create a custom widget or rename an existing one to ensure it displays correctly in localized interfaces.

Before you begin
Role required: admin

About this task
Follow these steps to add the widget title for translation in the Messages table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to the Messages table [sys_ui_message_list].
2. Select **New**.
3. On the form, fill in the fields.

New message form

Field	Description
Key	Widget title as it appears in the visualization library.
Language	Target language (for example, Japanese).
Message	Widget title that must be translated.
Application	Application for the widget. Select **Security Exposure Management**. **Note:** Cross-scope access isn't supported.

4. Select **Submit**.

Important: If you later rename a widget, search for its existing record in the Messages [sys_ui_message_list] table, and update the **Key** and **Message** fields with the new widget title.

Unified Security Exposure Management integrations

Unified Security Exposure Management supports multiple third-party integrations to help with vulnerability management, orchestration and remediation. This section provides guidelines for managing and developing integrations.

How integrations work

Integrations work in the following way:

1. Vulnerability entries are imported from the National Vulnerability Database (NVD) and third-party scanners.
2. Detection data from third-party scanners are matched against assets in your Configuration Management Database (CMDB).
3. When a match is found, a finding is created.
4. The findings are then:
   - Grouped into remediation tasks.
   - Risk-scored with business context.
   - Prioritized and assigned to the appropriate teams.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- **No cross-integration deduplication**: If multiple third-party integrations are active, findings aren't deduplicated across them. For example, Rapid7 and Qualys findings remain separate.
- **Detection count mismatches**: Variations between scanner counts (for example, Qualys) and ServiceNow findings are expected due to deduplication across IPs, ports, and so on

The following table provides a list of Unified Security Exposure Management integrations created by ServiceNow® and partners.

Integrations

Integration	Product installation	Category	Use case	Setup Guide	Built by
Import vulnerabilities and create vulnerable items					
Tenable	Vulnerability Response Integration with Tenable	Vulnerability Response	Match assets, import third-party vulnerabilities to create vulnerable items. **Note:** Tenable.io doesn't support launching rescan on agent-based machines.	Understanding the Tenable Vulnerability Integration	ServiceNow
Rapid7	Rapid7 Integration for Security Operations	Vulnerability Response	Match assets, import third-party vulnerabilities to create vulnerable items.	Understanding the Rapid7 Vulnerability Integration	ServiceNow
Qualys	Qualys Integration for Security Operations	Vulnerability Response	Match assets, import third-party vulnerabilities to create vulnerable items. **Note:** On-demand rescan is available.	Understanding the Qualys Vulnerability Integration	ServiceNow
CrowdStrike	CrowdStrike Falcon Exposure Management for Vulnerability Response	Vulnerability Response	Match assets and use NVD to create vulnerable items. Supports tag-based filtering on import.		Partner
Microsoft	Vulnerability Response Integration with Microsoft Threat and Vulnerability Management	Vulnerability Response	Match assets and import endpoint vulnerabilities to create vulnerable items.	Understanding the Microsoft Threat and Vulnerability Management Vulnerability integration	ServiceNow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Microsoft	Vulnerability Response Integration with Microsoft Defender for IoT (On-premises Management Console)	Vulnerability Response	Import vulnerabilities into ServiceNow Operational Technology Vulnerability Response and take risk-based action with production process context.	Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM	ServiceNow
Cisco (Kenna)	Kenna.VM (Vulnerability Management)	Vulnerability Response	Match assets and use NVD to create vulnerable items. Includes Kenna Risk score.		Partner
Tanium	Tanium Vulnerability Management	Vulnerability Response	Match assets and import third-party vulnerabilities to create vulnerable items.		Partner
Orca	Orca Security for Vulnerability Response	Vulnerability Response	Match assets and import third-party vulnerabilities to create vulnerable items.		Partner
Onapsis	Onapsis Vulnerability Integration	Vulnerability Response	Match assets and import third-party vulnerabilities to create vulnerable items for SAP assets and applications.		Partner
Synack	Synack - Vulnerability Response	Vulnerability Response	Import vulnerabilities from Synack.		Partner
Wiz.io	Wiz Integration for Security Operations	Vulnerability Response	Match cloud assets and import third-party vulnerabilities to create vulnerable items.	Understanding the Wiz Vulnerability Response Integration	Partner
Lacework	Lacework	Vulnerability Response	Import infrastructure vulnerabilities from your cloud asset sources. Supports vulnerability calculator and filtering by severity.		Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Recorded Future	Attack Surface Intelligence	Vulnerability Response	External attack surface assets and exposures imported into ServiceNow Vulnerability Response. Create vulnerable items from external asset detections. Includes Recorded Future threat and vulnerability enrichment.		Partner
Mandiant	Mandiant Attack Surface Management	Vulnerability Response	Import information about vulnerabilities and vulnerable items from the Mandiant Attack Surface Management platform.		Partner
IBM	IBM Guardium Data Protection	Vulnerability Response	Integrate IBM Guardium database vulnerability scan results with ServiceNow.		Partner
CyCognito	CyCognito App for Vulnerability Response	Vulnerability Response	Import issues and assets from Cycognito SAAS platform.		Partner
VMware	Carbon Black Cloud	Vulnerability Response	Ingest vulnerability data and context from Carbon Black Cloud. Create configuration items from Carbon Black Cloud endpoints and workload.		Partner
Nucleus	Nucleus Security for Vulnerability Response	Vulnerability Response	• Import findings from Nucleus Security Auto-update Vulnerable Items. • Bi-directional update via comments field. • Map custom fields.		Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
InfoSec Global (ISG)	InfoSec Global (ISG) AgileSec Analytics Integration for Vulnerability Response Module	Vulnerability Response	Import vulnerability findings on Cryptographic assets: Cryptographic Keys, Keystores, and Libraries		Partner
Censys	Censys ASM to Vulnerability Response Integration	Vulnerability Response	Scan, discover, and catalog vulnerabilities on internet-facing assets.		Partner
Import container findings, vulnerabilities, and images					
Palo Alto	Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute	Container Vulnerability Response	Ingest container vulnerabilities from Prisma Cloud Compute (formerly Twistlock) and use runtime context (cluster/ namespace and so on) to automate remediation workflow.	Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integration	ServiceNow
Aqua	Aqua Security Platform integration with Vulnerability Response for Containers	Container Vulnerability Response	Import container vulnerabilities from Aqua Platform. Docker and MID Server support.		Partner
Sysdig	Sysdig Container Vulnerability Response	Container Vulnerability Response	Import container vulnerabilities from Sysdig. Supports VI granularity, container, kubernetes, and host security		Partner
Lacework	Lacework	Container Vulnerability Response	Import container vulnerabilities and attempt to match based on docker configuration items (CIs). Supports vulnerability calculator and filtering by severity.		Partner
WIZ	Wiz Integration for Container	Container Vulnerability Response	Import all container vulnerabilities from Wiz.	Exploring the Wiz Container Vulnerability Integration	Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
	Vulnerability Response				
Qualys	Qualys Container Vulnerability Response Integration	Container Vulnerability Response	Import all container vulnerabilities from QCS.		Partner
CrowdStrike	CrowdStrike Falcon Cloud security for Container Vulnerability Response	Container Vulnerability Response	Import all container vulnerabilities from FCS.		Partner
Solution Intelligence					
Microsoft	Vulnerability Solution Management	Vulnerability Response - Content	Provides solution content for vulnerabilities.	Understanding the Microsoft Security Response Center Solution Integration	ServiceNow
Red Hat	Red Hat Security Data	Vulnerability Response - Content	Provides solution content for vulnerabilities.	Understanding the Red Hat Solution Integration	ServiceNow
Rapid 7	Rapid7 Integration for Security Operations	Vulnerability Response - Content	Provides solution content for vulnerabilities.	Rapid7 solution management	ServiceNow
Tanium	Tanium Vulnerability Management	Vulnerability Response - Content	Provides solution content for vulnerabilities.		Partner
CVRF Generic Framework	Supports CVRF Format	Vulnerability Response - Content	Provides solution content for vulnerabilities.	• Generic framework to ingest data from any solution vendor • Setting up vulnerability solution providers	ServiceNow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
CSAF Generic Framework	Supports CSAF Format	Vulnerability Response - Content	Provides solution content for vulnerabilities.	• Generic framework to ingest data from any solution vendor • Setting up vulnerability solution providers	ServiceNow
Vulnerability enrichment and threat scoring					
Recorded Future	Vulnerability Intelligence	Vulnerability Response - Intelligence	Use Recorded Future vulnerability intelligence to prioritize vulnerabilities.		Partner
Flashpoint	Flashpoint Ignite for Vulnerability Response	Vulnerability Response - Intelligence	Consume alerts as security incidents (email), Import TI and vulnerability context.		Partner
Shodan	Shodan Exploit Integration for Security Operations	Vulnerability Response - Intelligence	Vulnerability enrichment with exploit data.	Understanding the Shodan Exploit Integration	ServiceNow
Cisco (Kenna)	Kenna.VI + (Kenna Vulnerability Intel)	Vulnerability Response - Intelligence	Use Kenna.vi vulnerability intelligence to prioritize vulnerabilities.		Partner
Risk Based Security by Flashpoint	Flashpoint VulnDB	Vulnerability Response - Intelligence	Import RBS records into third-party vulnerabilities. Risk scores and software-based vulnerability matching.		Partner
Digital Shadows (Grey Matter by Reliaquest)	GreyMatter Digital Risk Protection Vulnerability Intelligence for Vulnerability Response	Vulnerability Response - Intelligence	Prioritize vulnerabilities using Digital Shadows risk factors and scoring based on analyst-curated threat intelligence.		Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Mandiant | Google	Google Threat Intelligence for SecOps	Vulnerability Response - Intelligence	Enriches vulnerability item records with Mandiant vulnerability intelligence for better prioritization.		Partner
CISA	Vulnerability Response Integration with CISA	Vulnerability Response - Intelligence	Use known exploitedvulnerabilities. Catalog to prioritize vulnerabilities.	CISA Known Exploit Vulnerability (KEV) Integration	ServiceNow
First.org	EPSS	Vulnerability Response - Intelligence	Use the Exploit prediction scoring system to prioritize vulnerabilities.	Understanding the Exploit Prediction Scoring System (EPSS) integration	ServiceNow
XM Cyber	XM Cyber - Vulnerability Response	Vulnerability Response - Intelligence	Asset Ingestion Link Additional Risk Data Application Risk Measures		Partner
Zafran	Zafran Threat Exposure Management Platform	Vulnerability Response - Intelligence	Ingest vulnerabilities from scanning tools, provide Zafran enrichment and then link to vulnerable items in Vulnerability Response. Intelligence includes mitigation factors, internet-facing, and custom risk score.		Partner
Patch orchestration in solution management					
Microsoft	Vulnerability Response Patch Orchestration with Microsoft SCCM	Vulnerability Response - Patching	Ingest the patch details and correlate the patch, solution, and asset details to suggest Security and IT which assets are missing patches.	Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM	ServiceNow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
HCL	Vulnerability Response Patch Orchestration with HCL Bigfix	Vulnerability Response - Patching	Ingest the patch details and correlate the patch, solution, and asset details to suggest Security and IT which assets are missing patches.	Understanding the HCL BigFix patch orchestration integration with Vulnerability Response	ServiceNow
Tanium	Tanium Patch Management for Vulnerability Response	Vulnerability Response - Patching	Patches CIs through the Vulnerability Response Patch Orchestration module. This can be used in addition to the Tanium VR integration to close the loop from identifying vulnerabilities with Tanium Comply to patching those vulnerabilities with Tanium Patch.		Partner
Import test, policies, results					
Qualys	Qualys Integration for Security Operations	Configuration Compliance	Import test, policies, results.	Qualys integration with Configuration Compliance	ServiceNow
Qualys	Qualys CSPM Integration	Configuration Compliance	Import test, policies, results.		Partner
Tenable	Vulnerability Response Integration with Tenable	Configuration Compliance	Import test, policies, results.	Understanding the Tenable Vulnerability Integration	ServiceNow
Tanium	Tanium Configuration Compliance Integration	Configuration Compliance	Import test, policies, results.		Partner
Palo Alto Networks	Expander Configuration Compliance	Configuration Compliance	Import attack surface and alerts from Expander.		Partner
Trend Micro	Conformity Connector	Configuration Compliance	Import misconfiguration and test results from Trend Micro Cloud One into ServiceNow.		Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Import cloud misconfiguration data (Cloud Security)					
Microsoft	Defender for Endpoint	Configuration Compliance	Import test, policies, results.		ServiceNow
Microsoft	Microsoft Defender for Cloud Integration for Security Operations	Configuration Compliance	Import the cloud resource configuration issues from Microsoft Defender for Cloud and automate remediation workflow.	Microsoft Defender for Cloud Integration for Security Operations	ServiceNow
Palo Alto	Vulnerability Response Integration with Palo Alto Prisma Cloud	Configuration Compliance	Import the cloud resource configuration issues from Prisma Cloud (formerly RedLock) and automate remediation workflow.	Understanding the Vulnerability Response Integration with Palo Alto Prisma Cloud	ServiceNow
Wiz	Wiz Integration for Configuration Compliance	Configuration Compliance	Import the cloud resource configuration issues from Microsoft Defender for Cloud and automate remediation workflow.	Exploring the Wiz Test Results and Issues Integrations with Configuration Compliance	Partner
Rapid7	Rapid7 InsightCloudSec CC Integration	Configuration Compliance	Import cloud misconfigurations and compliance issues		Partner
Lacework	Lacework Code to Cloud	Configuration Compliance	Import cloud misconfigurations and compliance issues.		Partner
Import dynamic, static analysis results and SCA					
Veracode	Vulnerability Response Integration with Veracode	Application Vulnerability Response	Import test, policies, results, DAST findings, SAST findings and SCA findings.	Veracode Vulnerability Integration	ServiceNow
Qualys WAS	Vulnerability Response Integration with Qualys WAS	Application Vulnerability Response	Import Dynamic Scan results from Qualys WAS application.		Partner
Microfocus	Fortify Application	Application Vulnerability Response	Import DAST and SAST findings.	Fortify on Demand	ServiceNow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Fortify	Vulnerability Integration			Vulnerability Integration	
Snyk	Snyk Security for Application Vulnerability Response	Application Vulnerability Response	Import SCA and SAST findings.		Partner
Open source vulnerability intelligence (SBOM workflows)					
Snyk	Snyk API and Web for Application Vulnerability Response	Application Vulnerability Response	Web App Scanning findings API Security findings		ServiceNow
GitHub	Github Application Vulnerability Integration	Application Vulnerability Response	Code Scanning Secret Scanning Dependabot alerts.	GitHub Application Vulnerability Integration	ServiceNow
HCL AppScan	Vulnerability Response Integration with HCL AppScan	Application Vulnerability Response	Import Dynamic Scan results from HCL AppScan.		Partner
Checkmarx	Checkmarx CxSAST Vulnerability Integration	Application Vulnerability Response	Import SAST findings. **Note:** Uses CxSAST API.		Partner
Checkmarx	Checkmarx One Vulnerability Integration	Application Vulnerability Response	Import SAST and SCA findings from Cx VulnerabilityOne API.		Partner
Invicti	Invicti Application Vulnerability Integration	Application Vulnerability Response	• Import applications, scan summaries, results • Import IAST findings. • Import SAST findings.	Invicti Vulnerability Integration	ServiceNow
Synopsys	Vulnerability Response Integration with Black Duck	Application Vulnerability Response	Import SCA findings.	Vulnerability Response Integration with Black Duck	ServiceNow
Sonatype	Sonatype Security for Application	Application Vulnerability Response	SCA – import open source vulnerabilities from Sonatype Lifecycle product.		Partner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
	Vulnerability Response				
Apiiro	Apiiro ASPM for Application Vulnerability Response	Application Vulnerability Response	Application Security Posture Management vulnerabilities, fix issues by assigning to code owners CMDB App is also available.		Partner
Rapid7	Rapid7 InsightAppSec Application VR Integration	Application Vulnerability Response	Fetch apps, scans, vulnerabilities, attacks, attack modules into ServiceNow Vulnerability Response. Web application scanning results.		Partner
NoName (by Akamai)	Akamai API Security Integration for AVR	Application Vulnerability Response	Create and update vulnerable items from NoName on API detections.		Partner
Tenable	Tenable WAS	Application Vulnerability Response	Application security findings.		Partner (Tenable)
Snyk	Snyk Vulnerability Intelligence for SBOM	Application Vulnerability Response - SBOM	Vulnerability Intelligence on Open-source components in SBOM.		Partner
Google (open source)	SBOM Response	Application Vulnerability Response - SBOM	Vulnerability intelligence information for a given version of a package or library.		ServiceNow
Google (open source)	SBOM Response	Application Vulnerability Response - SBOM	License and dependency information for a given version of a package or library.		ServiceNow
Veracode	Vulnerability Response Integration with Veracode	Application Vulnerability Response - SBOM	• Upload exported vulnerabilities to create AVITs. • Prioritize by NVD severity.		ServiceNow
Agile task creation for remediation					

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations (continued)

Integration	Product installation	Category	Use case	Setup Guide	Built by
Atlassian	Vulnerability Response Integration with Atlassian Jira	Vulnerability Response - Agile Tools	Create Jira tasks/ issues for Application and Container vulnerabilities. Bi-directional status updates between Vulnerability Response and Jira.	Understanding the Atlassian Jira integration with Vulnerability Response	ServiceNow

Custom integrations

You can manually create integrations not available in the ServiceNow Store. See Manually create a vulnerability integration for more information.

Configuring and managing integrations

- You can install, configure, schedule, and launch many integration applications.
- For integrations supporting multiple deployments, refer to Create domain-separated imports for an integration.
- The Rapid7 Vulnerability Integration application can be installed from Setup Assistant, but its configuration isn't supported within Setup Assistant. See Install the Rapid7 Vulnerability Integration for more information. You can install, configure, schedule, and launch on-demand many of the integration applications from within Setup Assistant.

Performance and timeout handling

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it's also older than one hour. If it is, this indicates that the import queue entry is stuck, and it's timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Related topics

Review Unified Security Exposure Management integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Review Unified Security Exposure Management integrations

The integration dashboard provides an overview of the installed third-party applications and the status of the integration runs.

In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you select any part of a report, a list opens to provide detailed information.

Access the Integration Dashboard

To open the dashboard, navigate to **Workspaces** > **Security Exposure Management Workspace** > **Administration** and select **Review** on any integration.

Use cases

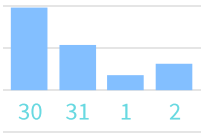
For examples of how different people in your organization would use this dashboard, see these use cases.

User	Dashboard use

Data visualization

Note: To learn more about a widget, select the information icon ⓘ.

Overview

Metrics	Type	Description
Integration runs	Vertical  Bar	The number of integration runs completed for each integration. Shows both successful and failed runs in the past 7 and 30 days. The most common causes for a failed run include: • Network interruption • Bit decay in the data transfer resulting in corrupted data during the transform If you encounter any of these conditions, select the **Full data import** check box, click **Execute Now**, and rerun the integration.
Ingestion health	Highlights	Provides information on the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview (continued)

Metrics	Type	Description
		• Import queue processing time. • Import queue wait time. • REST API time.
Processing health	Multiple lines	Provides performance metrics for assignment rules, remediation task rules, CI lookup time, risk rules, and VI creation time for the last 30 days, to identify the cause for any deviations in performance. The performance is calculated based on the time taken for each activity. These parameters are calculated and associated at the integration run level. Each parameter is color coded for easy identification.

Note: Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data.

Integrations

Name	Description
Name	Name of the integration.
Active	Status of the integration whether active or not.
Run	Run schedule of the integration
Day	Day on which the integration runs.
Time	Time at which the integration runs.
Last run status	Status of the last integration run whether failed or successful.
Notes	Notes

Note: If a Tenable.sc integration run fails for any reason, the authentication token for Tenable.sc automatically expires and a message is displayed on the Vulnerability Integration Process record. A new token is automatically generated for the next integration process. All the integration processes, failed and successful, are displayed on the Vulnerability Integration Process tab on the Vulnerability Integration Process record.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing. The **Last Record Processed** field is updated based on what is defined in the following system properties:

- sn_sec_cmn.record_threshold_heartbeat: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- sn_sec_cmn.maximum_heartbeat_delay: Defines the time after which the import queue entry must be timed out.

Using Unified Security Exposure Management

Unified Security Exposure Management provides a comprehensive platform for managing vulnerabilities and ensuring compliance across your organization. By unifying workflows across Vulnerability Response (VR), Application Vulnerability Response (AVR), Container Vulnerability Response (CVR), and Configuration Compliance (CC), you can view all findings in one place, streamline workflows and improve overall efficiency.

Create a dashboard in the Findings view page

As a vulnerability manager and analyst, create a configured dashboard using the visualization library widgets, and use the active widgets to drill down to specific findings.

Before you begin

Roles required:

- sn_vul.write_all
- sn_vul.app.write_all
- sn_vulc.write
- sn_vul_container.write_all

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select the **Create filter** icon.
3. On the *Create new dashboard* pop-up window, fill in the fields.

Create new dashboard fields

Field	Description
Name	Name of the filter.
Applies to	The modules the filter applies to.
Description	Description of the filter.
Condition	The condition to retrieve the records.
Refresh daily	Updates the visualization information every day.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **Next**.
5. Select the required visualization widgets.
6. Select **Create**.
   The dashboard is created and the widgets start fetching data.
7. To update the dashboard, select the **Edit filter** icon.

Reclassify unclassed hardware

Reclassify unclassed hardware by updating the lookup rules.

Before you begin

Role required: sn_sec_cmn.admin

About this task

The Host Import Map [sn_sec_cmn_src_cmdb_map] table displays the payload's incoming variables and their corresponding assignments in the Discovered Items table. Occasionally, discrepancies in naming conventions between the scanner and Discovery can lead to the hardware being left unclassified. While creating a new Unclassed Hardware CI, ensure that the name in the payload contains only the Host Name. Later, when Discovery identifies the asset, it can be reclassified into the appropriate CI class. If needed, a script can be written to generate a derived value that aligns with the CIs name in both Discovery and the Configuration Management Database (CMDB).

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from Discovered Items isn't supported.

Procedure

1. Navigate to the Host Import Maps [sn_sec_cmn_src_cmdb_map] table.
2. Select a source.
3. From the Target field list, select **Name**.
   The **Use script** check box becomes visible.

   Note:

   - The script is available only if **Name** is selected from the Target field list.
   - To add a script for other options in the Target field list, you must disable the UI policy by:
     - Disabling the 'Set Use script false'.
     - Disabling the 'Show or Hide Use Script'.
     - Removing the condition 'target field is name' in the 'Show or Hide Script policy'.
   - The Host Import Maps table is updated with two new columns: Script and Use script.

4. Select the **Use script** check box.
   The **Script** field displays the default script but you have an option to create a custom one. In this field, you can specify the source and derived values to align with the database's naming convention. The value generated by the script is stored in sourcePayload['DERIVED'][rule.source_field]. Ensure that the CI lookup rules are adjusted to utilize source payload, derived, and targeted attribute values when checking in the corresponding tables.
5. To apply the script to older duplicate records, do the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **All** > **Vulnerability Response** > **Discovered Items**.

b. Select the duplicate records.

c. In the Action on selected rows list, select **Reapply CI Lookup rules**.
It shows a match to an existing asset.

6. To apply the script for Tenable.io, do the following:
   a. Navigate to **Vulnerability Response Host Import Maps**.
   b. Select the script for the row with NetBIOS, HOSTNAMES, and FQDNS name as the **Source** field.
   c. Update the script for each element.

   Note: For Tenable.io, the scanner returns an array for NetBIOS, HOSTNAMES, and FQDNS name, for which the script doesn't work as expected.

   Because the Host Import Map for Tenable.io contains **netbios_name** in the **Source** field, you must write a script. During lookup, another source field **NETBIOS** is used, which has an array of values. So a new row is added in the table, and the same logic must be written in a loop in the script. Similarly, for **FQDNS** and **HOSTNAMES**.

7. To apply the script for Rapid7, do the following:
   a. Navigate to **All** > **Vulnerability Response Host Import Maps**.
   b. For Rapid7 rows with FQDN and HostName, update the Lookup Method to Script.

   Note: For Rapid7, the CI Lookup method is set to Field matching for FQDN and Hostname, which helps to prevent it from using the script.

Bulk edit in the Security Exposure Management Workspace

In the Security Exposure Management Workspace, the bulk edit feature enables you to update multiple findings simultaneously, streamlining the management and remediation process.

With bulk edit, you can select multiple vulnerabilities and apply consistent changes, such as assigning remediation owners, updating status, adding work notes, requesting exceptions, and requesting false positive. This saves time and effort by eliminating the need to edit vulnerable items individually, promoting efficient and consistent management of vulnerabilities.

Roles required:

You can perform the following tasks using the bulk edit feature in the Security Exposure Management Workspace:

- Assign records to an assignment group in bulk
- Request bulk exception in the Vulnerability Manager Workspace
- Remove assignments for host vulnerable items in bulk
- Bulk edit for false positive in the Vulnerability Manager Workspace
- Close records in bulk in the Vulnerability Manager Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using bulk edit in the Security Exposure Management Workspace

In the Security Exposure Management Workspace, you can update the state of the records, request exceptions and false positives, and assign records to an assignment group multiple findings simultaneously using the bulk edit feature.

Update the state of records in bulk in the Security Exposure Management Workspace

Update the state of multiple findings concurrently according to their remediation progress using the bulk edit feature in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **List**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the **Record Selection** field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the **Record Selection** field.
4. Select the **Bulk Edit** button.
5. On the Bulk Edit modal, fill in the following fields to update the state of the records.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: Records with invalid CI or CI decommissioned aren't updated.
State	Change for the **State** in the record. Choices are: ○ Do Not Update ○ Open ○ Under Investigation ○ Awaiting Implementation ○ Deferred For more information, seeRequest bulk exception in the Vulnerability Manager Workspace. ○ Closed For more information, see Bulk edit for false positive in the Vulnerability Manager Workspace ○ Resolved **Note:** Only the records for which the state transition is valid are updated.
Work notes	Text that you enter to describe the changes.

6. Select#**Edit**.

   A bulk edit asynchronous job updates the selected records.

Bulk edit host vulnerable items with patches and solutions

Recommend a patch or solution for multiple host vulnerable items concurrently using the bulk edit feature in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

About this task

In the Bulk edit modal, while adding a preferred solution and patch, you can also unassign or assign multiple host vulnerable items (VITs) to an assignment group simultaneously.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.

   Note: The selected records must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the List page, under Host Vulnerable items, open the Active or All list.
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the **Record Selection** field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the **Record Selection** field.
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the Record Selection field of Bulk Edit modal.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the Record Selection field of Bulk Edit modal.
4. Select the **Bulk Edit** button.
5. On the Bulk Edit modal, fill in the fields to recommend a patch or solution for multiple host vulnerable items.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records (VITs) in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Change for the **State** of the host vulnerable items. You can add preferred solution and patch only when you choose the following states. ○ Do Not Update ○ Open ○ Under Investigation ○ Awaiting Implementation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Preferred Solution	Solution that is targeted for remediating all the vulnerable items selected for bulk edit. Select the change for the **Preferred Solution** field in the vulnerable item. Choices are from a lookup list of available preferred solutions for the VITs selected. **Note:** ○ The set of available preferred solutions is an intersection of all potential solutions of the vulnerabilities across all selected VITs. ○ When selecting **Record selection** > **Vulnerability Entry** for a bulk edit, all VITs for the vulnerability will be set to the selected preferred solution. **Note:** This operation doesn't set the **Preferred solution** at the vulnerability entry level. Setting the **Preferred solution** at the vulnerability entry level would set the **Preferred solution** for all new VITs going forward. The bulk edit only modifies the current set of VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message is displayed asking you to select VITs with different criteria for setting the **Preferred solution**. ○ The total number of solutions that can be shown in the lookup list is limited to 170. If there are more than 170 solutions, a warning message is displayed. The updated value is shown in the Vulnerable item list view.
Preferred patch	Patch that is targeted for remediating all the vulnerability items selected for bulk edit. **Note:** ○ You must install Patch Orchestration to view the list preferred patches. ○ The set of available preferred patches is an intersection of all potential patches across all selected VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message displays asking you to select VITs with different criteria for setting the **Preferred patch**. ○ The total number of patches that can be shown in the lookup list is limited to 170. If there are more than 170 patches, a warning message is displayed.
Unassign	All the selected items are unassigned for assignment group and remediation owner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: ○ This field appears when you select the State as Do Not Update. ○ When you unassign records, a remediation task is created which is sent for approval. For more information, see Remove assignments for host vulnerable items in bulk
Assignment group	Assignment group for the records. All the active assignment groups appear in this field. **Note:** This field is deactivated when you select the Unassign check box.
Work notes	Text that you enter to describe the changes.

6. Select **Edit**.

Result
A bulk edit asynchronous job updates the selected host vulnerable items (VITs). The preferred solution and patch are added to the relevant host vulnerable items (VITs). Open a host vulnerable item, and view the preferred solution and patch in the Remediation section of the Details tab.

Assign records to an assignment group in bulk

Assign multiple records findings concurrently to an assignment group using the bulk edit feature in the Security Exposure Management Workspace.

Before you begin
Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **List**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Select the check box next to each item if you want to use the **Only Selected Items** option in the Record selection field.
- Apply filters if you want to use the **All records that match filter** option in the Record selection field.

4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to assign the records to an assignment group.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: - *Only Selected Items*: Select this option if you want to update the records you selected using the check box. - *All records that match filter*: Select this option if you want to update the filtered records. - *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. - *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items. - *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** - Records with invalid CI or CI decommissioned aren't updated. - Only the records in the Open, Under Investigation, Awaiting Implementation or Deferred state are updated.
Assignment group	Assignment group for the records. All the active assignment groups appear in this field. **Note:** This field is deactivated when you select the Unassign check box for VITs.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.

Result
Open a record for which you updated the assignment group and navigate to the Overview tab, the user group to which the record is assigned appears in the **Assignment group** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remove assignments for host vulnerable items in bulk

Remove yourself or your groups from the#**Assigned to** and#**Assignment group** fields on the findings if you determine that the records aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

About this task

The #unassign#feature is applicable for records in any state other than Closed or Resolved. When you remove assignments for host vulnerable items using the bulk edit feature, only relevant records are updated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. On the List page, under Host Vulnerable items, open the Active or All list.
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the Record Selection field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the Record Selection field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to remove assignments in bulk.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, Awaiting Implementation, or Deferred state are updated.
State	Select the state as Do Not Update.
Unassign	All the selected vulnerable items are unassigned from assignment group and remediation owner. **Note:** ○ This field appears when you select the State as Do Not Update. ○ When you unassign records, a remediation task is created which is sent for approval.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.
   A remediation task is created with the selected host vulnerable items (VITs).

   Your request is submitted for approval and the approver receives an email notification about your request.

   The state of the host vulnerable items (VITs) and remediation task (VUL) transitions to In Review. If a remediation task is updated with this feature, the **Assigned to** and **Assignment group** fields on all of its associated VITs are also cleared upon approval of your request.

Result

In the Security Exposure Management Workspace, on the List page, navigate to **Exception Requests** > **All** and open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The **Assigned to** and#**Assignment group** fields of all the host vulnerable items are cleared.
Rejected	The **Assigned to** and#**Assignment group** fields of all the host vulnerable items are not updated.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Request bulk exception in the Security Exposure Management Workspace

Request an exception for multiple findings concurrently using the bulk edit feature instead of manually selecting each record.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

About this task

When you request an exception for one or more records from the Bulk edit modal, a remediation task is created with the selected records.

Note: The Application Vulnerable Items (AVITs) from the scanners with the **Manage exceptions in ServiceNow** parameter set to false are not updated.

- If you select AVITs from various scanners, some with the **Manage exceptions in ServiceNow** parameter set to true and other set to false, the AVITs linked to the scanners with he **Manage exceptions in ServiceNow** parameter set to false are not updated.
- If you select AVITs from only the scanners with the **Manage exceptions in ServiceNow** parameter set to false, the *Defer* option does not appear in the **State** field in the Bulk Edit modal.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:
   - Select the check box next to each item if you want to use the *Only Selected Items* option in the Record selection field.
   - Apply filters if you want to use the *All records that match filter* option in the Record selection field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the following fields to request an exception for multiple findings (VITs, AVITs, CVITs, or TRs) simultaneously.

Bulk Edit modal fields

Field	Description
Record selection	Records to update. Choices are: ○ *Only Selected Items*: Select this option if you want to update the records you selected using the check box. ○ *All records that match filter*: Select this option if you want to update the filtered records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items. ○ *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Select the *Deferred* state to request an exception for the selected records. **Note:** ○ When you select this option, the Reason, Short description, Until, and Additional information fields appear. ○ When you defer records, a remediation task is created and this task is sent for approval.
Reason	Reason for deferring records: ○ Awaiting Maintenance Window ○ Fix Unavailable ○ Risk Accepted ○ Mitigating Control in Place ○ Other **Note:** The **Reason** field appears when you select the State as Deferred.
Short description	Brief note describing the reasons for deferral request. This information reflects in the **Description** field of the remediation task that is created for a deferral request. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Until	Date till which the record remains deferred.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This field appears when you select the State as Deferred.
Additional information	Any other necessary information. This information reflects in the Additional Information field in the Overview tab of the remediation task that is created for deferral and closed-false positive requests. If your deferral request is approved, this additional information appears as deferral notes for both VIT and remediation task. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.
7. On the Take Questionnaire modal, answer the questions and click#**Submit**.

   A remediation task is created containing the records that you selected. Your request is submitted for approval and the State of the records changes to#n Review.

   Note: The **Take Questionnaire** modal appears only when the questionnaire is enabled for exception requests in the Exception Management form. For more information on configuring a questionnaire for exception requests, see Configure Exception Management for Vulnerability Response, Configure Exception Management for Application Vulnerability Response, and Configure Exception Management for Container Vulnerability Response, and Configuration Compliance Exception Management overview.

   The approver receives an email notification about your request.

Result

In the Security Exposure Management Workspace, on the List page, navigate to **Exceptions** > **All**, open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The state of the Remediation task transitions to Deferred with the given Reason as sub-state. The state and reason are rolled down to the records.
Rejected	The state of the Remediation Task and its records doesn't change.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Bulk edit for false positive in the Security Exposure Management Workspace

Mark one or more records (VITs, AVITs, CVITs, or TRs) as false positive concurrently using the bulk edit feature from the Security Exposure Management Workspace instead of manually selecting each item.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

About this task

When you raise a false positive request for one or more records from the Bulk edit modal, a remediation task is created with the selected records.

Note: When you raise a false positive request for the Application Vulnerable Items (AVITs) using the bulk edit feature, the AVITs from the scanners with the **Manage False positive with Servicenow** parameter set to false are not updated.

- If you select AVITs from various scanners, some with the **Manage False positive with Servicenow** parameter set to true and other set to false, the AVITs linked to the scanners with the **Manage False positive with Servicenow** parameter set to false are not updated.
- If you select AVITs from only the scanners with the **Manage False positive with Servicenow** parameter set to false, the *False positive* option does not appear in the **Reason** field in the Bulk Edit modal.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **List**.

   Note: The selected records must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the List page, open Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:
   - Select the check box next to each item if you want to use the *Only Selected Items* option in the **Record selection** field.
   - Apply filters if you want to use the *All records that match filter* option in the **Record selection** field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to request false positive for multiple records.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ *Only Selected Items*: Select this option if you want to update the records you selected using the check box. ○ *All records that match filter*: Select this option if you want to update the filtered records. ○ *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items. ○ *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Select the **Closed** state.
Reason	Select the Reason as False positive. **Note:** ○ When you select this option, the Short description, and Additional information fields appear. ○ A remediation task is created when you mark the records as False-positive and this task is sent for approval. **Note:** The **Reason** field appears when you select the State as Deferred or Closed.
Short description	Brief note describing the reasons for Closed-False positive request. This information reflects in the **Description** field of the remediation task that is created for a Closed-False positive request. **Note:** This field appears when you select the State as Deferred or Closed-False positive.
Additional information	Any other necessary information. This information reflects in the Additional Information field in the Overview tab of the remediation task that is created for Closed-False positive request. If your false positive request is approved, this additional information appears as notes for both VIT and remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This field appears when you select the State as Deferred or Closed-False positive.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.
7. On the Take Questionnaire modal, answer the questions and select **Submit**.
   A remediation task is created with the selected records. Your request is submitted for approval and the State of the remediation task changes to#n Review.

   Note: The **Take Questionnaire** modal appears only when the questionnaire is enabled for false positive requests in the Exception Management form. For more information on configuring a questionnaire for false positive requests, see Configure Exception Management for Vulnerability Response, Configure Exception Management for Application Vulnerability Response, and Configure Exception Management for Container Vulnerability Response.

   The approver receives an email notification about your request.

Result

In the Security Exposure Management Workspace, on the List page, navigate to **Exceptions** > **All**, open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The state of the Remediation Task transitions to Closed with the Reason as False positive. The state and reason are rolled down to the records.
Rejected	The state of the Remediation Task and its records doesn't change.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Close records in bulk in the Security Exposure Management Workspace

Close multiple records (VITs, AVITs, or CVITs) concurrently using the bulk edit feature in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **List**.
2. On the List page, open Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
3. Perform one of the following:
   - Select the check box next to each item if you want to use the Only Selected Items option in the **Record Selection** field.
   - Apply filters if you want to use the All Vulnerable Items that match filter option in the **Record Selection** field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to close the selected records.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Select the state as Closed.
Reason	Reason for closing records: ○ False Positive **Note:** When you select this option to mark the records as false- positive, the Reason, Short description, and Additional information fields appear. For more information on bulk edit for false positive, see Bulk edit for false positive in the Vulnerability Manager Workspace. ○ Cancelled ○ Fixed

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The reasons, Cancelled and Fixed are not applicable to CVITs.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.

   A bulk edit asynchronous job updates the relevant records.

Use the List view in the Security Exposure Management Workspace

As a vulnerability manager, security manager and analysts, you can view remediation progress on records, drill down into findings, and view the status of their approval requests and exceptions.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management**.
2. Select the **List** icon.
   The consolidated list of records, remediation tasks, remediation efforts, libraries are displayed. For more information on the type of lists on the List page, see Security Exposure Management Workspace List view.
3. **Optional:** Select **My Lists** to create a list.
   For more information on how to create a list, see Create a customized list of records.
4. Refer to the following table for the actions that you can perform on the List page.

UI action	Description
Open a remediation effort	With **Active** selected under the **Remediation efforts** list, select a remediation effort link to open it. A Remediation Effort is a set of records that are associated with a watch topic. The records listed on a remediation effort are static. They are not updated by new import data or changes that you make to watch topics.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
	The related list items on the remediation effort record permit you to view overall remediation progress and status on the records associated with it. For more details and UI actions you can perform from a remediation effort, see Use Remediation Effort records.
To the left of the Number column with a list displayed, roll over a row and select the small information icon **(i)** for a record.	Details about the records are displayed in the right side panel of the page. Details include: ○ Assignment group ○ Vulnerability ○ Assigned to ○ Short description ○ Description You can edit the fields. If the Active check box is displayed, you can activate or deactivate the record. Select the **Update** to save your changes.
Refresh the list	With the refresh icon on the top right of the page, reload the current page.
Reset widths	Select the gear icon to adjust column widths on your lists. A copy of the original list is saved under **Your Lists**.
Copy the URL for the displayed page	Copy the URL for use elsewhere.
Export the page	In the modal, enter the file and delivery types and select **Export**.
Refine filters for the data on the page.	Select a column and expand the three vertical dots menu to view options that further filter the data in the column. For example, you might prefer to filter the Assignment group column from the active remediation tasks list by a specific assignment group.
Filter out items or match items from a row in a column	Select a cell in a column and refine the data displayed by choosing one: ○ Show Matching - display only items that match the selected cell in the column. ○ Filter Out - Filter out the items from the column that match the selected cell in the column.

5. You can create an application vulnerable item from the **Active** or **All** lists under *`Application Vulnerable items`* by selecting the **New** button on the upper right.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a customized list of records

You can create a customized list in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select the **List** icon and click **My Lists**.
3. Select **New list**.
4. In the New List modal, click **Start from existing** and search in the List choice list for an existing list to use as a template.
5. Edit the List Name.
6. Add filters.
   For example, you might want to create a list of active records for a particular scanner that you want to monitor for rescans. You might use the filters: `Active is true`, and `Source contains (name of your scanner)`.
7. Edit the columns that you want displayed on your list.
8. Click **Create**.
   Your new list is displayed.
9. Alternatively, click **Create your own**, enter a name, followed by **Select Source**.
10. Start typing in the field and select from the sources that display for your new list.
11. Click **Create**.
    Your new list is displayed.

    Note: If you leave the list module, the list displayed when you exit is the list you see when you return.

12. To delete a list, with the list displayed, click the gear icon on the upper right of the page.

Create a remediation task manually in the Security Exposure Management Workspace

You can create remediation tasks manually from the findings on the List page of Security Exposure Management Workspace. You can also create remediation tasks from the drill-down lists that appear when you click on the visualizations on the Home page.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

About this task

Manual creation of Remediation Tasks (RTs) in Security Exposure Management Workspace offers granular control over remediation task management by enabling you to group records (VITs, CVITs, AVITs, or TRs) into remediation tasks dynamically in real time.

You can create a remediation task manually, when you want to:

- group vulnerable items by something other than the Remediation Task Rules criteria. For example, you can create remediation tasks for a particular manager, or for active, new exploits, such as ransomware that includes different vulnerabilities.
- group ungrouped records.
- remediation task rules are inactive.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **List**.
2. On the List page, open the **Active** or **All** list in one of the following lists:
   - Host Vulnerable Items
   - Application Vulnerable Items
   - Container Vulnerable Items
   - Configuration Test Results
3. **Optional:** Select the check box of the records you want to update and then select the Selected items option in the Record selection field on the Create Remediation Task modal.
4. Select **Create Remediation Task**.
5. On the Create remediation task modal, fill in the following details.

Create remediation task modal

Field	Description
Record selection	○ **Selected items**: Updates the selected records only. ○ **All items**: Updates all the records in the list.
Short description	Brief note about the remediation tasks.
Grouping criteria	Choices are: ○ **Assignment group**: Records with same assignment group are grouped into one remediation task. ○ **Assignment group and configuration item**: Records with same assignment group and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	configuration item are grouped into one remediation task. ○ **Assignment group and vulnerability**: Records with same assignment group and vulnerability are grouped into one remediation task. ○ **Assignment group and risk rating**: Records with same assignment group and risk rating are grouped into one remediation task.
Managing records in other remediation tasks	Choices are: ○ **Skip records for new remediation tasks**: No action is taken on the records that are part of other remediation tasks. ○ **Move to new remediation tasks**: Records that are part of other remediation tasks are transferred to new remediation tasks. ○ **Keep in both current and new remediation tasks**: Records that are part of other remediation tasks are kept in both old and new remediation tasks.

6. Select **Create remediation task**.

Result

Remediation tasks are created based on the grouping criteria. An email notification is sent to the remediation owners in the assignment group, informing them that a remediation task has been created and assigned to their group. For examples on how remediation tasks are created based on the grouping criteria, see Examples for remediation task creation in the Security Exposure Management Workspace.

Enable or disable the import of test results for a Qualys test group

In Security Exposure Management Workspace control the import of the test results for the tests in a Qualys test group by using the **Enable/Disable import** button, which is available in the test group's record view.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management** > **Lists**.
2. In the **Libraries**, under the **Test Groups** list, open a Qualys test group in the record view.
3. Disable the import of the test results associated with a Qualys test group by selecting the **Disable import** button.
   From the upcoming data ingestion, the test results aren't imported for the Qualys test group. The value in the **Is Import disabled** field changes to *true*.
4. **Optional:** Enable the import of the test results by selecting the **Enable import** button.

Modify the severity for a CVE or TPE

As a vulnerability manager or analyst, you can modify the severity level of Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, or sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin, or sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.admin, sn_vulc.remediation_owner for configuration test results (CTRs)

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management** > **Lists** > **Libraries**.
2. Open the appropriate entry:
   - **CVEs (NVD)**: To modify the severity of a CVE.
   - **TPEs**: To modify the severity of a TPE.
3. Select **Modify severity** from the **More Actions** icon 
4. Select the new severity level from the drop-down.
5. Provide a justification for your update.
6. Select **Submit**.

Note:

- You can revert to the original source severity using the **Reset Severity** option from the **More Actions** menu. This option appears only after you modify the severity.
- The **Modified severity** field appears only when you change the source severity. If you reset it to the original value, the field is removed.
- The system will use the **Modified severity** for risk calculations starting from the next scheduled job onwards. If the severity is reset, the original source severity will be applied instead.

Use Remediation Effort records

When Vulnerability managers and analysts create remediation efforts (REs), remediation Tasks (VUL) are automatically assigned to IT teams for remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

You have to create a remediation effort before you can use it to monitor remediation progress on Remediation Tasks.

Role required: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin, or sn_vulc.admin

Procedure

1. If not selected, in the upper left, click the List icon.

   The List view with active Remediation Effort records is displayed.

2. From the List view landing page, with Active Remediation Efforts selected in the filtered lists, click a record to open it.
   The record displays. You can view the remediation tasks and records that are associated with the selected remediation effort.
3. Refer to the following table for the actions that you can perform on the remediation effort record.

   After you create a record, it may take a few minutes for the remediation tasks and large numbers of records to display.

UI action	Description
Add a tag	To the right of the header, click the small tag icon. You might want to add text that further helps you identify this record. For example, you might want to add a tag that this record has PCI or other critical data.
Add a work note to the record	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel.
Update the record	On the **Details** tab, for all fields that are editable, click a field to select it, make your changes, and click **Save** to update the record.
When displayed, click the filter icon to refine the data on the displayed page	With the **Remediation Tasks** or **Vulnerable Items** tabs selected, On the far right, click the filter icon to show the filters that apply to the tab. In the panel that is displayed, click **Advanced view** to add or change filter conditions for the items on the page. Click **Update** to save your changes. For example, on the **Vulnerable Items** tab, you might prefer to add the Age field and enter a range to display only records from a specific time period. Records that match the conditions that you set are displayed in the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
Refine filters for items in a column	Select a column and click the three vertical dots menu expand it and enter conditions to refine and group the data in the column.
Filter out items or match items from a row in a column	Say, for example, you want to view only records that have a specific vulnerability. From the list of records, select the row of the record in the **Summary** column. Click the vertical dot menu that is displayed and choose one: ○ **Show matching** - show all the other records that have this vulnerability. ○ **Filter out** - show all records that don't have this vulnerability.
Activate/deactivate a record	If you mark a remediation effort inactive (**Active** check box not selected) prior to fixing all its records, any remaining, active records on the record will be moved to a new remediation effort when you create one for this watch topic.

4. From the Remediation Tasks and Vulnerable Items tabs, you can drill down into an individual Remediation Task (VUL) and Vulnerable item (VIT) records.

What to do next

If you want to create a remediation task on-demand from a remediation effort, see Create a remediation task on-demand from Remediation Effort in the Vulnerability Manager Workspace.

Create a remediation effort in the Security Exposure Management Workspace

A remediation effort record is a static list of records that you create from a watch topic in the Security Exposure Management Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

You use remediation efforts to hand off the tasks IT teams use to fix vulnerabilities and mis-configurations.

- You can edit existing remediation efforts.
- Create remediation efforts that are created automatically on the dates and times that you set.
- Transfer records from existing remediation efforts into a new remediation effort.

The **Create Remediation Effort** button is disabled when the watch topic is inactive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Exposure Management Workspace** > **Watch Topics**.
2. On the Watch Topics page, select a watch topic that you want to create a remediation effort for.
3. To view the records that are associated with the selected watch topic, under the record header, click **Vulnerable Items**, **Application Vulnerable Items**, **Container Vulnerable Items** or **Configuration Test Results** tab in their respective watch topics.

   The records display.

   For example, in the header under the Vulnerable Items tab, you can view the total number of records that this watch topic has.

   The following columns and data are displayed:

Columns in the Vulnerable Items tab

Column	Description
Number	The record number.
Summary	Description of the vulnerability.
Configuration item	The asset associated with the vulnerability.
Risk rating	Quantified Risk Score separating records into Critical, High, Medium, Low, and None.
State	Status of the record.
Remediation status	Status of remediation for a record.
Assignment group	Assignment groups responsible for remediation. Assignment of records to groups is based on the assignment rules that you create.
Remediation effort	If it is assigned to a remediation effort, each record lists its assigned remediation effort. After it is added to a remediation effort, a record won't be added to any other remediation efforts that you create.
Assignment group	Assignment groups responsible for remediation. Assignment of records to groups is based on the assignment rules that you create.
Remediation effort	If it is assigned to a remediation effort, each record lists its assigned remediation effort. After it is added to a remediation effort, a record won't be added to any other remediation efforts that you create.
In remediation task	If `true`, this value indicates that a record is already in a remediation task. Records can be in multiple remediation tasks, but a record can be added only to one remediation effort.
Exploit exists	Indicates if a known exploit exists for a record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Description
Last opened	Date when the record was last opened in your ServiceNow AI Platform. If the record was closed and then reopened, this is the last time the record was reopened.

4. To create a remediation effort, click **Create Remediation Effort**.

   When you create remediation effort, records already in existing remediation efforts are not added to any new remediation efforts that you create from this watch topic.

   As records are updated or new records are created in watch topics, you can create remediation efforts.

5. Alternatively, you can Create a recurring remediation effort in the Security Exposure Management Workspace.

   The **Edit** button is available in the menu for existing remediation efforts. You have the option to modify the fields and conditions from a modal that is displayed. Any changes you make and save to the remediation effort record do not affect any of the other remediation efforts you have already created from the watch topic.

6. In step 1 of the Create Remediation Effort modal, fill in the fields.

   In the Short description field, enter text that describes the recurring remediation effort and helps you locate and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts.

7. In step 2, Task generation, choose one method from the list to bundle the records in the remediation tasks that you generate from this remediation effort after it is created.

Option	Description
By Assignment group	Records with same assignment group are bun dled into one Remediation Task.
By Assignment group and configuration item	Records with same assignment group and Configuration Item are bundled into one Re mediation Task.
By Assignment group and (vulnerability or configuration test)	Records with same assignment group and Configuration Item are bundled into one Re mediation Task.
None (No remediation tasks are created).	Use this method if you want to add records manually to a remediation task for this effort. See Create a remediation task on-demand in the Vulnerability Manager Workspace.

8. To automatically refresh the duplicate host vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** check box.

   Note: This check box is available only for Host Vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. In step 3, Transfer, verify how many records you want to add to the remediation effort and see how many records are available for transfer from other active remediation efforts.

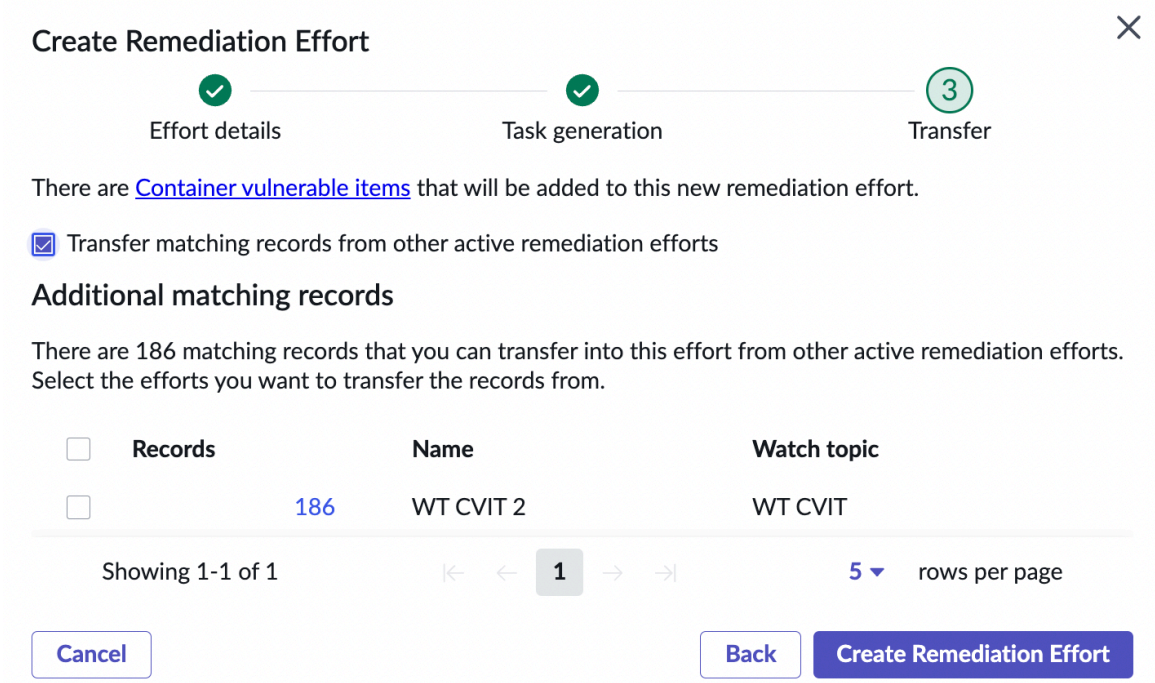
   If there are no new, active records to add, the following text is displayed:

   `There are no available active records that you can add to this new remediation effort.`

   Any additional records that are available for transfer to this effort are listed under `Additional matching records.`

   Select the **Transfer matching records from other active remediation efforts** check box and then select the check boxes for the records you want to transfer from other active remediation efforts.

   Version 18.0 Create Remediation Effort

   After you click **Create Remediation Effort**, in a few moments, the new remediation effort is displayed. Depending on the number of records, it may take some time to populate the new record. A message indicates if the record is still populating.

   The new remediation effort is created with any records that are available from the watch topic used to create it, in addition to any records that you selected for transfer from existing efforts.

   If you select records to transfer from an existing effort, and the existing effort transfers all of its records into your new effort, the remediation effort you moved the records from is closed. For more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by the records transfer, see Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces.

   Note: If there are not any records available from the watch topic, or any records selected for transfer, the **Create Remediation Effort** button is deactivated.

   The *`Populate Efforts`* scheduled job runs every 10 minutes to populate the data in the widgets based on the condition selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Click Remediation Progress tab to view the remediation progress. Click any item to view details including record type, risk score, risk rating, percentage of records remediated, records in deferred and non-deferred state and total number of records, conditions used in the watch topic, and remediation status. The Remediation Status information such as Remediation target and Remediation status is rolled up from the Vulnerable Items table. The highest record risk score is rolled-up from the Vulnerability Calculators table while risk score is rolled up from the **Vulnerability Rollup Calculators** > **Remediation Effort Rollup**.

The Remediation Tasks tab displays the tasks for all types of issues. The fields are populated when the following scheduled jobs run. They are executed automatically every 15 minutes:

- Rollup application vulnerable item values to vulnerability and group.
- Rollup container vulnerable item values to vulnerability and group.
- Rollup test result values to test result group and configuration test.
- Rollup vulnerable item values to vulnerability and group.

In the Lists view, you can view the Remediation efforts, Remediation Tasks, Vulnerable Items, Configurations Test Results and so on. You can open a remediation task or a vulnerable item and view the Details page. Click the More Actions ellipses and click **Start Investigation** to resolve a remediation task.

10. **Optional:** You can also edit existing recurring remediation efforts.

    (Optional) If there is an existing recurring remediation effort for a watch topic, **Edit recurring effort** is available from the menu in the upper right of a watch topic. Choose this option to edit the recurring effort.

    Any changes you make and save to the remediation effort record do not affect any of the other remediation efforts you have already created from the watch topic.

Create a remediation task on-demand from Remediation Effort in the Vulnerability Manager Workspace

Create a remediation task on-demand from a remediation effort. If you create a remediation task on-demand, you choose the records you want to add manually.

Before you begin

Role required: sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin

About this task

For version 18.0 of Vulnerability Response, you cannot create a Remediation Task from the record view of a Remediation Effort.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace**.
2. At the top left of the workspace with the Home page displayed, click the **List** view icon, to display the List landing page.
3. Under Remediation Efforts, click either **Active** or **All**.
4. From the list that is displayed, click a record to open it.
   The overview tab of the record is displayed.
5. Click the **Vulnerable Items** tab.
   The list of records displays.
6. To create a new remediation task, in the Number column, select the records you want to add.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Click **Create remediation task**.
8. In the modal that is displayed, fill in the fields.

Field	Description
Short description	Enter text that can help you identify this remediation tasks easily from your existing remediation tasks.
Assignment group	Choose an assignment group for the tasks. Use the filter to help you locate the group you want.

9. Click **Create**.
10. The new remediation task is displayed with the active records you selected.

Create a recurring remediation effort in the Security Exposure Management Workspace

You can create and schedule recurring remediation efforts that are generated automatically on the dates and times that you set.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

You can automatically create recurring remediation efforts on a schedule that helps you track vulnerabilities that might come up and require immediate and ongoing attention.

Starting with version 18.0, because you can't create a recurring remediation effort for an inactive watch topic, the **Create Recurring Effort** option is inactive. If you deactivate a watch topic that has a recurring effort already scheduled, then a new remediation effort is not created until the watch topic is activated. Also, the **Effort recurrence** and **Next recurrence date** details disappear on the upper right. After you activate the watch topic, a remediation effort is created at the upcoming schedule.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. On the Watch Topics page, select a watch topic that you want to create a recurring remediation effort for.

   You can create one recurring remediation effort per watch topic.

   Note: You cannot transfer records from recurring remediation efforts into new remediation efforts. However, you can transfer records from existing, non-recurring remediation efforts into new remediation efforts. See Transfer records to remediation efforts in the Vulnerability Manager Workspace for more information about transferring records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On a watch topic, on the upper right from the Create Remediation Effort list, select **Create Recurring Effort**.

   The Create Recurring Effort modal is displayed.

4. In step 1, Effort details, fill in the required fields.

   In the Short description field, enter the text that describes the recurring remediation effort that helps you locate it and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts. For example, `Vulnerabilities on External Facing Assets`.

5. Click **Next**.
   Task generation details are displayed.
6. In step 2, Task generation, choose one method from the list to bundle the vulnerable items in the remediation tasks that you generate from this remediation effort after it is created.
   - By Assignment group
   - By Assignment group and configuration item
   - By Assignment group and vulnerability
   - None (No remediation tasks are created). Use this method if you want to add records manually to a remediation task for this effort. See Create a remediation task on-demand in the Vulnerability Manager Workspace.
7. To automatically refresh the duplicate host vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** option.

   Note: This check box is available only for Host Vulnerabilities.

8. Click **Next** to continue.
9. In step 3, Recurrence, select the frequency.

Option	Description
Quarterly (Every 3 months)	Schedules Remediation Effort once in every three month. **Note:** If the month you select has only 30 days, the remediation effort is created on that last date of the month.
Monthly	Schedules Remediation Effort once in every month.
Weekly	Schedules Remediation Effort once in every week. **Note:** This option is available starting from the version 19.0 of Vulnerability Re sponse.
Daily	Schedules Remediation Effort everyday.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Note: This option is available starting from the version 19.0 of Vulnerability Response.

a. Define the recurrence schedule.

Use the lists to select the month/day/hour/minute you want the remediation effort created. The time zone for scheduling is by default your time zone.

Note: If you have many vulnerabilities, you might prefer to set the creation for off-hours.

If you want the job created on the last day of the month, the scheduled job creates the recurring remediation effort on the last day of the month. A message displays if the month does not have 31 days.

b. **Optional:** Select **Carry over vulnerabilities** to active vulnerabilities in this remediation effort to carry forward into each subsequent remediation effort that is created.

10. Click **Schedule recurrence**.
A message is displayed that the recurring remediation record was created. The new remediation effort is not displayed immediately, it is created when you scheduled it. It is displayed on your lists after it is created by the scheduled job.

The date the remediation effort will be created is shown on the corresponding watch topic. For more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by records transfer, see Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces.

Transfer records to remediation efforts in the Security Exposure Management Workspace

You can transfer records from existing remediation efforts into new remediation efforts in the Vulnerability Manager Workspace.

Before you begin

If confronted by a zero-day threat or a very critical vulnerability that you want to resolve quickly, you might want to consolidate any active records that you already have for this vulnerability into one remediation effort. However, each record can only be in one effort, and records can overlap among watch topics. So, to gather them all, you need to transfer these records from multiple existing efforts into one remediation effort.

Say, for example, you created a remediation effort that has one, high-priority vulnerability in it. Because this vulnerability is widespread and potentially impacts the other areas in your environment, you might have records that are associated with this vulnerability already in existing remediation efforts. To combine these records so they are all in one remediation effort, you can transfer any records from existing remediation efforts into a new remediation effort.

Note: You cannot transfer records from recurring remediation efforts into new remediation efforts. For more information, see Create a recurring remediation effort in the Vulnerability Manager Workspace.

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **All** > **Security Exposure Management Workspace**.
2. Select the watch topics icon.
3. On the Watch Topics page, select a watch topic that you want to create a recurring remediation effort for.
4. Click **Create Remediation Effort**.
   The Create Remediation Effort modal is displayed.
5. In step one, Effort details, fill in the required fields.

   In the Short description field enter text that describes the recurring remediation effort that helps you locate it and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts. For example, `Active Log4J Vulnerabilities`.

   a. In the Name field enter a name for your new remediation effort.
      By default the watch topic name is displayed.

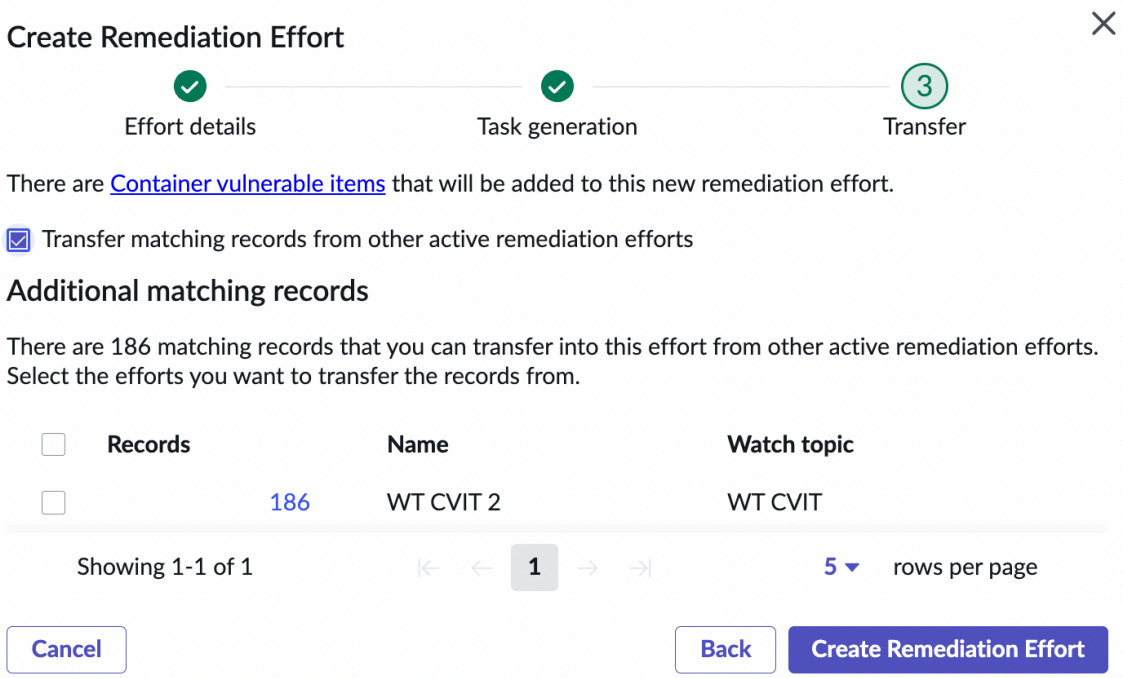
   b. In the Description field, enter text that will help you locate this remediation effort easily from the list of remediation efforts.

6. Click **Next**.
   Task generation details are displayed.
7. In step 2, Task generation, choose one method from the list to bundle the records in the remediation tasks that you generate from this remediation effort after it is created.
   - By Assignment group
   - By Assignment group and finding
   - By Assignment group and vulnerability
   - None (No remediation tasks are created). Use this method if you want to add records manually to a remediation task for this effort. See Create a remediation task on-demand in the Vulnerability Manager Workspace.
8. To automatically refresh the duplicate findings, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** option.
9. Click **Next**.
10. In step 3, Transfer, verify how many records will be added to the remediation effort and see how many records are available for transfer from other active remediation efforts.
11. To transfer records from other efforts, from the list, select the check boxes for the records you want.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select the **Transfer matching records from other active remediation efforts** check box and then select the check boxes for the records that you want to transfer from other active remediation efforts.

Version 18.0 Create Remediation Effort



12. Click **Create Remediation Effort**.

After a few moments, the new remediation effort is displayed. Depending on the number of records, it may take some time. A message indicates that the record is populating.

The new remediation effort is created with any records that are available from the watch topic used to create it, in addition to any records that you selected for transfer from existing efforts.

If you select records to transfer from an existing effort, and the existing effort transfers all of its records into your new effort, the remediation effort you moved the records from is closed.

Note: If there are neither any records available from the watch topic, nor any records selected for transfer, the **Create Remediation Effort** button is deactivated.

For more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by records transfer, see Transferring records or record carry over.

Approve or reject requests in the Security Exposure Management Workspace

Approve or reject requests that are submitted by remediation owners.

Before you begin

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver roles required for various approval requests

Approval type	Approval levels required	Approver roles	Additional information
False positive approvals	One	• sn_vul.false_positive_approver granular role for vulnerable items (VITs). • sn_vul.app_false_positive_approver role for application vulnerable items (AVITs) • sn_vul_container.false_positive_approver role for container vulnerable items (CVITs) • sn_vulc.false_positive_approver for configuration test results Or Approvers are required to be in the False Positive Approver user group.	
Exception approvals (deferrals)	Two	• One approver is required in the Approver - Level 1 group • One approver is required in the Approver - Level 2 group	An exception request for a record or remediation task is approved by using a default, two-level approval workflow. The exception request requires two levels of approvers. After the request is approved by the level 1 approver, it's sent on to the second-level approver and is then visible in approver 2's queue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver roles required for various approval requests (continued)

Approval type	Approval levels required	Approver roles	Additional information
Unassign approvals	One approver is required in the Approver – Level 1 group	• sn_vul.unassign_appr for AVITs and VITs • sn_vul_container.unas for CVITs • sn_vulc.unassign_app for configuration issues (CIs)	**Note:** By default, an approval configuration is provided and an unassign approval group is created. Users (Unassign Approver - Level 1) of this group can approve the request. This group contains an unassign approver role, sn_vul.unassign_approver, by default. You can modify or create a new group and update the approval configuration. To configure approval rules, navigate to the respective Approval Rules module, select any of the following approval rules, and navigate to the approval configuration in the **Approval Configurations** tab: • *Vulnerable item field change request* for a vulnerable item. • *Vulnerability field change request* for a remediation task. • *Application vulnerability field*

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver roles required for various approval requests (continued)

Approval type	Approval levels required	Approver roles	Additional information
Risk reduction approvals	Two	• One approver is required in the Approver - Level 1 group • One approver is required in the Approver - Level 2 group	The approval flow for risk reduction is same as the exception approvals (deferrals).

See Vulnerability Response personas and granular roles and Assign the Vulnerability Response persona roles using Setup Assistant for more information about assigning persona roles to users and users to groups.

Note: Add users to the approval groups before you submit approval requests. If you create requests before you add users to the approval groups, the requests might not be visible to those users that have the approval permission.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management**.
   If an approver doesn't have access to the workspace, approvals can be processed at **Vulnerability Response** > **My Approvals** in the classic environment.
2. Select the List view icon ( ).
   The List page is displayed.
3. In the Approvals filtered list, select **Assigned to me**.
4. Locate a request that you want to process and then select the link in the State column.
   The Vulnerability State Change Approval record (VCA#) is displayed.
5. Choose one of the following options to approve or reject the request.

Option	Description
Click the Details tab, enter text in the Comments field, and click Reject	○ A message is displayed indicating that there's a rejected approval for the Vulnerability State Change Approval record. ○ The state on the Vulnerability State Change Approval record transitions to Rejected. ○ The state on the remediation task or the record remains the same. ○ The Vulnerability State Change Approval record is no longer displayed on your Approvals list view in the workspace.
From either the Request or Details tabs, click Approve	○ A message displays indicating that the Vulnerability State Change Approval record is approved. ○ The state on the remediation task or the record transitions to Deferred.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ Active records on the remediation tasks transition to Deferred. ○ The Vulnerability State Change Approval record is no longer displayed on your Ap provals list view.

Add a compensating control to the library

As a Vulnerability Manager or Analyst, add a list of compensatory controls to the Compensating Controls library in the Security Exposure Management Workspace, which can be applied for the risk reduction of host vulnerable items and remediation tasks.

Before you begin

Role required: sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

About this task

Some commonly used compensating controls are shipped with the base system. You can view these compensating controls by navigating to **Workspaces** > **Security Exposure Management Workspace** > **Lists** > **Libraries** > **Compensating controls**. You can activate or deactivate these compensating controls as per your requirement.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. On the List page under Libraries, select **Compensating Controls**.
3. Click **New**.
4. On the Create Compensating Controls form, fill in the fields.

Create Compensating Controls form fields

Field	Description
Name	Name of the compensating control, which appears as an option in the **Compensating controls** drop-down of the Request exception modal.
Description	Brief information that provides details about the Compensating Control.
Active	Status of the compensating control. Only active controls appear in the **Compensating controls** drop-down of the Request exception modal.

5. Select **Save**.
6. On the Compensating Controls list under Libraries, select the desired compensating control and select **Edit**, activate or deactivate a compensating control and click **Save** to modify the compensating controls.
   All the active compensating controls appear as an option in the **Compensating controls** drop-down of the Request exception modal for risk reduction requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Starting from v21.0 of Vulnerability Response, you can associate compensating controls with CVEs or TPEs after adding a compensating controls to the library. For more information on how to associate compensating controls, see Associate compensating controls with CVEs or TPEs for risk change requests.

Related topics

- Understanding compensating controls for risk change
- Disable or enable risk change for a CVE or TPE
- Associate compensating controls with CVEs or TPEs for risk change requests
- Impact of the compensating controls on risk score and expiration date

Associate compensating controls with CVEs or TPEs for risk reduction requests

As a Vulnerability Manager or Analyst, you can associate relevant compensating controls with a Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Security Exposure Management Workspace, which can be used for reducing the risk posed by a vulnerability.

Before you begin

Role required: sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

About this task

- If you don't associate compensating controls to a CVE or TPE, all the active controls appear in the Select Compensating Controls field of the Request Exception form.
- If you associate a compensating control to a CVE, this compensating control is automatically associated with the TPE, which is mapped to the CVE.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. On the Lists page, under Libraries, open one of the following for which you want to associate the controls:
   - **CVE** from the CVEs list.
   - **TPE** from the TPEs list.
3. Select **Associate controls**.

   Note: The **Associate controls** button appears only when the risk reduction is enabled for a CVE or TPE. In other words, you can associate compensating controls only when risk reduction is enabled for a CVE or TPE. If the **Associate controls** button isn't visible, select **Enable risk reduction**.

4. On the Associate controls modal, select the compensating controls that can be applied to vulnerabilities associated with the CVE or TPE for risk reduction.
5. Select **Submit**.
   - The associated compensating controls appear in the Applicable compensating controls tab in the record view of the CVE and TPE.
   - While a remediation owner requests risk reduction, these associated compensating controls appear in the Select Compensating Controls field on the Request Exception modal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

- Understanding compensating controls for risk change
- Disable or enable risk change for a CVE or TPE
- Add a compensating control to the library
- Impact of the compensating controls on risk score and expiration date

Disable or enable risk reduction for a CVE or TPE

As a Vulnerability Manager and Analyst, you can disable or enable the risk reduction requests for the host vulnerabilities associated with a Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Security Exposure Management Workspace.

Before you begin
Role required: admin

About this task
The risk reduction for a CVE and TPE is enabled by default.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
   On the Lists page, under Libraries, open one of the following for which you want to disable the risk reduction requests:
   - **CVE** from the CVEs list.
   - **TPEs** from the TPEs list.
2. Select **Disable risk reduction**.
   The remediation owner can't request risk reduction for the host vulnerable items related to this CVE or TPE. In other words, the Request for Risk Reduction check box doesn't appear when the **Reason** is selected as `Mitigating Control in Place` on the Request Exception modal.
3. To enable the risk reduction requests for host vulnerable items, select **Enable risk reduction**.

Related topics

- Understanding compensating controls for risk change
- Add a compensating control to the library
- Associate compensating controls with CVEs or TPEs for risk change requests
- Impact of the compensating controls on risk score and expiration date

Examples for remediation task creation in the Security Exposure Management Workspace

When you create remediation tasks manually in the Security Exposure Management Workspace, records are grouped into a remediation task based on the grouping criteria you select.

Consider the following example where 10 records are selected for remediation task creation. After providing the record selection details and a brief description, select the **Grouping criteria** according to your requirement and then select how you want to manage the records that are already part of existing remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example: Remediation task creation based on the grouping criteria

Vulnerable items selected for remediation task creation

Vulnerable item id	Existing remediation tasks	Assignment group	Configuration item	Vulnerability	Risk rating
VIT10001	VUL10021, VUL10022	Remediation Manager	APSVR-NY-1672	CVE-2018-9020	4
VIT10002	-	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	LDAP Admins	DEV-IBM-NY-682	CVE-2012-5357	1
VIT10004	-	Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10006	-	Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10007	-	LDAP Admins	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008	-	LDAP Admins	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009	-	Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10010	-	LDAP Admins	DEV-SAP-SD-9388	CVE-2013-3906	4

The following list shows how the records are grouped into remediation tasks based on the grouping criteria selected when creating the remediation task.

Scenario1: Grouping criteria is selected as "Assignment group" and Managing records in other remediation tasks is selected as "Skip records for the new remediation tasks"

The records with the same assignment group are grouped into one remediation task. The records that are already part of existing remediation tasks are not added to the new remediation tasks. Here, three remediation tasks are created, each containing the records that are assigned to the **Remediation Manager**, **LDAP Admins**, and **Vulnerability Response** assignment groups.

Remediation task created in scenario 1

Remediation tasks created	Records in the remediation task
Remediation task 1 - VUL10001	This remediation task contains the records that are assigned to the **Remediation Manager** assignment group:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task created in scenario 1 (continued)

Remediation tasks created	Records in the remediation task
	• VIT10004 • VIT10006 • VIT10009 The VIT10001 record will not be moved to the VUL10001 remediation task.
Remediation task 2 - VUL10002	This remediation task contains the VIT10002 record that is assigned to the **Vulnerability Response** assignment group. The VIT10005 record will not be moved to the VUL10002 task.
Remediation task 3 - VUL10003	This remediation task contains the records that are assigned to the **LDAP Admins** assignment group: • VIT10007 • VIT10008 • VIT10010 The VIT10003 record will not be moved to the VUL10003 remediation task.

Scenario 2: Grouping criteria is selected as "Assignment group and configuration item" and Managing records in other remediation tasks is selected as "Transfer records to the new remediation tasks"

The records with the same configuration item that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records are removed from their old remediation tasks and moved to the new remediation tasks. Here, five remediation tasks are created.

Remediation tasks created in scenario 2

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10004	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **APSVR-NY-1672** configuration item. • VIT10001 The VIT10001 record will be removed from the VUL10021, and VUL10022 remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tasks created in scenario 2 (continued)

Remediation tasks created	Records part of remediation task
Remediation task 2 - VUL10005	This remediation task contains the records that are assigned to **Vulnerability Response** assignment group and with **DEV-IBM-NY-682** configuration item. • VIT10002 • VIT10005 The VIT10005 record will be removed from the VUL10022 remediation task.
Remediation task 3 - VUL10006	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **DEV-IBM-NY-682** configuration item. • VIT10003 • VIT10008 The VIT10003 record will be removed from the VUL10021 remediation task.
Remediation task 4 - VUL10007	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **CRMBK-SD-4210** configuration item. • VIT10004 • VIT10006 • VIT10009
Remediation task 5 - VUL10008	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **DEV-SAP-SD-9388** configuration item. • VIT10007 • VIT10010

Scenario 3: Grouping criteria is selected as "Assignment group and vulnerability" and Managing records in other remediation tasks is selected as "Keep records in both the current and new remediation tasks"

The records with the same vulnerability that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records will be added to their respective new remediation tasks without being removed from their old remediation tasks.Here, five remediation tasks are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tasks created in scenario 3

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10009	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **CVE-2018-9020** vulnerability. • VIT10001 The VIT10001 record will remain part of VUL10021, and VUL10022 remediation tasks as well.
Remediation task 2 - VUL10010	This remediation task contains the records that are assigned to **Vulnerability Response** assignment group and with **CVE-2018-9020** vulnerability. • VIT10002 • VIT10005 The VIT10005 record will remain part of VUL10022 remediation task as well.
Remediation task 3 - VUL10011	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **CVE-2012-5357** vulnerability. • VIT10003 The VIT10003 record will continue to be part of the VUL10021 remediation task also.
Remediation task 4 - VUL10012	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **CVE-2013-1710** vulnerability. • VIT10004 • VIT10006 • VIT10009
Remediation task 5 - VUL10013	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **CVE-2013-3906** vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tasks created in scenario 3 (continued)

Remediation tasks created	Records part of remediation task
	• VIT10007 • VIT10008 • VIT10010

Scenario 4: Grouping criteria as "Assignment group and risk rating" and Managing records in other remediation tasks is selected as "Keep records in both the current and new remediation tasks"

The records with the same risk rating that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records will be added to their respective new remediation tasks without being removed from their old remediation tasks. Here, five remediation tasks are created.

Remediation task created in scenario 4

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10014	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **4** risk rating. • VIT10001 • VIT10004 The VIT10001 record will continue to be part of VUL10021and VUL10022 remediation tasks.
Remediation task 2 - VUL10015	This remediation task contains the records that are assigned to **Vulnerability Response** assignment group and with **2** risk rating. • VIT10002 • VIT10005 The VIT10005 record will continue to be part of VUL10022 remediation task.
Remediation task 3 - VUL10016	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **1** risk rating. • VIT10003 • VIT10007 • VIT10008

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task created in scenario 4 (continued)

Remediation tasks created	Records part of remediation task
	The VIT10003 record will continue to be part of VUL10021 remediation task.
Remediation task 4 - VUL10017	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **2** risk rating. • VIT10006 • VIT10009
Remediation task 5 - VUL10018	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **4** risk rating. • VIT10010

Related topics

Create a remediation task manually in the Security Exposure Management Workspace

Exception Management Overview

When your organization can't comply with a published finding or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to a finding or remediation task (RT) that can’t be remediated.

Some findings might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the finding.

Exception Management provides administrators the ability to handle, configure, and review exception cases within the Security Exposure Management Administration Console. You can navigate to Exception Management from the **Workspaces** > **Security Exposure Management Workspace** > **Administration** > **Exception Management**.

In the Exception Management landing page, you can view the exception management configurations for all the four apps- Vulnerability response, Configuration compliance, Application Vulnerability Response, and Container Vulnerability Response. You can create a new questionnaire or to design your own questionnaire using the templates available in the smart assessment workspace to help review the exception requests for the Vulnerability Manager, Business Unit Head, or Service Owners.

You can personalize the columns and rows with the help of the setting icon on the right.

The Life-cycle of an exception

Definition of an exception

An exception is a request to defer the remediation of a finding or remediation task for a specified period. For example, as a remediation owner, you can request an exception if a patch isn’t available for a machine.

Requesting an exception

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As the remediation owner, you can ask for an exemption for a finding or remediation task using the exception management process. After the exception approver approves this request, the finding or remediation task moves to a **Deferred** state.

Approving an exception request

Findings or remediation tasks that can't be remediated immediately are reviewed by a vulnerability manager or business analyst, assessed for risk, and approved for deferral until they can be remediated. Approval rules for Exception Management are determined based on the configured approvers and approver levels. Once the required approvals are obtained, the request state transitions according to the type of request. If defined, Exception requests can follow a multi-level approval workflow. If no approver is configured for a specific request type, the request can’t be submitted. Approvals are typically carried out by the Vulnerability Manager or by Business Users who have been assigned the appropriate Approver role.

Tracking an exception request

After raising the exception, you can track its status by using the **Change Approvals** tab of the finding or remediation task. If an action is taken on a remediation task, you can't track the status of the individual findings in that remediation task.

Expiry of an exception request

When an exception request for a particular finding or remediation task expires, the impacted finding or remediation task reverts to its **Open** state.

Approver roles required for Security Exposure Management Workspace

You can see the required roles for the approvers in the Security Exposure Management Workspace.

Approver roles required for various approval requests

Approval type	Approver roles
False positive approvals	sn_vul.false_positive_approver • sn_vul.vulnerability_admin • sn_vul.vulnerability_analyst Approvers are required to be in the False Positive Approver user group.
Exception approvals (deferrals)	• sn_sec_exception.admin • sn_sec_exception.read • sn_sec_exception.approver
Unassign approvals	sn_vul.unassign_approver
Risk reduction approvals	sn_vul.exception_approver

Questionnaire support in Exception Management via Smart Assessment

Configure advanced questionnaires as part of the exception management process using Smart Assessment. This enables Remediation Owners to provide more detailed context for Exception Requests and enables Approvers to configure conditional questions to gather information for informed decision making.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roles Required

Smart Assessment Template Reader: **sn_vul_cmn.smart_assessment_template_manager** (Vulnerability admin and Template reader) enables admins to create and edit templates.

Smart Assessment actor: **sn_vul_cmn.smart_assessment_actor** enables you (Remediation Owners and Admins) to fill out the questionnaires/assessments.

Smart Assessment reader: **sn_vul_cmn.smart_assessment_reader** enables you (Approver) to read the submitted questionnaire responses.

Pre-requisite: The smart assessment plug-ins must be installed as the Smart Assessment is a dependency.

You can configure questionnaires as part of the Exception Management process using Smart Assessment. It enables Vulnerability Admins/Manager to configure conditional questions to gather the right information needed for informed decision-making, while enabling Remediation Owners to provide more detailed context for exception requests. This enhances collaboration between the Vulnerability Management and Remediation teams by streamlining the approval process and ensuring clarity and completeness of exception justifications.

In the **Exception Management Configuration** screen from any of the four options- **Vulnerability Response**, **Application Vulnerability Response**, **Container Vulnerability Response**, and **Configuration Compliance** you can select the Assessment for Compensating Control, request exception and false positive records.

You can use the **Smart Assessment** to manage the Questionnaires in Security Exposure Management Workspace.

Templates can be accessed/edited by the Smart Assessment Template Reader: **sn_vul_cmn.smart_assessment_template_manager**.

Questionnaire Configuration form fields

You can define distinct questionnaire for a distinct collection of vulnerabilities or remediation tasks by filtering the vulnerabilities or remediation tasks respectively.

The Questionnaire Configuration form appears when you select the **Design New Questionnaire** button in the configuration for Exception Management form for any one of the four applications.

Questionnaire Configuration form fields

Field	Description
Name	Name of the questionnaire.
Approval rule	Approval rule for which the questionnaire is applicable. • **Exception request for vulnerability groups** • **Exception request for vulnerable items** • **False positive for vulnerability groups** • **False positive for vulnerable items**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Questionnaire Configuration form fields (continued)

Field	Description
	• **Questionnaire for compensating controls for vulnerable groups** for remediation task's risk reduction requests. • **Questionnaire for compensating controls for vulnerable items** for vulnerable item's risk reduction requests.
Description	Short description for the questionnaire configuration.
Order	Questionnaire with lowest order appears during the requests.
Active	Enabled by default, signifying that the questionnaire is in use.
Table	Table for which the approval rule is applicable. • Finding [sn_vul_vulnerable_item for the approval rules related to vulnerable items. • Remediation Task [sn_vul_vulnerability] for the approval rules related to remediation tasks.
Condition	Condition for the records for which the questionnaire must appear. You can apply condition on all the fields of a vulnerable item and remediation task except **Reason**.
Questionnaire	Questionnaire that appears when a remediation owner is requesting an exception, false positive or risk reduction.

Configure an assessment template

Assessment templates contain the questions prompted during the request process (such as, when requesting an exception). The above-mentioned preconfigured templates are provided with smart assessment. You can also create your own templates as required.

Before you begin

Role required:

Template Reader Role: **sn_vul_cmn.smart_assessment_reader** enables you (Approver) to read the submitted questionnaire responses.

Template Actor Role: **sn_vul_cmn.smart_assessment_actor** enables you (Remediation Owner and Admin) to fill out the questionnaires/assessments.

About this task

In the Security Exposure Management workspace, you can select the template with the assessment target as Change Approval (CA), to be used for the exception request (such as,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception for Vulnerability Response, False Positive for Vulnerability Response). If you select the default template, it automatically populates the questions. If you choose to create your own template, it can be modified.

Procedure

1. Navigate to the **Assessment Workspace**.
2. Select an existing **Assessment Template** or select a **New Template**
3. Fill in the following details:
   - **Template Name**: Unique name for the template
   - **Assessment Name**: Name displayed in the system when viewing the assessment.
   - **Template Categories**: Templates are categorized for easier management. Some template categories are provided by default, for example, Vulnerability Response Questionnaire Templates. Alternatively, you can also create templates of your choice.
   - **Assessment Targets**: Specifies the table that the template is related to. For VR, it's the CA table (Change Approval table).

Use case for False positive or Request Exception Questionnaire

Scenario when the questionnaire for False Positive or Request Exception is raised but not filled completely.

When the questionnaire for False positive or Request exception is raised but not filled completely, the Change Approval (CA) record goes into "Draft" state. If you want to raise an exception from the same category, you are navigated to the previous questionnaire following a pop-up note regarding the same. In case you want to raise a False Positive record instead of an existing request exception, the system overrides the False positive Change Approval record. It then creates a new False Positive Change Approval record.

In case the questionnaire is half filled and the same Vulnerability Item (VIT)/ or any ITEM is opened in classic view, you're navigated to the workspace questionnaire to fill the remaining data if the same type of request is raised again. If the questionnaire in classic view is selectively filled and the same item is opened in the workspace, then the classic view questionnaire is opened in the workspace.

Defer a Remediation task

If you identify a finding or remediation task for which a fix is not yet available and can be safely deferred without additional analysis, you can use the **Request Exception** feature.

Before you begin

Role required: sn_sec_exception.admin

About this task

You can defer a finding or remediation task directly from its respective form in the Security Exposure Management workspace. Once submitted, the request is sent for approval.

A scheduled job runs every day checking for deferred remediation tasks that have reached their reopen date. On the day the task's deferral is set to expire, the task is reopened.

Note: You can manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move remediation tasks from the Closed or Deferred states.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Security Exposure Management Workspace** > **List** > **Remediation Tasks**.
2. Open a record.
3. Click **Request Exception**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Until	Select the date when the Defer state expires and the remediation task is reactivated. After the record is submitted, if email notifications are defined, members of the group receive an email when the expiration date is within one week. When the defer date expires, the remediation task is set back to **Open** and a second email notification is sent out.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ False positive ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Click **Submit**.
   The group is marked In Review. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **Change Approvals** tab.

Request an extension for a deferred remediation task

As a remediation owner, you're no longer required to wait until the deferred due date to make this request. Request an extension for a deferred remediation task before it reaches its deferred until due date.

Before you begin
Role required: sn_sec_exception.admin

About this task
You can also request an extension from the Security Exposure Management Workspace.

Procedure

1. Navigate to **Security Exposure Management Workspace** > **List** > **Remediation Tasks**.
2. Open a deferred remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date when the Defer state expires and the remediation task is reactivated.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the changes on the remediation task are rolled down to the vulnerable items as well, which are part of the remediation task. However, the vulnerable items should be in the deferred state and their current until data precedes the updated until date. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through multi-levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred remediation task is extended again, the extend deferral count increases in the backend.

Request a false positive for a vulnerable item or remediate task

Indicate a false positive request for a finding or a remediation task in the Security Exposure Management Workspace. A false positive is a condition where a scanner incorrectly reports that a finding exists in the system due to situations such as an incorrect classification, improper logic, or an algorithm in the scanner.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace**.
2. Select List icon .
3. Select the remediation task or vulnerable item.
4. Select **Mark as False Positive**.
5. Enter information about the request.
6. Select **Request Approval**.
7. Provide additional information about your request to the approver and select **Submit**.

> **Note:** The Take Questionnaire modal appears only when the **Enable questionnaire to mark false positive** check box is selected in the Exception Management Configuration form. .

Result

The state of the vulnerable item or remediation task transitions to In Review.

Your request is submitted for approval and the approver receives an email notification about your request.

You will receive an email notification upon approval or rejection of your request.

What to do next

In the Security Exposure Management Workspace, on the List page, navigate to **Exception Requests** > **My requests** and open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Record	Remediation task
Approved	The State of the record transitions to Closed with Reason as False positive.	The State of the remediation task transitions to Closed with Reason as False positive. The state is rolled down to the records in the remediation task accordingly. Navigate to the Details tab of a Remediation task and set the expiry date for false positive in the **Until** field if required. The remediation task reverts to the Open state after the specified date and the state is rolled down to the test results.
Rejected	The state of the record does not change.	The state of the remediation task and its records reverts to previous state.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of the false positive request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Approvals View

The approval process in Security Exposure Management for vulnerability and compliance exceptions is unified to simplify workflows, improve visibility, and streamline actions for Approvers.

The Approvals landing page provides a comprehensive view of all approval requests initiated by remediation owners to view specific requests, with navigation widgets such as:

- **All approvals**: Consolidated list of all approvals, including exception, false positive, risk reduction, and unassignment (e.g., a single view of everything awaiting your approval).
- **Overdue approvals**: Approvals that have crossed their due date (e.g., a risk reduction request that was supposed to be approved yesterday).
- **Pending approvals**: Approvals awaiting action beyond today across all request types.
- **Today's approvals**: Approvals due for action today (e.g., an unassignment request expiring by end of day).
- **Exception approvals**: Approvals specifically for exception requests (e.g., a request to allow delayed patching of a high-risk vulnerability).
- **False positive approvals**: Approvals for requests flagged as false positives (e.g., scanner incorrectly reporting a vulnerability on a host).

Each approval request contains interactive links that provide access to detailed information, including Record Reference for findings, Request Type, Request Number, Risk Rating, Remediation Status, Approval Assignment Group, and Current State. You can also access clickable links to view details related to associated findings. See Configure Approval List and Form View.

When opening a finding record (e.g., VIT, AVIT, CVIT, Test Results), users can view detailed attributes such as state, remediation status, assignment group, information about the finding, relevant detections, change approvals, and requested approvals.

You can defer a finding or remediation task directly from its respective form in the Security Exposure Management workspace. Once submitted, the request is sent for approval. This unification offers:

View the requester, purpose, impacted services, approval levels, and comments all in one place.

Approvers can approve or reject requests directly within the same record. See Reviewing an Approval Request.

Every comment and approval action is recorded and attributed.

All requests including pending, overdue, or completed, are easy to locate and manage in the single view. Links to legacy approval requests are available for items that remain in the old flow during the migration period.

Add an approver

Users added to the False Positive, Unassign, Exception Approver group can approve findings and remediation tasks (VULs). Granting a false positive, unassign, exception is a single-level approval process.

Before you begin

Role required: sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > > **User Administration** > **Groups**.
2. In the **Name** column, search and select the appropriate option.
3. On the Group form, navigate to > > (or **Group members** > **New** > **Edit**).
4. On the User form, create a record by entering the user details, and click **Submit**.
   All roles are granted to the user. The selected users are added to the Group Members list. These members can approve requests to mark VIs or remediation tasks as false positive. Once approved, the state of the record is updated to Closed and it is reopened only on the specified date.

Configure Approval List and Form View

Optimize the review and approval process by configuring list views and form layouts for unified exception and approval management.

Before you begin

Role required: Admin

About this task

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **Approvals**.
2. The default list displays all approvals in the Approvals list view.
3. Select application type such as: Application vulnerabilities (AVR), Container vulnerabilities (CVR), Infra Vulnerabilities (VR), and Misconfigurations (CC) to filter approvals by category.
4. **Optional:** or Select the 3-menu option to group requests by Approval Name, Record reference, Request Type, Number, Risk Rating, Remediation Status, Approval Assignment group, and state.

   Note: You can select the filter icon to view requests by status and list icon or gear icon to reset the columns according to your requests or to reset the widths.

5. Select any request to view the form and request details such as:
   a. **State**, **Approval Due Date** and **Approver**.
   b. **Overview tab** consists of details such as:
      - Approval Status: Provides an overview of the Change approval (CA) request.
      - Request details: Provides Change approval(CA) request details.
      - Remediation details: Provides remediation details for the Change approval (CA) request.
      - Impact summary: Provides approvers the visibility of the impacted count information such as, Impacted CIs, Total Findings, and Total Vulnerabilities on the Change Approval for a Remediation Task.
      - Vulnerability Intelligence: Provides vulnerability intelligence data such as CISA KEV information, Known ransomware indicators, and EPSS percentile. This tile is visible only when Intelligence and App-Vuln NVD plugins are installed.
   c. **Approvers tab** consists of details such as:
      - Approver name
      - Email ID
      - State

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. **Impacted services tab** consists of details such as Name, Business criticality, Used for, Service classification, Managed by, Owned by, Approval group, Location, Operational status.

> **Note:** Admins can see additional filtering options and widgets such as: **Pending approvals**, **Today's approvals**, **Exception Approvals**, **False Positive Approvals**

Reviewing an Approval Request

Review an approval request form to perform the required action according to the role assigned to you.

Before you begin

Role required: sn_sec_exception.approver, sn_sec_exception.admin

About this task

Procedure

1. The default list displays approvals in the **All Approvals** list view.
2. **Optional:** Or you can select request from the **Pending approvals** or **Today's approvals**.
3. Select a request to review details such as requester information, remediation details, exception request history and approval history (previous actions, comments, approvers).
4. Select the Approval History or Activity Stream option from the side panel associated with this request, to review the request history.
   The system displays the five most recent approved or rejected records for this request type in the Approval History tab, enabling you to make an informed decision. Additionally, in the Activity tab you can enter a comment, view work notes and the input stream in this section. Select the stack mode toggle to view Comments, Work Notes and Activity stream all in one view.
5. Select **Now Assist Recommendation** option from the side panel to generate tailored recommendations for this request.

   > **Note:** Now Assist analyses risk rating, request details, questionnaire answers, vulnerability, and asset information for a request to provide Approve or Reject recommendations, confidence score, and reasoning to the approvers.

6. Select Approve or Reject at the top-right corner of the form, if you're the assigned Approver for that request.
7. Navigate to completed records using the links provided in the form.
   Approved or rejected items are moved from the open to the completed section.
8. If there are remaining legacy approvals, select the "Old Approvals List" link at the top of the page to view and act on those items.

   > **Note:** Approvers receive notifications or reminders for pending requests based on system configuration.

Review questionnaire to approve or reject requets

Approvers review the questionnaire and make approval/rejection decisions based on the provided information. Remediation owners must fill out the questionnaire before submitting for approval, if questionnaire configuration was selected during exception rule configuration..

Before you begin

Role required: **sn_vul_cmn.smart_assessment_reader**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The following is the workflow of the smart assessment adaption:

- **Request for Exception/False Positive** when you request an exception or mark something as a false positive, the system checks if a questionnaire is required.
- If the **questionnaire option is enabled**, a **mandatory message** will prompt the user to complete the questionnaire before proceeding with the approval process.
- **Draft State**: The **Change Approval** (CA) record will remain in the draft state until the questionnaire is submitted, and the Vulnerability Item (VIT) will be in the open state.
- **Approver View**: Once remediation owners fill out the questionnaire and submit it, the Change Approval (CA) and Vulnerability Item (VIT) records move to in review status. Approvers can review the smart assessment questionnaires from "All > My Approvals" or view them in the review state. The VIT will be moved to deferred state upon approval of the records.

Procedure

1. Navigate to **Workspaces** > **Security Exposure Management Workspace** > **Approvals**to view the questionnaire in the list view as well as inside the request form view.
2. Once the record is **Approved**, VIT is moved to Deferred state.
3. You can view the questionnaire via a link submitted by the Remediation Owners in the request information in Overview page.

Employee service center for Vulnerability Response

Employee Service Center provides a standardised approval experience and process for Business Unit Heads, Service Owners, and IT Heads, who may not regularly log in to USEM. It enables them to manage approvals from a central location, such as Employee Center Approval Requests, ensuring that requests are routed to the right approvers, decisions are tracked transparently, and actions are completed efficiently. This improves operational efficiency, accountability, and the overall approver experience.

This feature enables users to manage and take action on various vulnerability-related approvals directly from the **Employee Service Center** (ESC), eliminating the need to navigate to **Vulnerability Response** > **My Approvals**.

The following approval types are displayed within the Employee Service Center:

- Request exceptions
- False positives
- Risk Reduction
- Unassigned items
- Extension requests

For Exception Rules:

- Creation
- Extension

These approvals are available under the **My Tasks** section for easier access and management. For more information related to employee center visit: Employee Center

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Managing Approvals via the Employee Service Center

The updated Employee Service Center experience consolidates vulnerability approvals under one interface.This allows customers to efficiently manage security exceptions without navigating multiple systems or UIs.

Before you begin

Role required: sn_vul.exception_approver

About this task

Viewing Tasks: In the **My Tasks** tab- All pending tasks related to vulnerability approvals are displayed.

Each task provides a summary including:

- Desired State
- Issue Description
- Reason for Exception
- Impacted services
- Insights tabs
- Activity

Navigating Approval Details: Each task lets the approver access:

- A direct link to the **CA record**.
- A link to the **questionnaire** (if the approver has permission)
- Related **VIT** record for further investigation.

Procedure

1. Navigate to **My Tasks**, select a request.
2. Filter requests by **Task Type**. Select **Vulnerability Approvals** to view all approvals related to Vulnerability Response.
3. View approvals details in the **Insights**, **Impacted services**, and **Activity** tabs.
4. Select **Approve** or **Reject**.
   If approved/rejected, the tasks move to the **Completed** tab. You can apply the **Task Type** filter to view the completed vulnerability approvals
5. Approvers can review the approved/ rejected tasks under the **Completed** tab.

   Detailed audit data is available, including who approved, comments provided, actions performed. No further actions are allowed in this tab.

Unified Security Exposure Management reference

Reference topic contains information about tables, roles, scheduled jobs and properties installed with the Unified Security Exposure Management application. It also includes additional references.

Security Exposure Management Workspace Components

When you activate the Unified Security Exposure Management (USEM) and Security Exposure Management Workspace applications, the system installs specific key components including tables, user roles, and scheduled jobs to support the operations required for assessing and managing security exposures.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following applications install Security Exposure Management-specific components:

- Unified Security Exposure Management
- Security Exposure Management Workspace
- Administration for Security Exposure Management
- Risk Scoring for Security Exposure Management
- Remediation for Attack Surface Management
- Exception Management for Unified Security Exposure Management

USEM also depends on components provided by some existing security operations applications. For details of those existing components, see:

- Components installed with Vulnerability Response
- Components installed with Application Vulnerability Response
- Components installed with Container Vulnerability Response
- Components installed with Configuration Compliance

To view the full list of installed components, use the Application Files table. For instructions, see Find components installed with an application.

Deprecated Components

Some tables and scheduled jobs from the existing security operations applications are not included in USEM, as they have been deprecated.

The following tables from the existing applications have been deprecated and have corresponding replacements or references in USEM.

Deprecated Tables	Mapped Table in Security Exposure Management
Security Calculator Group [sn_sec_cmn_calculator_group]	Risk Calculator [sn_sec_calculator_group]
Vulnerability Calculator [sn_vul_calculator_group]	
Risk Calculators [sn_vulc_calculator_group]	
Security Calculator [sn_sec_cmn_calculator]	Risk Calculator Rule [sn_sec_calculator_rule]
Vulnerability Risk Rule [sn_vul_calc_risk]	
Calculator [sn_vulc_calculator_risk_score]	
Configuration Compliance Risk Rule [sn_vulc_risk_rule]	
Security Classification Group [sn_sec_cmn_classification_group]	Classification Group [sn_sec_wf_classification_group]
Classification Group [sn_vul_classification_group]	
Security Classification Rule [sn_sec_cmn_classification_rule]	Classification Rule [sn_sec_wf_classification_rule]
Classification Rule [sn_vul_classification_rule]	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deprecated Tables	Mapped Table in Security Exposure Management
Exception Management Configuration [sn_sec_cmn_exception_config]	Exception Management Configuration [sn_sec_exception_config]
Exception Management Configuration [sn_vul_exception_config]	
Questionnaire Configuration [sn_sec_cmn_questionnaire_config]	Questionnaire Configuration [sn_sec_exception_questionnaire_config]
Policy Exception Reason Mapping [sn_sec_cmn_policy_reason_mapping]	Policy Exception Reason Mapping [sn_sec_exception_policy_reason_mapping]
Policy Exception Reason Mapping [sn_vul_policy_reason_mapping]	
Vulnerability Assignment Rule [sn_vul_assignment_rule]	Assignment Rule [sn_sec_wf_assign_rule]
Assignment Rule [sn_vulc_assignment_rule]	
Vulnerability Calculator Rule [sn_vul_calculator]	Remediation Target Rules [sn_sec_wf_ttr_rule]
Remediation Target Rule [sn_vul_ttr_rule]	
Remediation Target Rule [sn_vulc_ttr_rule]	
Risk rule field [sn_vul_risk_field]	Risk rule field [sn_sec_calculator_risk_field]
Risk rule field [sn_vulc_risk_rule_field]	
Vulnerability Remediation Status [sn_vul_m2m_ttr_status]	Remediation Status [sn_sec_wf_m2m_ttr_status]
Test Result Remediation Status [sn_vulc_m2m_ttr_status]	
Vulnerability Rollup Calculator [sn_vul_rollup]	Rollup Config [sn_sec_wf_rollup_config]
Risk Score Rollup Calculator [sn_vulc_risk_score_rollup]	
Exception Rule [sn_vul_auto_exception_rule]	Exception Rule [sn_sec_exception_rule]
Auto Exception Rules [sn_vulc_auto_exception_rule]	
Vulnerability State Change Approval [sn_vul_change_approval]	Change Approval [sn_sec_exception_change_approval]
State Change Approval [sn_vulc_state_change_approval]	
Vulnerability Compensating Control relationship [sn_vul_m2m_entry_compensating_control]	Vulnerability Compensating Control relationship [sn_vul_cmn_m2m_entry_compensating_control]
Auto-Close stale Test Results [sn_vulc_auto_close_stale_config]	Auto-close Rule [sn_vul_cmn_auto_close_rule]

Deprecated Scheduled Jobs
Populate risk fields for risk rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deprecated Scheduled Jobs
Rerun calculators
Reapply all vulnerability assignment rules
Send unassignment notification
Run severity calculator after vulnerability entry promotion
Evaluate remediation targets
Reassignment count for assignment rules
Remove Duplicate VI Remediation Status
Copy customized request exception questionnaire to compensating control
Rolldown until date from vulnerability group to vulnerable item
Check Vulnerable Item and Groups Deferment Expiration
Check Risk Mitigation Expiration
Associate existing AVIs with Auto Exception Rule
Associate existing VIs with Auto Exception Rule
Migrate the background jobs
Update Risk Rating for Test Results
Evaluate and notify remediation targets
Associate existing TRs with Auto Exception Rule
Check Remediation Tasks and Test Result Deferment Expiration
Associate existing Container VIs with Auto Exception Rule
Check Container Vulnerable Item Deferment Expiration

Security Exposure Management Workspace Roles

List of roles installed with Security Exposure Management, defining user permissions and access for Security Exposure Management-related tasks.

Application	Role title	Description	Contains roles
Vulnerability Response Common	sn_vul_cmn.usem_admin	Configures rules, integrations, and related settings for Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance.	• sn_vul.vulnerability_admin • sn_vul.app_sec_manager • sn_vul_container.vulnerability_admin • sn_vulc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Role title	Description	Contains roles
Administration for Security Exposure Management	sn_sec_wf.read_admin_rules	Read access to administration rules.	• sn_sec_calculator.read • sn_vul_cmn_ws.read_admin_rules • sn_vul_cmn.read_auto_close_rules
Administration for Security Exposure Management	sn_sec_wf.manage_admin_rules	Create, read, update, and delete administration rules.	• sn_vul_cmn.manage_auto_close_rule • sn_sec_wf.read_admin_rules • sn_vul_cmn_ws.write_admin_rules • sn_sec_calculator.admin
Exception Management for Unified Security Exposure Management	sn_sec_exception.approver	Approve or reject exception requests, false positive requests, and exception rules.	sn_sec_exception.read
Exception Management for Unified Security Exposure Management	sn_sec_exception.read	Read access to exception management configuration and exception rules.	None.
Exception Management for Unified Security Exposure Management	sn_sec_exception.admin	Create, read, update, and delete exception management configuration and exception rules.	sn_sec_exception.read
Risk Scoring for Security Exposure Management	sn_sec_calculator.read	Read access to records in the `sn_sec_calculator` scope.	None.
Risk Scoring for Security Exposure Management	sn_sec_calculator.admin	Create, read, update, and delete records in the `sn_sec_calculator` scope.	sn_sec_calculator.read

Security Exposure Management Workspace Tables

The following are the tables installed with Security Exposure Management. These tables store Security Exposure Management-related configuration, rules, findings, and other data required for exposure assessment, remediation, scoring, and exception management.

Application	Table	Description
Administration for Security Exposure Management	Assignment Rule [sn_sec_wf_assign_rule]	Contains the set of rules evaluated to set the assignment group on findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Table	Description
Administration for Security Exposure Management	Classification Group [sn_sec_wf_classification_group]	Stores classification group configurations for grouping related classification rules.
Administration for Security Exposure Management	Classification Rule [sn_sec_wf_classification_rule]	Stores classification rules that categorize findings based on defined conditions.
Administration for Security Exposure Management	Remediation Status [sn_sec_wf_m2m_ttr_status]	Stores status, rule and findings mapping for approaching and past due findings.
Administration for Security Exposure Management	Remediation Target Rules [sn_sec_wf_ttr_rule]	Stores remediation target rules that define remediation timeframes, notifications, and applicable conditions for findings.
Administration for Security Exposure Management	Rollup Config [sn_sec_wf_rollup_config]	List of vulnerability rollup calculators.
Exception Management for Unified Security Exposure Management	Change Approval [sn_sec_exception_change_approval]	Stores approval records with details on the reason and findings for each request, approval status, approver information, and related questionnaire.
Exception Management for Unified Security Exposure Management	Exception Management Configuration [sn_sec_exception_config]	Stores the configuration settings for the exception management feature.
Exception Management for Unified Security Exposure Management	Exception Rule [sn_sec_exception_rule]	Stores rules for automatically deferring findings based on matching criteria and execution order in exception management.
Exception Management for Unified Security Exposure Management	Policy Exception Reason Mapping [sn_sec_exception_policy_reason_mapping]	Maps policy exception reasons to their corresponding reasons in Vulnerability Response and Configuration Compliance.
Exception Management for Unified Security Exposure Management	Questionnaire Configuration [sn_sec_exception_questionnaire_config]	Stores questionnaire templates used for exception assessments.
Remediation for Attack Surface Management	Remediation Task Rule [sn_sec_rem_task_rule]	Contains the rules that define the criteria with which groups are automatically created for a set of findings.
Risk Scoring for Security Exposure Management	Calculator Configuration [sn_sec_calculator_config]	Stores configuration settings for risk calculators, including scoring logic.
Risk Scoring for Security Exposure Management	Risk Calculator [sn_sec_calculator_group]	Groups related risk rules, which are evaluated in order to calculate risk score.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Table	Description
Risk Scoring for Security Exposure Management	Risk Calculator Rule [sn_sec_calculator_rule]	Stores risk rules that calculates risk score on findings based on defined conditions.
Risk Scoring for Security Exposure Management	Risk rule field [sn_sec_calculator_risk_field]	Stores scoring criteria defined under a risk rule, containing weightage and weight breakdowns on field values.
Risk Scoring for Security Exposure Management	Risk Score Weight [sn_sec_calculator_risk_score_weight]	Stores risk score range to risk weight mapping.
Security Exposure Management	Dashboard [sn_sec_sem_dashboard]	Stores configuration for dashboards used in findings view.
Security Exposure Management	Widget Aggregation [sn_sec_sem_m2m_widget_dashboard]	Stores mapping between widgets, findings table, aggregation, and dashboards data.
Security Exposure Management	Widget Grouping [sn_sec_sem_widget_grouping]	Stores widget group definitions for aggregations associated with selected dashboard widgets.

Security Exposure Management Workspace Scheduled Jobs

The following are the scheduled jobs installed with Security Exposure Management. These jobs automate Security Exposure Management operations to ensure that exposure data is kept current and accurate.

Application	Scheduled job name	Description
Security Exposure Management	Trigger aggregation creation and running for dashboard	Initiates the creation and execution of dashboard aggregations.
Security Exposure Management	Create OOTB Findings View Dashboard	Creates the default out-of-the-box dashboard for findings.
Security Exposure Management	Refresh RO page related results	Refreshes results for remediation owner–related pages.

Security Exposure Management Knowledge Base articles

This section provides a curated list of essential ServiceNow Knowledge Base (KB) articles related to Security Exposure Management. These resources cover best practices, compatibility details, and workflow guidance for managing security exposures effectively.

KB articles list

KB ID	Title	Description
KB2556844	Migration Guidance to Unified Security Exposure Management	Provides comprehensive details on the migration process from Vulnerability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

KB articles list (continued)

KB ID	Title	Description
		Response applications to the new Unified Security Exposure Management (USEM) architecture.
KB0856498	Vulnerability Response Compatibility Matrix and Release Schema Changes	Details all released Store applications and associated schema changes.
KB1157979	Best Practices : Vulnerability Response Implementation for better performance	Offers implementation tips and best practices to optimize the Vulnerability Response (VR) application, which processes millions of vulnerabilities from third-party scanners.
KB0998706	CI matching in the Vulnerability Response	Explains how configuration items (CIs) are managed within the Vulnerability Response workflow.

Security Exposure Management Workspace remediation task rule examples

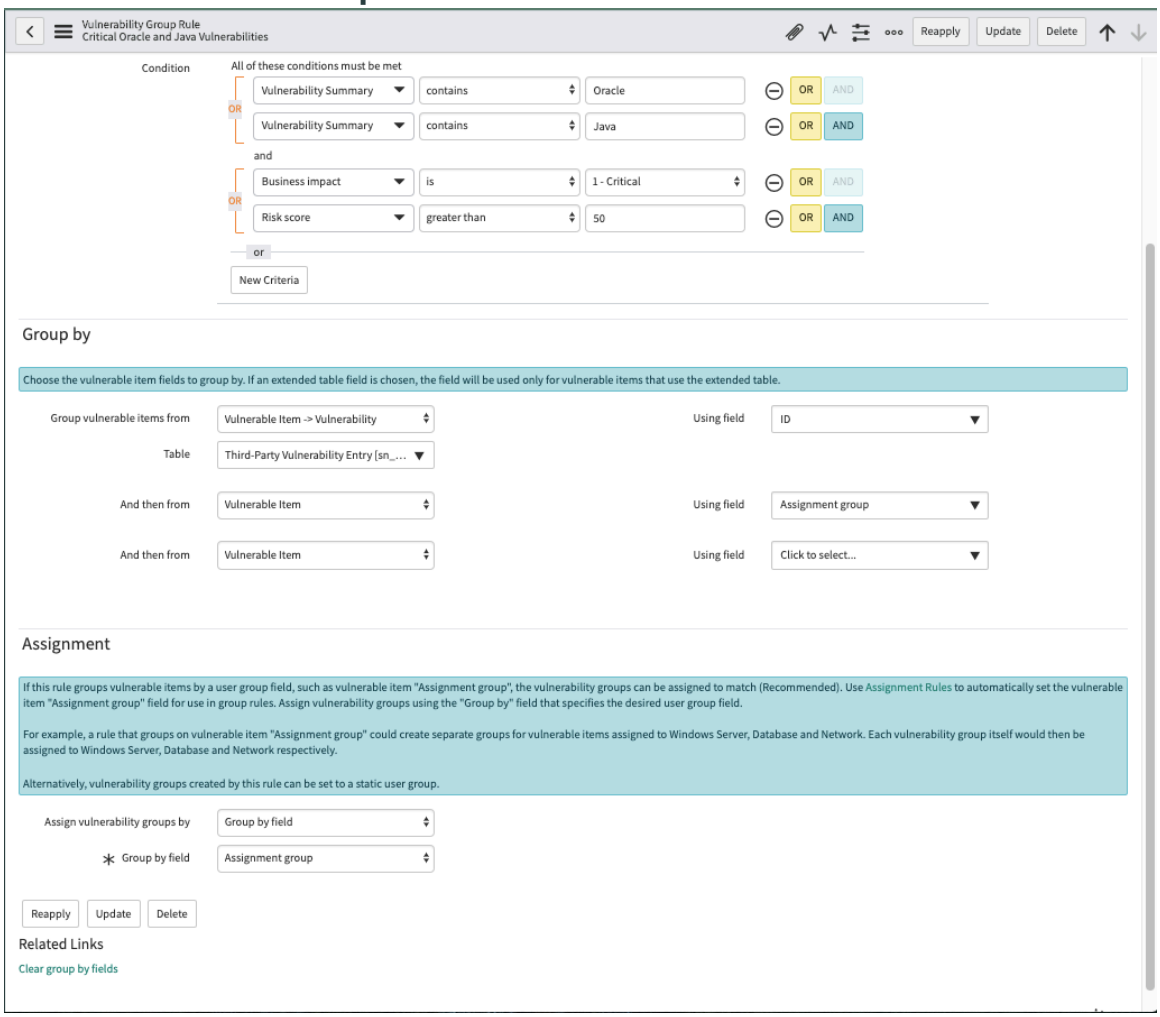
Examples of remediation task rules using vulnerability and risk, or impact, or configuration item (CI).

Remediation task rule to group high risk Java and Oracle vulnerable items

This example shows a walk-though of the rule that groups Java and Oracle findings by vulnerability and assigns them to their respective support groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task rule example

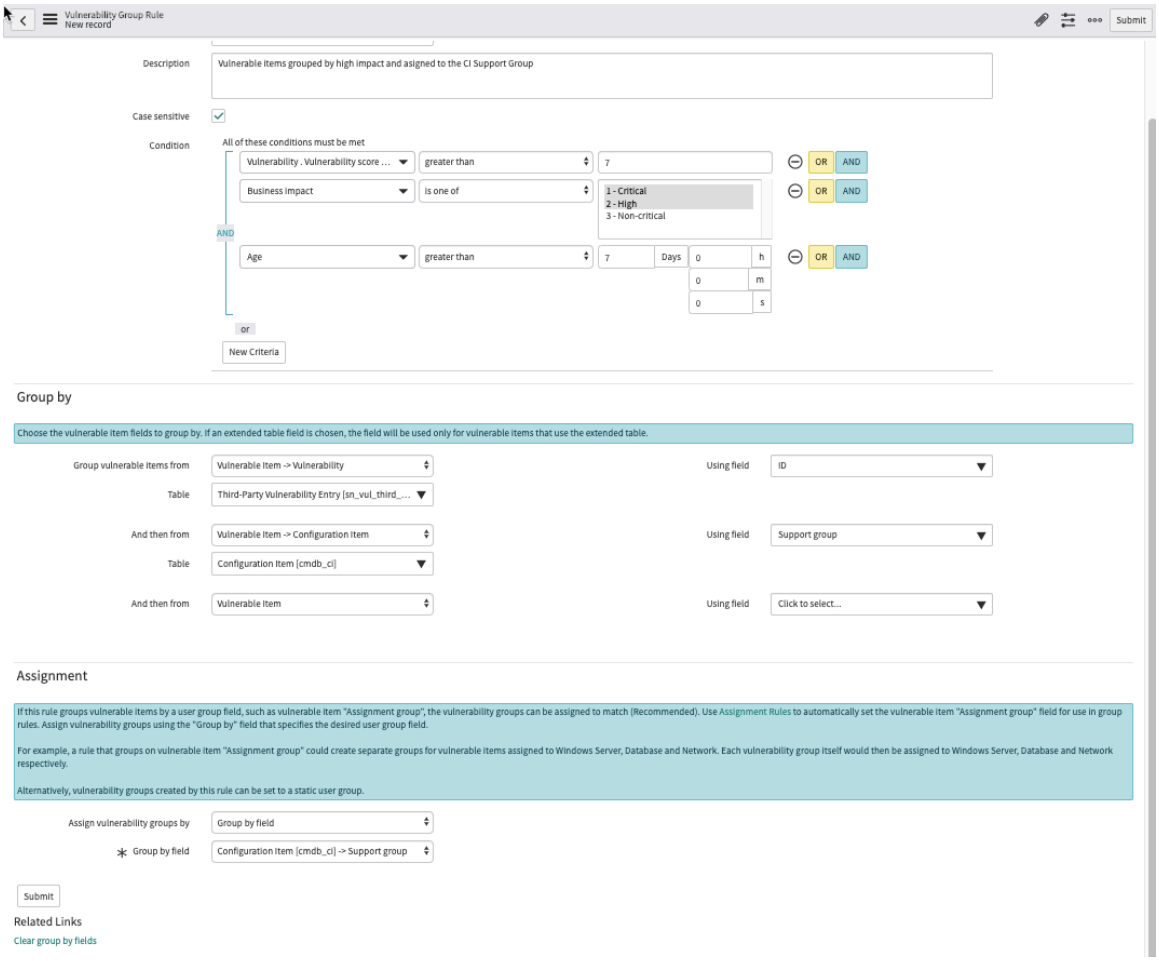


Right-click in the header to **Save**.

Remediation task rule to group all high impact vulnerable items by Vulnerability and CI support group

This example shows the form field settings for a group rule for high impact findings that assigns them to the CI support group.

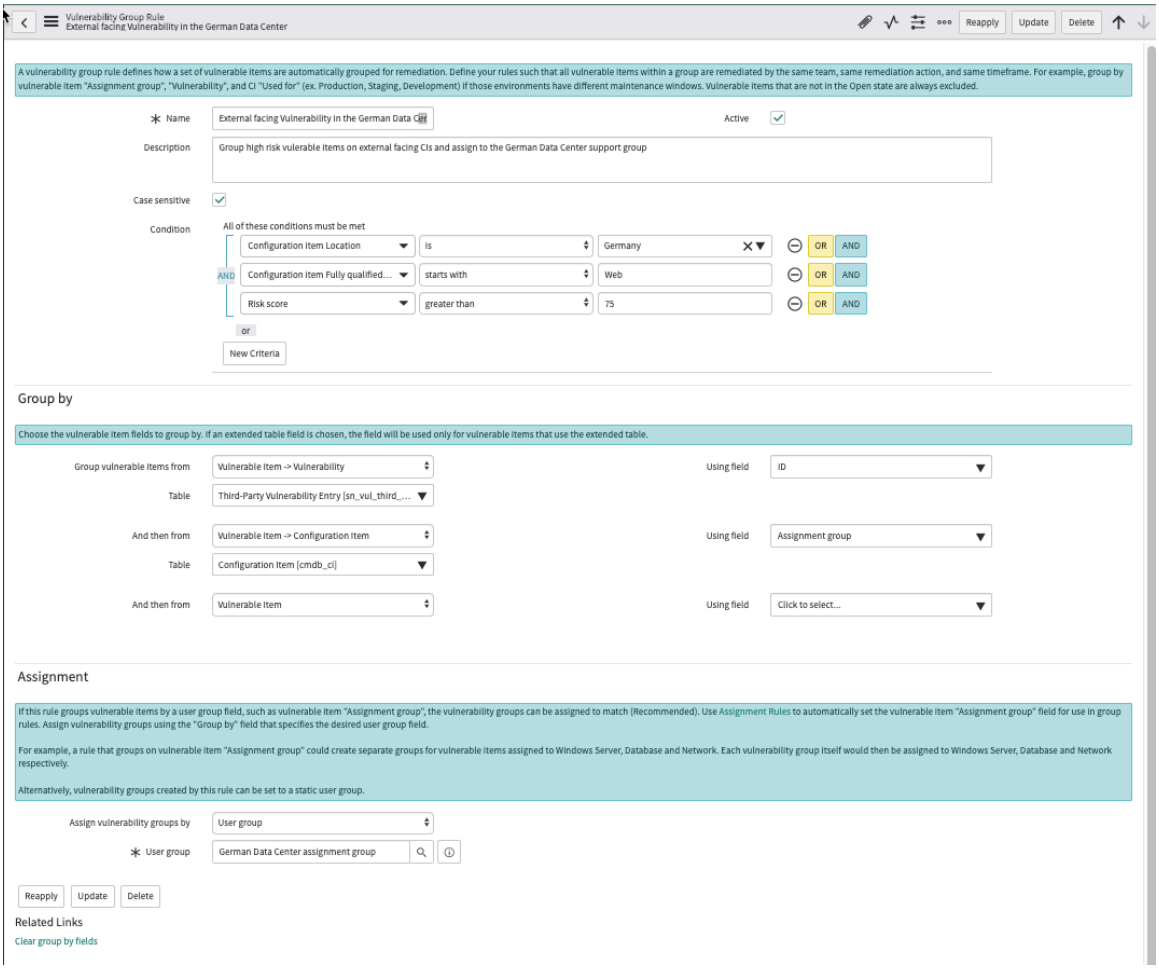
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Remediation task rule to group all the high risk vulnerabilities on an external-facing CI in a German data center

This example shows the form field settings for a group rule for high risk vulnerabilities on external facing CIs in a German data center. They are assigned to the German data center assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Migration upgrade reference information

Lists and tables of scheduled jobs, table deprecations, and new columns added to existing tables for migration to Security Exposure Management Workspace.

Scheduled jobs

Deactivate the scheduled jobs and scheduled jobs within integration-specific scopes for the Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance applications.

- Adding vulnerability and test fields for remediation tasks
- Associate existing AVIs with Auto Exception Rule
- Associate existing VIs with Auto Exception Rule
- Calculate Related VI Counts for Application Remediation Task
- Calculate Related VI Counts for Remediation Task
- Calculate Related VI Counts for Vulnerabilities
- Check Risk Mitigation Expiration
- Check Vulnerable Item and Groups Deferment Expiration
- Copy customized request exception questionnaire to compensating control
- Evaluate remediation targets
- Generate remediation digest

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Insert classic Remediation tasks Into Unified Remediation Task
- Migrate the background jobs
- Populate Approval Source
- Populate CC Number, Configuration Item and Business criticality into Unified Remediation Task Table
- Populate Container Number,Configuration and Business criticality into Unified Remediation Task Table
- Populate risk fields for risk rules
- Populate Vulnerable CIs table - Delete and Re-populate
- Populate Vulnerable CIs table - Delete and Re-populate for Test Results
- Populate Vulnerable CIs table - from Vulnerable CI manifest table
- Re-open deferred remediation tasks
- Reapply all vulnerability assignment rules
- Reassignment count for assignment rules
- Refresh and resolve duplicate VITs on remediation task
- Refresh associated Application vulnerable items for non-VGR based VG
- Refresh associated vulnerable items for non-VGR based VG
- Remove Duplicate VI Remediation Status
- Repair erroneous Vulnerable Items Last Opened and Closed
- Rerun calculators
- Rolldown state from vulnerability group to vulnerable item
- Rolldown until date from vulnerability group to vulnerable item
- Rollup application vulnerable item values to vulnerability and group
- Rollup VI values to vulnerability, Remediation Task (RT), and VI count on RT
- Run severity calculator after vuln entry promotion
- Send unassignment notification
- Set deferral counts
- Set related CI services for VI
- Update age closed for VITs and AVITs
- Update all old tags to remediation task table
- Update is_in_group on Vulnerable Items
- Update Last Open Detection Value To VITs
- Update Remediation tasks with rolled up states(AVR)
- Update Remediation tasks with rolled up states(VR)
- Update risk rating for vulnerability solutions
- Update Ungrouped Vulnerable Items
- Update Vulnerability on VG
- Vulnerability Response Age Closed Update
- Vulnerability Response CI count

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Vulnerability Response Risk and Remediation Status Upgrade
- Add default values for last_opened_dt_tm from last_opened
- Adding TR's CIs to service m2m table
- Associate existing Container VIs with Auto Exception Rule
- Associate existing TRs with Auto Exception Rule
- Auto-close Rule Processor
- Auto-Close Stale Test Results
- Calculate Business Criticality for CVIT
- Calculate Related CVIT Counts for Vulnerabilities
- Calculate Related VI Counts for Container Remediation Task
- Calculate remediation metrics for all the remediation tasks
- Calculate remediation metrics for all the tests
- Check Container Vulnerable Item Deferment Expiration
- Check Remediation Tasks and Test Result Deferment Expiration
- Delete inactive groupBys
- Evaluate and notify remediation targets
- Insert Remediation Tasks Into Unified Remediation Task
- Populate existing test result fields
- Process test result manifest records
- Re-apply CI Lookup Rules on the Changed Discovered items
- Reapply all assignment rules
- Reapply CI lookup rules
- Reassess the state of the remediation tasks
- Reassignment count for assignment rules - CC
- Reconcile unmatched discovered items
- Refresh App related Saved filters
- Refresh CC related Saved filters
- Refresh Container related Saved filters
- Refresh Host related Saved filters
- Remove Groups from Exception Rules
- Rollup container vulnerable item values to vulnerability and group
- Rollup Risk scores to Organization
- Rollup test result values to remediation task and configuration test
- Send unassignment notification - CC
- Set deferral counts
- Trigger aggregation creation and running for saved filter
- Update age closed for CC
- Update age closed for CVITs
- Update all old tags to compliance remediation task table

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Update all old tags to container remediation task table
- Update Awaiting Implementation state on CVITs
- Update remediation metrics
- Update remediation status for stale test results
- Update Remediation tasks with rolled up states (CC)
- Update Remediation tasks with rolled up states (CVR)
- Update Risk Rating for Test Results
- Update Rollup risk score for all non closed Result groups and Configuration tests
- Update Saved Filter Aggregations
- Vulnerability Response Container Count

USEM Data Model changes.

Deprecated tables	New tables
Vulnerability Assignment Rule (sn_vul_assignment_rule)	Assignment Rule (sn_sec_wf_assign_rule)
Security Classification Group (sn_sec_cmn_classification_group) Classification Group (sn_vul_classification_group)	Classification Group (sn_sec_wf_classification_group)
Security Classification Rule (sn_sec_cmn_classification_rule) Classification Rule (sn_vul_classification_rule)	Classification Rule (sn_sec_wf_classification_rule)
Security Calculator Group (sn_sec_cmn_calculator_group) Vulnerability Calculator (sn_vul_calculator_group)	Risk Calculator (sn_sec_calculator_group)
Security Calculator (sn_sec_cmn_calculator) Vulnerability Calculator Rule (sn_vul_calculator) Vulnerability Risk Rule (sn_vul_calc_risk)	Risk Calculator Rule (sn_sec_calculator_rule)
Risk rule field (sn_vul_risk_field)	Risk rule field (sn_sec_calculator_risk_field)
Vulnerability Remediation Status (sn_vul_m2m_ttr_status)	Remediation Status (sn_sec_wf_m2m_ttr_status)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deprecated tables	New tables
Remediation Target Rule (sn_vul_ttr_rule)	Remediation Target Rules (sn_sec_wf_ttr_rule)
Vulnerability Rollup Calculators (sn_vul_rollup)	Rollup config (sn_sec_wf_rollup_config)
Remediation Task Rule (sn_vul_grouping_rule) Remediation Task Rule (sn_vulc_grouping_rule)	Remediation Task Rule (sn_sec_rem_task_rule)
Exception Rule (sn_vul_auto_exception_rule) Auto Exception Rules (sn_vulc_auto_exception_rule)	Exception Rules (sn_sec_exception_rule)
Vulnerability State Change Approval (sn_vul_change_approval) State Change Approval (sn_vulc_state_change_approval)	Change Approval (sn_sec_exception_change_approval)
Exception Management Configuration (sn_vul_exception_config) Exception Management Configuration (sn_sec_cmn_exception_config)	Exception Management Configuration (sn_sec_exception_config)
Policy Exception Reason Mapping (sn_sec_cmn_policy_reason_mapping) Policy Exception Reason Mapping (sn_vul_policy_reason_mapping)	Policy Exception Reason Mapping (sn_sec_exception_policy_reason_mapping)
Questionnaire Configuration (sn_sec_cmn_questionnaire_config)	Questionnaire Configuration (sn_sec_exception_questionnaire_config)
Vulnerability Compensating Control relationship (sn_vul_m2m_entry_compensating_control)	Vulnerability Compensating Control relationship (sn_vul_cmn_m2m_entry_compensating_control)

New tables introduced to unify administration features

- Assignment Rule (sn_sec_wf_assign_rule)
- Classification Group (sn_sec_wf_classification_group)
- Classification Rule (sn_sec_wf_classification_rule)
- Risk Calculator (sn_sec_calculator_group)
- Risk Calculator Rule (sn_sec_calculator_rule)
- Risk rule field (sn_sec_calculator_risk_field)
- Remediation Target Rules (sn_sec_wf_ttr_rule)
- Rollup config (sn_sec_wf_rollup_config)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Approval configuration (sn_sec_cmn_approval_config)
- Approver level (sn_sec_cmn_approver_level)
- Remediation Task Rule (sn_sec_rem_task_rule)
- Auto-close Rule (sn_vul_cmn_auto_close_rule)
- Exception Rules (sn_sec_exception_rule)
- Change Approval (sn_sec_exception_change_approval)
- Exception Management Configuration (sn_sec_exception_config)
- Policy Exception Reason Mapping (sn_sec_exception_policy_reason_mapping)
- Questionnaire Configuration (sn_sec_exception_questionnaire_config)
- Vulnerability Compensating Control relationship (sn_vul_cmn_m2m_entry_compensating_control)
- Widget Grouping (sn_sec_sem_widget_grouping)
- Widget Aggregation (sn_sec_sem_m2m_widget_dashboard)
- Dashboard (sn_sec_sem_dashboard)
- Dashboard Widgets (sn_sec_sem_dashboard_widgets)

Security Support Common deprecated tables

- Security Calculator Group (sn_sec_cmn_calculator_group)
- Security Calculator (sn_sec_cmn_calculator)
- Security Classification Group (sn_sec_cmn_classification_group)
- Security Classification Rule (sn_sec_cmn_classification_rule)
- Policy Exception Reason Mapping (sn_sec_cmn_policy_reason_mapping)

Vulnerability Response deprecated tables

- Vulnerability Assignment Rule (sn_vul_assignment_rule)
- Vulnerability Calculator (sn_vul_calculator_group)
- Vulnerability Calculator Rule (sn_vul_calculator)
- Vulnerability Risk Rule (sn_vul_calc_risk)
- Risk rule field (sn_vul_risk_field)
- Classification Group (sn_vul_classification_group)
- Classification Rule (sn_vul_classification_rule)
- Vulnerability Remediation Status (sn_vul_m2m_ttr_status)
- Remediation Target Rule (sn_vul_ttr_rule)
- Vulnerability Rollup Calculators (sn_vul_rollup)
- Exception Rule (sn_vul_auto_exception_rule)
- Vulnerability State Change Approval (sn_vul_change_approval)
- Exception Management Configuration (sn_vul_exception_config)
- Vulnerability Compensating Control relationship (sn_vul_m2m_entry_compensating_control)
- Policy Exception Reason Mapping (sn_vul_policy_reason_mapping)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response common workspace deprecated table

Saved Filters (sn_vul_cmn_ws_saved_filter)

Configuration Compliance deprecated tables

- Auto Exception Rules (sn_vulc_auto_exception_rule)
- State Change Approval (sn_vulc_state_change_approval)

New columns introduced in findings tables

Vulnerable Item [sn_vul_vulnerable_item] table.

- remediation_plan
- remediation_commitment_dt_tm
- auto_exception_rule (reference=sn_sec_exception_rule)
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Application Vulnerable Item [sn_vul_app_vulnerable_item] table.

- remediation_commitment_dt_tm
- status
- age_duration
- source_risk_score
- times_found
- first_found_dt_tm
- resolution_dt_tm
- last_opened_dt_tm
- auto_exception_rule (reference=sn_sec_exception_rule)
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Test Result [sn_vulc_result] table.

- closed_by
- first_found_dt_tm
- last_found_dt_tm
- opened_at
- opened_by
- resolution_dt_tm
- last_state_changed_on
- sys_class_name
- integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- backup_state
- backup_substate
- business_criticality
- short_description
- status
- source_risk_score
- times_found
- close_notes
- substate
- state_inheritance_count
- priority
- reopened
- remediation_plan
- remediation_commitment_dt_tm
- auto_exception_rule (reference=sn_sec_exception_rule)
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Container Vulnerable Item [sn_vul_container_image_vulnerable_item] table.

- remediation_plan
- remediation_commitment_dt_tm
- auto_exception_rule (reference=sn_sec_exception_rule)
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Remediation task [sn_vul_vulnerability] table.

- remediation_commitment_dt_tm
- remediation_plan
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Application Remediation Task [sn_vul_app_vulnerability] table.

- remediation_commitment_dt_tm
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task [sn_vulc_result_group] table.

- remediation_commitment_dt_tm
- remediation_plan
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Container Remediation Task [sn_vul_container_vulnerability] table.

- remediation_commitment_dt_tm
- remediation_plan
- change_approval (reference=sn_sec_exception_change_approval)
- ignore_expiration_for_risk_reduction_dt_tm
- ignore_expiration_dt_tm

Security Exposure Management Workspace Roles

List of roles installed with Security Exposure Management, defining user permissions and access for Security Exposure Management-related tasks.

Application	Role title	Description	Contains roles
Vulnerability Response Common	sn_vul_cmn.usem_admin	Configures rules, integrations, and related settings for Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance.	• sn_vul.vulnerability_admin • sn_vul.app_sec_manager • sn_vul_container.vulnerability_admin • sn_vulc.admin
Administration for Security Exposure Management	sn_sec_wf.read_admin_rules	Read access to administration rules.	• sn_sec_calculator.read • sn_vul_cmn_ws.read_admin_rules • sn_vul_cmn.read_auto_close_rules
Administration for Security Exposure Management	sn_sec_wf.manage_admin_rules	Create, read, update, and delete administration rules.	• sn_vul_cmn.manage_auto_close_rule • sn_sec_wf.read_admin_rules • sn_vul_cmn_ws.write_admin_rules • sn_sec_calculator.admin
Exception Management for Unified	sn_sec_exception.approver	Approve or reject exception requests, false positive	sn_sec_exception.read

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Role title	Description	Contains roles
Security Exposure Management		requests, and exception rules.	
Exception Management for Unified Security Exposure Management	sn_sec_exception.read	Read access to exception management configuration and exception rules.	None.
Exception Management for Unified Security Exposure Management	sn_sec_exception.admin	Create, read, update, and delete exception management configuration and exception rules.	sn_sec_exception.read
Risk Scoring for Security Exposure Management	sn_sec_calculator.read	Read access to records in the `sn_sec_calculator` scope.	None.
Risk Scoring for Security Exposure Management	sn_sec_calculator.admin	Create, read, update, and delete records in the `sn_sec_calculator` scope.	sn_sec_calculator.read

Visualization widget fields

Use this reference to understand the fields available on the Visualization widget form. These fields define how the widget appears, behaves, and groups data.

Field	Description
Widget name	Enter a clear and descriptive title for the widget.
Visualization group	Select the group where this widget appears. (*Risk and exposure*, *Remediation progress*, *Asset impacted*).
Chart type	Choose the type of visualization (*Vertical Bar*, *Horizontal Bar*, *Donut*, *Pie*, *Single Score*).
Display order	Specify the position of the widget within its carousel. Lower numbers appear first.
Applies to	Select one or more findings tables (for example, Infra vulnerabilities, Application vulnerabilities, Misconfigurations). The system identifies intersecting columns between tables for data grouping.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Group by	Select the field to group the widget data by. Each widget must have a unique group by value.
Data filter [Optional]	Add filter conditions to refine the data displayed in the widget.

Re-evaluating the exceptions for selected records in the Security Exposure Management Workspace

In the Security Exposure Management Workspace, when you evaluate the exception rules for a set of records in the Re-evaluate and update the remediation properties modal, their deferral status and until date of deferral are updated as per the latest exception rules.

Scenarios

You may come across the following scenarios, when you evaluate the exceptions for a selected set of records in the Re-evaluate and update the remediation properties modal in the Security Exposure Management Workspace:

Scenario 1: when the selected records are already deferred manually and they match the condition of an exception rule, these records remain in the Deferred state without any changes.

Scenario 2: when the selected records match the condition in the exception rules and these records are in a non-deferral state (such as open, In Review, Under Investigation), then these records are deferred until the date defined in the exception rule.

Scenario 3: when the selected records are already in the Deferred state (that are deferred using the exception rule A), they remain in the Deferred state in the following scenarios:

- the exception rule expires and the records don’t match the condition
- the exception rule expires and the records match the condition
- the exception rule A expires and records match the condition of another exception rule B.

Scenario 4: Consider that the records are deferred using an exception rule. When you change the exception rule condition such that the Deferred state of the records is no longer valid and then reevaluate the exception rules for these records:

- the records move to the Open state
- the until date, Deferral date, Deferral count, and other fields are updated.

Example: Consider that you are evaluating the exceptions for following host vulnerable items (VITs)

Consider the exception rule with the following details:

Exception rule details

Field	Description	Value
Name	Name of the exception rule.	Deferring critical VITs
Valid from	Date from which this rule is active to defer the VIs.	20-08-2024

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception rule details (continued)

Field	Description	Value
Valid to	Date from which the remediation task stops accepting new VIs.	30-11-2024
Reason	Reason to create this exception rule.	Risk Accepted
Assignment group	Group that the remediation task that was created for tracking the deferred VIs is assigned to.	Remediation Group 1
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.	This rule has been created to defer the critical VITs automatically.
Condition	Filter condition for the VIs that can be defined while processing the VIs.	Risk rating = 5 - Critical
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run.	Yes
State	State of the exception rule.	Approved
Execution order	Unique order for each exception rule.	100
Deferred until	Date until when the VULs and VIs are deferred. On this date, the created VUL is closed, all the VIs move out of the group, and group rules are reapplied.	2024-12-23 16:10:29

The following table shows how the state changes when the exception rules are reevaluated for multiple VITs simultaneously:

Records for which exceptions are re-evaluated

VIT Number	State	Risk Rating	Updated state after reevaluating the exceptions -1	Until date - 1
VIT120067	Open	2 - Low	Open	-
VIT120068	In Review	3 - Medium	In Review	-
VIT120069	Under Investigation	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120070	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120071	Deferred	2 - Low	Deferred	2024-10-02 16:10:29

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Records for which exceptions are re-evaluated (continued)

VIT Number	State	Risk Rating	Updated state after reevaluating the exceptions -1	Until date - 1
				(Deferred manually)
VIT120072	Closed	5 - Critical	Closed	-

When the condition in the preceding exception rule is modified to `Risk rating = 2 - Low` and **Deferred until** is modified to `2024-12-31 14:10:23` the records are updated as follows:

Records for which exceptions are reevaluated

VIT Number	Updated state after reevaluating the exceptions -1	Risk-rating	Updated state after reevaluating the exceptions - 2	until date - 2
VIT120067	Open	2 - Low	Deferred	2024-12-31 14:10:23
VIT120068	In Review	3 - Medium	In Review	-
VIT120069	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120070	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120071	Deferred	2 - Low	Deferred (No change in the state)	2024-10-02 16:10:29 (No change in the until date)
VIT120072	Closed	5 - Critical	Closed	-

Vulnerability Response

The National Vulnerability Database (NVD) and other sources collect information about known vulnerabilities. These vulnerabilities can include weaknesses in software, operating systems that malware can exploit, and other attacks. The ServiceNow® Vulnerability Response application aids you in tracking, prioritizing, and resolving these vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response

Explore



Learn about the features of Vulnerability Response

Set up and Configure



Install and set up your Vulnerability Response application

Integrate



Extend Vulnerability Response by integrating it with other applications

Use the Vulnerability Response Workspaces



Learn how to monitor, manage, and remediate VITs in the Vulnerability Manager, IT Remediation and Vulnerability Assessment Workspaces.

Remediate



Use the features of Vulnerability Response to remediate your vulnerabilities and protect your assets

Analytics & Reporting



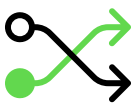
Monitor remediation progress

Reference



Get more details about Vulnerability Response release notes, components and reference information about fields, tables, and properties

Upgrade Vulnerability Response to USEM



Upgrade Vulnerability Response applications to Unified Security Exposure Management.

Troubleshoot and get help

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring the Vulnerability Response application

The ServiceNow® Vulnerability Response application imports and automatically groups vulnerable items according to rules that permit you to remediate vulnerabilities quickly. Vulnerability data is pulled from external sources, such as the National Vulnerability Database (NVD) and third-party integrations, and processed with applications developed by ServiceNow®.

Watch an overview about vulnerability response that defines vulnerable items, remediation tasks, and their life cycles.

Vulnerability Response and your enterprise environment

Typically, within an Enterprise environment, organizations use vulnerability scanners and assessment tools to identify and manage the risks vulnerabilities pose to their assets. Vulnerabilities that are identified by these tools translate as risks to the security and IT teams responsible for maintaining and securing an organization's assets. Some risks might include but aren't limited to the following types of identified vulnerabilities:

- Reliance on outdated software or misconfigured systems
- Unsecured network protocols
- Dependency on flawed third-party software libraries
- Poor or inconsistent system administration hygiene
- Baseline system images that are not hardened

As these potential risks are exposed, security and IT teams commonly face challenges in processing and handling the volume of vulnerability information generated from their scanning and assessment tools. Specifically,these teams find themselves overwhelmed when managing a high volume of identified vulnerabilities and crafting actionable response efforts to mitigate the potential risks that face their organizations.

You might identify these challenges to your own security posture by asking the following questions:

- Which identified vulnerabilities should be reviewed first?
- What do these identified vulnerabilities mean to our organization?
- Who should be accountable for and own identified risks?
- Who should be hands-on, working to resolve/mitigate these risks?
- How do we effectively mitigate identified vulnerabilities with the resources we have?
- What are the potential unintended outcomes of reducing the identified vulnerabilities?
- What process do we follow to remediate vulnerabilities, track the steps we've taken, and follow up to be sure our actions worked?
- How do we know if we are making progress reducing our over-all risk posture?

Vulnerability Response, Security Operations and the ServiceNow AI Platform®

The Vulnerability Response application is part of the Security Operations suite. Together these applications help you protect your assets by improving your overall security posture.

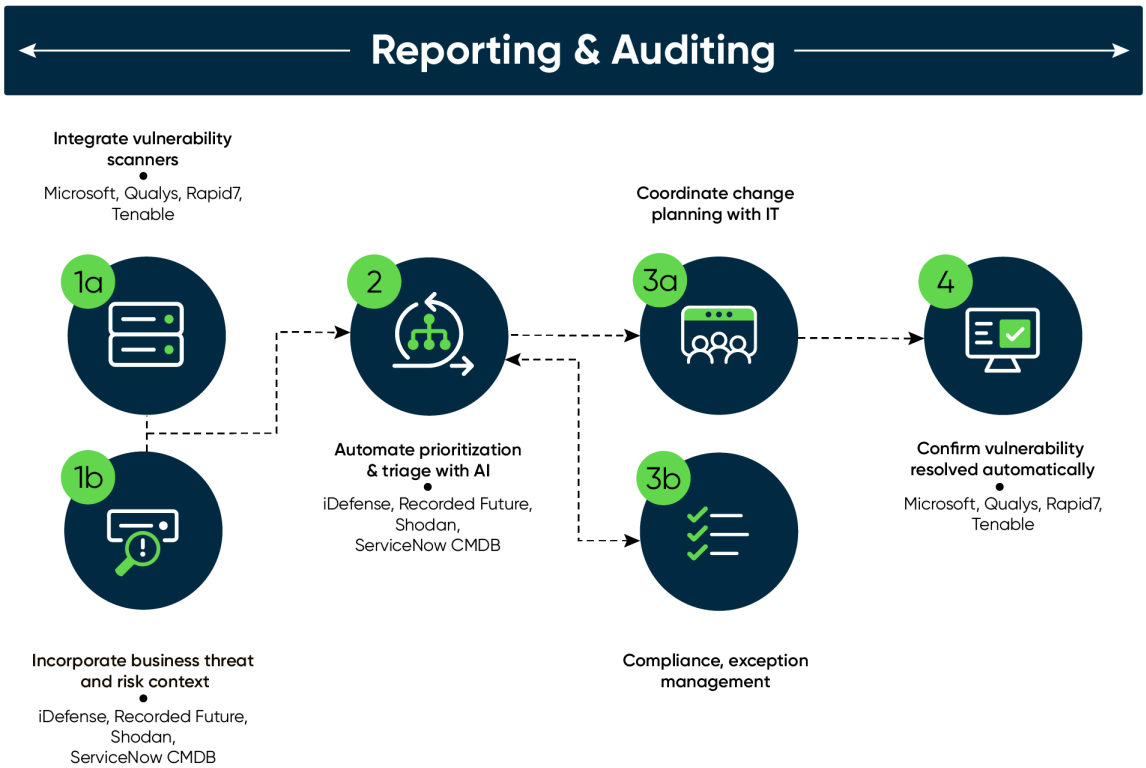
The ServiceNow Vulnerability Response application has two primary goals:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Help the security teams challenged with handling huge amounts of vulnerability data.
- Help the operations teams tasked with resolving vulnerabilities.

In this way, you can use the Vulnerability Response application to automate the flow of information, from integration through investigation, and then on to resolution.

The vulnerability management process in the ServiceNow AI Platform® might involve processes, data, reporting, and automation with the CMDB.



- Integrate third-party scanners and ServiceNow® applications with the Vulnerability Response application to ingest known vulnerability data.
- Enhance your ingested vulnerability data with exploit, threat intelligence, risk, and business context. Use this data to help you with patching and remediation strategies.
- Imported vulnerabilities from the NVD and detection data from third-party products are reconciled with the assets in your CMDB. Triage might include: creating remediation tasks composed of multiple vulnerable items, that is, your assets that are determined to have vulnerabilities, grouping these tasks by category, prioritizing them, and assigning them to teams.
- Employ coordinated change and exception management to help you resolve vulnerabilities that might require additional manual intervention, more time to resolve, or extensive research.
- Confirm vulnerabilities are resolved and updated automatically by detections from your scanner products.

Who might use Vulnerability Response in your organization

Vulnerability Response users generally fall into two personae.

Vulnerability Analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The vulnerability analyst persona is usually in Security, Risk and Compliance, or Management. These users monitor vulnerabilities and determine when to initiate the remediation processes.

Important: The vulnerability analyst primarily uses the Vulnerability Manager Workspace to monitor and create remediation tasks.

Remediation Owner

The Remediation Owner persona is usually a part of IT Operations, DevOps/ Engineering, or a Service Owner. These users complete the remediation tasks necessary to fix vulnerabilities. They might submit exception or change requests if controlled processes are required for asset maintenance or removal.

Important: The remediation owner primarily works on remediation tasks from within the IT Remediation Workspace.

Application Vulnerability Response

The Application Vulnerability Response (AVR) feature of the ServiceNow® Vulnerability Response application imports application vulnerable items (AVITs) and according to rules allows you to remediate application vulnerabilities. It is available by separate subscription. For Application Vulnerability Response documentation see Exploring Application Vulnerability Response.

Available versions

For a glossary of terms and more references that include links, troubleshooting, knowledge articles, in addition to field data on the forms and records found in Vulnerability Response, see Vulnerability Response reference information.

Release version	Release Notes
Vulnerability Response v26, v25.0, v24.0, v23.0	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Vulnerability Response applications and CSDM tables

The Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications manage (contribute data to) CSDM tables. These applications also use data from CSDM tables that other applications generate. Several ServiceNow products, therefore, benefit from and add value to these Security Operations applications. See Vulnerability Response applications and CSDM tables for more information.

Migrating from Vulnerability Response to Unified Security Exposure Management (USEM)

The Migration assistant for Unified Security Exposure Management is a centralized utility that guides and automates the migration from Vulnerability Response applications to Unified Security Exposure Management (USEM). USEM provides a unified foundation that consolidates data models, streamlines features, and enhances performance and scalability across all Security Exposure Management applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Why Migrate to USEM

Migrating to USEM delivers significant benefits, including improved performance, simplified workflows, advanced analytics, unified exception management, and better scalability; empowering security teams to respond faster to emerging threats.

How does the Migration assistant for Unified Security Exposure Management help

Migrating from Vulnerability Response products to USEM can be complex, involving changes to data models, plugins, integrations, and workflows. The Migration assistant for Unified Security Exposure Management simplifies this process through:

- **Guided experience**: A step-by-step interface ensures all critical actions and prerequisites are completed.
- **Conflict resolution**: Ensures that prerequisites are met of and assists in upgrading other related apps to USEM.
- **Post-migration verification**: Confirms that records and integrations are updated correctly and provides best practices for post-migration checks.

The tool is modular, reduces risk and manual effort, and automates data transfer, rule mapping, and configuration updates making your transition to USEM seamless and efficient.

Related topics

Migrate to Unified Security Exposure Management (USEM) from Vulnerability Response

Planning for migration from Vulnerability Response to Unified Security Exposure Management (USEM)

When upgrading to Unified Security Exposure Management (USEM) v30.0, you can choose between two primary methods: the Migration assistant for Unified Security Exposure Management and the Store App Manager. This topic outlines the capabilities of each method across key migration steps.

Migration assistant for Unified Security Exposure Management vs Store App Manager

Step	Activity	Migration assistant for Unified Security Exposure Management	Store App Manager
1	Pre-upgrade insights	# Supported	# Not Supported
2	Temporarily disable integrations	# Supported	# Not Supported
3	Introduce schema changes	# Supported	# Supported
4	Migrate data from rules	# Supported	# Supported
5	Introduce USEM functionality	# Supported	# Supported
6	Upgrade other VR Store Apps to v30.0 (USEM)	# Supported	# Not Supported

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Why choose the Migration assistant for Unified Security Exposure Management

The Migration assistant for Unified Security Exposure Management provides a more comprehensive and controlled upgrade path compared to the standard Store App Manager. It's designed to offer a robust and interactive experience, ensuring a smoother transition to USEM v30.0. The advantages of the Migration assistant for Unified Security Exposure Management are:

- **Comprehensive support**: It handles critical pre-upgrade assessments and ensures that all necessary schema changes and data migrations from existing rules are managed seamlessly.
- **Integration safety**: The toolkit can temporarily disable integrations during the migration, avoiding potential disruptions and promoting data integrity.
- **Full functionality and compatibility**: It fully supports the introduction of new USEM functionality and is essential for upgrading other Vulnerability Response Store Apps to be compatible with USEM v30.0.
- **Reduced risk**: By providing pre-upgrade insights and managing integrations, the toolkit significantly reduces the risk of upgrade failures.
- **Controlled process**: It offers a more guided and controlled migration, leading to a faster and more predictable outcome.
- **Enhanced visibility**: Provides better visibility into each step of the upgrade process and its dependencies.

In summary, for a successful and efficient upgrade to USEM v30.0, the Migration Assistance Tool is the preferred choice.

Related topics

Migrate to Unified Security Exposure Management (USEM) from Vulnerability Response

Installation of Vulnerability Response and supported applications

The Vulnerability Response application is available from the ServiceNow Store. The application supports other ServiceNow applications and third-party integrations that you also download from the ServiceNow Store. More options also are available to extend the basic setup.

Tasks for basic setup

The Vulnerability Response application is required as a first step. For more information about installing it, see Implementation checklist for the Vulnerability Response application and Install the Vulnerability Response application.

- After installation is completed, you can Configure Vulnerability Response using Setup Assistant.

  With the Setup Assistant, assign users and groups for access to the application, create or edit assignment rules, remediation task rules, and target dates, set up risk calculators.

- You can also select, install, and configure one or more supported third-party integrations from the Setup Assistant. These integrations retrieve vulnerability data from external systems and vendors. For more information about how integrations work and the integrations supported by Vulnerability Response, see Vulnerability Response integrations.
- Prior to implementing any third-party integrations, run the NVD integration and CWE scheduled job as part of your initial setup of Vulnerability Response.

  See Importing data with the NVD and CWE integrations and managing third-party libraries and Configure and run the scheduled job for updating CWE records for more information about installing, configuring, and viewing the NVD and CWE libraries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Select an analytics application, when applicable. The Performance Analytics Content Pack for Vulnerability Response application contains reports that cover all stages of the vulnerability management lifecycle.

  [Optional] Install and configure the Performance Analytics for Vulnerability Response [PA] application application.

- Select a solutions application, when applicable. Solution management helps you correlate the vulnerabilities in your environment with the solutions that could remediate them. [Optional] Install the Solution Management for Vulnerability Response application.

  Note:

  - When the Vulnerability Solution Management application is enabled, the Microsoft Security Response Center Solution Integration and the Red Hat Solution Integration are available to edit in Setup Assistant.

  - Vulnerability Solution Management requires a separate subscription. For more information, see Vulnerability Solution Management.

- [Optional] Install the ServiceNow Agent app and the Vulnerability Response Mobile app for the Mobile experience for Vulnerability Response.

Other setup tasks you can perform

These additional setup tasks add to your basic configuration and support remediation with options for reporting, email notifications, native integration configuration, and working with vulnerable items. Most of these tasks are performed outside of the Setup Assistant. See Additional Vulnerability Response setup and configuration tasks.

Advanced tasks outside of the basic setup

These optional configuration tasks are performed outside of Setup Assistant and require coding or advanced ServiceNow expertise and are not considered part of the basic configuration. See Advanced Vulnerability Response configuration tasks.

Vulnerability Response personas and granular roles

Before you can successfully remediate vulnerabilities with the Vulnerability Response application, you must assign personas and roles to your users and groups in Setup Assistant.

One of the first configuration steps required for the Vulnerability Response application is to assign roles to users and groups. Roles define what users and groups can see and do in Vulnerability Response, Performance Analytics for Vulnerability Response, and all third party integrations with Vulnerability Response.

You assign persona roles to existing users and groups in Setup Assistant. See Assign the Vulnerability Response persona roles using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

However, for more control over what users and groups can do and see in the Vulnerability Response application at the task level, you may prefer using granular roles. For more information, see Manage persona and granular roles for Vulnerability Response.

If you have already assigned roles using Setup Assistant and you want to manage granular role assignments for all users and groups from the User Administration module, see Manage persona and granular roles for Vulnerability Response for more information.

Persona roles and granular roles starting

Key terms.

Role

Roles define what users and groups can see and do in the Vulnerability Response application.

Group

A set of users who share certain roles and a common purpose.

Persona role

A pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

Inherited roles

A term that describes roles that users automatically acquire when they are assigned other roles. For example, any users or groups assigned with the sn_vul.remediation_owner persona role also inherit the sn_vul.read_assigned,sn_vul.write_assigned granular roles.

Access control list (ACL)

Access control lists restrict access to data by requiring users to pass a set of requirements before they can interact with it.

Starting from Vulnerability Response v16.5, to protect reports from being exposed, set the **All report_view ACLs** as *active=true*. This ACL ensures that the protected data is only available to authorized users.

You assign groups and users to persona roles in Setup Assistant.

Note: In Setup Assistant, the system admin role (admin) is required for the tasks in the first section, assigning roles and installing integrations. After you assign persona roles in Setup Assistant and install integrations, you may prefer to assign a user or group with the sn_vul.vulnerability_admin role to finish any remaining tasks in Setup Assistant and to manage the Vulnerability Response application.

The following table lists Vulnerability Response persona roles installed with the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

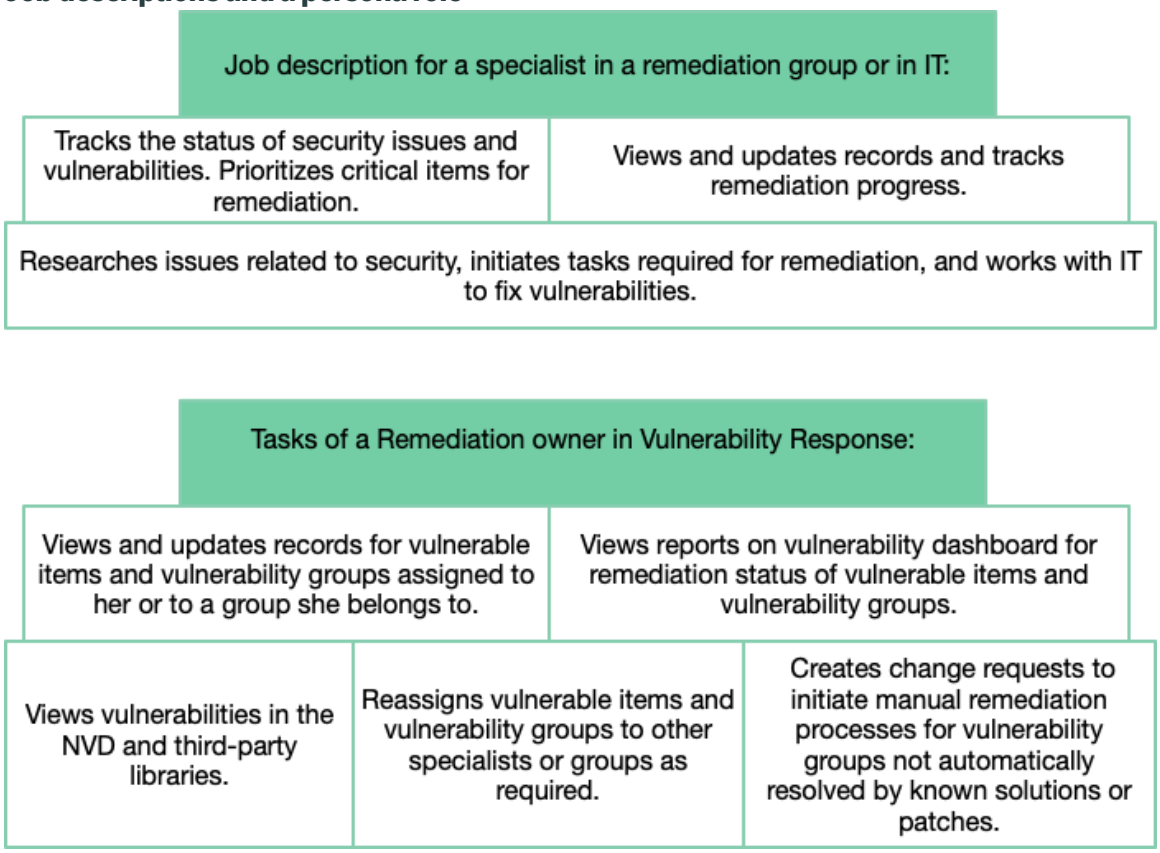
Persona roles for Vulnerability Response	Description
Assign sn_vul.vulnerability_admin - Vulnerability Admin to users or groups.	Users with this role have complete access to the Vulnerability Response (VR) application and its records. Users with this role configure all VR applications and rules and install third party integrations.
Assign sn_vul.vulnerability_analyst - Vulnerability Analyst to users and groups.	Users and groups with this role view and update all records for VI remediation.
Assign sn_vul.remediation_owner - Remediation Owner to users and groups.	Users and groups with this role remediate vulnerabilities assigned to them or to a group they belong to. Groups or users with this role view and update the records assigned to them or to a group they belong to.
Assign sn_vul.ci_manager to users and groups.	Users and groups with this role manage reclassification of unmatched configuration items (CIs) that are not found in the Configuration Management Database (CMDB).
Assign read access to specific areas in the application by task.	For example, assign sn_vul.read_all so a user can view all VR records. For read access to view remediation task rules, assign sn_vul.read_group_rules. Users and groups with this role do not update records.

Granular roles and persona roles

One way to think about persona roles is to consider how their descriptions may relate to job descriptions for various IT or vulnerability remediation positions in your organization. The following figure illustrates a possible job description for a remediation specialist in IT, and how the tasks associated with this job relate to the tasks of a remediation owner persona role in the Vulnerability Response application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Job descriptions and a persona role



Both the job description and the remediation owner persona role could be defined as a series of remediation tasks. In the preceding image, a job description and a persona role in green blocks sit atop the tasks that describe them. In this example, some of the typical job requirements for a specialist in a remediation group correspond directly to the tasks that make up the remediation owner persona in Vulnerability Response: Review and update records, track the remediation status of vulnerabilities, prioritize items for remediation, and apply fixes and patches with IT.

Sometimes, however, the jobs in your organization may not directly correspond to the tasks that make up one of the five persona roles in the Vulnerability Response application. For various reasons, such as protecting sensitive data, or complying with regulations, you must limit the broad access some of the persona roles provide to your users and groups. Or, conversely, you are required to provide users and groups with more access so they can perform their jobs. Using granular roles, you can easily customize roles and control the access users and groups have to Vulnerability Response, Performance Analytics for Vulnerability Response, and third party integrations.

The granular roles define the tasks

The names for the granular roles in Vulnerability Response usually describe what users can do and see in the Vulnerability Response application. For example, in the previous image, users and groups with the Remediation owner persona assigned have the sn_vul.read_assigned and sn_vul.write_assigned granular roles. These granular roles permit users or groups to view and update vulnerable items and remediation task records that are assigned to them. To view descriptions of specific granular roles, as a user with the system admin role, navigate to **User Administration** > **Roles** and locate the role that you want. Roles that are automatically inherited when a role is assigned are listed. Also, when a role depends on other role assignments, any required roles are also listed.

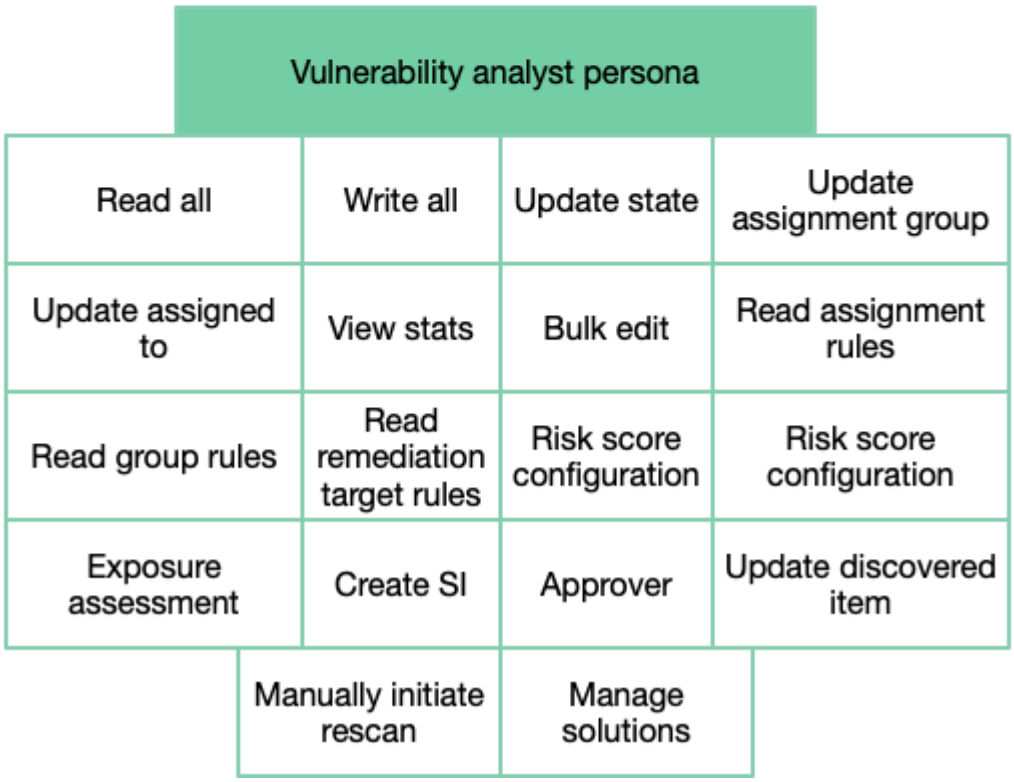
In the following image, the granular roles of both the remediation owner persona role and the vulnerability analyst persona are illustrated. Note that the remediation owner persona does not

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

include the read_all and write_all permissions of the vulnerability analyst persona. The granular roles, read_all and write_all, are required before users and groups can read and edit all of the vulnerable item and remediation task records. To customize these roles, simply add or remove granular roles to expand or limit access.

Granular roles and the remediation owner and vulnerability analyst personas





If you want your users and groups to have more access than the persona roles permit, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles.

Note: To assign and edit granular roles in the User Administration module, the system admin role is required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Granular roles with scripting access

The following roles provide scripting access to the listed tables:

Role	Table	Application
sn_vul.manage_auto_close_stale_vi	sn_vul_cmn_auto_close_rule	Vulnerability Response
sn_vul.app_manage_auto_close_rule		Vulnerability Response
sn_vul_container.manage_auto_close_stale_vi		Container Vulnerability Response
sn_vul_container.manage_assignment_rules	sn_vul_assignment_rule	Container Vulnerability Response
sn_vul.app_manage_assignment_rules		Application Vulnerability Response
sn_vul.manage_assignment_rules		Vulnerability Response
sn_vul_agile.write	sn_vul_agile_tool	Vulnerability Response
sn_vul_int_fw.configure_integrations	sn_vul_int_fw_integration	Vulnerability Response

Granular roles in the User Administration module

For an example of how to manage granular roles for a user or group, see Manage persona and granular roles for Vulnerability Response.

To assign persona roles, see Assign the Vulnerability Response persona roles using Setup Assistant.

Vulnerability Response assignment rules overview

Define the criteria by which vulnerable items (VITs) are automatically assigned to an assignment group for remediation.

A default assignment rule, **Assign to CI support group**, is included in the base system assigning vulnerable items to the **CI Support Group**. The Assign to CI support group rule assigns a VIT to whatever support group is set for the configuration item (CI) that is associated with the VIT.

Note: The assignment rules do not reevaluate manually created assignments.

Assignment type, whether **Manual** or **Rule** is available from the VIT form and the list view. Any VIT that was originally assigned by a rule but subsequently manually reassigned contains a reference to the original rule.

Use Assignment rule and Assignment type information to identify cases where the assignment rules did not find a correct match for the intended recipient. You can also use the information to identify which rules had the most reassignments.

The Assignment groups set by Assignment Rules are used by **Remediation Task Rules** to assign owners to remediation tasks (VULs).

Note: To make Rapid7 InsightVM asset tags available for use in the Condition filter for Assignment Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

Case sensitivity for the search text you enter in the condition builder is not supported on this record or form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assigning vulnerable items automatically

There are three different ways to assign vulnerable items using **Assign using**:

- User group: This option allows you to select any of the existing ServiceNow AI Platform® user groups.
- User group field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default, you see the following three group fields:
  - None: Indicates no default value for this mandatory field
  - Configuration Item: Approval Group
  - Configuration Item: Assignment Group
  - Configuration Item: Support Group
- Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow expertise. For more information on how to use the script editor to define complex conditions, see the KB0965240 KB article.

Run high priority rules (items that need special handling, where risk is critical, or a VIT should be handled by regulatory compliance) first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign VITs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.

Assignment rule evaluation process

Assignment rules are used to evaluate and assign a VIT when a new VIT is opened, that is, imported, created manually, or reopened. Unless you manually reapply assignment rules after the VIT or its state changes, a VI is evaluated once.

The following process is used for each new, updated or reopened VIT:

- For each vulnerability assignment rule, the VIT is compared to the assignment filter, lowest order rule first.
- Where the condition matches, the VIT is assigned an assignment group. The lookup stops.
- Where the conditions do not find a match among all the other rules, the VIT is assigned to the default assignment group, if a default rule exists.

  Once the vulnerable item has been assigned, the appropriate remediation task rule uses assignment as one of its criteria for placing the vulnerable items into a remediation task. See Vulnerability Response remediation tasks and remediation task rules overview and Filtering within Vulnerability Response for more information.

> **Note:** The default rule is the rule with the highest execution order value. A final rule to use that is a good catch-all is `active=true`. If there is no default rule, the VIT remains unassigned when the remediation task rule makes the assignment.

Reapplying assignment rules

When you change an assignment rule, use the **Apply Changes** button on the Assignment Rules list page to rerun all the changed rules on all active Open VIs, except those that were manually assigned.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If the *Reapply all vulnerability assignment rules* scheduled job has not run before the first time you use **Apply Changes**, then it runs all the assignment rules on all Open VITs except those VIs that were manually assigned. After that, all subsequent uses of **Apply Changes** rerun only the changed rules and any dependent rules. Changes to one rule may result in a VIT matching a different unmodified rule. Reapplying assignment rules does not regroup the vulnerable items.

The scheduled job [*Reapply all vulnerability assignment rules*] is inactive by default. When activated, it applies all the rules to all open VITs except those manually assigned. It can run **Daily**, **Weekly**, **Monthly**, **Periodically**, **Once**, or **On Demand**. Depending on how many active VIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

Upgrade customers should refer to the Vulnerability Response Release Notes for information regarding the impact of this feature on existing VITs.

Important: As a vulnerability admin and analyst, you can obtain the latest assignments for selected vulnerable items in the Vulnerability Manager Workspace. This method is more efficient than running the Assignment Rules for all vulnerable items in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

When an assignment group on an assignment rule changes, the vulnerable items can be automatically reevaluated and regrouped by enabling the system property sn_vul.rerun_task_rules and business rule Link to Remediation Tasks.

To enable the system property:

1. Navigate to **All** > **System Properties** > **All Properties**.
2. Open sn_vul.rerun_task_rules system property.
3. In the **Value** field, set the value to true.

When the system property is set to true, and the assignment rules are reapplied, the vulnerable items are unlinked from the remediation tasks, where the condition no longer matches.

Note: By default, the system property sn_vul.rerun_task_rules is set to false.

To automate the regrouping of vulnerable items, you must activate the business rule Link Remediation Tasks.

To enable the business rule:

1. Navigate to **All** > **System Definition** > **Business Rules**.
2. Open Link to Remediation Tasks business rule.
3. Select the **Active** check box to activate the business rule.

The business rule on being enabled, regroups the vulnerable items by moving them to the relevant group or by creating a group if they can't be grouped under any existing group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The vulnerable items are removed from the groups without deleting the groups.
- Only those items are removed which are created using remediation task rules or remediation effort.
- Regrouping is done automatically only when the assignment group changes as part of an assignment rule and not when it is manually changed.
- Assignment rules do not apply to VITs in the Deferred state. If a VIT is deferred, you must manually assign it if needed.

Regrouping in workspaces is performed for remediation tasks, which are created from a Remediation effort.

Vulnerability Response remediation tasks and remediation task rules overview

Configure remediation tasks (VULs) to help analysts and remediation specialists organize vulnerable items (VI) and analyze them in bulk. The criteria by which remediation tasks are formed is configured so that you do not have to manually assign vulnerable items into remediation tasks. Using remediation tasks, you can monitor progress and drive the remediation process more efficiently.

Tracking deferral counts for vulnerable items and remediation tasks

Track the number of times a vulnerable item, application vulnerable item, a container vulnerable item, or a remediation task is deferred. A scheduled job, **set deferral counts**, runs daily to post counts for the records that are deferred more than once in the Deferral count column. Records are displayed in the Multiple deferrals modules for VR, AVR, and CVR.

Refreshing vulnerable items automatically

Note: Vulnerable item refresh automation applies only to remediation tasks created using the condition filter or filter group. Automation does not apply to VIs that were added manually or grouped using Remediation Task Rules.

When the **Automatically update related vulnerable items** check box is selected, new VIs matching the remediation task filter criteria are automatically added to the task. Vulnerable items in the remediation task that no longer match the filter criteria are automatically removed from the task.

By default, when the remediation task leaves the **Open** state, the check box is cleared. If you want vulnerable items to continue being added to the remediation task, regardless of state, disable the *`Set auto refresh vulnerable items`* business rule.

You can select the check box again manually from the Under Investigation state. **Automatically update related vulnerable items** is not disabled when the remediation task moves into the **Awaiting Implementation** state. Once in the Awaiting Implementation state, no new vulnerable items can be added to the existing task, nor can existing vulnerable items be removed it.

Note: When a remediation task is created manually, and VIs are added using the **Condition** filter or **Filter Group**, the check box is unchecked. You have the choice to select the box or not.

Refreshing vulnerable items manually

For manually created remediation tasks with a **Filter Group** or **Condition** filter, when you click the **Refresh** associated vulnerable items related link on the **Remediation Task** page, any vulnerable items that match the filter criteria are added. Items no longer matching the criteria are removed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This action allows an immediate update of the list of vulnerable items and is used whether the **Automatically update related vulnerable items** check box is selected or not.

Manually created remediation tasks using **Condition** or **Filter Group** filter types are refreshed once an hour.

Understanding remediation task rules

Remediation task rules allow you to define how vulnerable items are automatically grouped and assigned. A default rule, **Vulnerability**, is included in the base system that gathers vulnerable items based on their vulnerabilities. However, you can group by any other set of values in columns accessible from the VI. These values could include configuration item (CI) support group, vulnerability severity, and, so on.

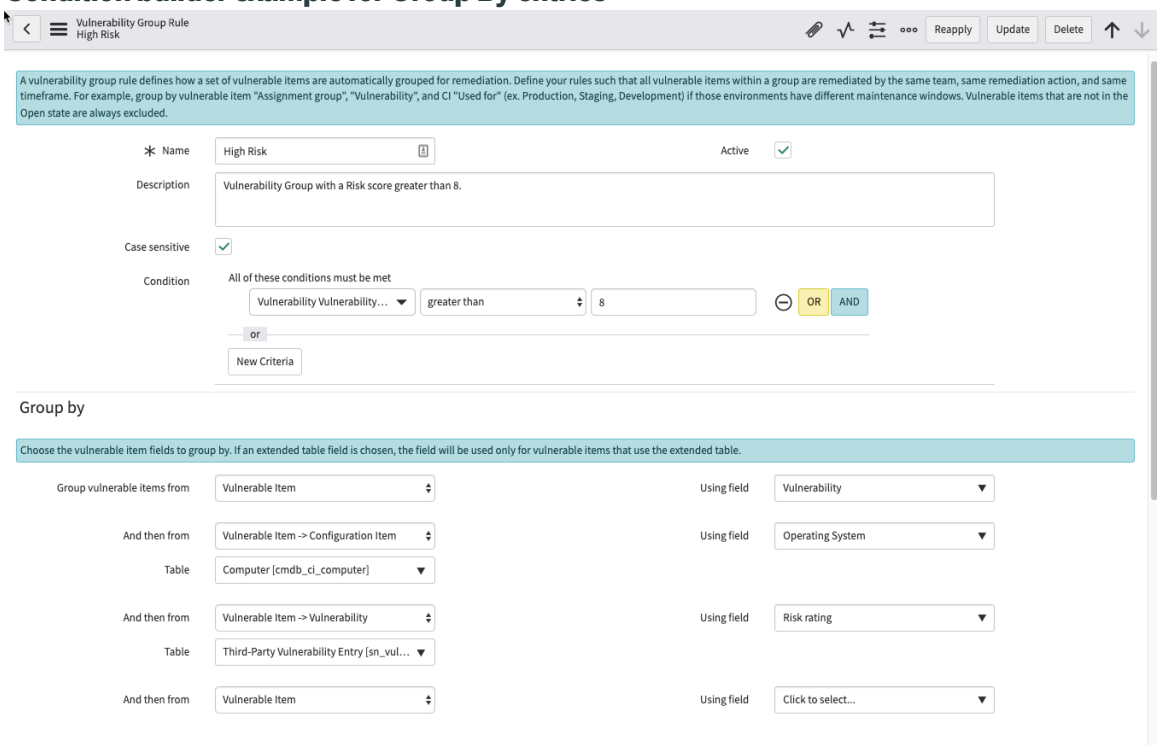
You can create any number of conditions. Once you set a Group by selection, another row appears. You can have up to six **Group by** selections. You can automate group assignment, as well. See Create or edit Vulnerability Response remediation task rules and Filtering within Vulnerability Response for more information.

Note: To make Rapid7 InsightVM asset tags available for use in the Condition filter for Remediation Task Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations.

For example, you can group your vulnerable items by the cost center of the vulnerable CI, or by the attack vector of the vulnerability. You can have one task rule for low severity vulnerabilities or low risk CIs. You can have another task rule for critical servers, and vulnerabilities with exploits — vulnerable items that expose the company to more risk.

A different set of rules can be used for vulnerable items that expose the company to more risk. The remediation task name is appended to the remediation task rule **Group by** values to make the short description of the new record. See Manually create a remediation task in Vulnerability Response for more information on available fields.

Condition builder example for Group By entries



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When a new vulnerable item is created, imported, or reopened after being closed, the vulnerability rules are evaluated against it. A VI is only evaluated once, automatically, unless it is reopened after being closed or the rules are reapplied manually.

The following process is used for each new or reopened VI:

- For each remediation task rule, the VI is compared to the remediation task rule filter.
- For each rule where the remediation task rule condition matches, the rule pulls the data from the **Group by** selections on the VI. It builds a group name and field. In this case, **High Risk: QID-32342:***Summary of QID-3242* (Name: vulnerability ID:vulnerability summary).

  Note: The short description field is limited to 160 characters. Longer vulnerability summaries are truncated.

  The rule checks to see if there is a matching **Open** remediation task that is assigned to the same assignment group as the VI.
  - If the task is found, the VI is added to the existing task in the **Open** state.
  - If no task in the **Open** state is found, the rule creates a **High Risk: QID-32342** task, assigns it to the same assignment group as the VI, and places the VI in the remediation task.

More than one remediation task rule can be defined, to group different kinds of vulnerabilities. Since each vulnerability is compared with the remediation task rule conditions before putting it in a remediation task, too many rules may have a performance impact.

By default, remediation task rules use the assignment group set by the **Assignment Rules** on the vulnerable item when grouping the items, and assigns the remediation task to match the vulnerable items.

As part of the default task rule, the assignment of these remediation tasks is controlled by the rules in the **Assignment Rules** module. For more information on assignment rules, see Vulnerability Response assignment rules overview.

When a task rule is deleted, from the form or list view, you have the option to delete all **Open** tasks created by that rule. Tasks not in the **Open** are excluded.

Reapplying remediation task rules

When you want to change a remediation task rule, use the **Reapply** button on the remediation task rule page to rerun the changed rule on all active **Open** remediation tasks created by that rule. It deletes and recreates remediation tasks based on the changed rule automatically.

Important: As a vulnerability admin and analyst, you can evaluate the remediation task rules for selected vulnerable items in the Vulnerability Manager Workspace. This method is more efficient than reapplying the Remediation Task Rules in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Vulnerability Response remediation target rules

Remediation target rules define the expected time frame for remediating vulnerable items (VI), much like SLAs provide a time frame for remediating the vulnerability itself. For example, if an asset contains PCI data (credit card data) then the vulnerability on that item must be fixed within 30 days according to PCI DSS.

Vulnerability managers can create remediation target rules by defining:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The remediation target
- The reminder target
- The reminder and notification recipients: Who should be notified when the vulnerable items (VIs) are past the reminder or remediation target date and haven't been remediated.
- The recalculation method: How the system updates the remediation target (RT) date when a vulnerable item's risk rating changes.

Vulnerability analysts and managers can see the remediation target date in the vulnerability item form and list views, as long as the vulnerable items aren't in Deferred, Resolved, or Closed state. Remediation target rules are run on import and rerun if a VI is reopened.

The **Remediation target date** is color-coded on the VI list view as dots, as follows:

- Vulnerable items that haven't reached their notification date are shown in green.
- Vulnerable items approaching the remediation target date are shown in orange.
- Vulnerable items past the remediation target date are shown in red.

A summary email, per remediation target rule, is sent when one or more VIs are either approaching their remediation target date or the remediation target date has passed.

Recalculation of remediation target date

Starting with Unified Security Exposure Management version 30.1.4 and Vulnerability Response version 26.4.4, administrators can configure how the system recalculates the remediation target date when a finding's risk rating changes.

- Under normal conditions, the system calculates the RT date as:

  Remediation Target = **Target from (date)** + **Target (days)**

- When the risk rating changes, the system calculates a new RT date using the formula below. The selected recalculation method determines whether this new date replaces the existing RT date.

  Recalculated RT date = **Field change time** + **Target (days)**

  Field change time captures when the risk rating changed. Target (days) uses SLA of new risk rating.

The following options define how the system applies the recalculated RT date when a risk rating changes:

Recalculation method	Description
Default calculation	Retains the existing RT date. The recalculated date isn't applied.
Recalculate from risk change date	Updates the Remediation Target date to: Field change time + Target (days) based on the new risk rating.
Recalculate from risk change date and always set to earliest target date	Compares the existing RT date with Field change time + Target (days) and applies the earlier date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recalculation method	Description
Recalculate from risk change date and set to earliest target date only when risk rating increases	If the risk increases: Compares the existing RT date and the recalculated RT date and applies the earliest date. If the risk decreases: Applies Field change time + Target (days) without comparison.

For configuration steps, see Recalculate a remediation target date.

Remediation target rules can be deactivated or deleted

When a rule is deactivated, the current remediation target dates for the VIs it was applied to are cleared. If a VI satisfies any active rule that rule is applied, otherwise the VI has no rule or target date, and its status is **No Target**.

When rules are deleted, the **Remediation target** date and related fields on closed, deferred, or resolved VIs are preserved. The **Remediation target** date and related fields on non-closed VIs are cleared and any dependent rules are reapplied.

Remediation target rule scenario

When multiple remediation target rules are applied to the same vulnerable item, the most restrictive rule is applied.

Note: Remediation targets are calculated from the **Last Opened** date plus the number of days (measured as 24-hour increments).

Starting from V17.1, remediation targets are calculated from the **Target from (date)**. The default value remains **Last opened date**.

For example, if a vulnerable item meets the condition for two remediation target rules:

Scenario: Vulnerable item last opened on 03/01/2018 at 10:00:00.

- Remediation target rule 1: Last opened on 03/07/2018; remediation target is 15 days since it was last opened; calculated remediation target date is 03/16/2018 10:00:00.
- Remediation target rule 2: Last opened on 03/10/2018; remediation target is 10 days since it was last opened; calculated remediation target date is 03/11/2018 10:00:00.

In this scenario, the Remediation target rule 2 applies to the vulnerable item since it has the more restrictive date. 10 days since the vulnerable item was first identified versus 15 days.

Note: Once the Remediation target rule is defined, remediation target dates are calculated by the *`Evaluate remediation targets`* scheduled job.

About the Evaluate remediation targets scheduled job

`Evaluate remediation targets` runs once at 4:00:00 daily.

It iterates through all active vulnerability rules, starting with those rules with the earliest remediation target date. It looks at all vulnerable items that:

- Aren't in a **Closed**, **Deferred**, or **Resolved** state.
- Have no remediation target date.
- Have a remediation target date that is later than the date in the remediation target rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Evaluate remediation targets adds a remediation target date, if one doesn't exist, or if a rule results in an earlier date than the one in the record, it updates the existing target date. Finally, it updates the **Remediation target** and **Remediation status** fields in the vulnerable item form.

Once the *Evaluate remediation targets* runs, available notifications are sent.

Evaluate remediation targets clears the remediation fields on the VI and stops sending notifications.

The *sn_sec_cmn.evaluate_targetmissed_records* property, when enabled, prevents the *Remediation Target Rules* scheduled job from evaluating missed VIs. This property is enabled by default.

Reapplying remediation target rules

When you change a remediation target rule, use the **Apply Changes** button on the Remediation Target Rules list page to rerun all the changed rules on all active Open VIs except those in the **Closed**, **Deferred** or **Resolved** state. Depending on how many VIs you have, this may take time.

Note:

If the scheduled job, *Evaluate remediation targets* is running, you can't initiate a reapply process. However, if a reapply process is already running, and the scheduled job it triggered, they run in parallel.

The reapply processes in Vulnerability Response and Application Vulnerability Response are independent and can run in parallel.

Important: As a vulnerability admin and analyst, you can obtain the latest remediation target date for selected vulnerable items in the Vulnerability Manager Workspace. This method is more efficient than running the Remediation Target Rules for all vulnerable items in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Related topics

Create or edit a Vulnerability Response remediation target rule

View the remediation target status of a Vulnerability Response vulnerable item

Create or edit remediation target notifications

Vulnerability classification groups and rules

Classification groups automate classification of values of a table based on the classification rules defined in the group. The condition for each rule is evaluated in order, and the first matching rule is used.

The Vulnerability Response base system includes the following two classification groups, which classify discovered items and vulnerabilities respectively:

- Discovered Items Classification
- Vulnerability Entry Classification

Whenever vulnerabilities and discovered items are imported, the vulnerability classification rules in the respective groups get executed. Based on the conditions set in the rule, the records get classified to the relevant classification group. You can create, edit, delete or reapply these rules to an existing vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- For a selected table, there can only be one active classification group.
- Once you create a group, you cannot delete it.

For more information, see Create and edit a classification rule, Apply a rule to an existing vulnerability, and Deactivate or delete a classification rule.

Machine Learning solutions for Vulnerability Response

Vulnerability Assignment Recommendations uses ServiceNow® Predictive Intelligence and machine learning to recommend assignment groups for vulnerable items (VIs) and remediation tasks (VULs, or RTs). You can reduce the time that you spend on identifying the owners for unassigned or incorrectly assigned vulnerability findings. Also, you can see a system-generated confidence score that evaluates if the recommended assignment group is suited to resolve the vulnerability.

The Predictive Intelligence capabilities are used in Vulnerability Response to provide better work experiences by creating and training a solution definition model that can predict the assignment group based on existing data.

For more information, see Predictive Intelligence.

Vulnerability Assignment Recommendations

With the Vulnerability Assignment Recommendations application (com.snc.vulnerability.recom), the system can assign recommendations in Vulnerability Response using ServiceNow Predictive Intelligence. This plugin requires:

- Vulnerability Response (`com.snc.vulnerability`)
- Predictive Intelligence (`com.glide.platform_ml`)

For more information, see Predictive Intelligence.

Confidence scores

Use the Vulnerability Assignment Recommendations application to generate the confidence score that reports the confidence level of the recommended assignment groups for the selected RTs or VIs. The confidence score evaluates whether the system is confident that the recommended assignment group is suited to resolve the vulnerability. Up to 10 recommendations appear. These recommendations are based on the highest probability for successful assignments. The first recommendation in the list means that the system has the highest confidence that it is the correct assignment group.

For example, on a scale of 0-100, for each assignment group, the confidence score suggests the probability of a VI or RT belonging to that particular group.

Related topics

- Predictive Intelligence
- Create and train a classification solution
- Create and train a similarity solution
- Create and train a clustering solution
- Configuring advanced settings for your ML solutions

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations

When data is imported from a third-party integration, Vulnerability Response automatically uses host data to search for matches in the Configuration Management Database (CMDB). It does this using **CI Lookup Rules**. These rules are used to identify configuration items (CIs) and add them to the vulnerable item record to aid in remediation.

Starting with version 19.0, navigate to **Security Operations** > **CMDB** > **Lookup Rules** to locate the list in your instance.

As assets are imported, a lookup is performed first on the **Discovered Items** list using third-party IDs to find matches to configuration item (CIs) from prior imports. When a host ID match is found, it is used as the **Configuration item** field in the vulnerable item record.

You can see how imported assets are mapped to CIs using the **Discovered Items** list. If a match is not found, or the host ID field is empty, the rules use the other host information to attempt to correctly identify the CI. If a match is still not found, a placeholder CI is created and is designated as an **Unmatched CI**. See Unmatched CIs for more information on how those CIs are handled.

CI lookup rules can be domain separated and are source-specific. Each source can have multiple deployments.

Note: CI lookup rules are shared by all deployments of the vulnerability source integration. If a rule is deleted or modified, the deletion or changes affect all deployments of the vulnerability integration.

When attempting a match, the first step is a vendor ID lookup for an exact match across source, source_instance, and vendor ID. Then, lookup rules are run in order, from lowest to highest and stop when a rule returns just a single CI as a match. If a rule is created in such a way that it returns more than one CI, only the first match is used.

Note: To avoid matching on low-level networking elements, if a matched CI is one of `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`, or `cmdb_ci_ip_address`, the parent CI is returned.

A system property to exclude CI classes is available. This property is not available with upgrade. See Ignore CI classes for upgrade information and instructions on setting the property.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the Discovered Item record in the **CI matching rule** field. Lookup rules are evaluated by lowest **Order** value first.

The CI lookup rules are shipped with their corresponding integration plugins.

Some of the Qualys CI lookup rules are:

- QUALYS HOST ID
- FQDN
- NetBIOS
- DNS
- IP

Some of the Rapid7 CI lookup rules are:

- MacAddress
- FQDN

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- HostName
- IP

Some of the Tenable.io CI lookup rules are:

- FQDN
- NETBIOS
- HOSTNAME
- MacAddress
- DNS

Note: The Tenable.io CI lookup rules prioritize and populate the non-empty network interface values (FDQN, IPV4, and MacAddress) over the regular FDQN, IPV4, and MacAddress values for a discovered item. When these network interface values are empty, the regular FDQN, IPV4, and MacAddress values are populated for a discovered item.

Some of the Tenable.sc CI lookup rules are:

- MacAddress
- FQDN
- NETBIOS

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined **CI Lookup Rules**. See Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

Note: For information on CI matching, see KB0998706.

Reapplying updated CI lookup rules

When you change a CI lookup rule, click **Apply Changes** on the CI Lookup Rules list page to rerun all the rules on the discovered items that:

- Were matched by the updated rules
- Are not matched by any rule

If the configuration item (CI) changes after reapplying the lookup rules, the discovered items are updated with the new CI. The impacted detections and vulnerable items are also updated. For more information, see Reapply CI lookup rules on selected discovered items.

Unclassed hardware

If an asset does not find a match in the Configuration Management Database (CMDB) by CI lookup rules, the asset is termed as an unclassed hardware.

When data is imported from ServiceNow built integrations, Vulnerability Response automatically uses host data to search for matches in the CMDB. The CI lookup rules are used to identify configuration items (CIs) and add them to the vulnerable item record to aid in remediation. If the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

assets are not found in the CMDB, the Identification and Reconciliation engine (IRE) runs its own identification rules defined on the hardware class and all its children and creates a CI under an Unclassed Hardware class. When Discovery finds this asset, instead of reclassifying the existing unclassed hardware, it creates a CI. This is because the identification rule relies on the name of the hardware CI.

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from discovered items is not supported.

The following extracts show the IRE payload for creating CI in Unclassed Hardware via Vulnerability Response and Discovery respectively.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
        "name": "asset01.company.com",//from NetBios,
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123"
    }

"settings": {
        "updateWithoutSwitch": true
    }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
        "name": "asset01",
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123",
        "os_domain": "company"
    }

"settings": {
        "updateWithoutSwitch": false
    }
```

In this case, the existing Unclassed Hardware CI is not reclassified to Windows server, and instead a new CI under Windows server is created. The reason being the identification rule relies on the name of the Hardware CI. If you notice the payloads, the name in the payload from Vulnerability Response is the same as either FQDN/NETBIOS, but it is just the host name for the payload from Discovery.

Related topics

Reclassify unclassed hardware

Unmatched CIs

Configuration items (CIs) are automatically matched to CIs in the Configuration Management Database (CMDB) when they are imported. By default, the **Security Operations** > **CMDB** > **Discovered Items** module lists those configuration items without a match.

If you think an unmatched CI belongs to an existing class in the CMDB, review your CI lookup rules. Otherwise, consider reclassifying the configuration item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The default filter for this list is set to **Unmatched**. You can view all discovered items from an import by removing the filter.

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from discovered items is not supported.

Related topics

- View and reclassify unmatched configuration items
- Reconcile unmatched discovered items
- Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules
- De-duplicating existing configuration items

Creating CIs for Vulnerability Response using the Identification and Reconciliation engine

You can create configuration items (CIs) in the Configuration Management Database (CMDB) using the Identification and Reconciliation engine (IRE) API. By using the IRE API to create CIs, you can prevent duplicate CIs from being created and you can reconcile CI attributes by allowing only authoritative data sources to write to CMDB.

A CI class (table) is the original table name in the instance database. CMDB contains base system classes that store data about CIs.

Using IRE for CI creation

Prior to Vulnerability Response v12.2, if a matched CI isn't found either in the Discovered Items list or CMDB, a CI is created in the Unmatched CI class (`sn_sec_cmn_unmatched_ci`). For more information, see Unmatched CIs.

Starting with v24.0.6 of Vulnerability Response, if IRE encounters exceptions that prevent the creation of CIs, the specifics of these exceptions are recorded in the Additional Information field. By examining the details in this field, you can determine the root cause and implement the necessary corrections to ensure the CI is successfully created.

Starting with Vulnerability Response v12.2 to v18.0, if no match is found when the CI lookup rules are applied, the asset information is sent to IRE and a CI is created in one of the *`Unclassed Hardware`* and *`Incomplete IP Identified Device`* classes. Starting from Vulnerability Response v18.0, a new class, *`Cloud Resource`* is also included. For more information on how to configure the categorization of unmatched cloud resources into your preferred CI class, see Updating CI class for unmatched cloud assets.

CMDB CI classes

Note: To use the new classes, activate the CMDB CI Class Models plugin. Otherwise, CIs are created in the Unmatched CI class.

If the host that you imported from a third-party scanner can't be found in the Discovered Items list or CMDB, it's created in one of the following new CMDB CI classes.

CMDB CI classes

CMDB CI Class	Description
Incomplete IP Identified Device (*`cmdb_ci_incomplete_ip`*)	CI is created in this table if only the IP address is available in the host information that is received from the scanner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CMDB CI classes (continued)

CMDB CI Class	Description
Unclassed Hardware (*cmdb_ci_unclassed_hardware*)	CI is created in this table if any of the following information is available in the host information that is received from the scanner: • Host name • IP address • DNS • NETBIOS • MAC address **Note:** If the MAC address is available, the network adapter entry is created and related to the unclassed hardware CI. If both the IP and MAC addresses are available, the IP address CI is also created and related to the unclassed hardware CI.
Cloud Resource (*cmdb_ci_cmp_resource*)	CI is created in this table if *Cloud Resource ID* is available in the host information that is received from the scanner. **Note:** If the Asset Type of a scanner integration is *Hybrid* and the *sn_sec_cmn.unmatched_cloud_resource_enab* system property is false, the CIs are created in the *Unclassed Hardware* class but not in the *Cloud Resource* class.

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from discovered items is not supported.

The system automatically uses an Unmatched CI class if one of the following occurs:

- The CMDB CI Class plugin is not activated.
- IRE raises an exception while creating a CI.

For more information, see Unmatched CIs.

Related topics

CMDB CI Class Models store app

Identification and Reconciliation engine (IRE)

Updating CI class for unmatched cloud assets

Starting with Vulnerability Response v20.0, you can categorize the unmatched cloud assets from Qualys, Rapid7 and Tenable scanners into *Unclassed Hardware* by using the *sn_sec_cmn.unmatched_cloud_resource_enabled* system property.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This system property with `false` as a default value is shipped with the base system. It classifies the unmatched cloud assets into a *`Unclassed hardware`* (*`cmdb_ci_unclassed_hardware`*) or *`Cloud Resource`* (*`cmdb_ci_cmp_resource`*) class for the integrations that bring in both infrastructure and cloud assets.

Starting with Vulnerability Response v20.0, the Asset Type column is added in the Third-party Integrations (`sn_sec_int_integration`) table to identify the integrations that support both infrastructure and cloud assets. The Asset Type column has the value, *`Hybrid`* for the scanners that bring in both infrastructure and cloud assets. For example, Qualys, Rapid7, and Tenable integrations have the value as *`Hybrid`* in the Asset Type column.

- For new installation of Vulnerability Response v20.0 and above, all the unmatched cloud assets are categorized into:
  - *`Unclassed Hardware`* class by default.
  - *`Cloud Resources`* class, if you change the *`sn_sec_cmn.unmatched_cloud_resource_enabled`* system property to `true`.
- For upgrades to Vulnerability Response v20.0:
  - If there are any assets in the *`Cloud Resource`* class, the *`sn_sec_cmn.unmatched_cloud_resource_enabled`* system property is set to true so that the unmatched cloud assets continue to add to the *`Cloud Resource`* (*`cmdb_ci_cmp_resource`*) class.
  - Otherwise, the *`sn_sec_cmn.unmatched_cloud_resource_enabled`* system property is set to false so that the unmatched cloud assets are categorized into *`Unclassed Hardware`* class.

Note: If you modify the value of the *`sn_sec_cmn.unmatched_cloud_resource_enabled`* system property, ensure to delete unmatched configuration items on the previously targeted CI class, and reapply the lookup rules. To know more about how to delete the existing CIs and reapply CI lookup rules so that the new CIs are created in the right class, see KB1533376.

Discovered Items

Assets are automatically matched to configuration items (CIs) in the Configuration Management Database (CMDB) when they are imported using **CI Lookup Rules**. Discovered Items give you visibility into how asset identification is mapped to CIs in the CMDB.

Discovered Items are considered **Matched**, **Unmatched**, or **Reclassified**. Identified CIs are in the **Matched** state.

To make it easier to find potential matching issues, the CI Lookup Rule that matched the CI appears in the **CI matching rule** field.

By default, the **Security Operations** > **CMDB** > **Discovered Items** module lists unmatched configuration items. You can view all discovered items from an import by removing the filter.

For a description of the fields in Discovered Items, see Discovered Items form fields. For more information on reconciling unmatched discovered items and reapplying CI lookup rules on selected discovered items, see Reconcile unmatched discovered items and Reapply CI lookup rules on selected discovered items respectively.

CI changes for discovered items

When a configuration item (CI) on a discovered item (DI) changes, the impacted detections and vulnerable items (VIs) are updated. The risk score, assignment rules, group rules, and remediation target rule are reevaluated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Starting with v24.0.6 of Vulnerability Response, you can view the updates to a CI in the Discovered Item table. Information including the previous CI, the updated CI, and the user who made the changes is documented in the Audit History related list.

If a VI exists with the same vulnerability and CI, the detections are updated with the existing VI and the current VI is closed with the substate as `invalidCI`. Work notes are added for the following reasons:

- When detections are moved from one VI to another.
- When a duplicate VI is closed.

If you do not want to update the CI for the existing VI, set the property `sn_sec_cmn.update_on_ci_change` to `false`. Then, when a CI changes, a new VI is created and the existing one is closed as an `invalidCI`.

The default value of the property `sn_sec_cmn.update_on_ci_change` is `true`.

Re-evaluating discovered items

When new data is received on a discovered item, the discovered item is not immediately re-evaluated. On receiving new data, the *`reevaluate_ci`* option is set to *`true`* by default.

The scheduled job *`Re-apply CI Lookup Rules on the Changed Discovered items`* evaluates all the discovered items whose source data is being changed by the scanner. It re-processes the discovered items and updates the vulnerable items related to the discovered item whose source data is changed. The value of this scheduled job is *`On Demand`* by default.

Note: You can also choose to run this scheduled job daily. For more information about how you initiate this job, job frequency, and viewing the number of records it processes, see KB1695110 Vulnerability Response: Re-apply CI lookup rules on the Changed Discovered items.

Vulnerability Response remediation task and vulnerable item states

With the Vulnerability Response application, you can use the state model to see the status of a remediation task, at any given time. Knowing how each state relates to and affects each other helps you to determine when and how to remediate your vulnerable items (VIs).

Remediation task states

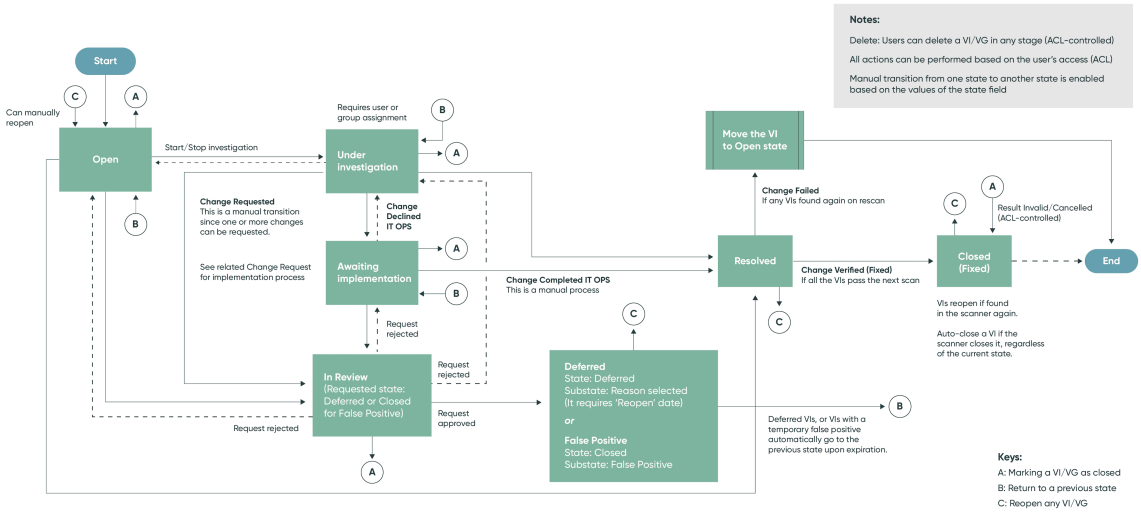
Complex use cases can sometimes result in a vulnerable item being in a different state than its remediation task. Understanding how states work helps to explain this behavior and can help with creating remediation tasks and creating or editing remediation task rules.

Note: Starting with v23.0 of Vulnerability Response, the **Vulnerable Item State Approval** workflow is deprecated and replaced by the flow Vulnerability State Approval Change in the flow designer.

Remediation tasks have many possible states as shown in the following diagram.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response state flow



Note: Each task form contains **Follow** and **Update** buttons that are standard for ServiceNow tasks.

For more information on remediation task states and actions you can perform on it at a respective state, see Vulnerability Response remediation task states.

For more information on detections, remediation task and vulnerable item states, see Detections, remediation tasks, and vulnerable item states.

For more information on remediation task and VI states, seeRemediation tasks and vulnerable item states.

For more information on remediation task state for VIs in multiple groups, see Remediation task state for Vulnerable Items (VITs) in multiple groups.

Vulnerable item age calculation and display

The age of vulnerable items (VIs) is displayed in the Vulnerability Response application with more detail.

Overview

The vulnerable item (VI) age is displayed in Days/Hours/Minutes format in the Age column on the Vulnerable Items list view, and in the Age and Age closed fields on VI (VIT) records. Age displayed in more significant digits may help you more accurately perform the following activities:

- Configure rules in the Auto Delete Rules module to target and delete specific VI records by Days/Hours/Minutes. Removing records with more accuracy may increase your performance, especially if you have a large number of VI records in your instance.
- View reports with more specific details in the Performance Analytics for the Vulnerability Response application.
- Create filters that identify only the VIs you want.
- Prune list views to display only the VIs you want.
- Dot-walk more easily.

A scheduled job calculated age and updated all active VIs. In instances with large numbers of VI records, this process could be slow and negatively impact performance. VI age is calculated more efficiently on-demand and displayed with more significant digits with an enhanced Age

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

column. The enhanced Age column is automatically added when you install or upgrade the Vulnerability Response application.

Note: If you perform an upgrade and the VI age is not displayed in the Vulnerable Items list view and in the Age and Age closed fields on active VI (VIT) records in Days/Hours/Minutes (9 Days, 18 Hours, 29 Minutes) format, the age column is not current in your instance. For more information about how to resolve this issue after an upgrade, see KB0749231.

The age column and fields are not editable. A vulnerability manager with the sn_vul.vulnerability_read permission or the Vulnerability admin persona can view this value, and IT remediation owners with the sn_vul.remediation_owner role can view it on records assigned to them.

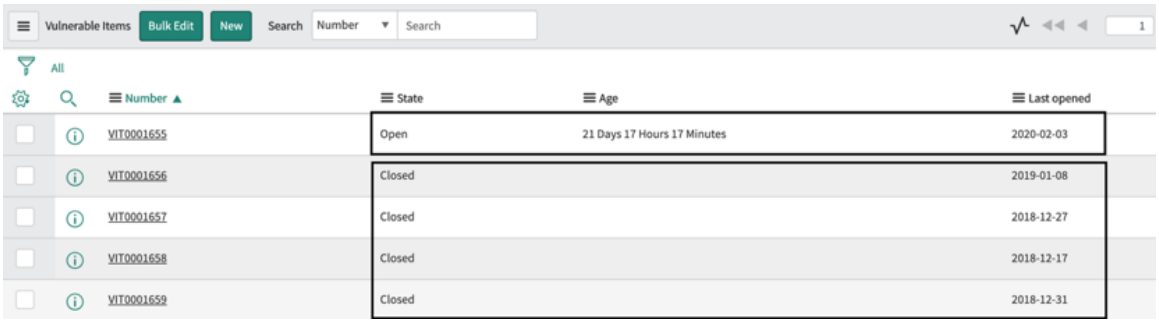
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

VI age is displayed as shown in the following images.

Vulnerable items list

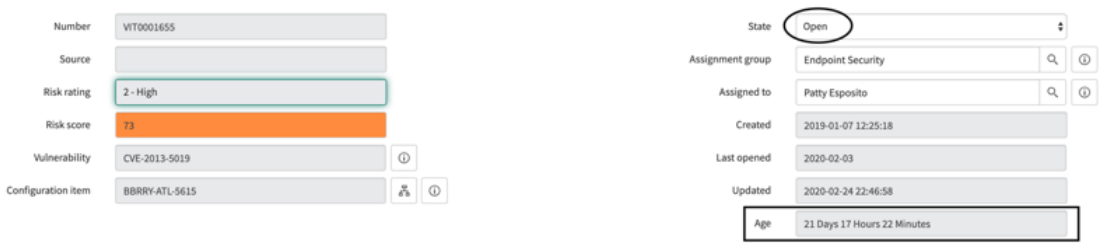
As shown in the following figure, on the Vulnerable Items list view, Age is displayed in the Age column in Days/Hours/Minutes (21 Days 17 Hours 17 minutes) only for active VIs. Active VIs are VIs in any states other than 'Closed'. This age value represents the number of days the VI has been active.

The age is not displayed for VIs in the ‘Closed’ state. For VIs previously in a ‘Closed’ state and then reopened, the value represents the number of days the VI has been active since the date it was last opened.



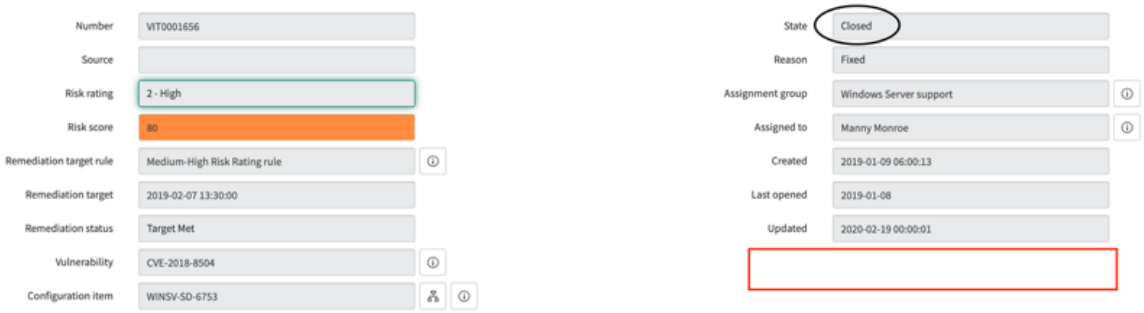
Age on VI records

On the VI records, the value of Age column in the list view is visible for active VIs in the Age field.



The value of the Age column is not displayed for VI records in the ‘Closed’ state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

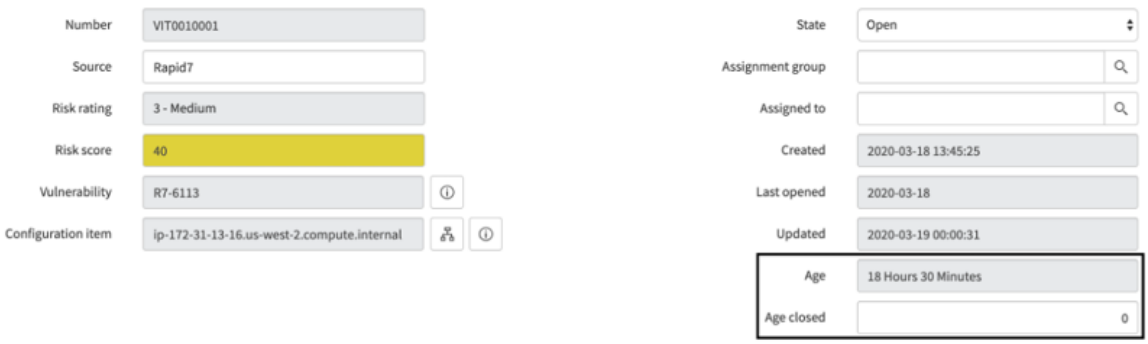


Age on the Vulnerable items list and VI records when a VI is updated

When a VI is in the 'Closed' state, the Age field is not displayed. When the VI transitions to 'Closed', the value in number of days from the Age column is displayed in the Aged closed field (9) as shown in the following figure. This value represents the number of days the VI was active before it transitioned to 'Closed.' For example, in the following image, this VI was active for 9 days, 18 hours, and 29 minutes, but only the number of days (9) is displayed on the closed record.



If this VI is reopened, when the VI state transitions back to 'Open', the Age closed field is reset to 0. Because the VI is active again, the age in Days/Hours/Minutes is displayed in the list view in the Age column and on the Age field on the VIT.



For more information on how to customize the Age and Age closed calculations, see the KB1703270 article.

Removing assignments from vulnerable items and remediation tasks

You can clear the **Assigned to** and **Assignment group** fields on vulnerable items directly from the vulnerable item and remediation task records that you determine might be incorrectly assigned to you or your groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview of the workflow

Remediation owners and vulnerability analysts can clear the **Assigned to** and **Assignment group** fields and update records for reassignment with the **Unassign** UI action.

Use case

If you determine that records aren't within your scope for remediation, or if you think that they have been incorrectly assigned to you or to your groups, you can remove yourself or your groups from the **Assigned to** and **Assignment group** fields on vulnerable item and remediation task records.

The Unassign UI action and more options menu

You can **Unassign** the following records with a UI action or from the more options menu



( ) in any state other than Closed or Resolved:

- Remediation tasks (VULs, AVULs, and CVULs) in both the classic environment and the workspaces.

  If a remediation task is updated with this feature, the **Assigned to** and **Assignment group** fields on all of its associated VITs that have the same assignment groups are also cleared.

  Note: If any VIT, AVIT, or CVIT on a remediation task has a different assignment group than its remediation task, it is not unassigned. In most cases, these vulnerable items have been manually assigned.

- Vulnerable items (VITs, AVITs, and CVITs) in the classic environment and the workspaces.

Any records that you update assignments for with the UI action or manually are displayed on the Unassigned module under their respective product modules.

For the steps to clear the **Assigned to** and **Assignment group** fields on records with the *Unassigned* UI action, see Remove assignments from vulnerable items and remediation tasks for more information.

Bulk edit

You can clear the assignment fields for multiple VIs on a list. After you select the VIs and select **Bulk Edit**, on the dialog that is displayed, select the **Unassign** check box.

System property and notifications

If you are an administrator with the sn_vulc.vulnerability_admin role, when you click **Unassign** on a record, by default, the *sn_vul.unassign_vr.approval_required* system property triggers the approval flow and creates a state change approval record in review state and approval request is raised for approver which displays in the **My Approvals** list.

Note: As a vulnerability administrator, you can set the *sn_vul.unassign_vr.approval_required* system property to **false** to disable the approval process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If the approver approves the request, *sn_vul.default_assignment_group* clears the **Assigned to** and **Assignment group** fields and populates the **Assignment type** field with **Unassigned**. As a vulnerability administrator, you can change the value in the *sn_vul.default_assignment_group* system property so that the assignment fields are cleared and a specific group is then assigned. For example, if a user clicks **Unassign** on a record and you want to redirect it to a specific group for review, you can add a system ID for the group of your choice in the Value field of the system property.

  Note: If you change this value, notifications for all the VITs, AVITs, and CVITs that are unassigned are sent to the group you specify.

- If the approver rejects your request, the reason for rejection displays in the **Notes** tab.

Alternatively, if *sn_vul.default_assignment_group* is not configured for a specific group, by default, users that you add to the Unassign notification user group are alerted when records are unassigned. The *sn_vul.default_assignment_group* system property determines the notifications to this group.

The assignment type, whether it's **Manual**, **Rule**, or **Unassigned**, is available from the VIT records and the list view. The **Unassigned** assignment type is displayed on records after the **Assigned to** and **Assignment group** fields are cleared by the system property.

See Approve or reject an unassign request in Vulnerability Response for more information about approving requests.

Monitoring your assignment rules with the scheduled job for this feature

A daily scheduled job counts the records when they transition to **Unassigned** assignment type. With this count, vulnerability analysts can monitor and adjust any assignment rules that might not be performing well based on any assignment rules that have higher counts of unassigned VIs.

The *Reassignment count for assignment rules* scheduled job runs daily and posts the total number of VIs that are unassigned by this feature for a particular assignment rule.

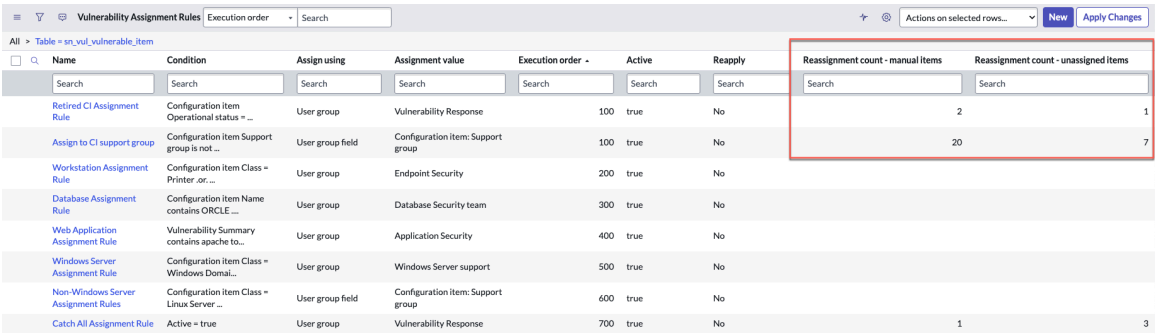
The counts gathered by this job apply to the vulnerable items and the unique assignment rules for Vulnerability Response and Application Vulnerability Response. Counts are displayed by assignment rule in each assignment rules list for each module.

The job also counts any records that are manually unassigned. Both the manual counts and the counts gathered by this feature are posted on the Vulnerability Assignment Rules list in two columns: *Reassignment count - manual items* and *Reassignment count - unassigned items*.

1. As a vulnerability admin, to view these counts, navigate to **Vulnerability Response** > **Administration** > **Assignment Rules**.
2. Click the gear icon in the upper right of the list and select the *Reassignment count - manual items*, and *Reassignment count - unassigned items* for display.
3. Any VI that was originally assigned by a rule but subsequently automatically or manually reassigned contains a reference to the original rule on the list view.

The following example shows reassignment counts for two assignment rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply	Reassignment count - manual items	Reassignment count - unassigned items
Search	Search	Search	Search	Search	Search	Search	Search	Search
Retired CI Assignment Rule	Configuration item Operational status = ...	User group	Vulnerability Response	100	true	No	2	1
Assign to CI support group	Configuration item Support group is not ...	User group field	Configuration item: Support group	100	true	No	20	7
Workstation Assignment Rule	Configuration item Class = Printer ,or ...	User group	Endpoint Security	200	true	No		
Database Assignment Rule	Configuration item Name contains ORCLE	User group	Database Security team	300	true	No		
Web Application Assignment Rule	Vulnerability Summary contains apache to...	User group	Application Security	400	true	No		
Windows Server Assignment Rule	Configuration item Class = Windows Domai...	User group	Windows Server support	500	true	No		
Non-Windows Server Assignment Rules	Configuration item Class = Linux Server ...	User group field	Configuration item: Support group	600	true	No		
Catch All Assignment Rule	Active = true	User group	Vulnerability Response	700	true	No	1	3

Vulnerability Response calculators and vulnerability calculator rules

Vulnerability calculators automate calculating initial values for the fields on vulnerable items. The condition for each calculator is evaluated in order, and the first matching calculator is used.

Vulnerability Calculators

The Vulnerability Response base system includes two vulnerability calculators that set the base **Risk Score** on the vulnerable item.

- **Default Risk Calculator**
- **Vulnerability Severity**

Vulnerability calculators can be built to prioritize and rate the impact of vulnerable items based on any criteria by using condition filters. Whether it is the business impact of the vulnerability, the class of the configuration item (CI), or the age of the vulnerable item, you can create additional vulnerability calculators to set other fields on vulnerable items. Or you can customize the existing vulnerability calculators. A calculator can be written to reflect any set of priorities. See Create a Vulnerability Response calculator and Filtering within Vulnerability Response for more information.

Additionally, you can use attributes in the configuration_item [cmdb_ci] in the Configuration Management Database (CMDB) to help you create logic for your Vulnerability Response risk calculators. If, for example, you determine that CIs that are external-facing in your organization are more vulnerable and might require immediate remediation, you can assign attributes such as *`Internet Facing`* for these CIs. This attribute, and others, are listed in the Common Service Data Model release notes . For current information and guidance on the CMDB, see the following topics:

- Common Service Data Model conceptual model
- CMDB schema model
- Vulnerability Response: Risk Score Calculation (KB1169927)

Each calculator contains a list of calculator rules, with a condition determining when to apply it. When the calculator is run, the condition for each calculator rule is evaluated in order, and the first matching calculator rule is used.

The **Vulnerability Severity** calculator calculates the **Risk Score** for vulnerable items using the normalized vulnerability severity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- Only one calculator per target field (**Risk Score**) can be active at a time. **Vulnerability Severity** is disabled by default.
- Whenever the risk score is updated on a VIT, the **Notes** section is updated with the following details:
  - Calculator group name
  - Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, click on any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If Template is selected, the risk score is updated according to the specified condition in the rule. If Script is selected, you can either add or update the existing script.

    The system property *sn_sec_cmn.risk_score_changes_add_worknotes* helps populate the work notes section. Starting with v25.0.3 of Vulnerability Response, the system property is inactive by default. If you enable it, only then you can see all the changes related to the risk score.

All enabled vulnerability calculators set the selected fields each time a vulnerable item is created, when an associated CI or vulnerability changes, or when the **Calculate Risk Score** related link in a vulnerable item is used. As an example, the Risk Score is automatically updated on vulnerable item records when the severity value is updated on a vulnerability that is imported. After a vulnerability import has updated a vulnerability score, the recalculate flag is enabled for that vulnerability. The risk scores for the vulnerable items that have the recalculate flag enabled (true) with that vulnerability are recalculated.

From an existing vulnerable item, if you click the **Calculate Risk Score** related link and either of the calculators is enabled, the **Risk Score** field in the vulnerable item is updated.

Note:

- The **Calculate Risk Score** related link is only visible when at least one vulnerability calculator is enabled.
- You can update the risk score for a vulnerable item in the Vulnerability Manager Workspace and IT Remediation Workspace by selecting the **Calculate Risk Score** button in its record view.
- Whenever the risk score on a VIT changes, the following details are documented in the Notes section of the VIT:
  - Calculator group name
  - Calculator name
  - Field values with their weightage and risk score contribution
  - Final risk score

Vulnerability Calculator Rules

The base system calculator **Default Risk Calculator** contains the rule**Default Risk Rule**, a specialized vulnerability calculator rule called a **Risk Rule**. It calculates **Risk Score** based on multiple values:

- Vulnerability severity
- Exploit information
- Criticality

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- External exposure of the CI with the vulnerability
- EPSS scores

You can adjust the values to use in the **Default Risk Rule** and how much weight to give each of these values. Weights are used to adjust how much each element counts when setting the base **Risk Score**.

You can customize the criteria for the default risk rule. For more information, see Define fields and weights for the risk rule for Vulnerability Response Risk Calculators.

For an example of how risk scores for risk rule calculators are determined, see Risk score calculation example for Vulnerability Response.

Assigning a weightage percentage

You can also assign weightage percentage (0-100) at the field value level, for example, you can assign a weightage percentage to each level of Severity (None to Critical).

If the severity weightage is 50 for the risk rule, and the following weightage values are assigned for the Severity level:

Vulnerability severity	Risk score
Critical	100
High	50
Medium	20
None	0

If the severity is critical, the equivalent weightage is 50. If the severity is high, the equivalent weightage is 25, and if the severity is medium, the equivalent weightage is 10. If the severity is None, the equivalent weightage is 0. For more information, see the Risk score calculation example for Vulnerability Response.

Vulnerability calculator rule settings

Each rule has an **Order** setting. However, the first one to match the conditions updates the **Risk score** field in the vulnerable item. For more information on vulnerability calculator rule settings, see Create a Vulnerability Response calculator. Non-scripted calculator rules typically create less of a performance impact than scripted calculator rules.

The base system **Vulnerability Severity** calculator contains calculator rules that assign each level of severity (None to Critical) a value (0-100) for **Risk Score** based on severity. **Unknown Severity** is automatically assigned a risk score of 100. These values can be adjusted and, like **Default Risk Calculator**, new calculator rules or new risk rules can be created.

Vulnerability Risk Score Weights

All vulnerabilities are assigned a risk score and rating based on factors such as severity, criticality, exploit information, and so on. The business rule *`Update Risk Rating from Risk Score`* on the vulnerable item table is responsible for calculating the risk rating. Whenever the risk score changes, the risk rating is calculated and populated on the vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Value (Risk Rating)	Weight (Risk Score)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

- The risk rating types are shipped in the base table as vr_risk_rating. These types are passed as part of the business rule on each table where the risk rating is calculated.
- The script is modified so that you can query the entries in the Risk Score Weights table values for the risk rating calculation.
- Add additional entries for an existing type or create a new type. When you create a new type, ensure that you add the labels for the new risk rating, and also modify the related scripts and business rules. You must also add a new style for the new risk score.
- Modify the script to query the records in the base table.

You can access the Risk Score Weights table by entering sn_sec_cmn_risk_score_weight (for versions below 30.0) or sn_sec_calculator_risk_score_weight (for versions 30.0 and above) in the filter navigator.

In addition, the risk score is automatically recalculated when the associated Common Vulnerabilities and Exposures (CVEs) or third-party entries (TPEs) on the vulnerability items (VIs) are linked to a CVE Known Exploit Vulnerability (KEV).

Tenable Vulnerability Integration and the Tenable Risk Rule

The Tenable Risk Rule is available with the Tenable Vulnerability Integration. The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with a new default risk calculator in Vulnerability Response. The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response.

This risk rule is disabled by default. See Configure the Tenable Vulnerability Integration using Setup Assistant.

Vulnerability Response vulnerable item detections from third-party integrations

View all of the information that is gathered by third-party scans in your ServiceNow AI Platform® instance. View the returned results of the scans on detection and vulnerable item (VI) records in your instance as these results are viewed on the scanners.

Overview

The Vulnerability Response application supports third-party Integrations that retrieve vulnerable item data from your enterprise environment. Detailed data about detections, that is, single, distinct occurrences of vulnerabilities as reported by the scanners of your third-party integrations, are imported and displayed on both the detection and the vulnerable item records in your ServiceNow AI Platform instance.

Third-party Integrations retrieve vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners. Detection data are paired with

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerable items and VI state is updated based on the state of the detections. If a VI is not found, a new one is created. Detections are only opened or closed by data found directly by a scanner.

In previous versions of Vulnerability Response, vulnerable item detections, the relationship between a CI (asset) in your environment and an imported vulnerability from a third-party scanner, created a unique vulnerable item in your ServiceNow AI Platform instance.

The granularity of the original data provided by the scanner is preserved. With detections, the detection data is paired with vulnerable items. During an ingestion, if a vulnerable item is not found, a new VI is created.

Starting from version 21.1.2 of Vulnerability Response, a system property *sn_vul.show_last_open_detection* is provided in the base system. By default, the value of this property is set to false, and the current behavior of aggregating the values from the initial detection to the VI remains unchanged. However, if it is set to true, a VI is automatically updated with the last open detection after an ingestion. The fields such as IP address, SSL, Port, Protocol, NetBIOS, and Proof are updated for the VI detections. If needed, you can customize the detection fields that should be updated by modifying the `DetectionBase` script.

To view the values for the last open detection, navigate to the **Last Open Detection** tab on the VI form view. To update all the VIs opened in the past year with the last open detection values, you can run the scheduled job *Update Last Open Detection Value To VITs* on-demand. This scheduled job is also provided in the base system.

Note: When a configuration item (CI) changes on a discovered item, the corresponding updates are also reflected in the detections. As a result, the detections may be moved from one VI to another VI. Based on this change and the value of the *sn_vul.show_last_open_detection* property, the values of the detections are rolled up to the source and target VIs.

Supported versions of Vulnerability Response

For more information about installing or updating the Vulnerability Response application, see Install Vulnerability Response.

Supported third-party integrations

A supported third-party integration with your Vulnerability Response application is required for vulnerable item detections. The following third-party integrations are supported by the Vulnerability Response application for vulnerable item detections:

- Qualys Host Detection Integration
- Rapid7 Data Warehouse:
  - Vulnerable Item Integration
  - Vulnerable Item Resolution Integration
- Rapid7#Vulnerable Item Resolution Integration (InsightVM)
  - Insight VM integration
  - Vulnerable Item Integration - API
- Tenable Vulnerability Integration
- Microsoft Defender Vulnerability Management

These third-party integrations are available with a separate subscription from the ServiceNow Store. For more information about these integrations, see Vulnerability Response integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and Security Operations and the ServiceNow Store for more information about obtaining entitlement.

To verify that your third-party scanner is configured for import, see Install and configure the Rapid7 Integration for Security Operations application and Install the Qualys Vulnerability Integration.

Key terms for vulnerable item detections

Vulnerability

Data about weaknesses in software, operating systems, and assets imported from internal and external sources. This data is imported and compared to existing assets (configuration items, CIs) listed in the CMDB.

Vulnerable item

A vulnerable item is created or updated when an imported vulnerability matches a CI in the CMDB.

Detection

A single, distinct occurrence of a vulnerability as reported by a scanner referred to as a Vulnerable Item Detection within the ServiceNow AI Platform environment. A detection includes enriched data about a vulnerability and any corresponding vulnerable items. This data is displayed on the Detection record (VID#) and the vulnerable item list view that includes the following details:

- First found (data)
- Last found (date)
- DNS name
- Net BIOSname
- IP address
- Port
- Protocol
- Proof
- SSL
- Times found

Note: Adding a business rule on the detection table will impact the performance of the ingestion.

Detection key

A hashed combination of fields that provided a way to identify and tie a detection to a vulnerable item. Detection keys are integration-specific.

Detection key configurations

Scanner	Vulnerability	Port	Protocol	Asset ID	Proof	NIC
Qualys	Yes	Yes	Yes	Yes	No	NA
Tenable	Yes	Yes	Yes	Yes	No	NA

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Detection key configurations (continued)

Scanner	Vulnerability	Port	Protocol	Asset ID	Proof	NIC
Rapid7	Yes	Yes	Yes	Yes	Yes (it is not case sensitive)	Yes

Note:

- If the detection key is not specified, or for versions earlier than Vulnerability Response 14.0, the detection key is a combination of vulnerability entry, port, protocol, asset ID, and proof.
- Starting with v19.0 of Vulnerability Response, a new detection key NIC is added for Rapid7 InsightVM, that is activated by default. Existing detections without NIC are updated with the first incoming NIC in the payload from Rapid7. The detection key is recalculated and repopulated on the detection including NIC. New detections are created if similar detections are seen with different NIC values. This data is not rolled up to the Vulnerable Item table. The NIC value is stored in a new column on the sn_vul_detection_key_config and sn_vul_detection table.

De dup

The process used by the Vulnerability Response application of collapsing of individual detections into a single VI when the data meets certain hard-coded criteria.

VI External ID

The value stored in the External ID field of the VI table. This value is a hash comprised of the combination of keys within a VI that represents what makes it unique within the application. It is composed of a CI and a vulnerable entry.

Reopen resolved vulnerable items

Vulnerable items set to **Resolved** in your ServiceNow AI Platform instance but not transitioned to **Closed/Fixed** by the subsequent integration runs are reopened if they are detected during rescans.

Closed VIs with a substate of **fixed** or **stale** are reopened if a new detection is created and the VIs can be matched with the new vulnerability.

As per the script include, *`DetectionBase`*, method *`_shouldReOpenVI()`*, if the VIT was earlier **Closed** with substate **Fixed**, **Stale**, or **CI Decommissioned**, it is reopened, and the detection is mapped to the existing VIT.

For example, say a VIT's closed date is later than the last_found date of a detection. You would expect these VIT records to remain closed. However, if you see a previously closed VIT reopened, it means that the VIT was closed by an earlier detection and the vulnerability was found again in a later scan. When a new detection is found that matches the closed VIT that has the same vulnerability on the VIT's configuration item, the VIT is reopened.

For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to **Resolved** but then not transitioned to **Closed/Fixed** by subsequent scans transition back to **Open** after the number of days you enter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For Qualys detections, if the scanner continues to find VIs that were set to **Resolved** but then not transitioned to **Closed/Fixed** by subsequent scans, these VIs move back to **Open** when the last found date is later than the Resolved date.

View detection data

You view the data imported from vulnerable item detections on the VI record. For more information, see View Vulnerability Response vulnerable item detection data and Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records.

Vulnerability Solution Management

Automatically correlate the vulnerabilities in your environment with the solutions that could remediate them. Identify the remediation actions that apply to your vulnerabilities and prioritize them by the greatest reduction in vulnerability risk.

Vulnerability Solution Management

Security and IT teams often spend a significant number of time researching vulnerability findings to identify the most effective treatments for their environment. Given the volume and complexity of vulnerabilities in large organizations, translating vulnerability findings into remediation tasks is a manual, tedious, and error-prone process.

With Vulnerability Solution Management, you can automatically correlate your vulnerability findings with the solutions that remediate them. Identify the software patches, configuration updates, and other controls that have the highest impact for your organization without the manual overhead.

Vulnerability Solution Management requirements

Vulnerability Solution Management is a feature available within the Vulnerability Response application. Vulnerability Solution Management requires a separate subscription.

For more information about getting entitlements for applications from the ServiceNow Store, see Get entitlement for a Security Operations product or application. See Install the Solution Management for Vulnerability Response application for more information about installing the application after you have downloaded it onto your instance.

After it's installed, Vulnerability Solution Management provides you access to the Microsoft Security Response Center and the Red Hat solution data from within Vulnerability Response.

Note:

You can configure both solution applications from within the Setup Assistant. See Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant.

See Understanding the Microsoft Security Response Center Solution Integration and Understanding the Red Hat Solution Integration for more information on the imported solutions.

Available versions

For the most current version of Vulnerability Solution Management, verify you have the most current version of Vulnerability Response installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Release version of Vulnerability Solution Management	Compatible versions of Vulnerability Response	Release Notes
Vulnerability Solution Management v10.3	Vulnerability Response v18.0	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

About solutions and supersedence

A superseded update is a complete replacement of a previous release or releases. For example, a hot fix update may be superseded by a Service Pack. Solutions are related to vulnerabilities. Solutions can also relate to other solutions in a supersedence chain. Solutions address vulnerabilities in preceding solutions as well as they're cumulative. Vulnerability Solution Management automatically associates vulnerabilities from preceding solutions with superseding solutions. If an older vulnerability is found, any higher superseding solution can address it, but the highest supersedence solution is preferred, as it's the most cumulative.

Potential versus Preferred Solutions

A potential solution is one that could address a vulnerability. Vulnerabilities often have many potential solutions. A preferred solution is the single solution targeted for remediating a vulnerability or vulnerable item (VI). It communicates intention, and enables more detailed deployment metrics.

Preferred Solutions

Vulnerability Solution Management automatically sets the most effective solution (**Preferred Solution**) for the detected vulnerability based on highest supersedence when only one highest supersedence solution exists. If more than one highest supersedence exists for the vulnerability, no value is set. In Vulnerability Response, a **Preferred Solution** is the Microsoft Security Response Center or Red Hat solution with the highest supersedence derived from the solutions associated with the vulnerability.

Preferred Solution values can be set on the vulnerable item or the vulnerability. When set directly on the vulnerability, all vulnerable items associated with the vulnerability inherit that solution. Change the **Preferred Solution** values for multiple vulnerable items using the bulk edit feature. When bulk edited, only the **Preferred Solution** on the vulnerable item is updated as setting the **Preferred solution** at the vulnerability entry level would set the **Preferred solution** for all new VIs going forward. Bulk editing only applies to current vulnerable items.

Note: If multiple highest supersedence solutions exist for a vulnerability, **Preferred Solution** values at the vulnerability level are cleared, as that solution depends on the affected asset. When multiple highest supersedence solutions exist for a vulnerability, set a **Preferred Solution** on the vulnerable item. You can set a different solution using the **Lookup** list on the **Vulnerable Item** form.

All preferred solutions for the vulnerable items in a remediation tasks are in a related list on the **Remediation Task** record.

Not all solution imports result in full data refreshes. The supersedence process is updated when:

- A vulnerable item is created.
- Data has changed on an active VI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v22.0 of Vulnerability Response, the solutions aren't queued in the above two cases.

- A new mapping is created for a third-party entry with the CVE.
- New solution data was released since last import, an existing solution is updated.

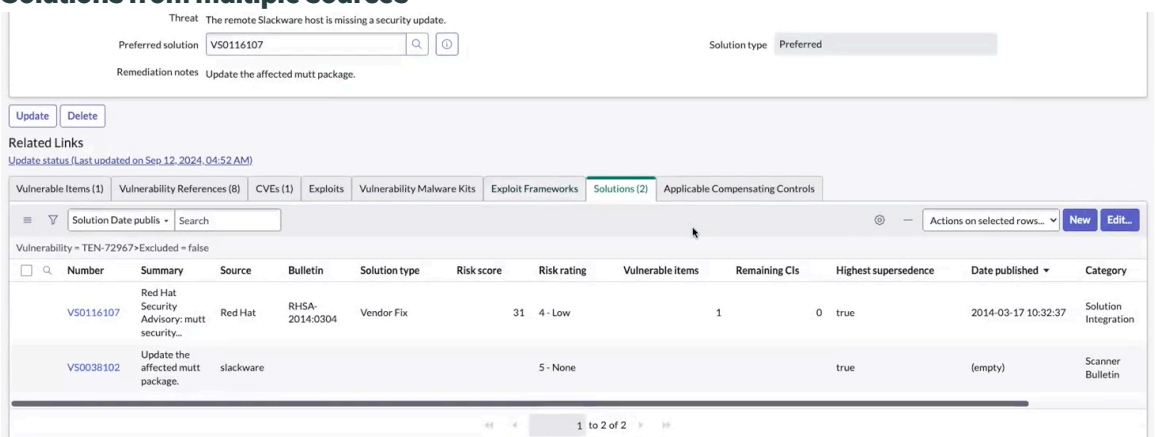
Starting with v24.0.6 of Vulnerability Response, you can ingest solution from scanners in addition to vendor solutions. The remediation data from scanners such as Tenable, Qualys, and Microsoft TVM is leveraged to create the solutions. These scanner solutions are imported using the following integrations:

- Tenable.sc Plugin Integration
- Tenable.io Plugin Integration
- Qualys Knowledge Base (Backfill)
- Microsoft TVM Machine Vulnerabilities Integration (Full Import)
- Microsoft TVM Machine Vulnerabilities Integration (Delta Import)

When the vulnerability integrations run, a payload of remediation information is created before processing third-party entries. For Tenable and Qualys, the remediation data is received at the vulnerability or third-party entry level. Conversely, for Microsoft TVM, solutions are created at the detection level, enabling a direct population of preferred solutions on the vulnerable items without the need for further processing. These solutions are created based on this remediation information and processed as needed. On processing, the preferred solution is populated on the vulnerabilities and rolled-down to the vulnerable items. The preferred solution is populated in the following order:

- Manual selection: If you select a solution manually, it isn't overridden.
- Vendor solutions (Microsoft, RedHat, CVRF, and CSAF imports): If you don't select a solution manually, the vendor solution is selected automatically.
- Latest solutions (if enabled): If there are multiple higher-superceding solutions available for a vulnerability, then the **preferred solution** field remains empty. In such cases, if you enable the property *sn_vul.latest_solutions*, the latest higher supersedence vendor solution is populated as the preferred solution.
- Scanner Bulletin solutions (if enabled): If you don't select a solution manually or vendor solutions are unavailable, the **Preferred solution** field is populated with the scanner solutions provided there's a single scanner solution. You must enable the property *sn_vul.populate_scanner_solutions* to populate the scanner solutions.

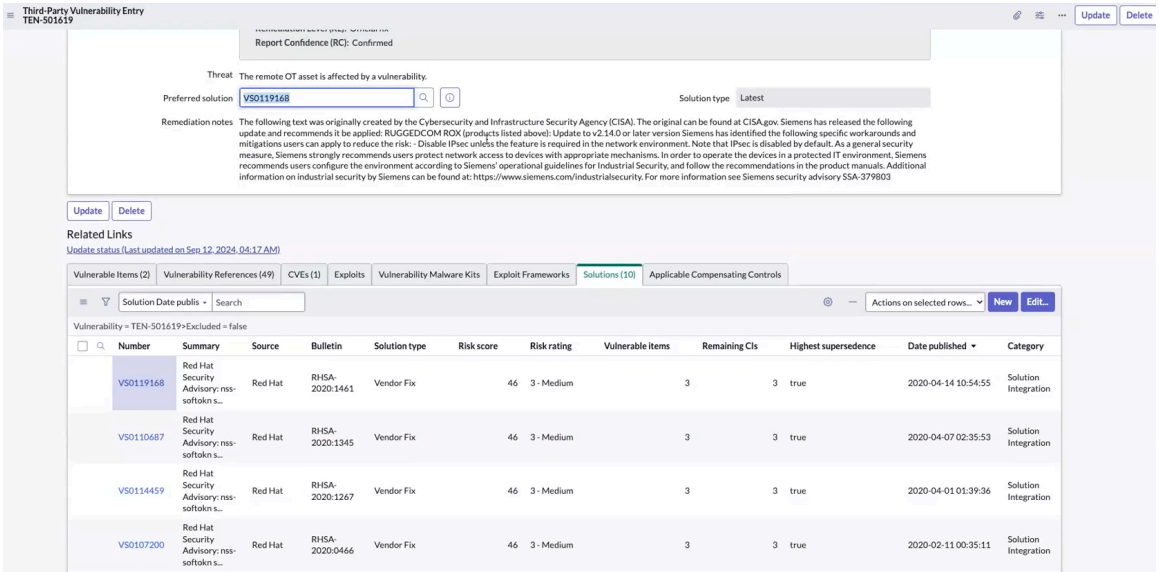
Solutions from multiple sources



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

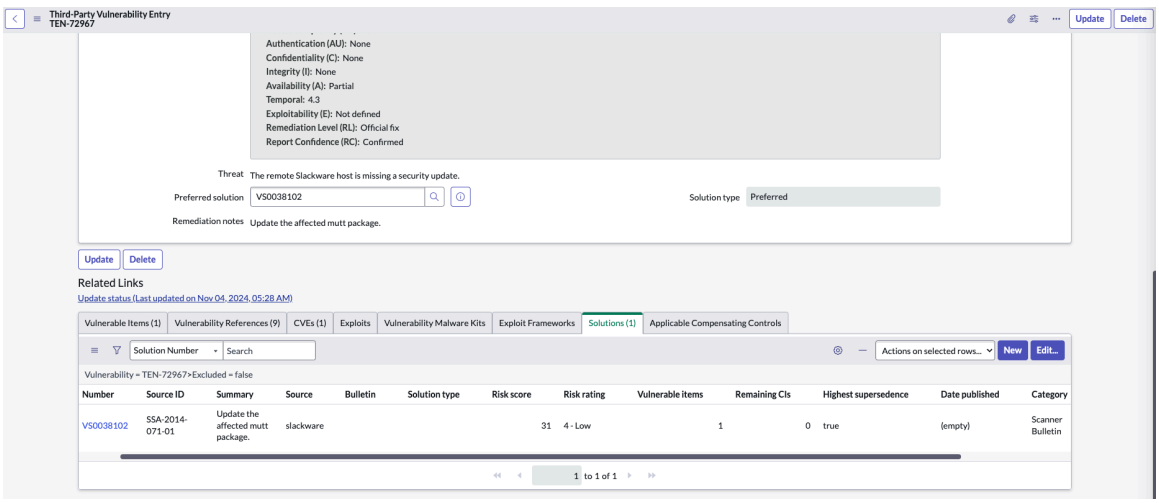
This example illustrates the selection of a solution if multiple solutions are available from different sources. In this case, there are two solutions for a vulnerability - one from a vendor and another from a scanner. As the solution VS0116107 is received from a vendor i.e., Redhat, that has higher preference, it is selected as the preferred solution.

Solutions from same vendor



This example illustrates the selection of a solution if multiple solutions are available from the same vendor i.e., Redhat in this case. If the *sn_vul.latest_solutions* property is enabled and no other vendor solutions are available for a specific vulnerability, these solutions are processed, populating preferred solutions on the vulnerabilities and subsequently on vulnerable items. If you enable the property *sn_vul.latest_solutions*, the latest solution is selected as the preferred solution.

Solutions from same scanner



This example illustrates the selection of a solution if only one solution is available from the scanners. If the *sn_vul.populate_scanner_solutions* property is enabled, the solutions are processed, populating the preferred solutions on the vulnerabilities and subsequently on the vulnerable items. If there are multiple scanner solutions, the **Preferred solution** field is left empty due to ambiguity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enhancing solution management and performance optimization

Solutions are received from various integrations, including Microsoft and Redhat. The former provides monthly updates, and establishes a chain of dependencies to track the preferred solution for vulnerabilities. However, other integrations don't follow this update format, and don't need to establish a chain of dependencies for them. Previously, a processing logic was used that involved creating a graph to maintain precedence and identify the highest superseding solutions. These solutions were suggested as the preferred solution for the vulnerabilities. However, as constructing the graph is time-consuming, the other integrations are excluded from this process. To improve the performance, starting from v22.0 of Vulnerability Response, the method `utility.processNonGraphSolutions()` is called in the *Process Vulnerability Solutions Metrics Queue* scheduled job. This method handles solutions from integrations other than Microsoft.

Secondly, the solutions are queued up from various sources using the scheduled job *Process Vulnerability Solutions Metrics Queue*. This scheduled job involves rolling up solutions from NVD entries to third-party entries, populating preferred solutions on vulnerabilities and updating the remediation status metrics on the solutions. In the following scenarios, only the remediation status metrics must be updated:

- When the preferred solution changes on the vulnerabilities
- When the VITs are created or deleted
- When a VIT import is completed

Though the solutions are queued up to update only the remediation status metrics, they still attempt to roll up solutions from NVD entries to third-party entries and populate the preferred solutions. To optimize this process, in the Vulnerability Solution table, the column **Update status** is introduced. When the remediation status metrics on solutions must be updated without requiring the roll-up or population of preferred solutions, the solutions are no longer queued. Instead, the **Update status** column is directly updated as true. This approach enables handling cases where only the remediation status metrics must be updated, resulting in time and resource savings. In the scheduled job, once the processing of the queued solutions is completed, solutions that are marked with an Update status as true are identified. Then, they're iterated through these solutions, calculating the counts and updating the remediation status metrics accordingly. This step plays a significant role in improving the performance of the scheduled job, as the number of solutions that must be queued is reduced. To view remediation status metrics, navigate to Vulnerability Solution [sn_vul_solution] table and select a vulnerability solution. Then, select the **Remediation Status** tab. The tab provides the following fields:

Remediation Status metrics

Field	Description
Preferred Solution Targets - Remediation status for VIs for which this is the preferred solution	
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
Remaining CIs	Number of CIs associated with one or more active vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
Total VIs	Number of active and closed vulnerable items for which this solution is preferred for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Status metrics (continued)

Field	Description
	remediation. This count excludes deferred vulnerable items.
Total CIs	Number of CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
% VIs remediated	Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred. This count excludes deferred vulnerable items.
% CIs remediated	Percent complete for CI remediation. Applies to VIs for which this solution is preferred. This count excludes deferred vulnerable items.
Preferred Solution Targets (Includes Deferred) - Remediation status for VIs, including deferred, for which this is the preferred solution	
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is preferred for remediation.
Remaining CIs	Number of CIs associated with one or more active vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
Total VIs	Number of active and closed vulnerable items for which this solution is preferred for remediation.
Total CIs	Number of CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation.
% VIs remediated	Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred.
% CIs remediated	Percent complete for CI remediation. Applies to VIs for which this solution is preferred.
Potential Solution Targets - Remediation status for all VIs with a vulnerability related to this solution	
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is potential solution for remediation. This count excludes deferred vulnerable items.
Remaining CIs	Number of CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation. This count excludes deferred vulnerable items.
Potential Solution Targets (Includes Deferred) - Remediation status for all VIs, including deferred, with a vulnerability related to this solution	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Status metrics (continued)

Field	Description
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is a potential solution for remediation.
Remaining CIs	Number of CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation.

Thirdly, the availability of a preferred solution for vulnerabilities and VITs must be ensured to remediate the vulnerabilities. However, in situations where multiple higher superseding solutions exist for a vulnerability, a preferred solution isn't populated due to ambiguity. To address this scenario, an approach is implemented that involves running the processing logic and populating the preferred solution when it's available. In cases where there's only one higher superseding solution, it's populated as the preferred solution. When multiple higher superseding solutions are present, the preferred solution field remains empty. However, the aim is to populate the highest superseding solution, which is published as the latest, as the preferred solution. To achieve this, a system property *sn_vul.latest_solutions* is introduced. By default, this property is set to false. If you want to enable the capability of populating the latest solutions as the preferred solution when no preferred solution is available, then you can enable this property. Once enabled, the **Solution type** column is updated in the vulnerability table with the following options:

- Preferred: When the preferred solution is populated
- Latest: When no preferred solution is available, the latest solution from the set of highest superseding solutions is selected based on the date published value. The field to be selected as the latest solution can be customized using the *sn_vul.latest_solutions* system property. By default, the value is set to "date published," but it can be changed to "last modified" to select the solution based on the last modified column in the solutions.
- Manual: When the preferred solution type is updated manually. The precedence for this type of solution is the highest.

In certain scenarios, the preferred solution on a vulnerable item (VIT) may differ from the preferred solution on the corresponding vulnerability. This occurs when the preferred solution is manually updated on a VIT and not on the vulnerability. In such cases the **Solution type** field is hidden on the VIT.

What Vulnerability Solution Management does

- Automatically associates new vulnerable items (VITs) and remediation tasks with solutions during Microsoft Security Response Center Solution Integration and Red Hat Solution Integration import.

  MSRC solutions are associated with the latest bulletin the solution appears in.

- Automatically associates vulnerable items and remediation tasks with solutions when vulnerability records are associated manually with solutions.

  Note: Vulnerable items manually reassigned to another solution aren't automatically updated with solution changes at the vulnerability level.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- MSRC: Creates supersedence chains during import that you can view in the solution's related list.
- Indicates whether a solution is a highest-supersedence solution or not.
- Lists the Solution **Risk score** associated with each solution to provide you with the biggest opportunities for risk reduction.
- Maintains **Remediation Status** for solutions on **third party Vulnerability Entries**, **Remediation Tasks**, and **Vulnerability Solution** records so you can track remediation progress.

  It contains:

  - Vulnerable item counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.
  - Configuration Item (CI) counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.
  - Vulnerable item counts by percent remediated, for those VIs with Potential Solutions, with and without those VIs in the Deferred state.
  - Configuration Item counts by percent remediated, for those VIs with Preferred Solutions, with and without those VIs in the Deferred state.

What you can do with Vulnerability Solution Management

- Create, update, view, or delete solutions associated with vulnerabilities, so that you can track vulnerability solutions that aren't covered by third-party solution content. Solution Integration with the Rapid7 Data warehouse is not supported.
- Associate third-party vulnerabilities and NVD entries with a solution record.
- Remove and reassociate vulnerable items and remediation tasks with a solution.
- View the **Preferred Solution** applicable to a given vulnerability on the vulnerability and vulnerable item forms.
- View a **Preferred Solutions** related list on remediation task forms that list all the solutions that have been preferred by at least one active VI within that group.
- View the **Remediation Status** details on a solution that show the risk reduction associated with deploying the **Preferred Solution** on vulnerability, vulnerable item, remediation tasks, and solution forms.
- View vulnerabilities applicable to a given solution on the solution form.
- MSRC: View the superseding solutions for a given solution on a vulnerability, to find the latest update to deploy, or an earlier, more focused, efficient update.
- View lists of solutions sorted for different characteristics.
  - All: Solutions sorted by Date published and Number.
  - MSRC: Highest Supersedence: Solutions with active, non-deferred vulnerable items. Sorted by **Highest supersedence**, **Date published**, and **Number**.
  - With Vulnerable Items: Solutions with active, non-deferred vulnerable items. Sorted by **Highest supersedence** or **Preferred**, **Risk Score**, and **Number**. If deployed, the top entries in the list provide the largest risk reduction for the assets in your environment.

Solution record Risk score and Risk rating

Note: The Solution record **Risk score** and **Risk rating** are distinct from those fields used for vulnerabilities, vulnerable items, and remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Solution record **Risk score** is a weighted calculation based on the vulnerable item **Risk score** and a count of active vulnerable items with this solution as their **Potential Solution**. The solution **Risk score** provides an estimation of the reduction in risk that the solution is expected to accomplish.

The solution record **Risk score** is calculated as follows:

- It starts by taking 85% of the highest or maximum **Risk score** of an active vulnerable item with that potential solution.
- The solution record **Risk score** then tabulates the total number of vulnerable items with that potential solution. For each range of the number of vulnerable items, it adds some points and arrives at a total.
  - 0–09 vulnerable items adds no points
  - 10–99 vulnerable items adds 5 points
  - 100–999 vulnerable items adds 10 points
  - 1000 and beyond vulnerable items adds 15 points

  For example, for a vulnerable item **Risk score** of 80, the Solution record **Risk score** would start at 68. If there were 200 active total vulnerable items with that potential solution, then the final Solution **Risk score** would be 78.

The Solution record **Risk rating** separates the Solution record **Risk score** into ranges from Critical to None. Solution **Risk rating** rates the risk reduction for the vulnerable items that this solution remediates.

Upto VR v16.1, risk ratings separated the resulting Solution **Risk score** into the following ranges:

- 1 — Critical (90+ Solution **Risk score**)
- 2 — High (70-89 Solution record **Risk score**)
- 3 — Medium (30-69 Solution record **Risk score**)
- 4 — Low (1-29 Solution record **Risk score**)
- 5 — None (0 Solution record **Risk score**)

Starting from VR v16.1, risk ratings separate the resulting Solution **Risk score** into the following ranges for Solution Management:

- 1 — Critical (90+ Solution **Risk score**)
- 2 — High (70-89 Solution record **Risk score**)
- 3 — Medium (40-69 Solution record **Risk score**)
- 4 — Low (1-39 Solution record **Risk score**)
- 5 — None (0 Solution record **Risk score**)

Use Cases

View the status deployment progress of a current patch cycle using the highest-supersedence module, sorted by date.

View highest value solutions using the With Vulnerable Items module, sorted by risk score.

Solution lists communicate key solution details, risk scores, and deployment metrics. Use **Risk score** and active VI counts for prioritization. See which solutions in the current patch cycle aren't progressing, possibly an indication of a missed deployment prerequisite.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Add **%VIs remediated(percent_nd_pref_vis_remediated)** from the **personalize List Columns** menu for remediation progress on the Vulnerability Solutions form.

Understanding the Microsoft Security Response Center Solution Integration

Review and implement proposed remediation solutions provided by the Microsoft Security Response Center Solution Integration.

Microsoft Security Response Center Solution Integration is included in the Vulnerability Solution Management feature of Vulnerability Response, available by separate subscription. See Vulnerability Solution Management for more information on how Vulnerability Response incorporates solutions.

Microsoft Security Response Center investigates reports of security vulnerabilities affecting Microsoft products and services, and provides solution information to help manage security risks. Solutions are known remediations imported into your Microsoft Security Response Center Solution Integration from the Microsoft Security Response Center product.

The Microsoft Security Response Center Solution Integration contains entry points to Microsoft Security Response Center product, invoked as scheduled jobs. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. Scheduled jobs run automatically and in the order specified. You can also execute individual scheduled jobs manually.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Available versions

For the most current version of Vulnerability Solution Management and Microsoft Security Response Center solutions, verify you have the most current version of Vulnerability Response installed.

For more information about installing and configuring Vulnerability Solution Management and solution integrations, see Install the Solution Management for Vulnerability Response application and Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant.

Release version of Vulnerability Response	Version of Vulnerability Solution Management	Release Notes
Vulnerability Response v15.0	v10.3	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Roles

Microsoft Security Response Center Solution Integration tasks involve the following roles.

- sn_vul.vulnerability_admin or sn_vul.admin (deprecated): Can read, write, and delete records.
- sn_vul.vulnerability_write: Can read and write records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability.read: Can read records.
- sn_vul.remediation_owner: Can read and write internal notes on records assigned to the remediation specialist group or individual. (Contained in the itil role.)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Microsoft Security Response Center Solution Integration

To view the Microsoft Security Response Center Solution Integration, navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.

The following integration is included in the base system.

Microsoft Security Response Center Solution Integration

Integration	Description
Microsoft Security Response Center Solution Integration	Retrieves solutions and National Vulnerability Database (NVD) mapping to associate solutions with vulnerabilities, vulnerable items, and remediation tasks. **Note:** The Microsoft Security Response Center Solution Integration does not provide solutions prior to 2016.

Solutions

To view imported solutions in a list, see View a solution.

Understanding the Red Hat Solution Integration

You can review and implement proposed remediation solutions provided by the Red Hat Solution Integration in the Vulnerability Response application.

Red Hat Solution Integration is included in the Vulnerability Solution Management feature of Vulnerability Response, available by separate subscription. See Vulnerability Solution Management for more information on how Vulnerability Response incorporates solutions.

Red Hat Solution Integration investigates reports of security vulnerabilities affecting Red Hat products and services, and provides solution information to help manage security risks. Solutions known as remediations are imported into your Red Hat Solution Integration from Red Hat.

Starting from version 21.0 of Vulnerability Response, Red Hat transmits payloads in the Common Security Advisory Framework (CSAF) format rather than the Common Vulnerability Reporting Framework (CVRF) format. CSAF, an XML-based standard, differs in both structure and format from CVRF. To accommodate this change, a new CSAF parser has been developed. This parser interprets the CSAF format, extracting the required fields to populate the tables accordingly.

Note: By default, you will receive the payload in the CSAF format.

The following extracts show the integration script for parsing the payload received from Red Hat in the CSAF and CVRF formats respectively.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is
 provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as
 necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF
 payload is expected
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is
 provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as
 necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF
 payload is expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Red Hat Solution Integration contains entry points to the Red Hat product, invoked as a scheduled job. The scheduled job simplifies the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems. It runs automatically. You can also execute the scheduled job manually.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Available versions

For the most current version of Vulnerability Solution Management and Red Hat solutions, verify you have the most current version of Vulnerability Response installed.

For more information about installing and configuring Vulnerability Solution Management and solution integrations, see Install the Solution Management for Vulnerability Response application and Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant.

Release version of Vulnerability Response	Version of Vulnerability Solution Management	Release Notes
Vulnerability Response v15.0	v10.3	For compatibility information, see KB0856498 Vulnerability Response Compatibility

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Release version of Vulnerability Response	Version of Vulnerability Solution Management	Release Notes
		Matrix and Release Schema Changes

Roles

Red Hat Solution Integration tasks involve the following role: sn_vul.configure_rhsa_integration

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Red Hat Solution Integration

To view the Red Hat Solution Integration, navigate to **Vulnerability Response** > **Administration** > **Integrations**.

The following integration is included in the base system.

Red Hat integration

Integration	Description
Red Hat Solution Integration	Retrieves solutions and National Vulnerability Database (NVD) mapping to associate solutions with vulnerabilities, vulnerable items, and remediation tasks.

Solutions

To view imported solutions in a list, see View a solution.

Rapid7 solution management

Solutions are known remediations that are imported into your Rapid7 Vulnerability Integration from either the Rapid7 data warehouse or Rapid7 InsightVM. Rapid7 data warehouse imports both solutions and superseding solutions. With Rapid7 InsightVM, you get solutions as part of the Rapid7 Vulnerable Item Integration - API.

Starting from version 21.0 of Vulnerability Response, there's a change in how solutions are created by Rapid7 InsightVM. Instead of relying on **solution_summary**, **solution_fix**, or **solution_type** fields, Rapid7 InsightVM now creates solutions using the solution_id provided by the scanner. This means that even if these fields are empty, a solution is created as long as a solution id is available.

To view imported solutions as a list, navigate to **Rapid7** > **Solutions**.

If the Vulnerability Solution Management plugin is activated, then the latest version of Rapid7 Vulnerability Integration provides the following key features concerning solutions:

- The Rapid7 solution management is moved to vulnerability solution management.
- A new integration Rapid7 Prerequisite Solution Management for the data warehouse is introduced. The integration fetches the prerequisite solution from the Rapid7 data warehouse.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The related list of Rapid7 (solution) on third-party entries (TPE) is hidden.
- The previously imported data can be viewed in the new data model. Rapid7 Solutions, Solution Supersedence, and Vulnerability Solution map are reimported and the **Import since** field is set to empty. The field is populated in Solution management.
- The detections are updated to populate the solution field. Detections show the solutions as they're part of Vulnerability Solution Management.
- Rapid7 gets higher preference over other solutions while setting the preferred solution on TPE for Rapid7 data warehouse.
- The solutions roll up to vulnerable items (VI) from detections for Rapid7 InsightVM.

Note: If you have not activated the Vulnerability Solution Management plugin, then the application works as is.

Vulnerability Solution Management

If you have activated the Vulnerability Solution Management plugin, then the Rapid7 solutions for both Rapid7 data warehouse and Rapid7 InsightVM get populated in the Vulnerability Solutions [sn_vul_solution] table. However, if you have not activated the Vulnerability Solution Management plugin, then Rapid7 Vulnerability Integration works as is and imports the solutions in the custom [sn_vul_r7_solution] table.

To view the vulnerability solutions table, navigate to **All** > **Vulnerability Response** > **Vulnerability Solutions** where you can view and compare the solutions from different vendors. To view imported solutions in the custom table, navigate to **All** > **Rapid7 Vulnerability Integration** > **Solutions**.

Note: Group by Source to view solutions based on vendors.

Rapid7 Prerequisite Solution Management integration

If you have activated the Vulnerability Solution Management plugin, a fix script gets executed and changes the order of integrations. The new Rapid7 Prerequisite Solution Integration for Rapid7 data warehouse maps the solutions with the prerequisite solutions. The integrations run in the following sequence:

1. Rapid7 Solution Integration
2. Rapid7 Prerequisite Solution
3. Rapid7 Superseding Solution Integration
4. Rapid7 Vulnerability Solution Map Integration
5. Rapid7 VI Solution Integration (From v19.0 of Vulnerability Response)

Note: If you run the integrations manually, start with the Rapid7 Solution Integration#. Do not alter the Next Integration chain in the Rapid7 Integration. The sequence is defined in the Next Integration column.

Rapid7 (Solutions) related list on TPE

If you have activated the Vulnerability Solution Management plugin, then you can do the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can view the TPEs by navigating to **All** > **Vulnerability Response** > **Third-Party**.
- You cannot see the Solutions (Rapid7) related list, which was available in the older releases.
- You can see the Rapid7 related solutions in the Solutions related list along with the solutions from other sources, such as RedHat, Microsoft (MSRC), and so on.

If you have not activated the Vulnerability Solution Management plugin, then the following occurs:

- The related lists functionality remains the same.
- You can see the Solutions (Rapid7) related list.
- The Solutions related list is hidden.

Preferred solution on TPE and VIs

Rapid7 gets the solution from the data warehouse at the third-party entry (TPE) level and for Rapid7 InsightVM at the detection level.

For a Rapid7 data warehouse, the solution is managed in the following manner:

- The preferred solution is set on the TPE based on vulnerability and solution mapping.
- If the vulnerability from Rapid7 has a single highest supersedence solution from Rapid7, then it's set as the preferred solution irrespective of other solutions from vendors attached to that vulnerability.
- In all other cases, the flow of the preferred solution stays the same.#For more information on the default behavior of preferred solutions, see Vulnerability Solution Management.

For Rapid7 InsightVM, the solution is managed in the following manner:

- The preferred solution is rolled up from detections to#VIs.
- If there's a single detection and solution from Rapid7, then the solution is rolled up#to VI.
- If there are multiple detections and all have the same solution from Rapid7, then the solution is rolled up to VI.
- If multiple detections have multiple solutions from Rapid7, then the latest solution is rolled up to the VI.

Starting from v19.0 of Vulnerability Response, the preferred solution, generated by Rapid7 Data Warehouse, is directly populated onto vulnerable items by Rapid7 bypassing the need for Vulnerability Solution Management. This change ensures that any uncertainty regarding potential solutions for these vulnerable items is eliminated.

To achieve this direct population through Rapid7, the following steps are taken:

- A new integration, Rapid7 VI Solution Integration, is established and integrated into the existing Rapid7 Vulnerability Integration workflow.
- A new table [sn_vul_r7_rapid7_vi_solution_import] is created.
- A new transform map Rapid7 VI Solution Transform is created.
- The script include Rapid7AssetsImportProcessor is modified to exclude the processing of solutions generated by Rapid7 within Vulnerability Solution Management.

Upon execution of the Rapid7 VI Solution Integration, the unprocessed data obtained from Rapid7 is stored in the newly created table. Subsequently, the Rapid7 VI Solution Transform is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

triggered, processing this data and populating the preferred solution directly onto the Vulnerable Item table.

Note: The Rapid7 VI Solution Integration fills in the preferred solution exclusively when the Vulnerability Solution Management plugin has been installed.

Starting from v22.0 of Vulnerability Response, the solutions from Rapid7 are no longer queued up on running the scheduled job *`Process Vulnerability Solutions Metrics Queue`*. This scheduled job involves rolling up solutions from NVD entries to third-party entries, population of preferred solutions on vulnerabilities and updating the remediation status metrics on the solutions. In the following scenarios, only the remediation status metrics must be updated:

- When the preferred solution changes on the vulnerabilities
- When the VITs are created or deleted
- When a VIT import is completed

Though the solutions are queued up to update only the remediation status metrics, they still attempt to roll up solutions from NVD entries to third-party entries and populate the preferred solutions. To optimize this process, in the Vulnerability Solution table, the column **Update status** is introduced. When the remediation status metrics on solutions must be updated without requiring the roll-up of solutions from NVD entries to third-party entries or the population of preferred solutions, they're no longer queued. Instead, the **Update status** column is directly updated as true. This approach enables handling cases where only the remediation status metrics must be updated, resulting in time and resource savings. In the scheduled job, once the processing of the queued solutions is completed, solutions that are marked with an Update status as true are identified. Then, they're iterated through these solutions, calculating the counts and updating the remediation status metrics accordingly. This step plays a significant role in improving the performance of the scheduled job, as the number of solutions that must be queued is reduced.

Solution supersedence chain imported from Rapid7 data warehouse for a vulnerability

You can view the superseding solutions for a solution by selecting a vulnerability solution and selecting the Superseding Solutions related list. You can view the preceding solutions by selecting the Preceding Solutions related list. When you attach any solution to the TPE, then the superseding solution of that solution gets attached to that TPE.

Change the maximum depth of solution supersedence chain in a graph by system property

The solution supersedence chain received in the Rapid7 data model is too long to create the graph during the population of the preferred solution. So, to restrict the depth of the chain, a system property named *`sn_vul.max_recursion_depth`* with a value 500 is created. If the chain depth is more than 500, then the rest of the chain is ignored. To change the maximum depth of the chain, navigate to the [sys_properties] table and change the value of the property.

Upgrading the Rapid7 application

If you upgrade the Rapid7 Vulnerability Integration plugin, and haven't yet activated the Vulnerability Solution Management plugin, then the application works as is.

Whether you activate the Vulnerability Solution Management plugin before or after upgrading the Rapid7 application, the **Import since** field remains empty for the following integrations:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Rapid7#Superseding Solution Integration
- Rapid7 Vulnerability Solution Map Integration
- Rapid7 Solution Integration

Note: From the next integration run, the data is populated to the vulnerability solution table.

For Rapid7 InsightVM, the data is received at the detection level. When the Rapid7 InsightVM integration runs, the solutions are imported in the vulnerability solution table.

Generic framework to ingest data from any solution vendor

A generic framework for solution intelligence integration is available to support ingestion of data in different file formats from solution vendors. These formats speed up information exchange and processing and facilitate the sharing of critical security-related information in a standardized reporting format.

The supported file formats are:

Common Vulnerability Reporting Framework (CVRF)

The Common Vulnerability Reporting Framework (CVRF) is an XML-based language. Major vendors such as Oracle, Red Hat, Cisco, and Microsoft support the CVRF format.

Common Security Advisory Framework (CSAF)

The Common Security Advisory Framework (CSAF) is an open-source standard that provides JSON-based structured, machine-readable security advisories. Major vendors such as Siemens, Red Hat, Hitachi, and Schneider support the CSAF format.

The CVRF or CSAF supported solution management includes the following key features:

- Configuration through Setup Assistant
- Support of importing CVRF or CSAF data through file import
- Support of importing CVRF or CSAF data through CVRF or CSAF URL
- Support of importing CVRF or CSAF data through advisories
- Mapping of solutions with related vulnerabilities

The Vulnerability Response plugin takes care of updating the metrics statuses of the created solution.

SUSE Solution Integration: This feature enables automated ingestion of remediation solutions from third-party vendor SUSE through CSAF. The purpose is to streamline vulnerability response by importing vendor-provided solution advisories, parsing them, and creating actionable solution records within the platform. This ensures that security teams have quick access to accurate and up-to-date remediation guidance for vulnerabilities affecting SUSE products.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Details
SUSE Solution Integration	• Activation: Integration is activated upon solution management installation, you can activate as per requirement. • URL-based: The integration pulls CSAF IDs from a provided URL endpoint. • Pre-Configured URL: The URL is preconfigured in setup assistantunder Common Security Advisory Framework.

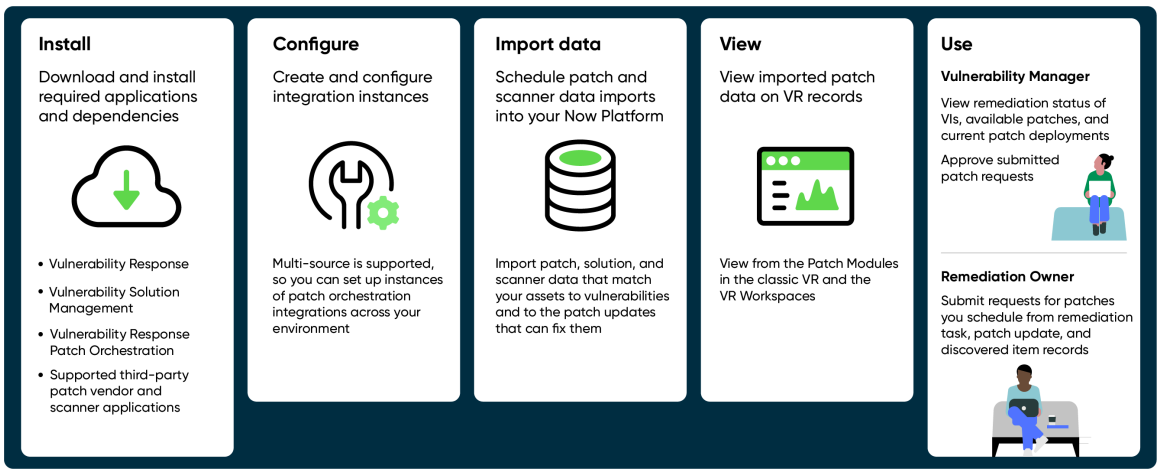
For more information on how to configure the solution providers, see Configure vulnerability solution providers.

Patch orchestration with Vulnerability Response

You can manage patches and patch deployments for critical vulnerabilities for large groups of your assets with Patch orchestration with Vulnerability Response. Vulnerability Response Patch Orchestration and the patch orchestration integrations are available on the ServiceNow® Store.

Understanding patch orchestration with Vulnerability Response

Patch orchestration with Vulnerability Response uses data from scheduled imports from third-party solution integrations, patch vendors, and vulnerability scanners. This data is correlated in the Vulnerability Response application. This organization of data permits you to complete the steps of the vulnerability remediation cycle. Start with identifying vulnerabilities, then apply patches and updates, and finally close vulnerable items using third-party scanner data all from within your ServiceNow AI Platform® instance.



Patch orchestration with Vulnerability Response is supported in both the classic environment and the Vulnerability Response workspaces.

For information about patch orchestration in the workspaces, see Patch orchestration with the Vulnerability Response Workspaces.

With patch orchestration in Vulnerability Response, vulnerability managers and analysts and IT remediation specialists can perform the following remediation tasks:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- See more context and information about the types of patches and vendors that make up their solutions (patches).
- View and monitor vulnerability and solution data, as well as vulnerability remediation progress from records in the Vulnerability Response Workspaces or in the classic environment.
- Deploy patches supported by third-party solution vendors for their Windows, CentOS, macOS, Oracle, and other assets at regular, scheduled intervals. You can schedule patches during off-hours to avoid conflicts with those at work.
- Using imported detection data provided by third-party scanners, identify assets that have vulnerabilities and are not patched or are not successfully updated by scheduled patches.
- Initiate and schedule available patches for assets that require updates from Patch Update, remediation task, and discovered item records in the Vulnerability Response application.
- Monitor patch deployments with an optional approval process for patch requests submitted by your remediation specialists.

Key terms

Configuration item (CI)

CIs are the existing assets that are listed in your#Configuration Management Database (CMDB).

Vulnerable item (VI)

An imported vulnerability that matches an existing asset in your CMDB. Vulnerable items (VITs) are grouped into remediation tasks, or lists, according to certain criteria that specify remediation actions for VIs.

Instance

Refers to a distinct account of a solution vendor application. For example, each user account can be an instance in the HCL BigFix application. This term also refers to a unique, secure web address for a ServiceNow AI Platform® instance.

Solution

There are two types of solutions in the context of this integration, potential and preferred. A potential solution is one that might address a vulnerability. Vulnerabilities often have many potential solutions. #A preferred solution matches the most effective solution for a specific, detected vulnerability.

Patch

Software updates that fix vulnerabilities. Patch vendors use their own names for patches, for example, In the HCL BigFix application, patches are called, Fixlets.

Preferred patch

Preferred patches are software updates that are intended to fix specific vulnerabilities. Patches, once deployed, map to the vulnerable items that are related to specific vulnerabilities and fix them.

Deployment

Deployment for the purposes of this integration refers to when you apply, initiate, or schedule a patch to a machine.

Deployment in the ServiceNow AI Platform can also refer to an integration that supports multi-source. A single integration existence is referred to as a deployment of your integration. A deployment refers to the integrations and products across your environment. For example, you might have multiple deployments of a third-party scanner or a solution vendor integration in your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions of applications and dependencies required for the patch orchestration integration

- The Vulnerability Response application and the dependency plugins, Security Support Common and Security Support Orchestration.
- Vulnerability Solution Management.
- Vulnerability Response Patch Orchestration application available in the ServiceNow® Store.
- A supported third-party patch vendor application, such as The Vulnerability Response patch orchestration integration with HCL BigFix or the The Vulnerability Response patch orchestration integration with Microsoft SCCM.
- Supported third-party scanner integrations with Vulnerability Response.

Roles required

Users need roles that are specific to the patch orchestration integration you are using to view data and schedule patches from the Vulnerability Response application. See the configuration information for the supported integrations you are using listed below for more information.

- Understanding the HCL BigFix patch orchestration integration with Vulnerability Response and The Vulnerability Response patch orchestration integration with Microsoft SCCM.
- In the Vulnerability Response workspaces and the classic environment, the sn_vul_patch_orch.read_patch role, which permits users to view but not edit data, is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles.

  The roles you need to assign that are required to configure the connections to the patch vendors and schedule patches are integration-specific. See Configure the Vulnerability Response patch orchestration integration with HCL BigFix and Configure the Vulnerability Response Patch Orchestration with MS SCCM for more information.

There is a submission and approval process for patch requests included with the applications. By default, a system property is activated [**sn_vul_patch_orch.patch_approval_required**] in the Vulnerability Response Patch Orchestration application in your ServiceNow AI Platform instance.

This system property is activated so that when patch deployments are scheduled, they are submitted for review and approval to users assigned to the Level 1 - Patch update approval group. If you want users with the sn_vul_patch_orch.configure_patch role to schedule patches without approval, you can deactivate the [**sn_vul_patch_orch.patch_approval_required**] property. You might prefer to leave approvals activated so that scheduled patches do not conflict with normal working hours. If you deactivate the approval system property, any user with the sn_vul_patch_orch.configure_patch role can schedule and deploy patches without review and approval.

For more information, and how to deactivate this system property, see the configuration topic for your supported integration.

- Configure the Vulnerability Response patch orchestration integration with HCL BigFix.
- Configure the Vulnerability Response Patch Orchestration with Microsoft SCCM integration.

Schedule patches from Vulnerability Response records

Remediation specialists can schedule patch updates to resolve vulnerable items and monitor remediation progress all from records in the Vulnerability Response application.

You can schedule patches from the following records:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Patch Update
- Remediation task
- Discovered item

Records that roll up active VI counts in Vulnerability Response

To avoid potential performance issues with rolling up all the patches to all the vulnerabilities, the scheduled job that picks up changes only modifies the active VI count. These count changes and related data are rolled up to the following records in the Vulnerability Response application:

- VIT (vulnerable item)
- RT (remediation task)
- Vulnerability solution
- Patch Update

For more information about viewing patch data and patch data roll up to records, and viewing patches without solutions, see the following topics.

- Patch data and state rollup for patch orchestration in Vulnerability Response.
- Viewing patch data and scheduling patches in Vulnerability Response.
- View patches without solutions in Vulnerability Response.

Bulk edit vulnerable items with patches

You can bulk edit vulnerable items in the classic environment that have patches from the classic environment. For more information about how bulk editing works, see Edit vulnerable items in bulk in Vulnerability Response. The preferred patches for all the VIs selected for bulk edit. This option for edit only works if there are preferred patches mapped to all the VIs selected.

Patch Orchestration Data Model Enhancements

The Patch Management Data Model plugin — a standalone, free plugin that encapsulates the data model currently used in the VR Patch Orchestration application. This includes key tables such as Collection, Patch Update, Patch Deployment, and others.

This plugin decouples the patch-related data model from the VR module, making it independent and reusable across other ServiceNow applications. This plugin is now a dependent plugin for VR Patch Orchestration.

Key Enhancements:

- Tables such as, collection device, patch update, patch deployment tables in the existing patch orchestration plugin will be moved to the new data model plugin.
- New tables will be created for these elements in the new plugin.The data from the old tables will be migrated to the new tables. Migration scripts and scheduled jobs will handle this process automatically. The old tables and references will be deprecated.

Exception Management overview

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to a vulnerable item (VI) or remediation task (RT) that cannot be remediated according to the policy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Some vulnerabilities might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the vulnerability.

Life cycle of an exception

Definition of an exception

An exception is a request to defer the remediation of a VI or RT for a specified period. For example, as a remediation owner, you can request an exception if a patch is not available for a machine.

Requesting an exception

As the remediation owner, you can ask for an exemption for a VI or RT using the exception management process. After the exception approver approves this request, the VI or RT moves to a **Deferred** state.

Approving an exception request

VIs or RTs that can't be remediated immediately are reviewed by vulnerability analysts, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level workflow. If only the first-level approver is present, the exception can be requested and approved. However, if there's no first-level approver, an exception can't be requested. See Add an exception approver for more information.

Note:

- Starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

  Once an exception request for a VI or RT is approved, you can perform the following actions:

  - Reopen
  - Delete
  - Update the **Assignment to** or **Assignment groups** fields
- Starting with v23.0 of Vulnerability Response, the **Exception Rule State Approval** workflow is deprecated and replaced by the flow Exception Rule Approval in the flow designer.

Tracking an exception request

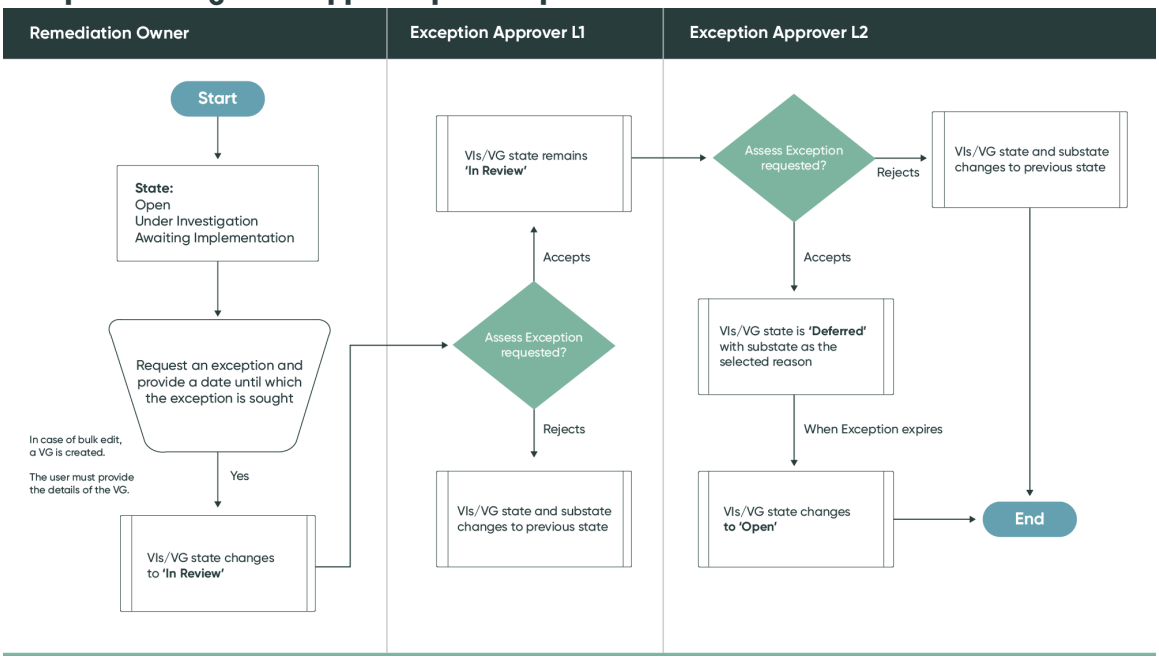
After raising the exception, you can track its status by using the **State Change Approvals** tab of the VI or RT. If an action is taken on an RT, you can't track the status of the individual VIs in that RT.

Expiry of an exception request

When an exception request for a particular VI or RT expires, the impacted VI or RT reverts to its **Open** state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception management approval process prior to VR v15.0



If a single VI or all the VIs in a RT pass in the next scan, then the VIs and, where applicable, the RT **State** field changes to **Closed** with the substate **Fixed**.

Multiple deferrals

Track the number of times a record or a remediation task is deferred. A scheduled job, *`set deferral counts`*, runs daily to post counts for the records that are deferred more than once in the Deferral count column in the Multiple deferrals module for VR. All counts for records associated with a remediation task are collected and posted if a remediation task is deferred more than one time.

Related topics

- Request exceptions for remediation tasks and records from the Vulnerability Manager Workspace
- Request an exception in the IT Remediation Workspace
- Request an exception using GRC: Policy and Compliance Management in the IT Remediation Workspace

Exception rules overview

Exception rules for Vulnerability Response enable you to automate the deferral process for vulnerable items (VIs). Request an exception for the vulnerable items (VIs) that can't be remediated or deferred immediately, by identifying the impacted vulnerabilities, configuration items (CIs), or VIs. Defer the matching VIs based on the rule when the system identifies them by automating the VI deferral process.

Using exception rules in your organization

Use exception rules to automatically defer new and existing VIs for a specific period if they match the approved rule condition. Automation minimizes the risk of missing service level agreements and makes it easier to manage multiple items, because you are eliminating manual intervention.

Deferral rules support ordering, that is, the rule with the highest priority is run first. When a high-priority rule is applied on a VI, no subsequent rules are applied on it again even if the condition matches the VI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- You can only create rules if you select Vulnerability Response in the Exception Management configuration. For details, see Configure Exception Management for Vulnerability Response.
- When VIs are deferred by an exception rule, they are copied to the deferral vulnerability group (VG) that is created. The VIs continue to be part of the VGs they were part of earlier.

The life cycle of an exception rule is as follows:

- Creating an exception rule
- Approving an exception rule request
- Activating an exception rule
- Deferring an exception rule
- Expiry of an exception rule

Creating an exception rule

You can create an exception rule to automatically defer the VIs that match the defined conditions for the specified period. After you create an exception rule, submit it for approval.

Approving an exception rule request

Approving an exception rule request is a two-level process. If only the first-level approver is present, the exception rule can be assessed and approved by a single approval. However, if there's no first-level approver, an exception rule approval can't be approved. After the rule is approved, a remediation task (RT) is created. See Approve an exception rule request for more information.

Note:

Starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

After an exception rule request is approved, you can perform the following actions:

- Cancel
- Delete

Activating an exception rule

After an exception rule is approved, a remediation task is created in a Deferred state by default. Starting from the "Valid from" date, the exception rule runs on all the VIs that are created and also on the ones that are moved from the Closed to the Open state.

Note: If you enable the Execute on existing data option, a scheduled job runs once on the existing data on the "Valid from" date.

Deferring an exception rule

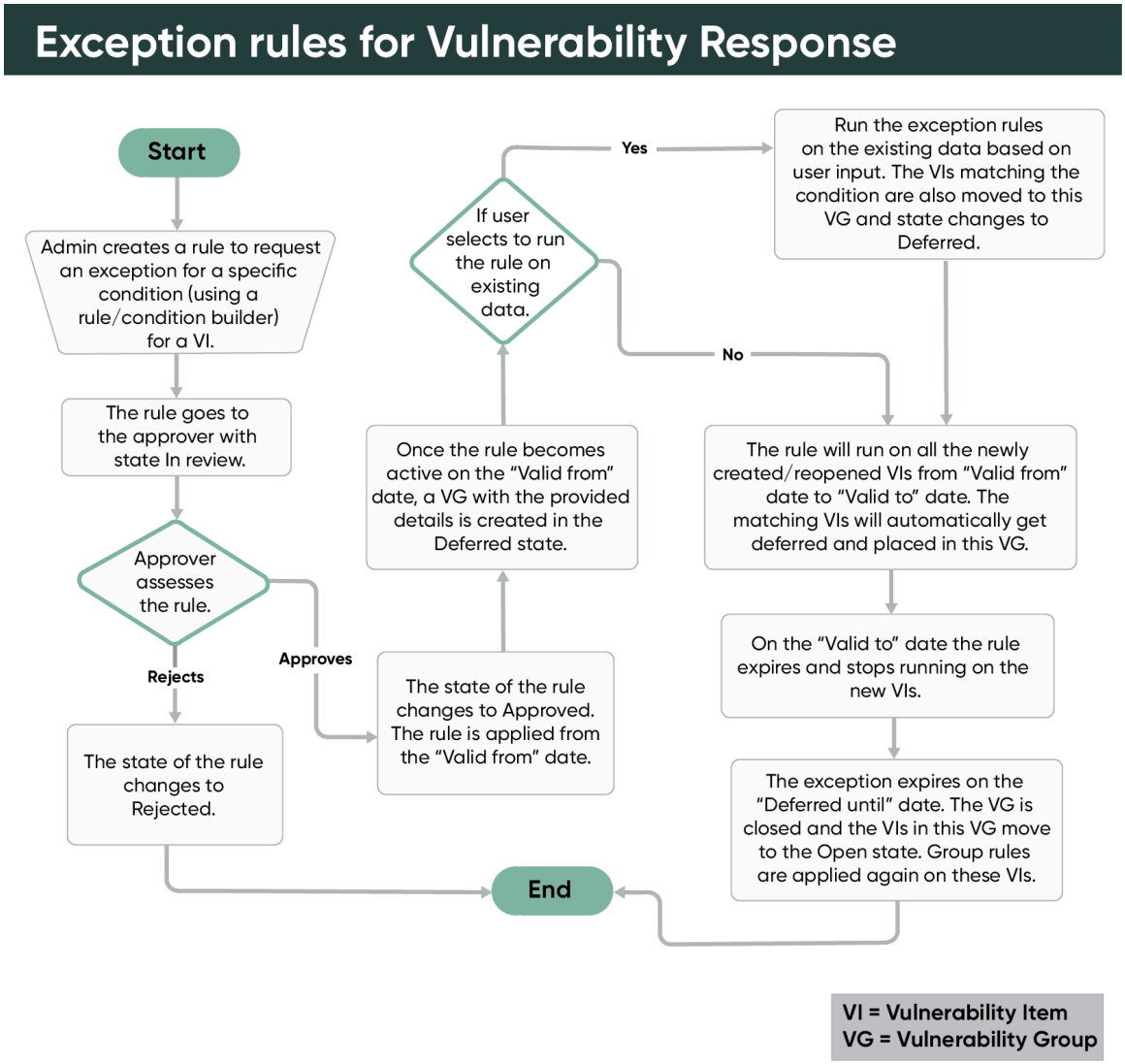
You can defer VIs that match the conditions defined in this exception rule, up to the "Deferred until" date that is defined for the rule. On this date, the remediation task that you created for the exception rule is closed and all the VIs in this group move back to the Open state. Group rules are applied on them again to allocate them to the required RTs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Expiry of an exception rule

After the exception rule expires, it no longer runs on new or reopened VIs. The associated RT remains in the Deferred state until the "Deferred until" date.

Exception rules work flow prior to v15.0



Exclusion rules overview

Exclusion rules provide a way to filter or exclude detections from getting converted into vulnerable items (VITs) during the ingestion process in Vulnerability Response.

These rules can be set up to handle various scenarios such as:

- Excluding vulnerabilities with low severity or risk that don't require immediate remediation.
- Improving the remediation process by prioritizing the most critical VITs for action.
- Reducing the processing time during data import by excluding a percentage of detections from VIT conversion.

During the process of ingesting data, there are distinct approaches for handling new and existing detections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For new detections:
  - If a new detection doesn't meet the conditions of an exclusion rule, a detection is created with the VITs.
  - If a new detection meets the conditions of an exclusion rule, the rule gets associated with the detection, but VIT is not created. Populate the matching Exclusion Rule reference on Detection record. The Exclusion rule column is populated with Exclusion Rule reference on the Detection record accordingly.
- For existing detections:
  - If the detection doesn't meet the conditions of any exclusion rule, it proceeds with the normal workflow.
  - If an existing detection matches the conditions of an exclusion rule, the VIT associated with that detection stays in its current state but the rule gets associated with the detection. The state of the VIT is governed by the value defined in the *sn_vul.close_vit_with_excluded_detections* property. By default, the value in this property is set to False. If the value is set to False,then the detections under a VIT get excluded and state of the VITs stays in its current state. However, if the value is set to True, the following scenarios may occur:
    - If every detection under a VIT is excluded, the VIT's status is updated to Closed Excluded.

      Note: Starting from v22.1.2 of Vulnerability Response a new substate called Excluded has been added,

    - If one detection is marked as Closed while the remaining are excluded, the VIT is designated as Closed Fixed.
    - If the VIT has open detections, then the VIT remains Open.

Related topics

Create an exclusion rule

False Positive overview

A false positive is a condition wherein the scanner reports that a vulnerability exists in the system, but in reality there is no vulnerability. There can be multiple reasons like incorrect classification, improper logic or algorithm in the scanner. The remediation owner can mark vulnerable items (VIs) or remediation tasks (RTs) as false positives.

Important: You can mark the host vulnerable items as false positive in bulk in the Vulnerability Manager Workspace. For more information on how to mark the host vulnerable items as false positive in bulk, see Bulk edit for false positive in the Vulnerability Manager Workspace.

Life cycle of a false positive

Meaning of false positive

The scanner sometime gives a warning, when in reality there is no vulnerability. For example, if a configuration item has been decommissioned but the scanner is still raising an issue related to it, mark it as a false positive.

Marking as a false positive

For details on marking a VI or RT as a false positive, see Mark as a false positive.

Working with the false positive

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Once a VI or RT is marked as a false positive, the state is updated to Closed and the substate is changed to False Positive. The following actions can be performed:

- Reopen
- Delete
- Update the date in the **Until** field. This date is then used as the expiry date for the false positive.

Note: If not approved, the VI or RT reverts to its previous state.

Approving a false positive

The approver can approve the false positive from their approval workflow.

Note:

Starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Reopening a false positive

A VI or RT in a false positive substate can be reopened anytime.

Tracking a false positive

Use the **State Change Approvals** section to track the status of the false positive. Once approved, the state of the VI or RT is updated to Closed and the reason is False Positive.

Expiry of a false positive

Only the false positive approver can set an Until date for the false positive, for the VI or RT to expire. Also, only false positives for which the approver has provided an Until date can expire. This date can be provided after the false positive is approved.

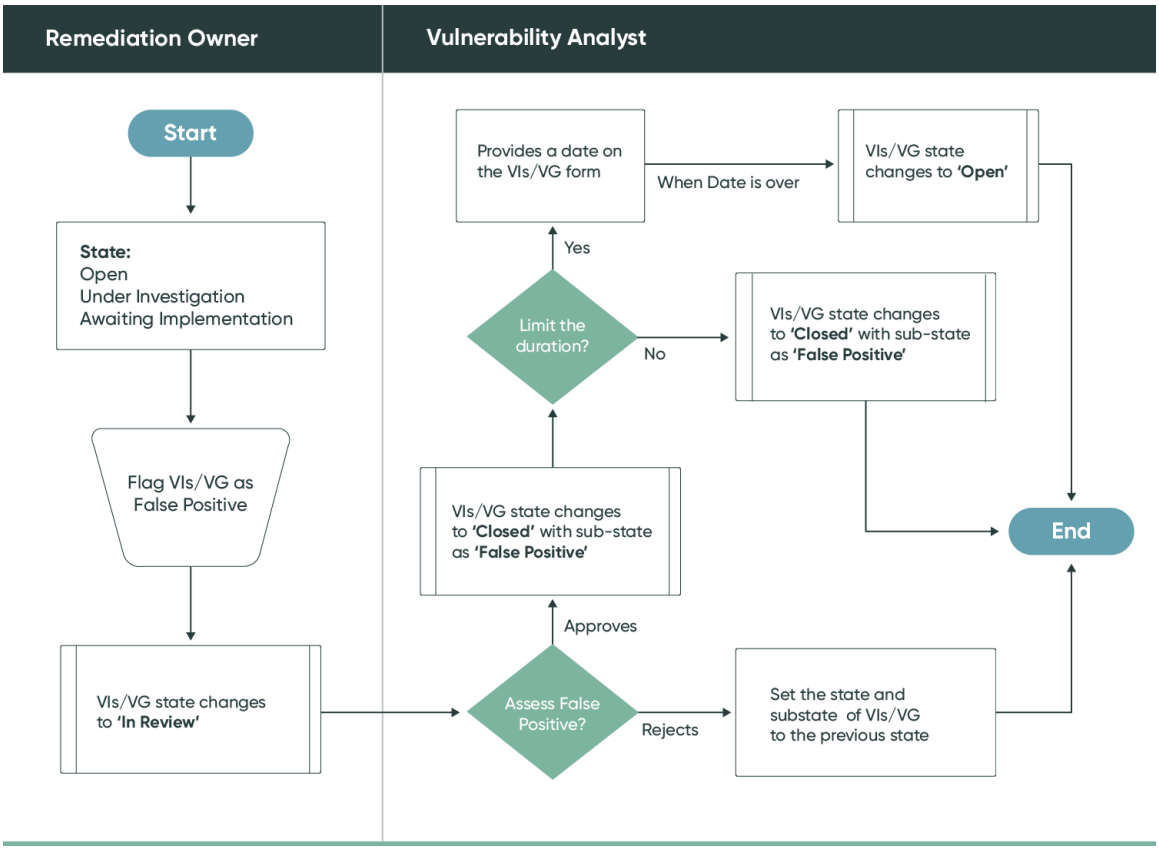
A false positive without an Until date is a permanent false positive. After the false positive expires, the state of the VI or VR moves back to Open.

Note:

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

False positive approval process prior to v15.0



The approval process is automatic if all VIs pass the next scan. The VIs auto-close regardless of the current state. The VIs or, where applicable, the RT **State** fields change to **Closed** with the substate **Fixed.**

For more information, see Marking and approving a false positive.

Related topics

Request a false positive in the IT Remediation Workspace

Questionnaire support in Exception Management via Smart Assessment

Configure advanced questionnaires as part of the exception management process using Smart Assessment. This allows Remediation Owners to provide more detailed context for Exception Requests and enables Approvers to configure conditional questions to gather information for informed decision making.

Roles required

Smart Assessment Template Reader: **sn_vul_cmn.smart_assessment_template_manager** (Vulnerability admin and Template reader) allows admins to create and edit templates.

Smart Assessment actor: **sn_vul_cmn.smart_assessment_actor** enables you (Remediation Owners and Admins) to fill out the questionnaires/assessments.

Smart Assessment reader: **sn_vul_cmn.smart_assessment_reader** enables you (Approver) to read the submitted questionnaire responses.

Pre-requisite: The smart assessment plug-ins must be installed as the Smart Assessment is a dependency on Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can now configure questionnaires as part of the Exception Management process using Smart Assessment. It allows Vulnerability Admins/Manager to configure conditional questions to gather the right information needed for informed decision-making, while enabling Remediation Owners to provide more detailed context for exception requests. This improves collaboration between the Vulnerability Management and Remediation teams by streamlining the approval process and ensuring clarity and completeness of exception justifications.

Questionnaires and smart assessments are accessible in Workspace as well as the Classic User Interface as some workflows still require the older style questionnaires, while the new assessment is more user friendly and is only supported in Workspace.

In the **Exception Management Configuration** screen, you can now select the Assessment for Compensating Control, request exception and false positive records.

Note: In case you chose to complete “Assessment to request exception” field, the system allows you to consider the smart assessment template, or else the classic questionnaires are considered.

You can use the two options provided below: :

- **Smart Assessment**: Manage the Questionnaires in Vulnerability Workspace.
- **Existing Questionnaire**: You can access the existing questionnaire in both the Workspace and Classic experience.

The above templates can be accessed/edited by the Smart Assessment Template Reader: **sn_vul_cmn.smart_assessment_template_manager**.

Configure Assessment template

Assessment templates contain the questions that will be prompted to users during the request process (e.g., when requesting an exception). We are providing certain preconfigured templates with the smart assessment enhancement. You can also create your own templates as required.

Before you begin

Role required: Template Reader Role: Allows users to read templates, Template Actor Role: Allows users to fill out and submit the assessments

About this task

In the Vulnerability Response workspace, users can select the template they want to use for the exception request (e.g., Exception for Vulnerability Response, False Positive for Vulnerability Response). If the user selects the default template, it automatically populates the questions. If they choose to create their own template, they can modify it accordingly.

Procedure

1. Navigate to Assessment Workspace.
2. Select an existing **Assessment Template** or select a**New Template**
3. Fill in the following details:
    - **Template Name**: A unique name for the template
    - **Assessment Name**: The name displayed in the system when viewing the assessment.
    - **Template Categories**: Templates are categorized for easier management. For example, a category could be Vulnerability Response Questionnaire Templates.
    - **Assessment Targets**: Specifies the table that the template is related to. For VR, it is the VCA table (Vulnerability Change Approval table).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Smart Assessment workflow

Remediation owners and admins must fill out the questionnaire before submitting for approval. Approvers review the assessment and make approval/rejection decisions based on the provided information.

Before you begin

Role required: Assessment Reader

About this task

The following is the workflow of the smart assessment adaption:

- **Request for Exception/False Positive** when a user requests an exception or marks something as a false positive, the system checks if a questionnaire is required.
- If the **questionnaire option is enabled**, a **mandatory message** will prompt the user to complete the questionnaire before proceeding with the approval process.
- **Draft State**: The VCA record and the VIT (Vulnerability Item) remain in the draft state until the questionnaire is submitted.
- **Approval Request**: Once the user fills out the questionnaire and submits it, the VCA and VIT records move to in review status.

Procedure

1. Select an assessment template.
2. Fill out the questionnaire in the **Smart Assessment** workspace.
3. Submit the questionnaire.

   the VCA and VIT records will transition to **in review**.

   Note: If the user doesn't fill out the questionnaire, the request remains stuck in the **Draft**state.

Questionnaire for False positive or Request Exception

When the questionnaire for False Positive or Request Exception is raised but not filled copmpletely.

In case, when questionnaire for False positive or Request exception is raised but not filled completely, the VCA record goes into “Draft” state. If you want to raise an exception from the same category, you will be navigated to the previous questionnaire following a pop-up note regarding the same. In case, you want to raise a False Positive record instead of an existing request exception, the system will override the Vulnerability State Change Approval (VCA) and create a new False Positive Vulnerability State Change Approval (VCA) record.

In case the questionnaire is half filled and same Vulnerability Item (VIT)/ or any ITEM is opened in classic view, you will be navigated to workspace questionnaire to fill the remaining data if the same type of request is raised again. If questionnaire in classic view is selectively filled and same item is opened in workspace, then the classic view questionnaire will be opened in the workspace.

Watchdog for Vulnerability Response

The watchdog is used to track tables based on the conditions you specify. For example, it can be used to log details of integration run failures in Vulnerability Response.

You can choose to be notified about these failures. Based on this notification, you can plan the remediation. The default watchdogs are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Integration run failed: If the integration run State is set to Complete and Substate is set to Failed, users and user groups are notified if the condition returns a count greater than 0, that is, the integration run fails.
- Long running integrations: Script to verify if the integration run is exceeding the set time. This watchdog proactively alerts you whenever there is a delay in the completion of the integration run.

Watch log

The watchdog comes with a watch log, which provides a count of the number of times the condition has been met.

Overview dashboard

Use the Overview dashboard to monitor the watchdog for the past 30 days. You can create multiple widgets to track other watchdog topics you are monitoring.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Report

Name	Description
Last 30 days WatchDog failure	All the conditions met in the past 30 days.

For more information, see Configure watchdog and Error handling for detections.

Change management for Vulnerability Response

As an IT remediation owner, you can create and manage change requests (CHG) directly from remediation tasks (RT) in the Vulnerability Response application. Change requests help you initiate and track change activities on your assets so that you can remediate your remediation tasks and their corresponding vulnerable items.

Change requests and the vulnerability workflow

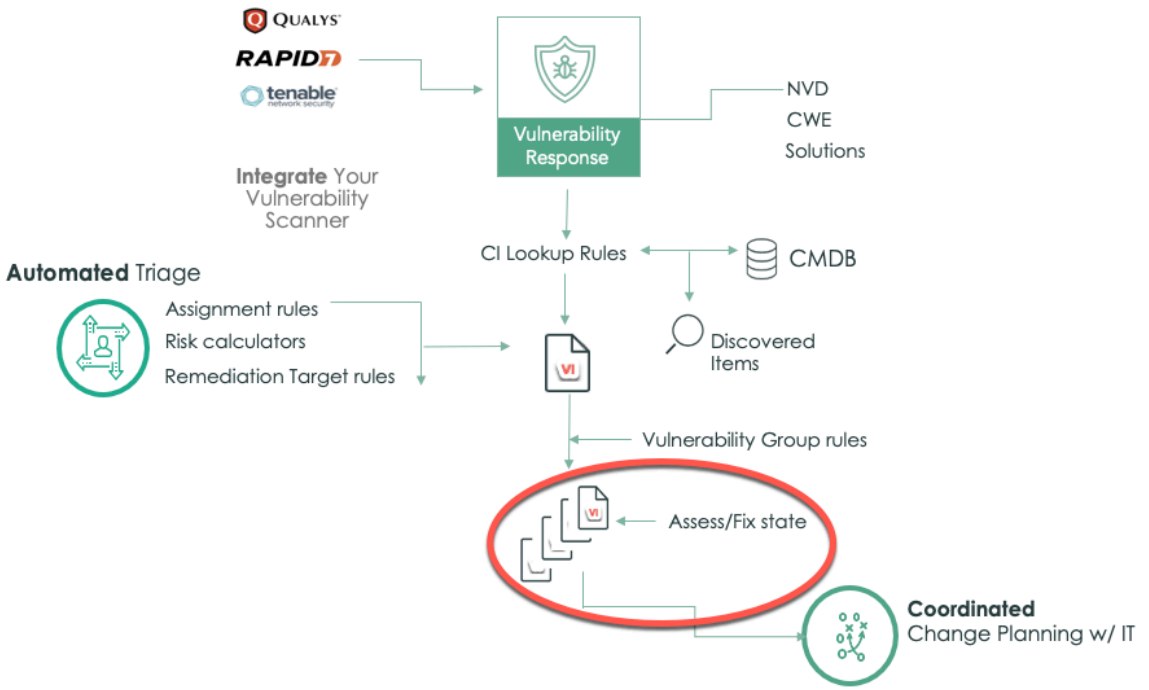
If you are not familiar with the Vulnerability Response application, for more information see Exploring the Vulnerability Response application.

The following image illustrates the flow of information for Vulnerability Response, from integration (scanner) set up through automated triage and into investigation.

Change requests and change management are part of the remediation process (Assess/Fix state) in the Vulnerability Response workflow shown in the following figure. During this phase, you might use change requests to initiate and track the remediation of vulnerabilities. You can create and manage change requests directly from the remediation task and list investigation and remediation tasks that include solutions for impacted assets for the configuration items (CI) in your CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Change requests in Vulnerability Response



When to use change requests in vulnerability response

As an IT remediation owner, you might create change requests from a remediation task if a manual and controlled process of any kind is required for modification or removal of supported configuration items (CIs) in your CMDB. Creating and managing change requests directly from a remediation task record helps you investigate and resolve vulnerabilities quickly. The VIs of a resolved remediation tasks can be scanned and verified during the next scheduled scan in your ServiceNow AI Platform and returned to the automated triage of the Vulnerability Response workflow. Manual interventions that might require change requests include the following examples:

- A software patch, fix, or other task by IT that is required on vulnerable items prior to RT resolution.
- You determine a subset of the vulnerable items in a remediation task requires further investigation or reassignment to another department.
- You determine that a subset of vulnerable items in a RT with a large set of vulnerable items can be moved into a new remediation task.
- You might associate a remediation task to an existing change request to avoid duplication of remediation tasks.

Types of change requests for an RT

The Vulnerability Response application utilizes the three types of service changes supported by the ITSM Change Management product on your ServiceNow AI Platform® instance — standard, emergency, and normal. The type of change you select determines which state model is invoked and the change process that must be followed. Change requests record the detailed information about the change, such as the reason of the change, the priority, the risk, the type of change, and the change category. See Change types.

As a Vulnerability Response IT remediation owner, you have the following options for creating normal, standard, and emergency change requests directly from a remediation task:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can create change requests that contain pre-populated information from the remediation task to streamline the process and save time.
- You can associate a remediation task to an existing change request to avoid creating duplicate change requests that share similar information and vulnerable items.
- Using a set of conditions, you can filter out a subset of vulnerable items and split a remediation task. The items that you select are automatically moved to a new RT.

You can filter vulnerable items using values from any fields from a remediation task and apply the change request to only those items that match your filter criteria.

Related topics

Create a change request from a remediation task

Associate a remediation task to an existing change request

Split a remediation task

State synchronization between change requests and remediation tasks

Software exposure assessment using Software Asset Management (SAM Foundation)

Use the ServiceNow® Vulnerability Exposure Assessment application to determine your total installed software count for a specific software package on your assets. When used with the ServiceNow® Software Asset Management (SAM) Foundation application, evaluate your exposure, create vulnerable items, and manage remediation for the vulnerable software you discover.

Important: You can perform the exposure assessment by Common Vulnerabilities and Exposures (CVE) and software to leverage the additional capabilities in the Vulnerability Assessment Workspace. For more information, see Explore the Vulnerability Assessment workspace.

Determine your exposure to vulnerable software by providing the vulnerable software information (publisher, product, edition and version) without using the Common Vulnerabilities and Exposures (CVE) database. Assess cases of a zero-day (current day) vulnerabilities to software for the following cases:

- When products do not yet have CVE data.
- When there is a lag between the time a vulnerability becomes publicly known and the CVE data with the vulnerability is updated in the NVD.
- When you learn about the vulnerability in-between the scheduled scans of your vulnerability scanner.

With the Vulnerability Exposure Assessment application, if you know the publisher and product for the vulnerable software, using the records that list the installed software in your network created by the SAM Foundation application, you can assess your exposure to potentially malicious software packages on-demand.

Knowing the scale of your exposure to this type of vulnerability permits you to proactively respond by implementing a red alert and uninstalling the software, or informing your security operations center (SOC) to look for a specific patch. You can create vulnerable items and assign tasks to the remediation specialist for further investigation remediation. View a remediation task (VUL) list to verify that the vulnerable items you want are created and associated correctly to the VUL.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Configure the Vulnerability Exposure Assessment

Assess your exposure to vulnerable software

Vulnerability Crisis Management

Create and track critical vulnerability events through the Vulnerability Crisis Management (VCM) workflow. Create vulnerability assessment records, record key attributes of the vulnerability to calculate risk, perform assessment to identify exposure level, and engage stakeholders for a coordinated and swift response to vulnerabilities.

Managing vulnerability crisis events

Vulnerability Crisis Management is a complete workflow to handle vulnerability crisis events with the following capabilities.

- Efficiently identify vulnerable configuration items by correlating critical vulnerabilities with software installation inventory from Software Asset Management and Software Bill of Materials (SBOM) inventory, scanner-reported vulnerabilities, and Configuration Management Database (CMDB).
- Convert assessment results into vulnerable items for remediation.
- Initiate a major security incident, to ensure a swift and coordinated response to the threat.
- Engage and collaborate with teams across the organization, facilitating a unified response to vulnerabilities.
- Provide regular status reports to cross-functional stakeholders and involved teams to maintain transparency and communication throughout the crisis.

Vulnerability Crisis Management using the Vulnerability Assessment Workspace

Note: Starting with v1.0.1 of Vulnerability Crisis Management, the application is available as a separate subscription in the store. You can access Vulnerability Crisis Management from the Vulnerability Assessment workspace only if you have fine-grained entitlement or have installed the application from the store. Previously, Vulnerability Crisis Management was included with the Vulnerability Emergency Response plugin. Starting with v3.2.2, the Vulnerability Emergency Response plugin has been renamed to Vulnerability Exposure Assessment.

On identifying a vulnerability of interest, the vulnerability event manager creates an vulnerability assessment record with information on the threat intelligence source, vulnerability characteristics, and affected products. This information is used for further impact and exposure analysis.

After the record for a vulnerability of interest has been created, a risk assessment is performed. This assessment comprises structured risk scoring, reviewing the record, and the observations of the analyst performing the task. The initial risk score for a vulnerability of interest is calculated using the attributes available at the time of event creation. The risk score for the assessment may change as additional intelligence becomes available. Use the risk score to determine the potential impact of exploitation and establish response priorities.

After the assessment for a vulnerability of interest has been created and determined to present risk to the organization's infrastructure, you can analyze the threat further by updating the risk assessment with an in-depth exposure assessment with the software installation inventory from Software Asset Management, Software Bill of Materials (SBOM) inventory, scanner-reported vulnerabilities, and Configuration Management Database (CMDB). Impacted Configuration Items

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and Applications are automatically identified through assessment. Additional impacted items can be added manually.

Once the assessment is completed, Vulnerable Items or Application Vulnerable Items can be created for the exposure results that do not already have a associated vulnerable Item. Risk score calculator of vulnerable items can be leveraged/configured to adjust risk score for vulnerable items linked to vulnerability assessment records. The Vulnerability Assessment record can be assigned exposure level and event priority. Based on the event priority, the Vulnerability Event Manager can choose to propose, promote or link the vulnerability assessment to a Major Security Incident.

Use Major Security Incident Management to track and manage remediation activity, link ongoing security incidents, create ad-hoc tasks, engage affected teams, send status reports and collaborate using collaboration integrations available in Major Security Incident Management.

ServiceNow® Software Asset Management and Software Bill of Materials (SBOM) assessment- processing logic

Using the Software Asset Management data, the CPEs coming from NVD for the CVE, and then the discovery models are fetched using the string-matching logic. After fetching the discovery models, a scan for related installations is run, the related configuration items are fetched, and the Affected Configuration Item table is populated. You can provide further details like Publisher, Product, Version and Edition. Based on these, all the matching discovery models and the software installations for the record are fetched. Subsequently, the related configuration items are fetched and the Affected Configuration Item table is repopulated.

For SBOM, the associated software for the CVE from the related (m2m) table (between CVE and Software) is fetched. After pulling in the software details, the related SBOM components are identified by matching the product and version from the SBOM component to the product and version of the software identified.

After the associated components are found, the entities related to the components are fetched. The product model from the entities and the related CI (if found) are fetched and the configuration item is saved in the Affected Configuration Item table. If the configuration item is without vulnerable items you can use it to create the vulnerable item. If a configuration item is not found, the product model is saved in the Affected Software Model table and can be used to create application vulnerable items.

For more information on using the Vulnerability Crisis Management workflow, see Using the Vulnerability Assessment workspace.

Related topics

- Exploring vulnerability assessment
- Explore the Vulnerability Assessment workspace
- Assessment tab

Domain separation and Vulnerability Response

Domain separation is supported in Vulnerability Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

How domain separation works in Vulnerability Response

With domain separation you can standardize VR (Vulnerability Response) procedures, across the customer base you serve, with lowered operational costs and a higher quality of service.

Separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

Domain separation support in Vulnerability Response by version releases

Release	Support level	Notes
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	
Washingtondc	Standard	

Domain separation for the Vulnerability Response application covers the following product functionality:

- Ingests the vulnerable items from third-party scanners (for example, Qualys, Rapid 7, or Tenable) in the correct domain. The data ingests in the same domain as that of the integration user, whose credentials are used for integration.
- Re-scans specific assets from Vulnerability Response in the domain from which it was requested.
- Uses the CMDB CI lookup process to ensure that the CI information from the scanners matches the CIs in CMDB of the integration user's domain.
- Calculates risk scores at the vulnerable item level as per the risk score calculator defined in the same domain as that of the integration user.
- Remediation target rules are executed on vulnerable items as per the remediation target rules defined in the same domain as that of the integration user.
- Remediation task rule(s) can be defined, and stay in, the same domain as the domain of the integration user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Remediation tasks created using the remediation task rules stay in the same domain as where the group rules are created.
- Deferral workflow goes through the approval process in the same domain for which the deferral is requested.
- Reports and dashboards display the vulnerable item-states such as age of vulnerable item, open vulnerable items by CI, vulnerabilities by impact, and remediation target date status in the domain to which it belongs.
- Knowledge from third-party scanners or the National Vulnerability database (NVD) can be ingested in the global domain and data can be shared across multiple clients.

Note: In all the above cases the overarching principles of visibility in separated domains separation in the ServiceNow AI Platform apply.

For more information on how to create and support domain-separated imports, see Create domain-separated imports for an integration and Create and support multiple domains in the background jobs framework.

Use cases

The Vulnerability Response application manages the life cycle of a vulnerability item end to end. The following use cases are domain-separation aware:

- **Ingest** vulnerable items (vulnerabilities on asset) from your third-party integration.
  - Ingest data from multiple instances
  - De-duplicate the vulnerable item
  - Match up with CMDB CI
- **Enrichment** of vulnerable item with risk scores and remediation target dates
  - Asset enrichment (CMDB)
  - Risk score and remediation target date enrichment
- **Group** vulnerable items and assign the remediation task
  - Automatically group the vulnerable items
  - Automatically assign the remediation task
- **Remediate**
  - Remediation tasks
  - Comprehensive remediation life cycle
  - Deferral workflow
- **Measure** the security posture of the organization and vulnerability management program
  - Vulnerability trend, most vulnerable asset, vulnerability by age
  - Remediation status by the remediation target date

Setup

Setting up domain separation for Vulnerability Response does not require any additional steps. All Vulnerability Response tables acquire the Domain column after the instance is domain separated. You can direct vulnerability integration import data to specific domains. See Create domain-separated imports for an integration for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Domain-separated data

Data can be domain separated, which means:

- Vulnerable item ingested from third-party scanners stays in the same domain as the domain of the integration user, and is not accessible from any other domain.
- Vulnerabilities, vulnerable items (instances) or assets in one domain cannot be viewed from other domains.
- The risk scoring algorithm, the remediation task rules and the remediation target rules cannot be viewed by anyone outside the domain.
- Vulnerability information from the NVD can exist in the global domain and be shared with all customers.
- Remediation tasks in one domain cannot be viewed from another domain.
- Deferral workflows created in one domain are not visible in another domain.
- All email notifications are contained within the domain they belong to.

Note:

The scheduled import templates available on the instance are by default set to "Domain: global". So, to avoid any conflicts when there are multiple domains on instances, adapt the following practice:

- Distribute the import templates available on the instance across the number of domains involved in the integration.
- Update the import template record's domain to the sys_id of the target domain.
- If necessary, create import templates for each domain.
- Ensure each domain has 2 import templates.
- sn_vul_sched_import_pool: This table records should be domain separated if domain separation is present on instance

How vulnerability analysts manage their own application data

- Analysts create their own application installation, multi-source application management, and CI lookup rules.
- Analysts can configure specific integrations exclusively for use within the domain.
- Analysts can create their own deferral and change management workflows.
- Analysts can create their own remediation task rules, risk-scoring logic to accurately prioritize vulnerabilities, auto-assign remediation tasks and assign to the correct assignment group.
- Domain users create a manual vulnerability item and then close the item.

Business logic and processes that can be domain-separated by instance owner

- Vulnerability Response users and groups
- Vulnerability Response integrations
- Complete setup configuration (user and group management, application installation, multi-source application management, CI lookup rules, remediation task rules, risk calculators, remediation target rules etc.)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Complete remediation life cycle including deferral
- Schedule jobs

Related topics

Domain separation for service providers

Service Mapping in Vulnerability Response

Service mapping helps organizations gain a comprehensive understanding of your IT infrastructure and the relationships between various components. It enables automatic discovery and mapping of services, applications, and infrastructure components, providing a visual representation of the dependencies and relationships.

In Vulnerability Response, the scheduled job *Set related CI services* establishes connections between the affected business services and the configuration items (CIs) associated with the vulnerable items (VITs). The linking process takes place once the integration import is finished and at a designated time. To enhance the performance of this scheduled job, several changes have been implemented beginning with v21.1.2 of Vulnerability Response. They are:

- Risk score calculation: The process of calculating risk scores involves the utilization of the *Set related CI services* scheduled job. Once the CI is processed, this job stores the necessary data in the Related Services [sn_vul_m2m_ci_services] table. Previously, in Configuration Compliance, risk calculation involved directly accessing the Configuration Management Database (CMDB) Application Programming Interface (API) *CIUtils* to retrieve services for each test result during import. However, the current process relies on the output of the scheduled job from the Related Services [sn_vul_m2m_ci_services] table to calculate the risk score in Configuration Compliance. Additionally, the base system calculator has been modified to utilize the Related Services [sn_vul_m2m_ci_services] table.
- Size of services: The service value in the system property *sn_sec_cmn.services_affected_by_CI_max_size*, which is related to the *Set related CI services* scheduled job is decreased from 1000 to 500.
- Depth of services: The depth in the system property *sn_sec_cmn.services_affected_by_CI_max_depth*, which is related to the *Set related CI services* scheduled job is reduced from 10 to 5. The service value is also decreased from 1000 to 500.
- Exclusion of CMDB classes: A system property *sn_sec_cmn.ignoreCIClassForService* has been introduced to enable configuration of CMDB classes for which service calculation should be skipped. In the base system, this property is set for *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ip*, *sn_sec_cmn_unmatched_ci* as these classes are created by Vulnerability Response and may not have any service mapping. Previously, service calculation was based on the VIT. However, the logic has been modified to use the discovered item instead. The discovered item is used to calculate the service, which is then associated with the CI in the same table.
- Scheduled job for full refresh of services: An on-demand scheduled job *Full refresh-related CI services for VI*, has been introduced to perform a complete refresh of services. When you upgrade to v21.0 of Vulnerability Response, the *Set related CI services* job runs for a longer duration at first as the base table uses discovered items instead of vulnerable items. As a result, the job must process all the discovered items that have been scanned within the last 90 days. Additionally, if you require more frequent service refreshes, it can be accommodated by scheduling weekly periodic refreshes or performing a full refresh. If you have performed activities, which resulted in changes to the services associated with your CIs, and you want Vulnerability Response to reflect these changes, you

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

can run the on-demand scheduled job *Full refresh related CI services for VI*. This job takes all the discovered items recorded in the last 90 days and refreshes the associated services accordingly.

Related topics

Service Mapping

CIUtils - Global

Vulnerability Response implementation

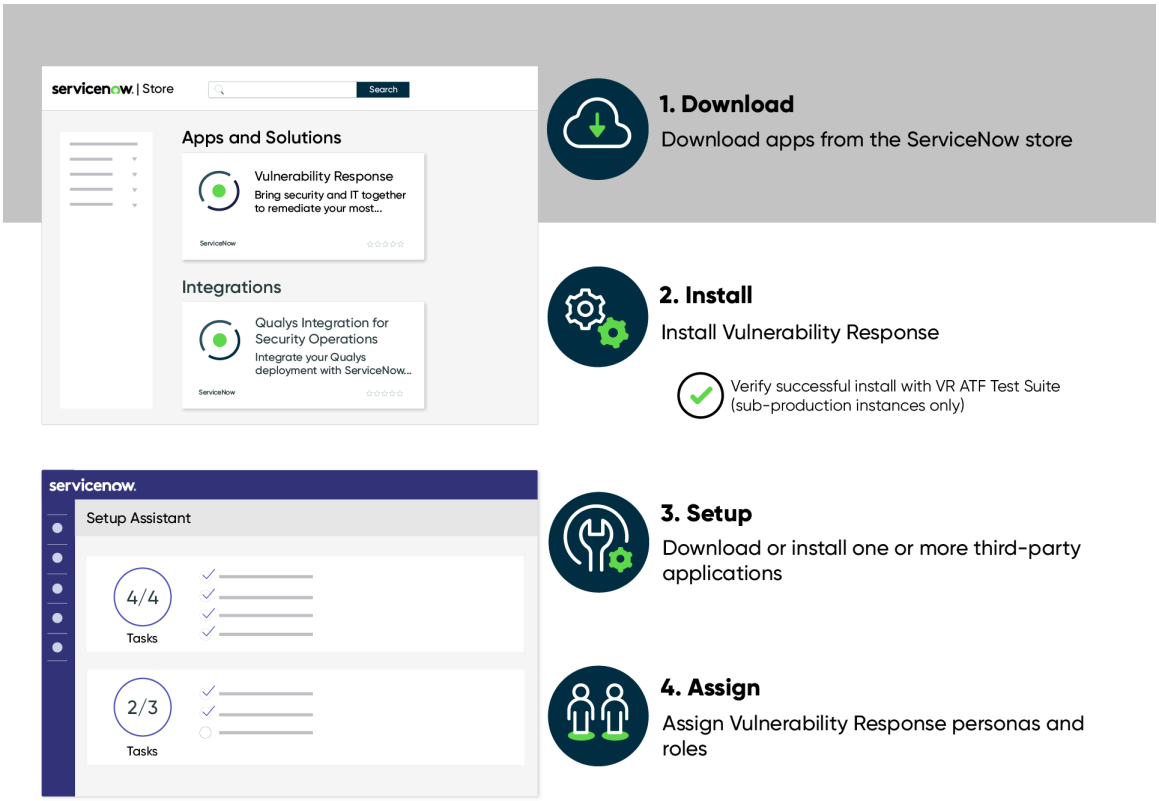
Use the steps illustrated in the following images to download the Vulnerability Response application from the ServiceNow Store, install it on your ServiceNow AI Platform® instance, and configure it using the Setup Assistant.

An installation and configuration example for installing the base system, the Vulnerability Response application and a third-party scanner application, the Qualys application, is illustrated in the following images. Required roles and mandatory tasks, as well as optional steps, are also listed.

- For more information about each step illustrated in the following images and a checklist with links to supporting documentation, see Implementation checklist for the Vulnerability Response application.
- You can extend the concepts and sequence of steps presented in this example to installing and configuring other supported applications for Vulnerability Response. For a list of support applications, see Installation of Vulnerability Response and supported applications.
- The admin role is required to download and install the Vulnerability Response application and the Qualys Vulnerability application used for this example.
- The admin role also assigns the Vulnerability admin [sn_vul.vulnerability_admin] persona and other Vulnerability Response persona roles to users and groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Admin tasks

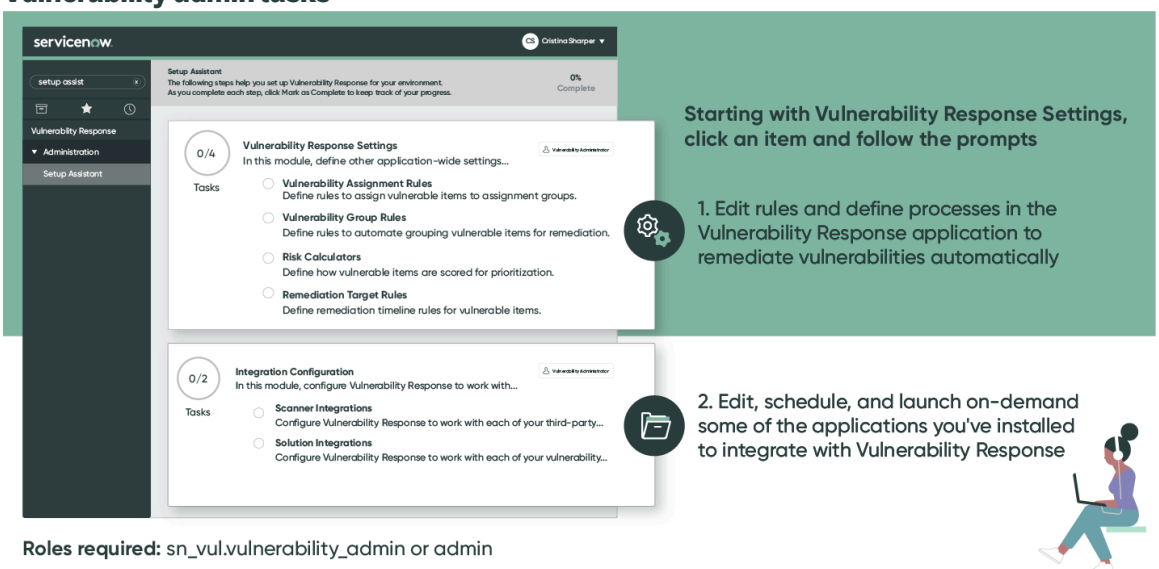


The sn_vul.vulnerability_admin role configures the Vulnerability Response and Qualys applications in Setup Assistant and verifies expected results.

Follow the steps and prompts in Setup Assistant starting with the Vulnerability Response Settings section to continue with the installation and configuration. Reviewing these settings helps you understand and verify the processes of Vulnerability Response as you continue to set up your environment.

Role required: sn_vul.vulnerability_admin or, alternatively, admin.

Vulnerability admin tasks



Roles required: sn_vul.vulnerability_admin or admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Review the descriptions, default settings, and demo data that you installed with the applications in the following sections:

- Vulnerability Assignment Rules - automatically assign vulnerable items (VIs) to the appropriate assignment group.
- Remediation Task Rules - automatically group vulnerable items (VIs) as they are imported based on certain conditions.
- Risk Calculators - Default Risk Calculator is enabled.
- Remediation Target Rules - Define remediation time lines for VIs and remediation tasks (RTs).
- Review and edit the settings for the third-party applications and installed solutions you installed and define conditions for your data imports. Enter your third-party account information and configure import settings, and schedules, configuration item (CI) lookup rules, as well as other settings.

See Implementation checklist for the Vulnerability Response application for more information.

For additional information while customizing or implementing the Vulnerability Response application, see KB1000704.

Migrate to Unified Security Exposure Management (USEM) from Vulnerability Response

Use the Migration assistant for Unified Security Exposure Management tool to migrate to the Unified Security Exposure Management (USEM) platform for a smooth and secure transition.

Before you begin

Role required: Admin

Ensure that you:

- Run the migration in a sub-production instance before attempting to use it in production.
- Install the Unified Security Exposure Management application from the store.
- Upgrade to USEM using the Migration assistant for Unified Security Exposure Management tool if you are migrating from a version below 30.0.

About this task

The Migration assistant for Unified Security Exposure Management tool provides a guided user interface and helps with preparation, conflict resolution, post-migration verification, and more. It verifies that all records and integrations are correctly updated.

The Migration assistant for Unified Security Exposure Management tool is included with the Unified Security Exposure Management application. Install the Unified Security Exposure Management application [sn_vul_usem_common] before you install v30.x of any of the other Vulnerability Response applications.

The Unified Security Exposure Management application [sn_vul_usem_common] is available in the ServiceNow® Store.

See the Migration Guidance to Unified Security Exposure Management Knowledge Base article for more details about the migration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. **Accessing the**Migration assistant for Unified Security Exposure Management tool: Navigate to **All** > **Vulnerability Response** > **Administration** > **Migration assistant for Unified Security Exposure Management**.
2. **Preparation**: Review the customizations that may have to be resolved after upgrading to USEM.
3. **Migration**:
   a. Review the ordered list of applications to upgrade in the Migration assistant for Unified Security Exposure Management.
   b. Upgrade applications in the order displayed (core applications first, then integrated applications).

      Note: Follow the upgrade order strictly to avoid dependency issues.

   c. Confirm all applications display the status `Completed`.
   d. Verify all post-upgrade scheduled jobs are completed (status shows `upgrading job, running` until jobs are finished).

      Note: You can't proceed until all upgrades are complete.

4. **Optional: Resolve conflicts**: Address any upgrade conflicts found.
5. **Complete migration**:

   The post-migration step restores the turned off items and validates the results.

   a. Navigate to the post-migration page of the Migration assistant for Unified Security Exposure Management.
   b. Select **Enable all** to restore integrations and jobs.
   c. Review the summary showing the number of integrations restored, scheduled jobs re-enabled, and migration rules successfully migrated.
6. **Verify completion**:
   a. Run sample Vulnerability Response jobs or check integration connectivity to verify instance functionality.
   b. Review any unresolved upgrade conflicts.
   c. Review the list of re-enabled integrations and jobs
   d. Review the number of successfully migrated VR migration rules
   e. Review any unresolved upgrade conflicts (if applicable)

   Your instance is ready to operate with USEM. You're redirected to the lookup rule page.

Result

The migration to Unified Security Exposure Management is complete. All integrations and jobs are re-activated, migration rules are successfully migrated, and the instance is ready for use.

Install Vulnerability Response

Before you run the Vulnerability Response application in your ServiceNow AI Platform instance, you must get entitlement and download the application from the ServiceNow Store, install it on your ServiceNow AI Platform instance, and complete a few installation steps in Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

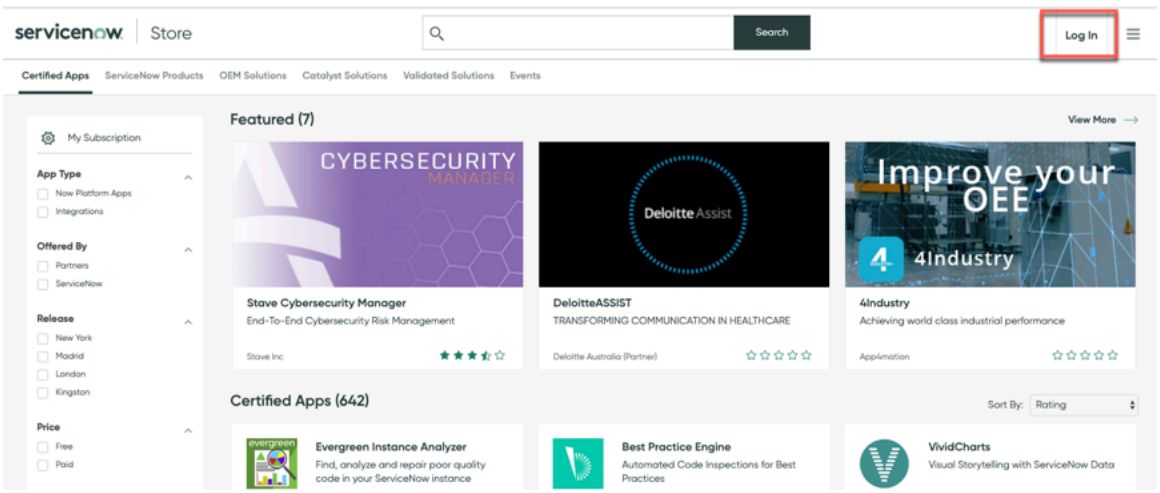
Setup tasks	Description
Verify that you have the required ServiceNow roles assigned for your instance.	The admin role is required for installation. If not already assigned, the System Administrator [admin] also assigns the Vulnerability Admin, sn_vul.vulnerability_admin or sn_vul.admin (deprecated)] role.

Role required: admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

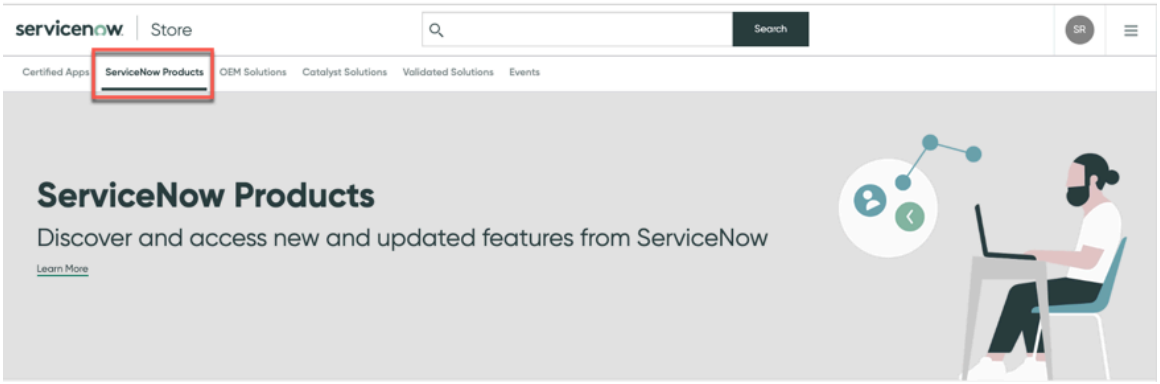
Procedure

1. To get entitlement and download the Vulnerability Response core application, navigate to the ServiceNow Store.
2. In the upper right of the page, click **Log In**.

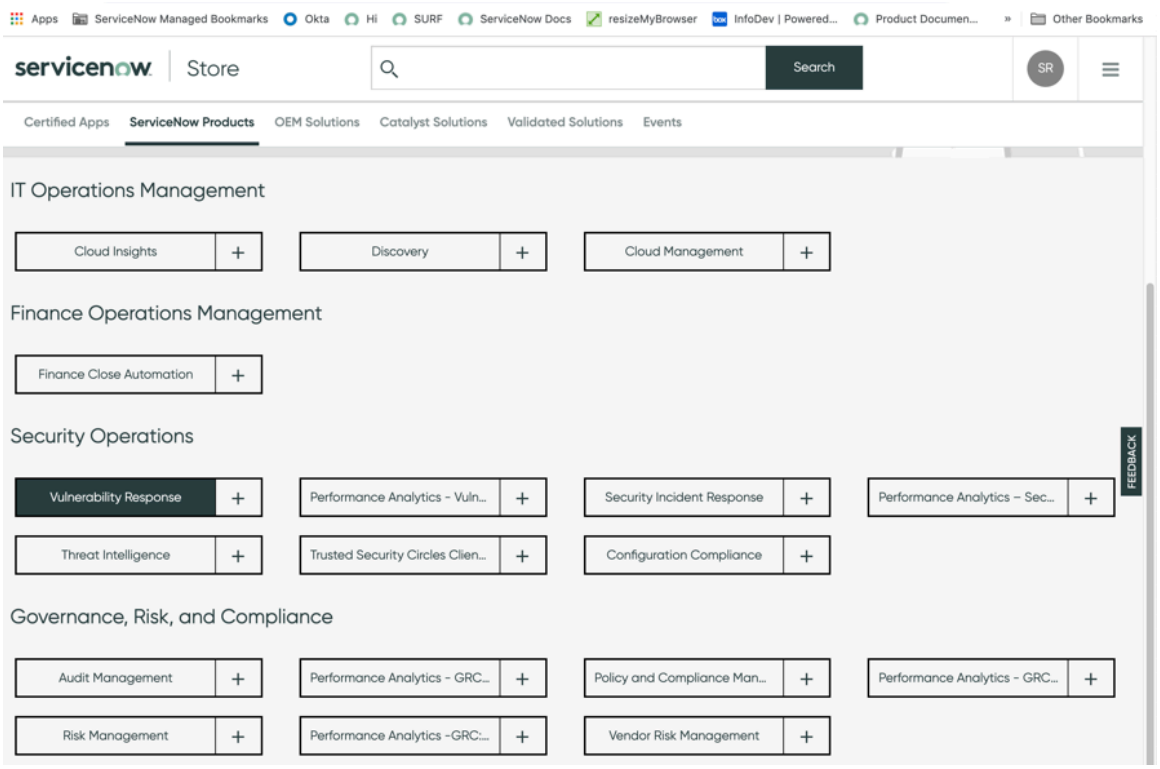


3. In the dialog that is displayed, enter your HI credentials and click **Login**.
4. On the page that is displayed, if not selected, click the **ServiceNow Products** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

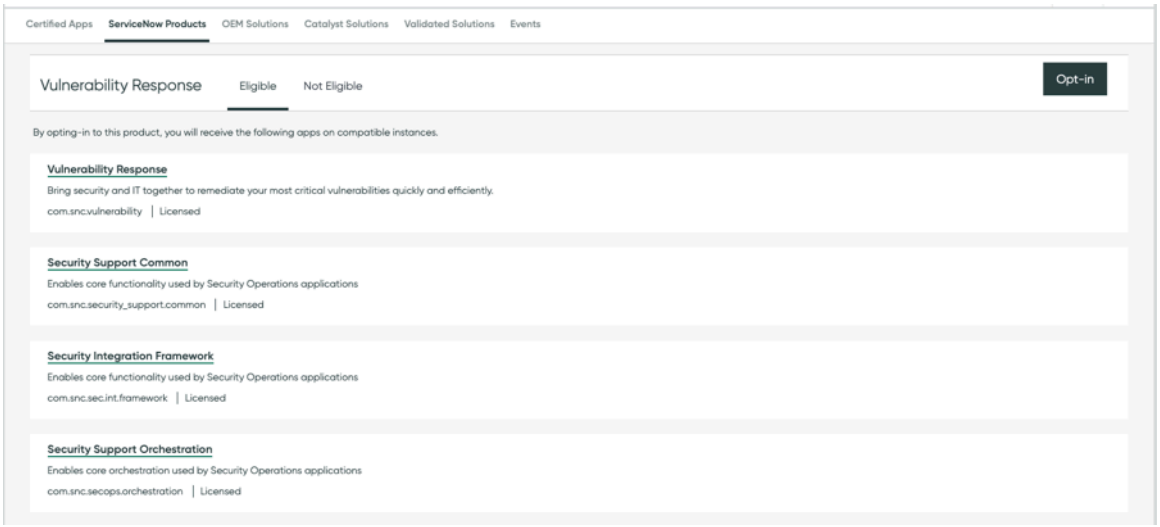


5. To view the associated applications that you are eligible for with the Vulnerability Response application, on the product list page, click the **Vulnerability Response** product.

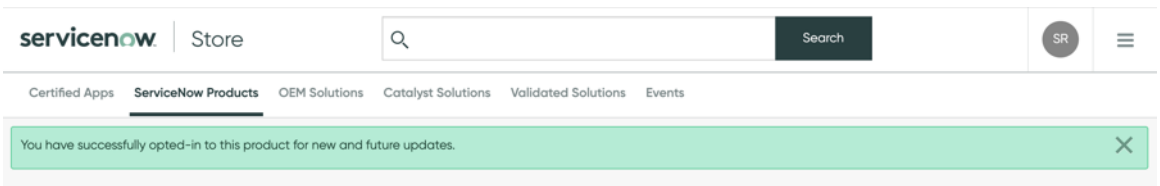


The Eligible tab lists all the applications you are eligible for if you opt-in. For more information on an application, click a link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. To get the Vulnerability Response core application, click **Opt-in**.
7. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**. A message is displayed that indicates you have successfully opted-in for the application.



With the ServiceNow Products tab selected and displayed, a green check mark replaces the plus sign to the right of the Vulnerability Response application, as shown in the following figure.



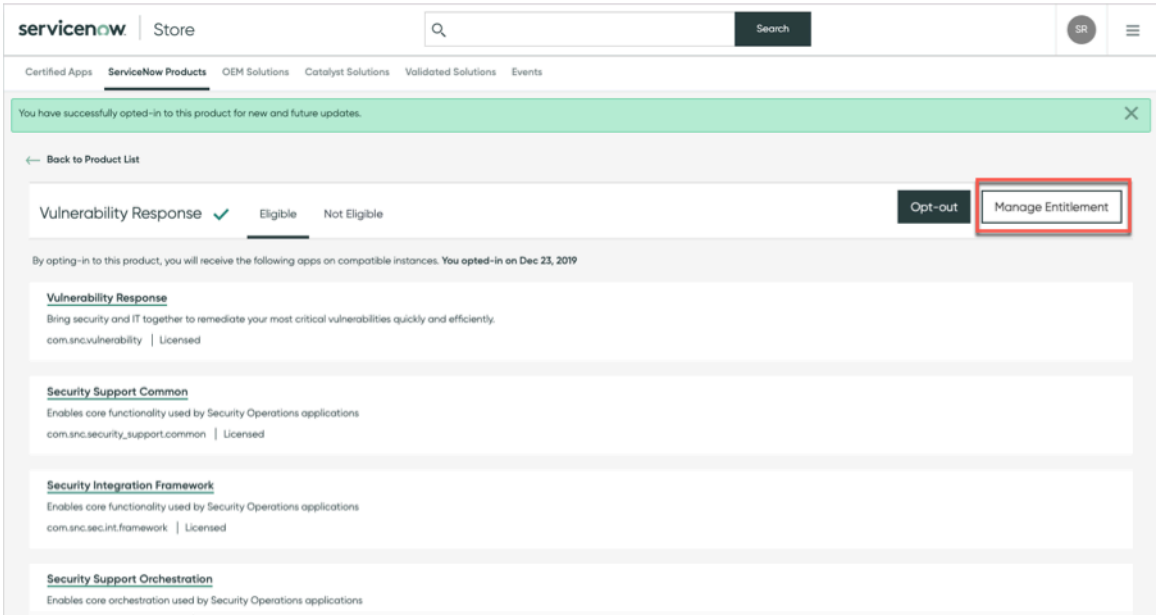
After you have accepted the terms and conditions and managed entitlements for any of the applications on the **ServiceNow Products** tab, on the Products List page, you can click the plus sign (+) to get entitlement and opt-in for the other applications on this page with a single click.

8. Skip to step 10 to install the application on your ServiceNow AI Platform instance.
9. **Optional:** Alternatively, to manage your entitlement for the Vulnerability Response application on other ServiceNow AI Platform instances, follow these steps.

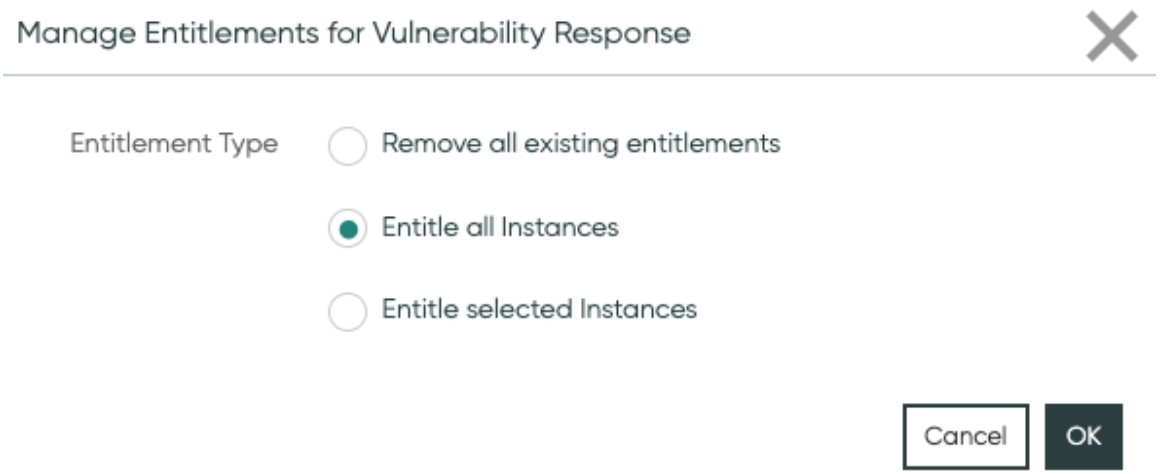
   a. If the Manage Entitlement button is not displayed, click the Vulnerability Response application on the Product List to display it.

   b. With the Eligible tab selected, click **Manage Entitlement**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. In the Manage Entitlements for Vulnerability Response dialog that is displayed, choose one:

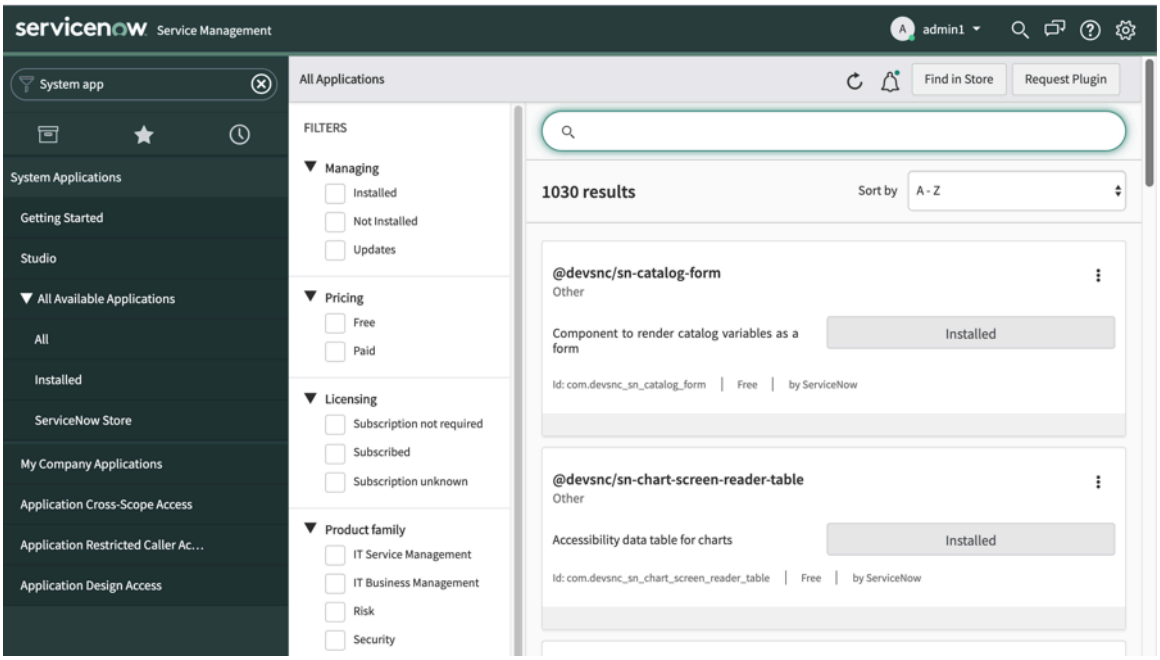


d. Click **OK** or **Cancel** to continue.
You are ready to activate plugins and install the application on your ServiceNow AI Platform instance(s).

10. Log in to the ServiceNow AI Platform instance that you want to install the Vulnerability Response application on.

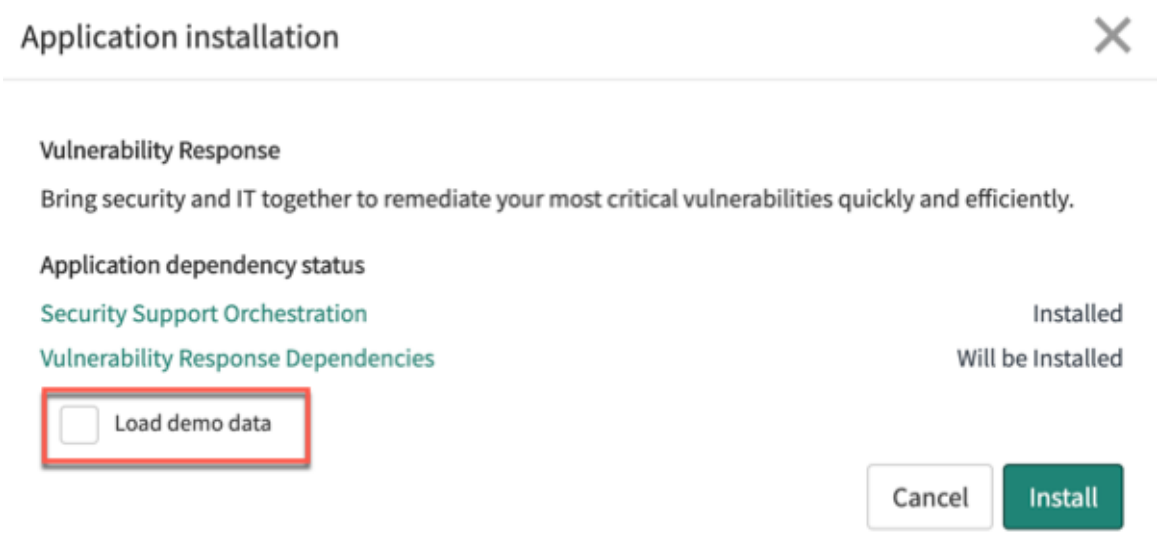
11. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



12. From the applications listed, locate the Vulnerability Response application (sn_vul), select a version from the choice list, and click **Install**.
    The Application installation dialog is displayed. Any dependencies that will be installed are displayed.
13. **Optional:** If you want demo data, select the Load demo data check box and click **Install**.

> **Note:** If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Workaround to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.

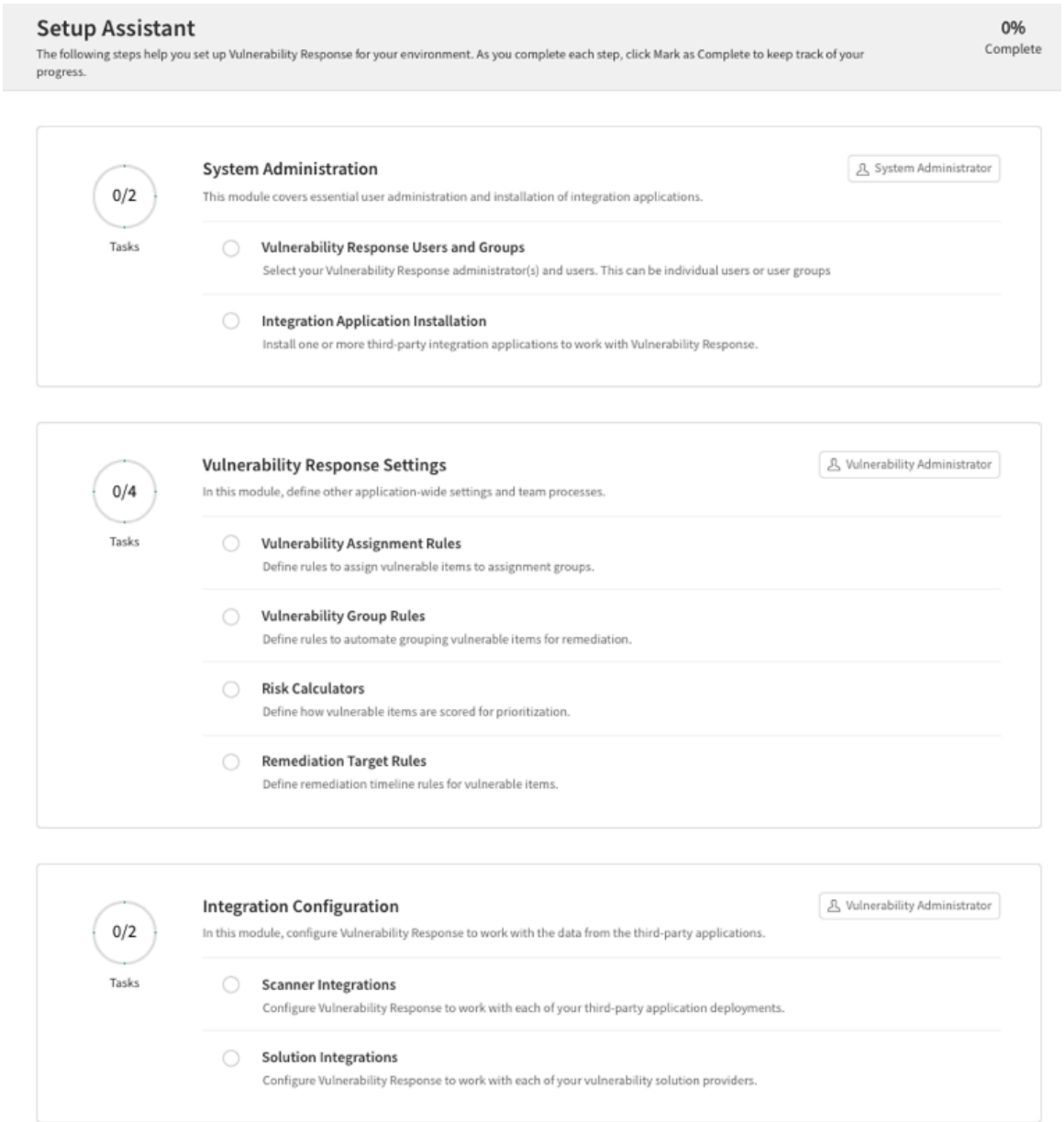


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This installation may take some time. A message is displayed in the Install dialog after the application is successfully installed.



14. Click **Close**.
15. After installation is successfully completed, navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant**.



16. Follow the instructions on the forms in each section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

For more information on Vulnerability Response settings, installing applications, configuration, integrations, group rules, risk calculators, and remediation target rules, see Configuring Vulnerability Response using the Setup Assistant.

Components installed with Vulnerability Response

Several types of components are installed with activation of the Vulnerability Response application, including tables, user roles, and scheduled jobs.

View filtered lists for components installed with an application

Starting with v24.0.6 of Vulnerability Response, the most frequently used system properties are now accessible within the Vulnerability Response application. To view these system properties, navigate to **All**Vulnerability Response**Properties**.

Filter the Applications Files table so that only the roles, scheduled jobs, and tables that are installed with an application are displayed. The application you want to view these components for should be installed so that its files are loaded onto the instance and into the metadata table. Follow these steps to view filtered lists from the Applications Files table.

1. In the filter navigator, enter **sys_metadata.list** to navigate to the metadata table.
2. Select the condition builder (filter icon), and select, **Application** > **is** followed by the name of your application. For example, **Application** > **is** > **Vulnerability Response**.
3. In the condition builder, to add a second filter, select **AND**, then select, **Class** > **is a** and choose one of the following classes from the list: **Role**, **Scheduled job**, or **Table**.
4. Select **Run**.

The results for the class you selected are displayed in a filtered list.

Roles installed

Note: Roles, Scheduled jobs, and Tables for Application Vulnerability Response can be found in Components installed with Application Vulnerability Response.

Role title [name]	Description	Contains roles
sn_vul_prisma.configure_prisma_integration	Secures the CRUD + report_view operations on sn_vul_prisma_hosts_import table and report_view operation on sn_vul_prisma_host_attrb table.	
sn_vul.view_manager_workspace	Views Vulnerability Manager Workspace.	
sn_vul.delete	Deletes source records and vulnerable items. Prior to v23.0, the admin role had the privilege to delete the source records.	• sn_vul_cmn.delete • sn_vul.delete_vulnerable_
sn_vul_cmn.delete	Deletes source records.	
V23.0: sn_vulc.bulk_edit	Performs bulk edit operation on test results.	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
sn_vul.app_bulk_edit	Performs bulk edit operation on application vulnerable items (AVITs).	sn_vul.app_write_all
sn_vul_container.container_bulk_edit	Performs bulk edit operation on container vulnerable items (CVITs).	sn_vul_container.write_all
sn_vul_cisa.configure_intelligence_integration	Configures Intelligence integrations.	
Vulnerability managers and senior analysts [sn_vul.vulnerability_admin or sn_vul.admin (deprecated)]	Update properties and vulnerability integrations. The sn_vul.vulnerability_admin or sn_vul.admin (deprecated) role is required for Vulnerability Response administration including vulnerability integrations, remediation task rules, calculators, and remediation target rules and tasks, reports, and third-party integration configuration.	• sn_vul.vulnerability_write • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (wh Qualys Vulnerability Integ installed.) • sn_vul_r7.admin (when th Vulnerability Integration is • sn_vul_shodan.admin (wh Shodan Exploit Integratio installed.) • sn_vul.configure_nvd_int (when the NVD integratio installed.) • treemap_admin (when the Performance Analytics ap installed.)
Patch orchestration	Configures supported third-party patch vendor integrations. View and apply patch data and patch records.	• sn_vul_patch_orch.config Configure and apply patc • sn_vul_patch_orch.read_ Can view patch records a • sn_vul_bigfix.configure_in Configures the BigFix Pat Orchestration Integration application. This role con sn_vul_bigfix.read_integr connection_admin granu that permit the user to co BigFix console. • sn_vul_sccm.configure_in This role contains the sn_vul_sccm.read_integra connection_admin granu that permit the user to co SCCM console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
		• sn_vul_bigfix.read_integr Users with this role can vi only) the#ecords of the V Response and the BigFix Orchestration Integration and patch orchestration c • sn_vul_sccm.read_integra Users with this role can vi only) the#ecords of the V Response and the Micros Patch Orchestration Integ application and patch orc data.
Vulnerability analysts [sn_vul.vulnerability_write]	The sn_vul.vulnerability_write role is required for managing remediation tasks and vulnerable items, and monitoring remediation progress.	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (when Vulnerability Integration is • sn_vul_shodan.write (whe Shodan Exploit Integratio installed.)
V19.0: Vulnerability Event Manager [sn_vul_analyst.vul_event_manager]	The sn_vul_analyst.vul_event_manager role is used to assess the impact of a new vulnerability or software, or add a zero-day vulnerability to identify the impacted assets and create vulnerable items (VIs).	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emergenc • sn_vul.manage_exposure
Others [sn_vul.read_all] The sn_vul.vulnerability_read role is deprecated.	The sn_vul.read_all role is required for anyone needing visibility into vulnerability management. For example, IT and security executives or someone who wants to drill down from high-level dashboards to the items that comprise the dashboard visuals. **Important:** Starting with v24.0.6 of Vulnerability Response, the sn_vul.read_all role has the privilege to access the Vulnerability Manager Workspace.	• sn_sec_cmn.read • sn_vul_qualys.read (when Vulnerability Integration is • sn_vul_shodan.read (whe Shodan Exploit Integratio installed.) • pa_viewer (when the Perf Analytics application is in • sn_vul_tenable.read_inte (when the Tenable Vulner Integration is installed.) • sn_vul.view_manager_wo
sn_vul.read_assigned	View vulnerable items assigned to you or your assignment groups	sn_vul.view_rem_workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	in both the Classic UI and IT Remediation Workspace. **Important:** Starting with v24.0.6 of Vulnerability Response, the sn_vul.read_assigned role has the privilege to access the IT Remediation Workspace.	
VR System import administrator [sn_vul.vr_import_admin]	System run-as user. Runs scheduled jobs. **Note:** This user is the default run-as user for each integration record. Don't change.	• import_admin • sn_vul.vulnerability_write
Remediation owner [sn_vul.remediation_owner]	View and update permission for vulnerable items, remediation tasks assigned to you or your group. Can view all vulnerabilities and solutions. Has write access to the**Internal notes field** on the solution record.	Contained in the itil role.
CISOs and vulnerability executives [sn_vul.vulnerability_ciso]	View the CISO dashboard in Performance Analytics for Vulnerability Response.	• sn_vul.ciso_read • sn_vul.read_all
False positive approver [sn_vul.false_positive_approver]	Approves/rejects false positive requests.	sn_vul.view_manager_works
Exception approver [sn_vul.exception_approver]	Approves/rejects exception requests.	sn_vul.view_manager_works

Scheduled jobs installed

Scheduled job	Description
Populate OOTB saved filters for Host and App module	Migrates modules related to Host and App module.
Populate OOTB saved filters for CC module	Migrates modules related to CC module.
Populate OOTB saved filters	Migrates modules related to container module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
for Container module	
Refresh Host related Saved filters	Refreshes all the aggregation data related to saved filters of Host module.
Refresh CC related Saved filters	Refreshes all the aggregation data related to saved filters of CC module.
Refresh Container related Saved filters	Refreshes all the aggregation data related to saved filters of Container module.
Refresh App related Saved filters	Refreshes all the aggregation data related to saved filters of App module.
Trigger aggregation creation and running for saved filter	Creates, updates, runs, and refreshes the aggregations related to the saved filter.
Version 19.0 of Vulnerability Response and v4.0 of the Veracode Vulnerability Integration	The Veracode CWE Integration retrieves Veracode - specific Common Weakness Enumeration (CWE) data for threat information and remediation recommendations. The Veracode SBOM Integration ingests release, version, and vulnerability information that originates in Veracode about the components in your software projects. The integration generates SBOMs in CycloneDx JSON format and uploads them into your instance Veracode Categories Integration retrieves enhanced Categories data from Veracode. The Veracode DevOps Integration lets DevOps users view summary details for third-party vulnerability scans without a SecOps license. JSON-based APIs for the following Veracode integrations: Application Vulnerable Item, Scan Summary, Application List. The XML-based API versions of these integrations are deprecated.
Associate existing VIs with Auto Exception Rule	Automatically associates the Auto Exception Rule with existing VIs.
Auto-Close Vulnerable Detections	Automatically closes the stale vulnerable detections based on the configuration defined in the table 'sn_vul_auto_close_config'.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Version 16.1: HCL BigFix Collection, Fixlet, and Actions Integrations.	Manage patches and patch deployments for vulnerabilities with patches from the HCL BigFix product.
Calculate Related Counts for All Solutions	Inactive by default. Processes solutions data once nightly instead of continuously. Starting with v22.0, you can run this job only on demand. As this scheduled job processes all the solutions, it can impact performance. Therefore, it is recommended to run this job only once if the solution data is corrupted.
Calculate Related VI Counts for Vulnerability and Remediation Task	Captures manual and VI import changes for the day. Reconciles vulnerability and solution relationships and recalculates totals. Solutions data is queued and processed separately by the **Process Vulnerability Solution Metrics Queue** scheduled job.
Check Mid-Server Timeout	Pings the Mid-Server and errors out after 30 seconds.
V19.0: Check potential vulnerability exposure	Processes the delta CVEs, software, and installations to get the exposure.
Check Run State WaitComplete	Marks an integration run as complete once they're verified as fully done.
Check Vulnerable Item and Groups Deferment Expiration	Sends notifications if vulnerable items or vulnerabilities have expired (and if they expire in one week). Checks if any exception rule is applicable on a deferred VI and updates the **Reason** and **Until** fields according to the exception rule. The state of the VI remains Deferred until the latest expiry date.
Close cancel VITs that do not have a CI associated	Automatically closes vulnerable items that don't have an associated configuration item (CI) and haven't been updated for three days. State is set to Closed/Cancelled.
Close VI on exp record delete	Closes a VI when it's deleted.
Compliance Results Integration	Imports test results along with policies, configuration tests (controls) and citations with authoritative sources for processing in the Configuration Compliance application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Compliance Results Backfill Integration	Part of a chained integration run with the Tenable.io Assets Integration, imports configuration assessment data for ignored assets that are discovered (imported through assets integration).
CR State Synchronization	Script retrofits all existing remediation task to CHG relationships so they are synchronized. Enables synchronization going forward.
Version 15.0 Scan Credential Integration	Imports and securely stores temporarily Tenable.io credentials used to access the scanner for on-demand rescans.
CWE Comprehensive 2000 Integration	Vulnerability integration that pulls in vulnerability information from the Common Weakness Enumeration (CWE) dataset, curated by the MITRE Corporation.
V18.0: Delete Stale Split Action Records	Daily job to clean up stale records in split task intermediate tables.
Disable VR solutions when solutions application not active	Disables and hides the Vulnerability Solution Management feature when the Solution Management for Vulnerability Response application isn't installed.
Evaluate remediation targets	Sets or updates remediation target dates on all vulnerable items. Determines the status of remediation target dates against rules.
• Fixing the detections for updated key for Rapid7 • Fixing the detections for updated key for Qualys • Fixing the detections for updated key for Tenable	Cleans up detection data automatically by an integration-specific scheduled job that is triggered post-upgrade to Vulnerability Response.
Version 16.1: Generate remediation digest	This job automatically generates an email digest for any users in the Remediation Owner user group. The job is activated by default.
V19.0: Insert CISA exploited CVE to exposure config	Inserts CISA CVEs into the Exposure Configuration table to calculate the exposure.
V18.0: Insert Classic Remediation Tasks Into	One-time scheduled job to insert all the remediation tasks created in the classic UI into the Unified remediation task (sn_vul_remediation_task).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Unified Remediation Task	
Microsoft Security Response Center Solution integration	Vulnerability Solution Management integration that retrieves solutions from the Microsoft Security Response Center.
Version 16.1: Microsoft SCCM Collection, Patch Update, and Deployments Integrations	Manage patches and patch deployments for vulnerabilities with Microsoft SCCM patches.
Pick up throttled integration process	Creates the integration process for the Shodan Exploit Integration.
Populate affected products text	After upgrade, handles existing solutions to populate affected products text. This job runs only once.
Populate new CR Count Column	Automatically populates the new CR count column for customers with existing data in the remediation task [sn_vul_vulnerability] table.
Process Vulnerability Solution Metrics Queue	Processes the queued solutions data by: • Rolling up solutions from NVD entries to third-party entries • Populating preferred solutions on vulnerabilities, and • Updating the remediation status metrics on the solutions In addition, it also processes the solutions that are marked for update statuses. **Note:** If you're using only Rapid7, you can disable this schedule job to improve performance.
Populate records in vulnerability vendor mapping table Populate records in vulnerability vendor mapping table for Rapid7 vulnerabilities	Inserts records into vulnerability vendor mapping table for existing vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Re-open deferred vulnerability groups	Reopens deferred remediation tasks when the deferment date has passed.
Reapply all vulnerability assignment rules	Reevaluates assignment rules against all **Open** VIs.
Version 16.5: Reassignment count for assignment rules	Runs daily and posts the total number of VIs and remediation tasks that are unassigned by this feature for a particular assignment rule.
Red Hat Solution Integration	Vulnerability Solution Management integration that retrieves solutions from the Red Hat Security Advisory.
V17.1: Refresh and resolve duplicate VITs on remediation task	Finds duplicate vulnerable items for the items in the remediation task with the 'Automatically refresh duplicate VIs' as active.
Refresh associated vulnerable items for non-remediation task rule-based remediation task	Updates the remediation task with vulnerable items matching the Filter Group and Condition groups criteria.
Repair erroneous Vulnerable Items Last Opened and Closed	Repairs existing UI data corrupted by defects previously fixed.
Rerun calculators	Reapplies the calculators to any vulnerable items affected by the change. This triggers a recalculation of the cumulative risk scores of their remediation tasks. **Note:** Rerunning calculators can take a long time depending on your environment.
Retry Cancelled Integration Import Sets	Retries canceled integration import sets. Retries 5 times before returning an error.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Retry Integration Processes	Retries integration processes. Retries 5 times before returning an error.
Rollup vulnerable item values to vulnerability and group	Computes the risk score, number of vulnerable items, and remediation target status for remediation tasks, using the rollup calculator. **Note:** Starting with v23.0 of Vulnerability Response, the scheduled job is enhanced to create background jobs with multithreading capabilities. This upgrade involves segmenting the job into several smaller child jobs, which are executed either in parallel or concurrently. This modification enables processing of multiple records simultaneously, thus significantly speeding up the overall task.
Run severity calculator after vuln entry promotion	Runs the severity calculator after a previously missing vulnerability has been updated with its score and other data from a third-party provider, such as Qualys Cloud Platform, Rapid7 Nexpose. **Note:** Starting with v25.0.3 of Vulnerability Response, the scheduled job is enhanced to create background jobs with multithreading capabilities. This upgrade involves segmenting the job into several smaller child jobs, which are executed either in parallel or concurrently. This modification enables processing of multiple records simultaneously, thus significantly speeding up the overall task.
V19.0: Run exposure assessment for configured CVEs	Calculates exposure for all the CVE records in the Exposure Configuration table.
V19.0: Run software exposure	Calculates exposure for all the software records in the Exposure Configuration table.
Scheduled Vulnerability Data Source Processor	Checks the import queue for entries to process and assigns a scheduled import job based on available resources.
Scheduled Vulnerability integration process attachment cleanup	Removes integration XML attachments once they're 14 days old. This retention time isn't configurable.
Scheduled Vulnerability Integration timeout checker	Cancels integration runs that take over 60 minutes to complete.
Set related CI services for VI	Once the integration import is complete, it links the affected business services to CIs connected to vulnerable items, at the specified time. For more information, see Service Mapping in Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Set deferral counts	Collects the number of times a vulnerable item, application vulnerable item, a container vulnerable item, or a remediation task is deferred.
Trigger next integration	Triggers the next integration in a chained integration run.
Template Integration	A single template record is sent to Tenable.io during rescan.
Update Ungrouped Vulnerable Items	Determines whether a vulnerable item is in a remediation task and adds or removes it from the **Ungrouped Vulnerable Items** list. **Note:** This job runs post-upgrade and, depending on your data set, can take a long time to complete.
Update Vulnerability on VG	Updates the **Vulnerability** field on the Remediation Task (sn_vul_vulnerabilty) table after upgrade. This job is triggered once and inactive afterward.
Vulnerability Import Template	Engine that processes the import queue. One of 10.
Vulnerability Response Age Closed Update	Updates Age closed column on VI table.
Vulnerability Response CI count	Calculates the number of CIs scanned by third-party scanners in the last 30 days.
Vulnerability Response Risk and Remediation Status Upgrade	Updates the risk rating on data when you upgrade.
v20.0: Check Risk Mitigation Expiration	Checks if compensatory controls have expired for a Vulnerable Item and a Remediation Task. If they expired, it reverts the risk score to original risk score and sends an email notification indicating that compensatory controls have expired. Also sends an email notification if compensatory controls are set to expire within 7 days.

Tables installed

Table	Description
v24.0.6 Prisma Hosts Import [sn_vul_prisma_hosts_import]	Import set table for the hosts.
v24.0.6 Prisma Host Attributes [sn_vul_prisma_host_attrb]	Asset attribute table for hosts integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
v22.0 sn_vul_cmn_auto_close_rule	Closes stale detections automatically based on filter conditions.
sn_vul_cmn_ws_saved_filter	Stores the data of saved filter.
sn_vul_licensing_usage	Contains the duplicate asset, Incomplete IP Asset, Total scanner assets counts and Final usage.
sn_vul_m2m_entry_compensating_control	Represents association between vulnerability entries and compensating controls.
v21.0 Rapid7 Scan Engine [sn_vul_r7_scan_engine)	Store the records imported Scan Engine data responsible for discovering assets during a scan and checking them for vulnerabilities.
v21.0 Rapid7 Scan Engine Import [sn_vul_r7_scan_engine_import]	Used by the Rapid7 Scan Engine integration to stage import data prior to processing.
Version 19.0: [sn_vul_veracode_cwe_import]	Extends the Veracode Category table for CWE remediation recommendations.
Version 19.0: [sn_vul_veracode_category_import]	Stores imported category data.
Version 19.0: [sn_vul_veracode_sbom_import]	Stores imported SBOM data originating from Veracode.
V17.1: Add Proof to the VI Key [sn_vul_proof_key_vulnerability]	Rapid7 vulnerabilities for which proof must be included in the VI key. Starting with v24.0.6 of Vulnerability Response, a column 'Regular Expression to Split Tenable VITs' is added. It stores the regular expression entered by a user that is used to parse the proof from the payload.
Assessed Vulnerable Items [sn_vul_m2m_exp_sw_vi]	Assigns a remediation task to an assignment group during remediation task creation.
Assignment Rule [sn_vul_vgr_assignment_rule]	Assigns a remediation task to an assignment group during remediation task creation. Prior to v15.0: Assigns a remediation task to an assignment group during remediation task creation.
Associate Change Request [sn_vul_action_associate_cr]	Staging table used to process new remediation task-CHG associations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
	Prior to v15.0: Staging table used to process new VG-CHG associations.
Asynchronous Vulnerable Item Job [sn_vul_async_vi_job]	Contains background jobs that process vulnerable items. Only one job type is supported; used to edit vulnerabilities in bulk.
Asynchronous Vulnerable Item Job Type [sn_vul_async_vi_job_type]	Contains the types of background jobs, and references the relevant script. Only has one processor, the **VulnerabilityBulkEditProcessor**
Auto-Close Stale Detections [sn_vul_auto_close_config]	Stores the configuration for how stale detections are automatically closed.
Configure Vulnerable Item Granularity [sn_vul_action_vi_granularity_config]	Stores the UI form used to enable or disable Include Port from the configuration page in the Configure VI Granularity module.
Create change request [sn_vul_action_create_cr]	Used to create change requests from remediation task.
Create Vulnerable Items [sn_vul_action_create_vi]	A staging table which is used as a place holder for information. This table does not store any records.
Collection [sn_vul_patch_orch_collection]	Stores collection data from distinct instances.
CWE [sn_vul_cwe]	Catalog of Common Weakness and Enumeration (CWE) software vulnerabilities.
CWE Applicable Platform [sn_vul_cwe_m2m_cwe_platform]	Contains the imported CWE applicable platform data.
CWE Category [sn_vul_cwe_category]	Contains the imported CWE category data.
CWE Common Consequence [sn_vul_cwe_consquence]	Contains the imported CWE common consequence data.
CWE External Reference [sn_vul_cwe_reference]	Contains the imported CWE external reference data.
CWE Observed Example	Contains the imported CWE CVE data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
[sn_vul_m2m_cwe_cve]	
CWE Platform [sn_vul_cwe_platform]	Contains the imported CWE platform data.
CWE External Reference [sn_vul_cwe_reference]	Contains the imported CWE related external reference data.
CWE Relationship [sn_vul_m2m_cwe_relation]	Contains the imported CWE relationship data.
CWE View [sn_vul_cwe_view]	Contains the imported CWE view data.
CWE Weakness [sn_vul_cwe_weakness]	Contains the imported CWE weakness data.
Version 16.1: Device Collection [sn_vul_patch_orch_m2m_src_ci_collection]	Stores collections data about discovered items.
Version 16.1: Device Update [sn_vul_patch_orch_m2m_src_ci_update]	Stores data about the deployed patches, along with deployment status, that are on displayed on discovered item records.
Discovery Model Vulnerable Software Match [sn_vul_discovery_model_software_match]	Supplements the matching of vulnerable software to a discovery model.
Exception Management Configuration [sn_vul_exception_config]	Stores the configuration settings for the exception management feature.
Exception Rule [sn_vul_auto_exception_rule]	Contains the set of rules evaluated for Exception Management.
Exploit [sn_vul_exploit]	Contains the definitions of exploits: publicly available code that takes advantage of a vulnerability.
Exploit Framework sn_vul_exploit_framework	Contains the names of exploit frameworks: full software packages that are capable of running many exploits.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Exposed Discovery Models [sn_vul_m2m_exp_sw_model]	Stores the mapping between the Discovery model and Vulnerability Exposure Assessment.
Exposure Assessment [sn_vul_exp_by_sw]	Stores the records for exposure assessment.
V19.0: Exposure Manifest sn_vul_analyst_exposure_manifest	Manifest table for delta processing.
Exposure Vulnerability Entries [sn_vul_m2m_entry_exp]	Stores the mapping between Vulnerability (sn_vul_entry) and Exposure Assessment.
Malware Kit [sn_vul_malware_kit]	Contains the details of malware kits: pre-written tools that make it easy to run an exploit or set of related exploits without doing additional coding or configuration work
Missing asset table [sn_vul_tenable_missing_asset]	Contains temporary asset IDs for ignored configuration compliance assessment data with unmatched assets.
Microsoft Response Center Solution Update [sn_vul_msrc_update]	Contains the last time that the solution data was updated by Microsoft. Used to compare against the nightly import to determine the delta data for download.
Microsoft Security Response Center Solution Import [sn_vul_msrc_solution_import]	Used by the Microsoft Security Response Center Solution integration to stage import data prior to processing.
Microsoft Security Response Center Solution Integration [sn_vul_msrc_integration]	Extends the Vulnerability Integration [sn_vul_integration] table for the Microsoft Security Response Center Solution Integration.
National Vulnerability Database Entry [sn_vul_nvd_entry]	Documented vulnerability from the NIST National Vulnerability Database.
NVD CVSS Import [sn_vul_nvd_cvss_import]	Contains staging data that hasn't yet been transformed to the Vulnerability Response schema during NVD import.
Version 16.1 [sn_vul_patch_orch.patch_approval_required]	When patch deployments are scheduled from a patch integration, requests are submitted for review and approval to users assigned to the Level 1 - Patch update approval group. This property is activated by default.
Version 16.1: Patch Deployment [sn_vul_patch_orch_deployment]	Stores information about deployed patches about Collections and CIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Version 16.1: Patch Update [sn_vul_patch_orch_update]	Stores information about the patches that are available on distinct instances.
Version 16.1: Potential Patch [sn_vul_patch_orch_m2m_vuln_patch]	Stores data about patches and vulnerabilities that identify the patches that might be used to resolve a vulnerability.
V19.0: Potential Vulnerability Exposure sn_vul_analyst_m2m_pot_exp_sw_model	Exposure assessment table for CVE.
Product category [sn_vul_product_category]	Contains the imported product category data.
Red Hat Security Advisory [sn_vul_rhsa_update]	Compares the Red Hat solutions against the nightly job to determine the delta data for import.
Red Hat Solution Imports [sn_vul_rh_solution_import]	Used by the Red Hat Solution Integration to stage import data prior to processing.
Red Hat Solution Integration [sn_vul_rh_integration]	Extends the Vulnerability Integration [sn_vul_integration] table for the Red Hat Solution Integration.
Related Business Services [sn_vul_m2m_ci_services]	Links CIs to Business Services for impacted services lookup. Contains a flag indicating whether it was added by Service Mapping.
V18.0: Remediation Effort Counts [sn_vul_daily_count_re]	Daily count of remediation efforts. This table is updated daily.
V18.0: Remediation Effort Record [sn_vul_remediation_effort_record]	Tracks the remediation progress for remediation efforts (RE). Contains references to the REs.
Remediation Target Rule [sn_vul_ttr_rule]	Defines the expected time frame for remediating a vulnerable item. Extends Application File.
V18.0: Remediation Task [sn_vul_remediation_task]	Stores all the remediation tasks for VR, AVR, CVR, and test result groups. Consists of information related to [sn_vul_vulnerability] table records. Users who cannot view records in [sn_vul_vulnerability] table list view, can see those records information in the [sn_vul_remediation_task] table list view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
	This table is accessible to the users in Vulnerability Manager workspace or IT Remediation Workspace
REST Integration [sn_vul_rest_integration]	Extends the Vulnerability Integration [sn_vul_integration] table for the REST-based Integrations.
SAM NVD Vulnerability Detection [sn_vul_sam_config]	Contains which CI and Vulnerabilities are monitored with SAM NVD and whether SAM NVD vulnerability detection is enabled or not.
Scheduled Import Pool [sn_vul_sched_import_pool]	Collection of scheduled import set records used to facilitate simultaneous data source imports.
Select Vulnerable Item [sn_vul_action_select_vi]	Base staging table used to handle split VG, create CHGs, and associate CHGs
Setup Status [sn_vul_setup_status]	Internal only: Used by the Setup Assistant. Whenever Setup Assistant is opened, it shows the status of the steps Completed, and the percentage on the right top corner comes from this table.
Severity Map [sn_vul_severity_map]	Contains the mappings from source severity to normalized severity.
Solution Scanner Mapping [sn_vul_solution_scanner_mapping]	Maps vendor, scanner, and keywords for exclusion or inclusion.
Split vulnerability group [sn_vul_action_split_vg]	Staging table used to split remediation tasks.
Third Party Vulnerability Entry [sn_vul_third_party_entry]	Documented vulnerability from a third-party source.
[sn_vul_tenable_io_template	A template record is sent to Tenable.io and then imported during rescan for items that have Tenable.io as a source.
Update Manifest [sn_vul_update_manifest]	List of remediation tasks that have been updated and require recalculation by the rollup calculator.
V17.1: Usage by CI classes [sn_vul_licensing_usage_by_ci_classes]	Contains the usage count aggregated by the CI class.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
VR Configuration Item Count [sn_vul_vr_configuration_item_count]	Contains the 90-day rolling cumulative average of configuration items imported from third-party integrations.
Vulnerability Assignment Rule [sn_vul_assignment_rule]	Contains the set of rules evaluated to set the assignment group on VIs.
Vulnerability Calculator [sn_vul_calculator_group]	Contains the vulnerability calculator rules. The order of the calculator determines which calculator is evaluated first, and in each calculator, one calculator rule, at most, is used.
Vulnerability Calculator Rule [sn_vul_calculator]	Contains the rules for all of the calculators. For each calculator, the calculator rules are reviewed in order. The first calculator matching the condition uses the values within that rule.
Vulnerability CVEs [sn_vul_m2m_entry_cve]	Links NVD Common Vulnerability Exposures (CVE) data to vulnerable entries.
Vulnerability Data Source Import Queue Entry [sn_vul_ds_import_q_entry]	Queue for attachments before they're processed by a data source. Utilized by vulnerability integrations.
Vulnerability Entry [sn_vul_entry]	Documented vulnerability.
Vulnerability Entry Scan [sn_vul_entry_scan]	Stores the relationship between a scan and vulnerability entry.
Vulnerability Exploit Framework [sn_vul_m2m_framework_vul]	Contains the relationship between Exploit frameworks and vulnerabilities.
V19.0: Vulnerability Exposure Assessment sn_vul_analyst_sam_config	Exposure assessment configuration table for CVE.
Vulnerability Granularity Configuration [sn_vul_granularity_config]	Stores and maintains the state of include or exclude Port for the Configure VI Granularity module.
Remediation Tasks [sn_vul_vulnerability]	Collection of vulnerable items organized for remediation.
Remediation Task Change Requests [sn_vul_m2m_vg_change_request]	Stores the association of remediation tasks and CHG requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Remediation Task Items [sn_vul_m2m_vul_group_item]	Association of remediation tasks and vulnerable items.
Remediation Task Rules [sn_vul_grouping_rule]	Contains the rules that define the criteria with which groups are automatically created for a set of vulnerable items.
Vulnerability Integration [sn_vul_integration]	Schedulable record to import vulnerability data from an external source. Extends Scheduled Script Execution.
Vulnerability Integration Data Source [sn_vul_int_data_src]	Data source to use with a vulnerability integration.
Vulnerability Integration Log [sn_vul_integration_log]	Records log information output by vulnerability integration runs.
Vulnerability Integration Process [sn_vul_integration_process]	Single process occurrence for a vulnerability integration.
Vulnerability Integration Queue [sn_vul_integration_queue]	Queues the import requests for an integration run when all the Data Sources are in use.
Vulnerability Integration Run [sn_vul_integration_run]	Vulnerability integration invocations. **Note:** If an integration run is in progress, only one integration can be in ready state in the backlog.
Vulnerability Integration Run Stats [sn_vul_integration_stats]	Stores the breakdown of each step: for example, REST API time, VI creation time, and so on for an integration run
Vulnerability Item Task [sn_vul_m2m_item_task]	Vulnerable items associated with problems, changes, and security incidents.
Vulnerability Malware Kit [sn_vul_m2m_malware_kit_vul]	Contains the relationships between vulnerabilities and malware kits.
Vulnerability Prerequisite Solution [sn_vul_m2m_solution_prerequisite]	Contains the source-specific prerequisites to applying a solution, when available.
Vulnerability Rate limit [sn_vul_rate_limit]	Defines a rate limit to be used on a scanner.
Vulnerability Reference	External references for known vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
[sn_vul_reference]	
Vulnerability Remediation Status [sn_vul_m2m_ttr_status]	Status of the vulnerable item against the closest applied remediation target rule.
Vulnerability Risk Rule [sn_vul_calc_risk]	Specialized calculator rule used with the Risk Score calculators. Takes weights indicating which values, related to a VI, to use to calculate the Risk Score.
Vulnerability Rollup Calculator [sn_vul_rollup]	List of vulnerability rollup calculators.
Vulnerability Scan [sn_vul_scan]	Vulnerability scan. Contains what to scan, with what scanner, and a summary of the scan results.
Vulnerability Scan Configuration Item [sn_vul_m2m_scan_configuration_item]	Associates CMDB CIs that are queued to be scanned.
Vulnerability Scan Queue Entry [sn_vul_scan_q_entry]	Scan record queued for scanning or processing. Facilitates the requests within stated rate limits.
Vulnerability Scan Source [sn_vul_m2m_scan_source]	Associates sources to a scan record and signifies all the records that are queued to be scanned.
Vulnerability Scan Task [sn_vul_m2m_scan_vulnerability]	Associates vulnerability tasks for the sources of a scan record.
Vulnerability Scanner [sn_vul_scanner]	Defines third-party scanners to use in scans.
Vulnerability Scanner Rate Limit [sn_cmn_scanner_rate_limit]	Associates a scanner with a rate limit.
Vulnerability Software [sn_vul_m2m_entry_software]	Contains associations between vulnerabilities and vulnerable software.
Vulnerability Solution [sn_vul_solution]	Contains the relationship data between the vulnerability and the possible solutions for it. Starting with v24.0.6 of Vulnerability Response, a new column titled Scanner Bulletin is added to this table.
Vulnerability Solution	Links the Vulnerability Entry (sn_vul_entry) table to the Vulnerability Solution (sn_vul_solution) table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

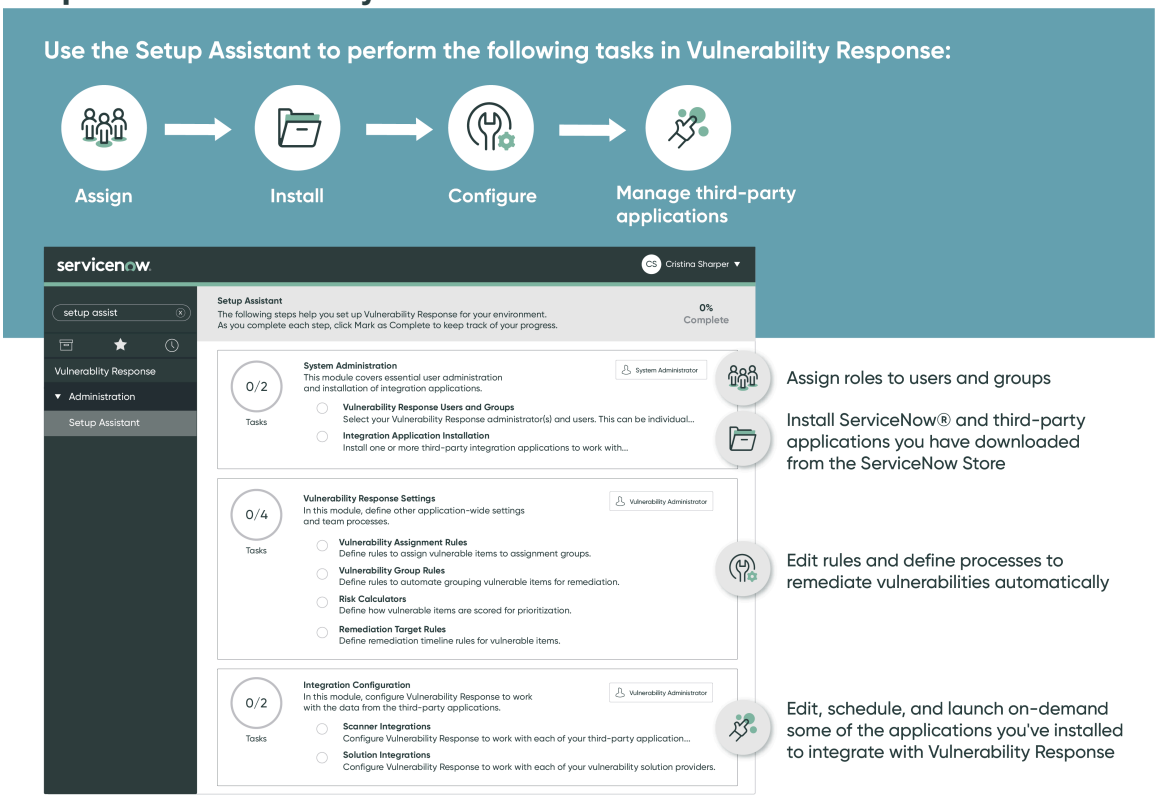
Table	Description
[sn_vul_m2m_vulnerability_solution]	
Vulnerability State Change Approval [sn_vul_change_approval]	Tracks the approval process for vulnerabilities.
Vulnerability Superseding Solution [sn_vul_m2m_solution_supersedence]	Contains the source-specific relationship between solutions.
Vulnerability Update Manifest [sn_vul_vuln_update]	Contains a list of vulnerabilities that need their rollup data updated after their vulnerable items are updated, closed, or have risk score changes.
Vulnerability Vendor Mapping [sun_vul_vulnerability_vendor_mapping]	Contains a list of vulnerabilities and their vendors.
Vulnerable Item [sn_vul_vulnerable_item]	Contains the occurrence of a vulnerability on a configuration item.
Vulnerable Item Detection [sn_vul_detection]	Contains the vulnerable item detections from third-party integrations.
Vulnerable Software [sn_vul_software]	Software that is known to have certain vulnerabilities.

Configuring Vulnerability Response using the Setup Assistant

Setup Assistant walks you through setting up Vulnerability Response and certain third-party integrations for your environment. Setup Assistant provides almost everything you need to install and set up your environment so that you can use Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup Assistant functionality



Now Platform® roles: admin and vulnerability admin

Using Setup Assistant requires two different ServiceNow AI Platform® roles: admin and vulnerability admin.

Refer to the following sections to supplement the instructions and prompts provided in Setup Assistant.

System Administration - assign users and groups and install integration applications

Role required: admin

A list of users and integrations should be obtained from the Vulnerability Manager prior to beginning these tasks.

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant**.
2. In the first section, System Administration, the admin the assigns roles to users and groups and installs supported integrations.

   Assign Vulnerability Response personas and roles to users and groups in Setup Assistant.

   Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

3. Assign roles in Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Assign the role of sn_vul.admin to users or groups.
- Assign the sn_vul.admin role for Vulnerability Response administration and configuration including vulnerability integrations, remediation task rules, calculators, and time-to-remediate rules.
- Assign the sn_vul_vulnerability_write role for the creation and update of remediation tasks and vulnerable items.

  Note: All other users automatically receive Write access only to remediation tasks that are assigned to them.

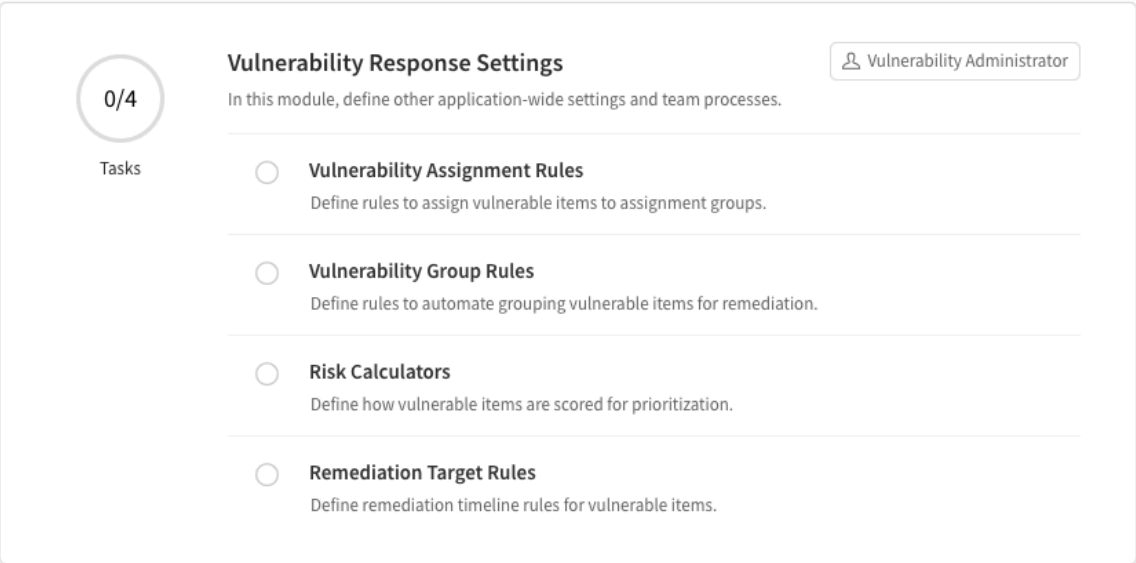
- Assign the sn_vul_vulnerability_read role to view remediation tasks, vulnerable items, and other vulnerability information.

  Note: Users with the itil role are automatically granted the sn_vul.remediation_owner role allowing them to see remediation tasks and vulnerable items assigned to them, vulnerability entries, and, solutions in the Vulnerability Response application on their instance and in the Mobile Agent application. No additional assignment is needed.

4. Install third-party integration applications.
   - See Installation of Vulnerability Response and supported applications and Vulnerability Response integrations for more information about applications that are supported by Vulnerability Response.
   - For more information about using setup assistant to install supported apps, see Install Vulnerability Response third-party applications using Setup Assistant.

Vulnerability Response Settings

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin



In Vulnerability Response Settings, the vulnerability administrator defines application-wide settings and defines rules for Vulnerability Response. Alternatively, the admin can perform these tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Create Vulnerability Assignment Rules.

   Create rules that define the automatic assignment of remediation tasks for resolution. At least one rule is shipped with the base system. See Vulnerability Response assignment rules overview for more information.

   Note:

   The reapply feature requires a baseline application of the rules. Once your rules are created, activate the *Reapply all vulnerability assignment rules* scheduled job to execute, at your convenience. Otherwise, you will be required to reapply all rules to all Open VIs prior to changing them.

   When the job is complete, set the **Run** field in the scheduled job to fit your environment. Depending on the number of active VIs you have, evaluating and updating them daily can have non-trivial performance impact. For larger environments, consider updating once a week or even once a month.

   Reapplying assignment rules does not regroup the vulnerable items.

2. Create remediation task rules.

   Create rules that define the automatic creation of remediation tasks for resolution. At least one rule, **Vulnerability,** is shipped with the base system. You can reapply the rules from the form or list view.

   - When a group rule is deleted, from the form or list view, you have the option to delete all **Open** groups created by that rule. Groups not in the **Open** state are excluded.
   - See CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations for more information on creating rules for your environment.
   - See Exploring the Vulnerability Response application for more information on using Vulnerability Response to remediate vulnerabilities.

3. Create and enable Risk Calculators.

   Enable risk calculators that define how vulnerable items are scored for prioritization. Several risk calculators are shipped with the base system. See Vulnerability Response calculators and vulnerability calculator rules information on creating or editing risk calculators for your environment.

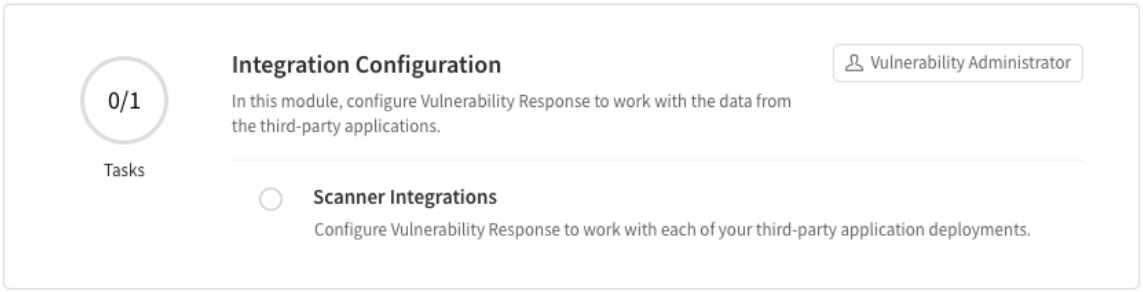
4. Create Remediation Target Rules.

   Create remediation target rules for categories of remediation. At least one rule is shipped with the base system. See Vulnerability Response remediation target rules for more information on creating rules for your environment.

Integration Configuration

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



In the Integration Configuration section, configure, schedule, edit, and launch on-demand the following third-party vulnerability scanner integrations and, if the Solution Management for Vulnerability Response application is installed, solution providers.

- See Configure the Qualys Vulnerability Integration using Setup Assistant for more information about configuring the Qualys Vulnerability Integration.
- Configuration of the Vulnerability Response Integration with Tenable application is supported. See Configure the Tenable Vulnerability Integration using Setup Assistant.
- After you install the Vulnerability Solution Management application, the **Solution Integrations** option is displayed below **Scanner Integrations**. Click **Solution Integrations** to configure your installed vulnerability solution providers from this section of Setup Assistant. The Red Hat Solution Integration and Microsoft Security Response Center Solution Integration are supported.

  See Vulnerability Solution Management for more information about installed solutions. See Install the Solution Management for Vulnerability Response application for more information about installation.

  See Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant for more information about configuring your installed solutions.
- If an integration is multi-sourced, you can have multiple deployments of the same third-party integration.
- The settings from your original third-party integration are used as a template for the settings of each new integration.

  Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

  Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

Note: Multiple vulnerability integrations for Rapid7 InsightVM are not available within Setup Assistant. See Create domain-separated imports for an integration for information on configuring and creating multiple Rapid7 InsightVM integrations.

Additional tasks

See Additional Vulnerability Response setup and configuration tasks for more information on setup tasks not included in Setup Assistant.

Assign the Vulnerability Response persona roles using Setup Assistant

Assign the Vulnerability Response persona roles to groups or users with Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

If you have already assigned persona roles in Vulnerability Response using Setup Assistant and you want more information about editing and managing your granular roles and role assignments in the User Administration module, see Manage persona and granular roles for Vulnerability Response.

If you are an upgrade customer, you can continue using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner roles available in previous versions of Vulnerability Response has not changed.

However, for more control over what users and groups can do and see in the Vulnerability Response application at the task level, you may prefer using persona and granular roles.

If you have not already assigned the sn_vul.vulnerability_admin persona role using Setup Assistant, follow the steps below to assign it. Once assigned, the vulnerability administrator with this persona role has permission to complete the Setup Assistant tasks after the first section, and manage rules and third-party integrations in the Vulnerability Response application.

For an overview about persona roles and granular roles, see Vulnerability Response personas and granular roles.

If you are an upgrade customer, use the following table as a reference.

Previous assignment	Recommended assignment [User persona]	Description
sn_vul.admin	sn_vul.vulnerability_admin [Vulnerability Admin]	Provides complete access to the Vulnerability Response (VR) application. Users with this role configure VR applications and rules and install third-party integrations.
sn_vulnerability_write	sn_vul.vulnerability_analyst [Vulnerability Analyst]	Allows viewing and updating of all records for VIT remediation.
sn_vul.remediation_owner	sn_vul.remediation_owner [Remediation Owner]	Allows users and groups to remediate vulnerabilities assigned to them or their group, and update the related records.
sn_vul.admin	sn_vul.ci [CI Manager]	Allows management of unmatched configuration items not found in the CMDB, including updating discovered items.
sn_vul.admin	sn_vul.exception_approver [Exception Approver]	Allows approval of exceptions, deferrals, and closures of remediation tasks and vulnerable items.
sn_vul.vulnerability_read	sn_vul.read_all or sn_vul.read_group_rules	Grants read-only access to specific areas in the application. Use sn_vul.read_all to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Previous assignment	Recommended assignment [User persona]	Description
		view all VR records, or sn_vul.read_group_rules to view remediation task rules. Users with these roles cannot update records. **Note:** Several other read roles are available in the Vulnerability Response scope for more granular access.

To view the granular roles a user or groups with a persona role inherits by default, navigate to **All** > **User Administration** > **Roles**. Locate the role you want, and click it to open the record. The Contains Roles tab lists all the granular roles of the persona role as well as any inherited roles.

You may prefer to verify that you have all your required users and groups created before you assign roles in Setup Assistant. Alternatively, to add new users and groups from inside Setup Assistant, click the **User Administration module** link in the form shown in the following figure.

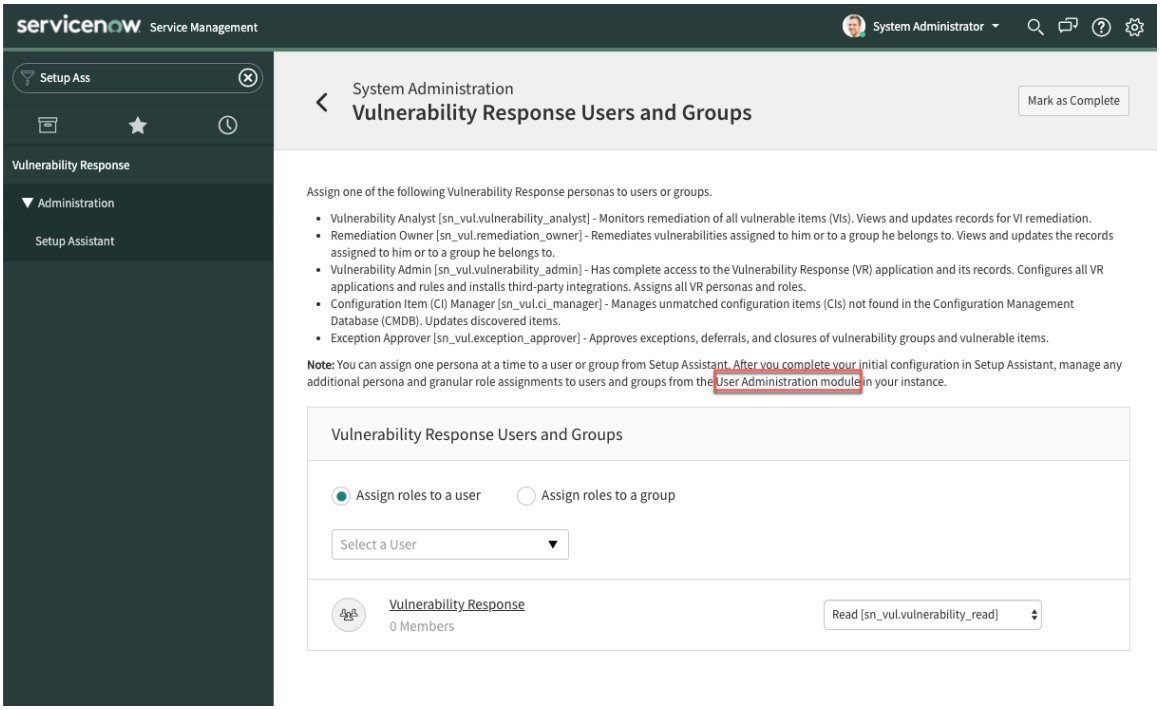
For the following example, to limit access to the Vulnerability Response application, this example shows how to assign a user with the vulnerability admin persona. Usually, you may prefer to assign persona roles other than sn_vul.vulnerability_admin to groups.

Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration Setup Assistant**.
   The Setup Assistant page is displayed.
2. Click Vulnerability Response User and Groups.
   The System Administration Vulnerability Response Users and Groups page is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. With Assign roles to a user selected, choose an existing user from the list.

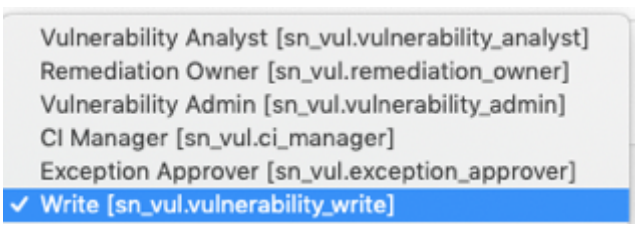
   You can only assign a user or a group with one persona role.

   On the right of the form, after you select a user or group, the default persona, Remediation owner [sn_vul.remediation_owner] is assigned by default and remains displayed in the list until you change it.

   Note: If you are upgrading to a newer version of Vulnerability Response and you previously assigned the sn_vul.vulnerability_read or sn_vul.vulnerability_write role to a user or group prior to the upgrade, it is displayed along with the new persona roles, as shown in the following figure.

   If you are an upgrade customer, you can keep using your existing roles for the Vulnerability Response application. Access for users and groups assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions and remediation owner prior to v10.3 has not changed.

   Note that for existing users or a groups currently assigned with the sn_vul.vulnerability_read or sn_vul.vulnerability_write roles, these roles are displayed along with the persona roles in the list. Once you assign a persona role, the old role is no longer available going forward. For example, as shown in following figure, the Write [sn_vul.vulnerability_write] role is no longer displayed as an option for this user or group after it is assigned one of the persona roles.

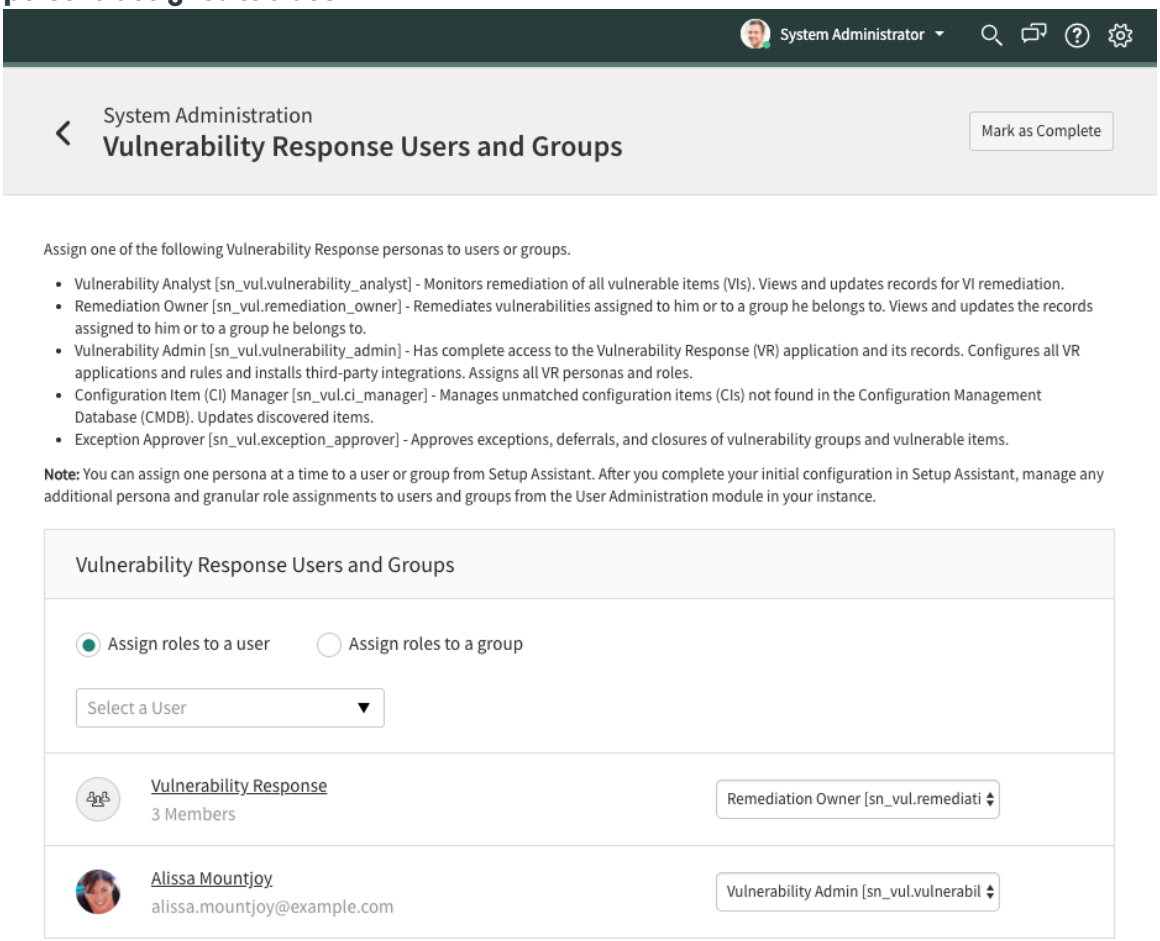


4. From the list on the right of the form, select **Vulnerability Admin [sn_vul.vulnerability_admin]**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A message is displayed that indicates the user or group is successfully assigned with the persona.

Remediation Owner persona assigned to a group, and Vulnerability admin persona assigned to a user



5. Using the descriptions of the persona roles listed above, continue to assign any users and groups to the remaining persona roles: Remediation Owner, Vulnerability Analyst, CI Manager, and Exception Approver.
   You have successfully completed assigning persona roles to users and groups using Setup Assistant.
6. **Optional:** To edit the users in a group from Setup Assistant, follow these steps.

   a. With the group displayed on the form, click the name of the group you want to edit.
   The Group record is displayed.

   b. With the Group Members tab selected, click **Edit**.
   The Edit Members form is displayed

   c. Use the slushbucket to select or remove users.

   d. Click **Save** to save your changes and return to the Group record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Click **Update** to return to Setup Assistant.

f. On the Setup Assistant page, click **Vulnerability Response Users and Groups** to continue with your configuration in Setup Assistant.

What to do next

As system admin, continue with the configuration of Vulnerability Response in Setup Assistant. Note that after the first section is completed, you can have a user you assigned with the vulnerability admin persona role complete the tasks in Setup Assistant. For more information about managing granular roles and examples, see Manage persona and granular roles for Vulnerability Response.

Manage persona and granular roles for Vulnerability Response

After you complete your initial assignment of persona roles using Setup Assistant, manage additional granular role assignments to users or groups from the User Administration module in your instance.

Before you begin

If you have not already completed your initial set up and configuration for Vulnerability Response using Setup Assistant, or assigned persona roles to users and groups, navigate to **Vulnerability Response** > **Administration** > **Setup Assistant**. See Assign the Vulnerability Response persona roles using Setup Assistant.

For key terms and an overview of persona roles, see Vulnerability Response personas and granular roles.

A persona role is pre-configured role in the application that is made up of multiple granular roles. The persona roles in Setup Assistant, Vulnerability Admin, Vulnerability Analyst, Remediation Owner, Configuration Item Manager, and Exception Manager, are designed to correspond to common job titles for managers, analysts, and service owners in an IT organization or vulnerability remediation group.

If you want your users and groups to have more access than one of the roles permits, you can add more granular roles to users and groups. Conversely, if you want to limit access for specific users and groups at the task level, you can remove granular roles. Also, you can build custom roles to suit your needs.

Role required: admin

Procedure

1. To manage granular roles for users and groups, choose one to continue.

Option	Description
Edit the granular roles for a user or group	Assign or remove granular roles for users or groups, or edit granular roles so that only se lect users within a group have expanded or limited permissions. An example follows the table.
Create a new role	Create a new role using one or more granular roles from the library for a specific job title, or to fulfill a specific requirement.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	An example follows the table.

The names for the granular roles in Vulnerability Response usually describe what users can do and see. To view descriptions of specific granular roles, navigate to **All** > **User Administration** > **Roles** and locate the role that you want. Role description, roles that are automatically inherited when a role is assigned, and any roles that depend on other roles are also listed.

2. To assign or remove a granular role for a user or a group, follow these steps.
   As an example, assume you want to assign an IT manager with a role that permits this manager to view records but not update or edit them. To view records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for all third party integrations, you assign this user with the sn_vul.read_all granular role.

   a. Navigate to **All** > **User Administration** > **Users**.

   b. Locate the user, and, in the Name column, click the record to open it.
   The user's record is displayed.

   c. If not selected, select the Roles tab.
   The roles currently assigned to the user are displayed.

   d. Click **Edit**.
   The Edit members form is displayed.

   e. In the Collection field of the slushbucket, enter the name of the role if you know it, or, enter `*sn_vul` to view only the granular roles available for Vulnerability Response.

   f. Locate and move sn_vul.read_all to the Roles List.

   Note: Use the same process to remove specific granular roles from users in the slushbucket by moving the role from the Roles list to the Collection list.

   g. Click **Save**.
   The user record is displayed with the new granular role.

   h. Click **Update** to save your changes and return to the Users list.
   You have provided a user with permission to read but not update records in Vulnerability Response, Performance Analytics for Vulnerability Response, and for third party integrations.

3. To edit a group so that only specific members have expanded access with more granular roles, follow these steps.
   As example, assume you want to permit certain users in the Remediation Owner (sn_vul.remediation_owner) group to create vulnerable items manually, but you don't want to expand that permission to all users in the group. The permission to create vulnerable items manually is granted by the sn_vul.create_vulnerable_items granular role. To grant this permission to only select users from this group, follow these steps.

   a. Navigate to **All** > **User Administration** > **Groups**.

   b. Locate the Remediation Owner group, and, in the Name column, click the group to open the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The group record is displayed.

c. If not selected, select the Group Members tab.
The current members of the group are displayed.

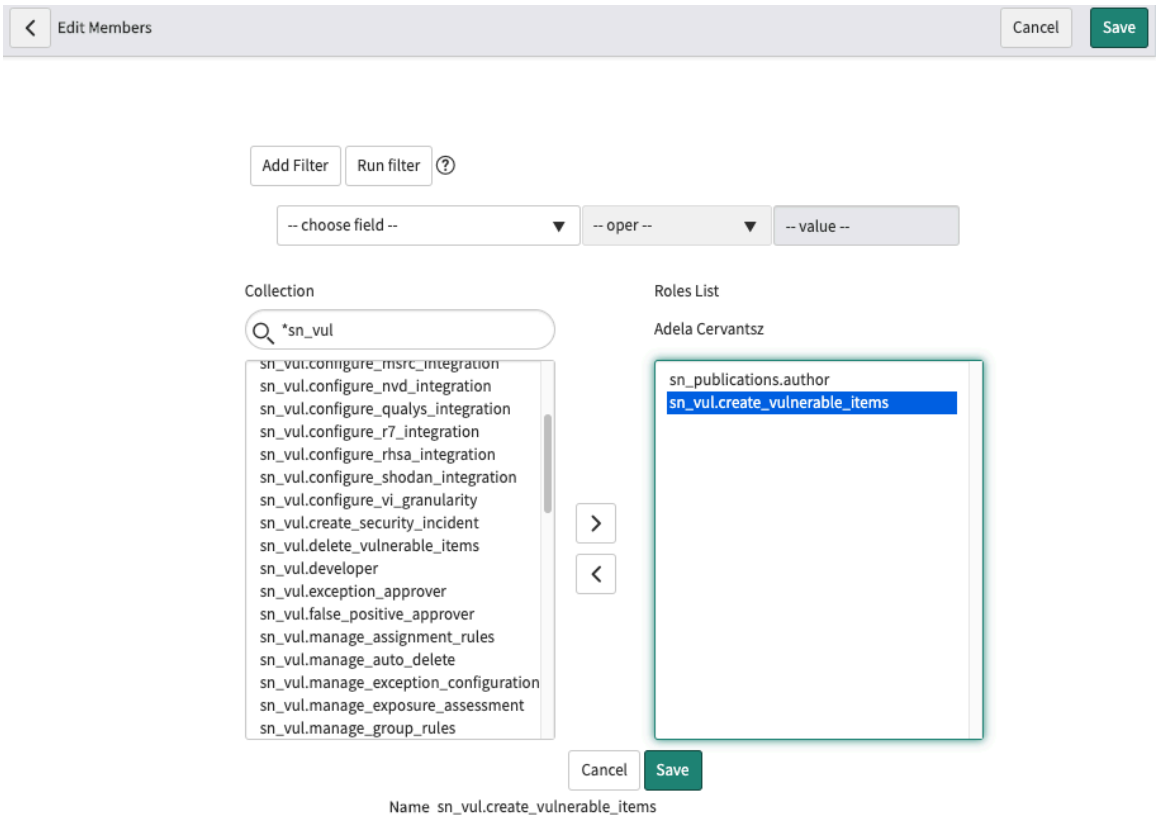
d. Click a name from the list you want to assign the granular role to and open the record.

e. On the record, scroll to the Roles tab and select it.
The roles assigned to the user are displayed.

f. Click **Edit**.
The Edit members form is displayed.

g. In the Collection field, enter the name of the role if you know it, or, enter `*sn_vul` to view all the granular roles available for Vulnerability Response.

h. Locate and move sn_vul.create_vulnerable_items to the Roles List.



i. Click **Save**.
The user record is displayed with the new granular role.

j. Click the back arrow to return to view the users in the record for the Remediation Owner group

k. Click names from the list you want to assign this granular role to, open their records, and use the slushbucket to assign the role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

l. After you complete your edits, Click **Update** to save your changes and return to the groups list.
You have provided some users in the Remediation Owner (sn_vul.remediation_owner) group permission to create vulnerable items manually.

4. To create a new role using only granular roles you select, follow these steps.
For this example, assume you want to create role for a compliance auditor. This role works closely with Governance, Risk, and Compliance (GRC), and the job requires the following permissions and tasks within Vulnerability Response:
   - Manages remediation deadlines for vulnerable items and vulnerability groups
   - Approves exception requests for extending deadlines or deferring remediation
   - Manages the clean up of older vulnerable items with auto-delete
   - Define risk scores
   - Reads all records in Vulnerability Response but is not permitted to edit them.

   a. Navigate to **All** > **User Administration** > **Roles**.

   b. In the Roles list, click **New**.

   c. In the Role record, fill out the fields.

   Create a name, select the application that contains this record, and enter a short description for your new role. For more information about the other fields on the form, see Create a role

   Note: When creating a name for your new role, you may prefer to use a name that is easily recognized in the roles list and describes the functionality of the role. For this example, you may prefer a title such as, Compliance Auditor - GRC-VR.

   d. Click **Submit**.
   The Roles list is displayed.

   e. Locate your new role and click it to open the record.

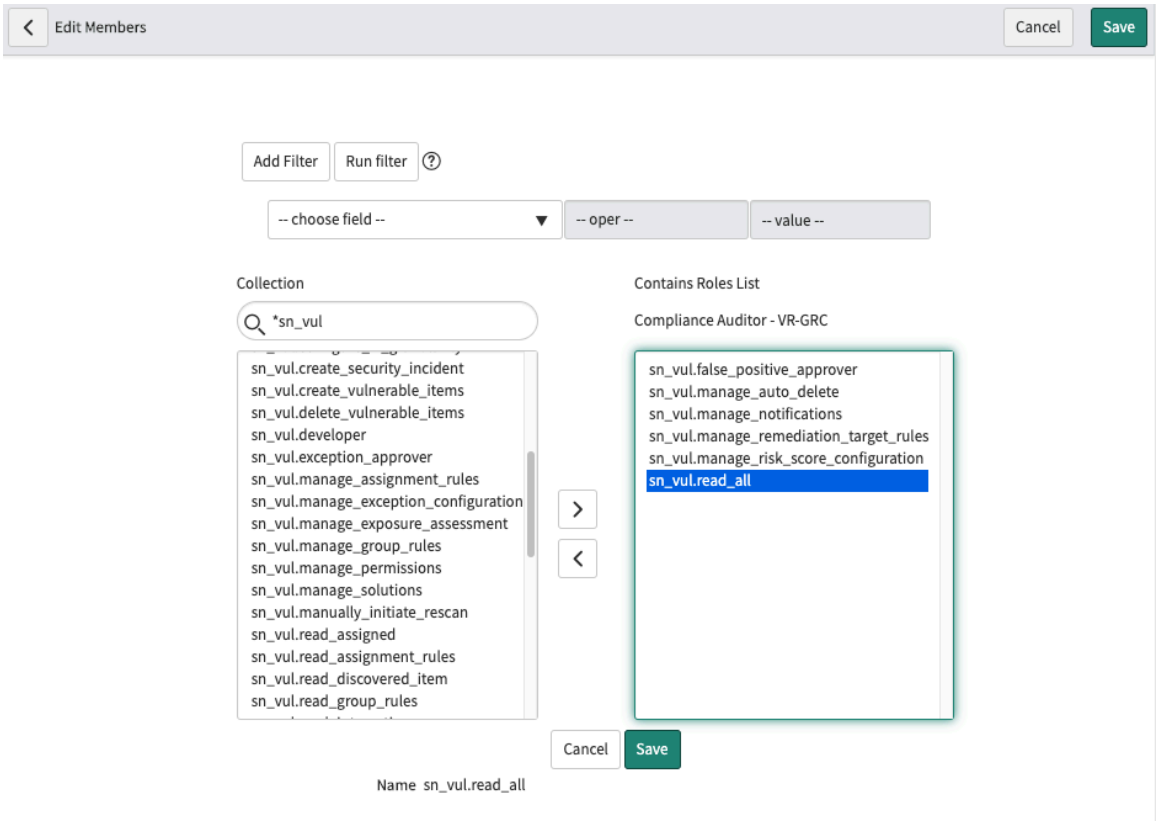
   f. Click **Edit**.
   The Edit Members form is displayed.

   g. Use the slushbucket to add granular roles to your new role.

   For this example, the required roles for this new role are displayed in the right column in the following figure.

   To display only the granular roles for Vulnerability Response, in the Collection field, enter `*sn_vul`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



h. Click **Save**.
The record for your new role is displayed. Starting with the Contains Roles tab, continue editing the role as required.

i. Click **Update** to save your changes.
Your new role is displayed on the Roles list.

Install Vulnerability Response third-party applications using Setup Assistant

Install the third-party integration applications you have entitlement for in Vulnerability Response using the Setup Assistant.

Before you begin

Setup Assistant supports the installation of most third-party integration applications with Vulnerability Response, but you continue with the configuration for some applications you install from configuration modules in your instance. See Vulnerability Response integrations for a list of applications that are supported by Vulnerability Response.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

- After it is installed, the Vulnerability Solution Management feature of Vulnerability Response provides you access to the Microsoft Security Response Center Solution Integration and the Red Hat Solution Integration in Setup Assistant.
- Vulnerability Solution Management is available by separate subscription. See Vulnerability Solution Management for more information on how Vulnerability Response incorporates solutions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you can install and activate third-party applications from Setup Assistant, perform the following tasks to ensure a smooth installation:

Setup Tasks	Description
Verify that you have valid ServiceNow entitlements for the integration applications that you want to install.	Navigate to **Subscription Management** > **Subscriptions** in your instance to verify entitlements. The list displays the subscriptions your organization has purchased. For more information about getting entitlements for a Security Operations application from the ServiceNow Store, see Get entitlement for a Security Operations product or application.
(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application.	For more information about installing and activating the Vulnerability Response application, see, Install and configure Vulnerability Response.
If not already installed and activated, you must activate and import vulnerability data with the NVD Integration and CWE scheduled job prior to running a third-party scanner application to import data.	Run the NVD and CWE integrations as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product. See Understanding the NVD integrations for more information.
Verify you have completed any setup tasks required for the third-party integrations for Vulnerability Response.	Review any required setup tasks for each integration that you want to install at Vulnerability Response integrations.

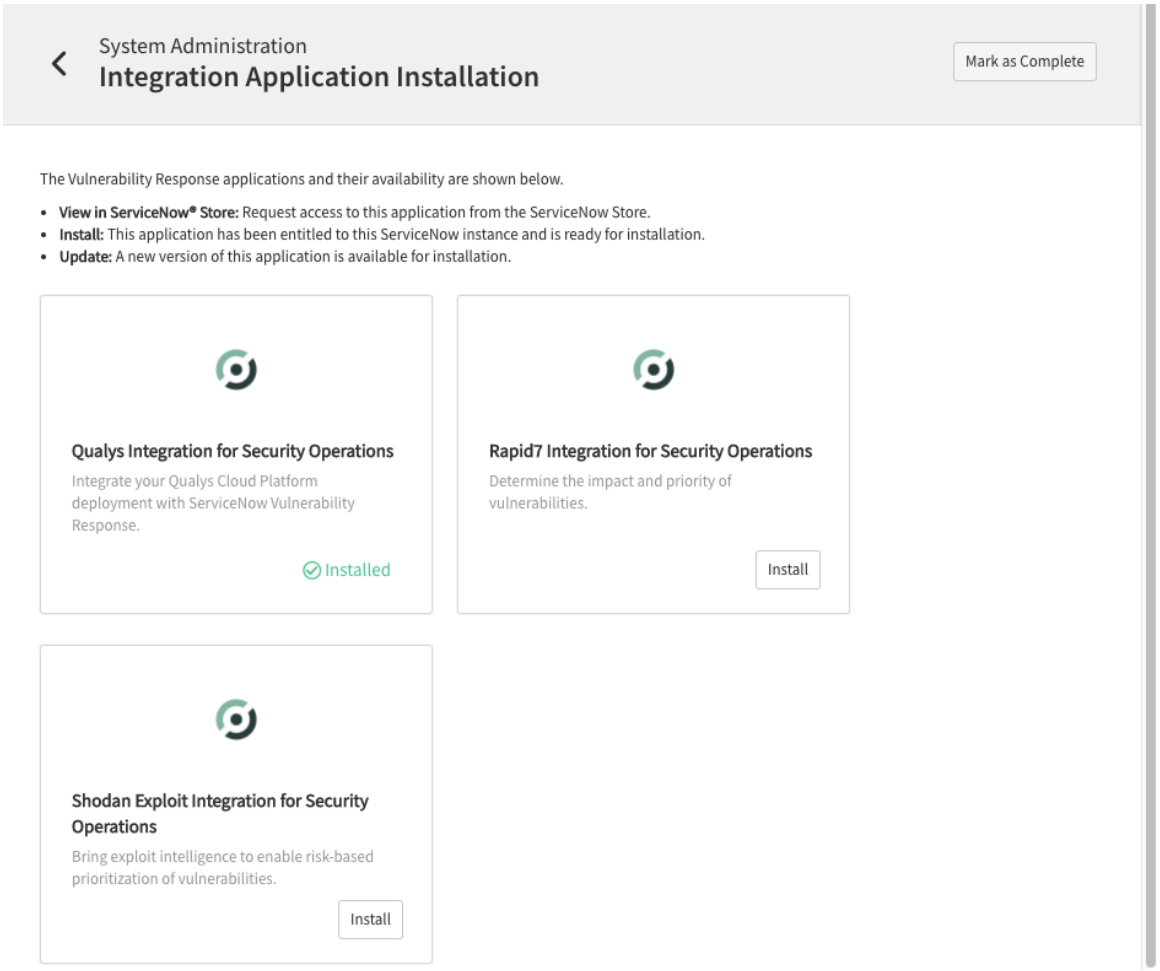
Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **System Administration** > **Integration Application Installation**.

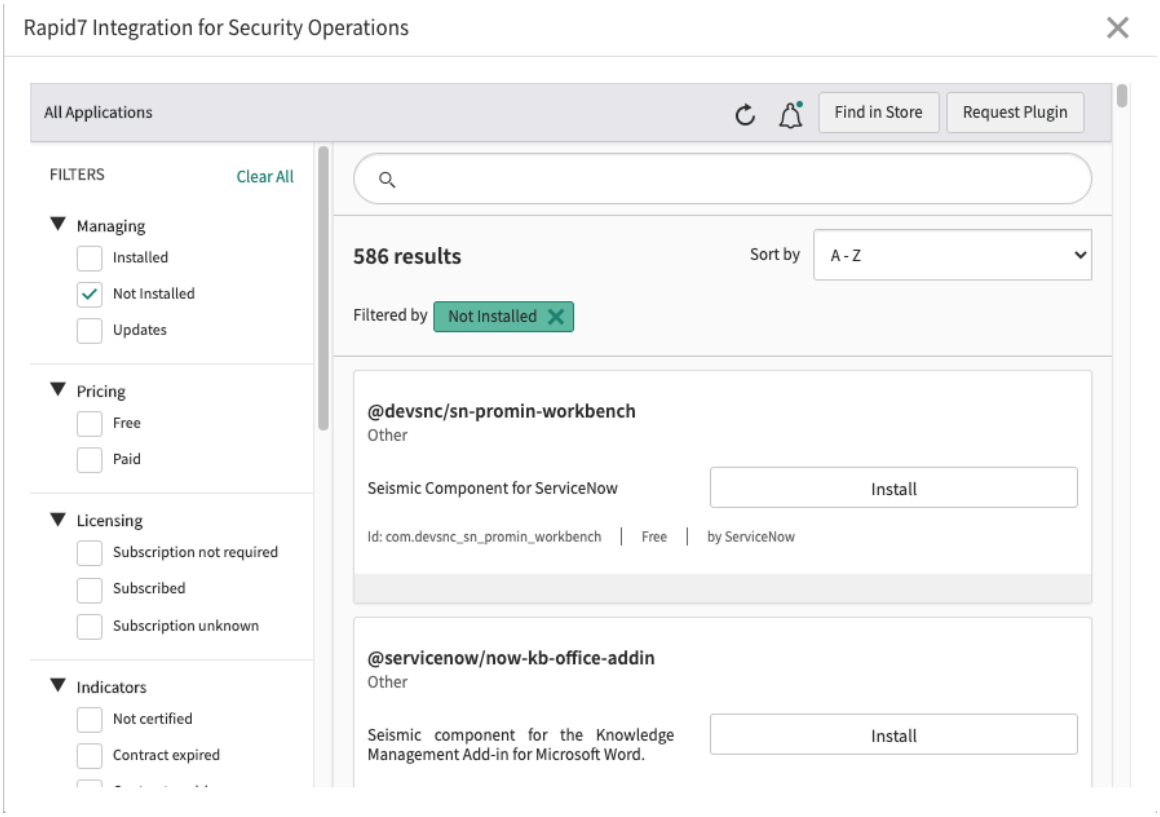
   After a few moments, the applications you have entitlement for and that are available for installation on your instance are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Locate the application want to install and click **Install** on the application tile.
   The All Applications dialog is displayed with the name of the application tile you clicked, for example, Rapid7 Integration for Security Operations, as shown in the following figure.

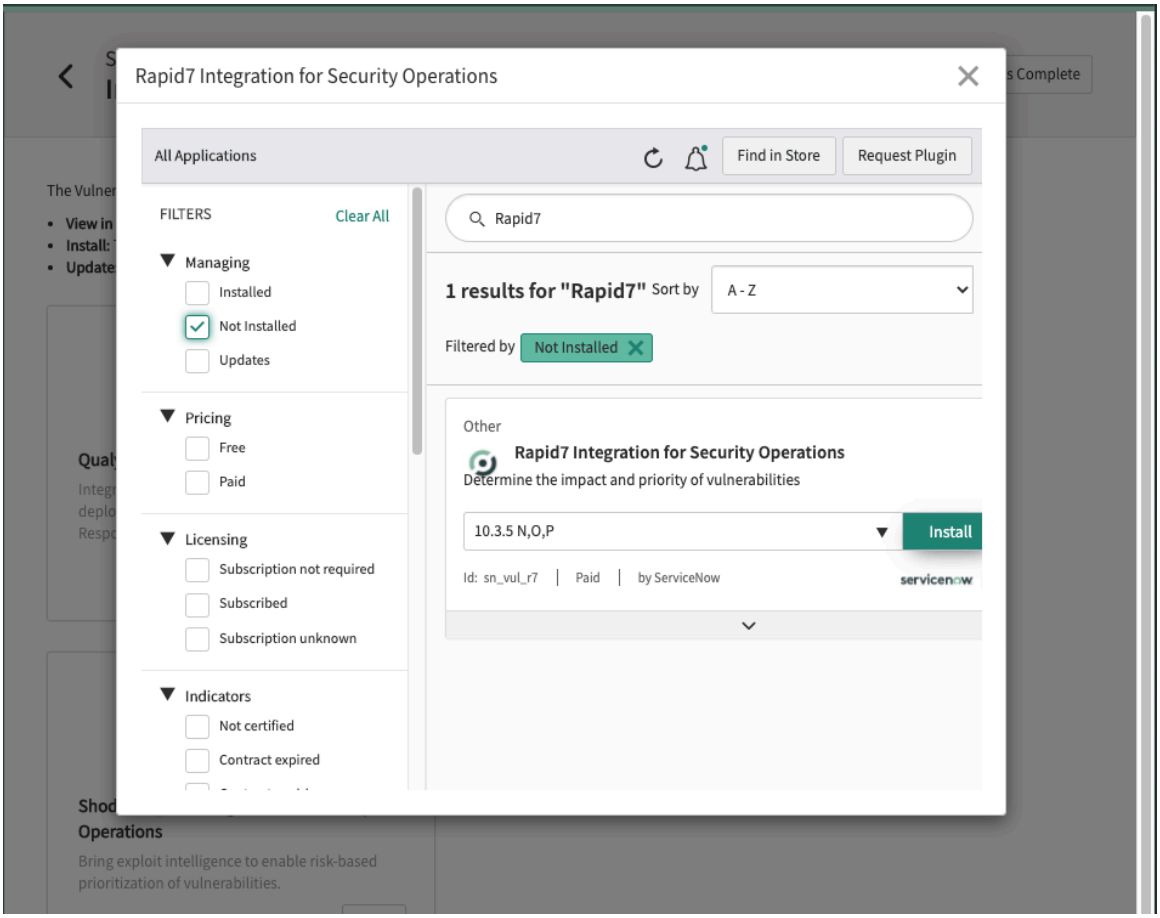
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Locate the application, select a version from the choice list, and click **Install**.

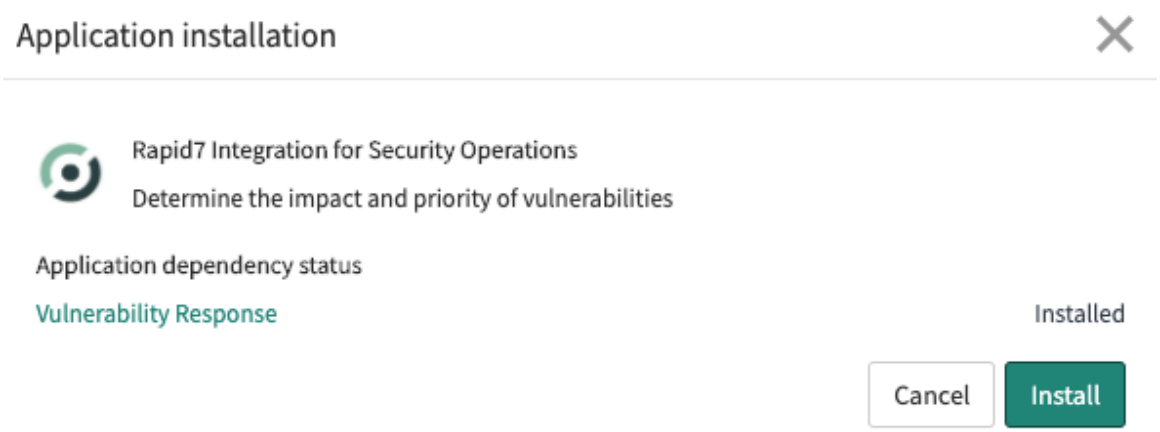
   If an update is available for the application, the **Update** button is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Application installation dialog displays the application dependency status. Any required dependencies not already installed are automatically installed along with the application.

4. In the Application installation dialog, click **Install**.



The Install dialog indicates when the installation is successfully completed.

5. Close the dialog.
The All Applications page is displayed that shows your application is successfully installed.

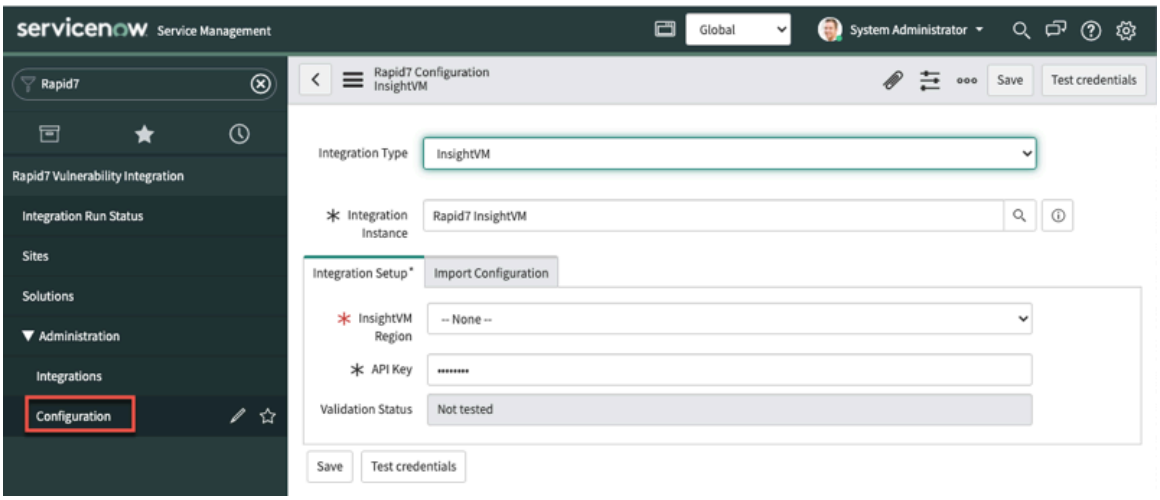
After installation and activation, you can configure, schedule, and launch the following applications and installed solutions directly from the Integration Configuration section of Setup Assistant:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Qualys Vulnerability Integration
- The Vulnerability Response Integration with Tenable.
- The Microsoft Security Response Center Solution Integration
- The Red Hat Solution Integration
- Microsoft Security Response Center Solution Integration
- The Microsoft Defender Vulnerability Management Integration

For other applications not listed above, navigate directly to the configuration module of the application to continue with the configuration and to enter any required third-party credentials. For example, the following image shows the location of the Configuration and module for the Rapid7 application.

For more information about configuring specific applications, see the installation and configuration product documentation by product name provided for each application.



What to do next

Continue with the configuration of your application in Setup Assistant if your application is supported.

If your application is not supported for configuration in Setup Assistant, navigate directly to the configuration module of the application to continue with the configuration. To view supported applications in Setup Assistant, see, Installation of Vulnerability Response and supported applications.

Importing data with the NVD and CWE integrations and managing third-party libraries

If not already installed, download and run the NVD integration and run the CWE scheduled job as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product. The Vulnerability Response Integration with NVD is available on the ServiceNow Store.

Ingesting CWE and NVD data

Imported data from the NVD and CWE integrations are used to enrich the vulnerability data in your instance and help you decide whether to escalate remediation for a vulnerability, vulnerable item, or remediation task. After an initial import, you can update library records on-demand or configure a scheduled job to update records regularly. Vulnerability Response stores them under **Libraries**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Common Vulnerability Scoring System (CVSS), included in NVD and third-party entries, captures the main characteristics of a vulnerability. Vulnerability Response uses CVSS data to produce a normalized value reflecting vulnerability severity. When the severity is computed, the vulnerability provides a better understanding of the risk posed by this vulnerability to your organization. Severity helps you assess and prioritize vulnerability remediation.

If this is your first installation of Vulnerability Response, or prior to ingesting data for the first time with a third-party scanner product:

1. Perform an initial import of CWE data with the CWE Comprehensive 2000 Integration.

   See Configure and run the scheduled job for updating CWE records for more information. You perform CWE updates **On Demand** from the integration record by default, and you must configure it if you want it to run as a scheduled job.

   Note: Schedule the CWE update to run prior to the NVD database update. The default day for the NVD update is **Weekly** on **Monday**.

2. Verify the Vulnerability Response Integration with NVD application is installed, and data from the NIST National Vulnerability Database Integration - API (CVE only) or the NIST National Vulnerability Database Integration - API (CVE and CPE) is successfully imported.

   Activation of this plugin on production instances may require a separate license. After it is installed, the NIST National Vulnerability Database Integration - API (CVE only) integration is activated by default. It runs daily. See Understanding the NVD integrations and Install the Vulnerability Response Integration with the NIST National Vulnerability Database for more information.

3. Third-party libraries are updated as scheduled jobs. Refer to your integration documentation at Vulnerability Response integrations for more information about third-party integrations.

Viewing imported vulnerability data and vulnerable items

The following libraries are available:

Libraries	Description
NVD	List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics including exploits.
CWE	List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations screen, it is for reference only.
Third-party	List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs.

Related topics

View Vulnerability Response vulnerability libraries

Install the Solution Management for Vulnerability Response application

Before you can use the Solution Management for Vulnerability Response feature of Vulnerability Response in your instance, you must complete the installation of the Vulnerability Solution

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Management application. This application is available as a separate subscription in the ServiceNow Store.

Before you begin

Complete the following setup checklist prior to installation. Perform these setup tasks for a smooth installation.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

The Microsoft Security Response Center Solution Integration and Red Hat Solution Integration are the solution applications available in Solution Management for Vulnerability Response after you install Vulnerability Solution Management.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	Solution Management for Vulnerability Response requires the Vulnerability Response application. For the most current version of Vulnerability Solution Management, verify you have the most current version of Vulnerability Response installed. See KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes. If the application is not installed and activated see, Install Vulnerability Response.
Verify that you have entitlement to the application.	To verify you have entitlement to the Vulnerability Solution Management application, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. To get entitlement for the Vulnerability Solution Management application from the ServiceNow Store and download it onto your ServiceNow AI Platform instance, see Get entitlement for a Security Operations product or application.
Ensure that your NVD records are up-to-date for the last 10 years.	See Importing data with the NVD and CWE integrations and managing third-party libraries.
Ensure your third-party vulnerabilities are up-to-date.	See Vulnerability Response integrations for information on third-party vulnerability integrations.
Verify that you have the required ServiceNow AI Platform roles assigned for your instance.	The following roles are required for installation and verification of expected results: Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
	application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response. • The system administrator [admin] installs the application. If not already assigned, the admin assigns the vulnerability admin [sn_vul.vulnerability_admin or sn_vul.admin (deprecated)] role. • The vulnerability admin oversees configuration and verifies expected results.

Roles required: admin to install the Vulnerability Solution Management application and vulnerability admin to configure it.

Procedure

1. Navigate to the ServiceNow Store.
2. Click **Log in** and enter your HI credentials.
3. Click the **ServiceNow Products** tab to view the available ServiceNow products.
4. Click plus (**+**) sign next to **Vulnerability Solution Management** to view all the associated applications that you are eligible for.
5. Click **Opt-in** to verify you have entitlement to Vulnerability Solution Management to the application.
6. If you already have entitlement, skip to step 10 to install the application on your ServiceNow AI Platform instance.
7. Select the check box and click **Accept** to agree to the terms and conditions at the prompt.
   A message is displayed that indicates you have successfully opted-in for the application.
8. **Optional:** Click Manage Entitlement if you want to manage your entitlement for Vulnerability Solution Management on other ServiceNow AI Platform instances.

   Note: If the **Manage Entitlement** button is not displayed, click the **Vulnerability Solution Management** application on the Product List to display it.

   a. Choose an option

   b. Click **OK** or **Cancel** to continue.
   You are ready to activate plugins and install the application on your instances.

9. Log in to the ServiceNow AI Platform instance that you want to install the Vulnerability Solution Management application on.
10. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
11. Locate the Vulnerability Solution Management application (sn_vul_solution) and click **Install**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Application installation dialog displays the application dependency plugin status. Any required dependencies not already installed are automatically installed along with the application.

12. Click **Install**.
    This installation may take some time. A message is displayed in the Install dialog box after the application and its dependencies are successfully installed.

    The vulnerability admin can now configure the application from within the Setup Assistant.

13. Click **Close**.

    The Microsoft Security Response Center Solution Integration and Red Hat Solution Integration are the solution applications available in Solution Management for Vulnerability Response after you install Vulnerability Solution Management.

    View the Vulnerability Solutions by navigating to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations**. See Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant for more information.

What to do next

After you configure the application and the available solutions, check that the CVEs and Solutions agree using Vulnerability Solution [sn_vul_m2m_vulnerability_solution] table.

Install and configure the Performance Analytics for Vulnerability Response [PA] application

Before you can use the Performance Analytics for Vulnerability Response application, you must get entitlement and download the application from the ServiceNow Store, install it on your ServiceNow AI Platform® instance, and complete a few installation and configuration steps. The PA application is not installed as part of the Vulnerability Response application. It is available as a separate subscription.

Before you begin

If you already have the application on your instance and you are updating to a newer version of the application, proceed to step 8 in the following steps to continue with the update and configuration.

For a fresh installation, complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

To verify that plugins and applications are installed and activated, navigate to **All** > **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response dependencies plugin (com.snc.vul_dep) is installed and activated.	**Vulnerability Response Dependencies** This plugin contains all the dependency plugins required to support the application. To verify that the plugin is installed and activated, in your

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

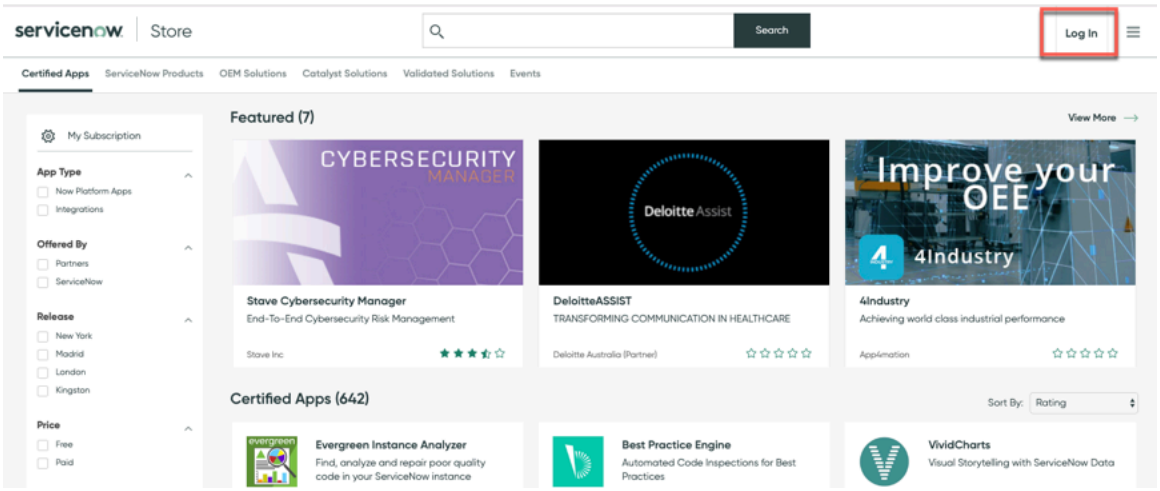
Setup tasks	Description
	instance you want the application navigate to **System Applications** > **All Available Applications** > **All**. If you are prompted to update other dependency plugins, Click the links in the dialogs and follow the prompts to continue.
Verify that the ServiceNow Vulnerability Response application (sn_vul) is installed and activated.	**Vulnerability Response** To verify that the plugin is installed and activated, in your instance you want the application navigate to **System Applications** > **All Available Applications** > **All**. If you are prompted to update other dependency plugins, Click the links in the dialogs and follow the prompts to continue. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.
Verify that you have the required ServiceNow roles for your instance. Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.	The following roles are required for installation, configuration, and verification of expected results: • The Performance Analytics Admin [pa_admin] or the system [admin] installs the application and verifies the expected results. • The Vulnerability Admin [sn_vul.vulnerability_admin or sn_vul.admin (deprecated)] oversees configuration and verifies expected results with the PA dashboards. • The Remediation Owner [sn_vul.remediation_owner] oversees change management tasks and reads and updates assigned records. The sn_vul.remediation_owner role is also automatically assigned when any user is assigned the itil role.
Verify the Performance Analytics and Vulnerability Response applications are compatible.	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Role required: admin or pa_admin

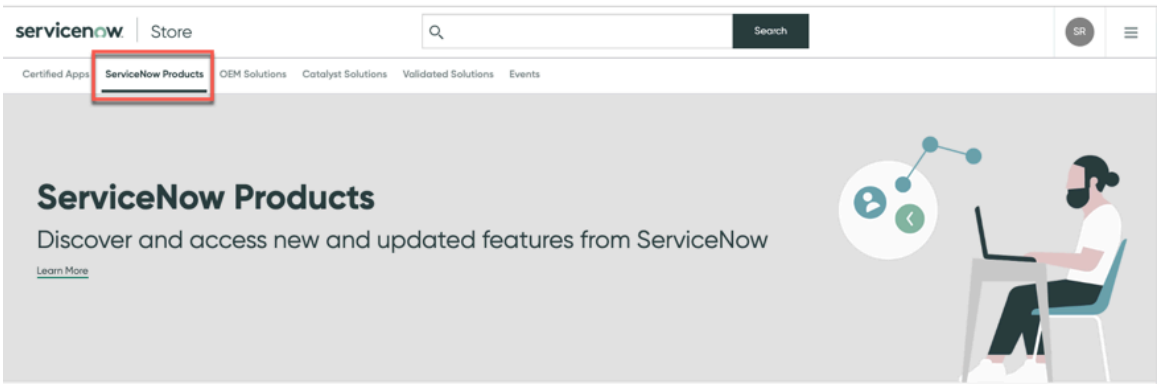
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To get entitlement and download the application on your ServiceNow AI Platform instance, navigate to the ServiceNow Store.
2. In the upper right of the page, click **Log in**.



3. In the dialog that is displayed, enter your HI credentials and click **Login**.
4. On the page that is displayed, if not selected, click the **ServiceNow Products** tab.

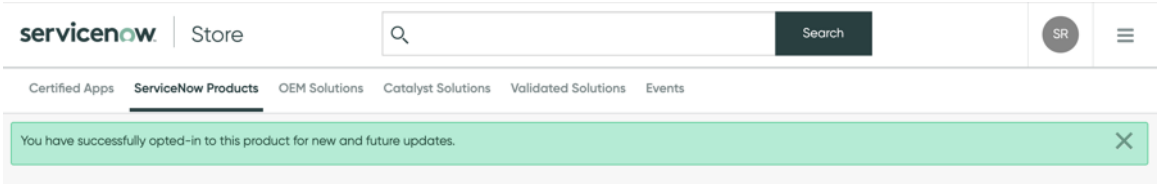


5. On the product list page, click **Performance Analytics - Vulnerability Response**.



6. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
   A page with the Opt-in button is displayed.
7. To get the Performance Analytics for Vulnerability Response application, click **Opt-in**.
8. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

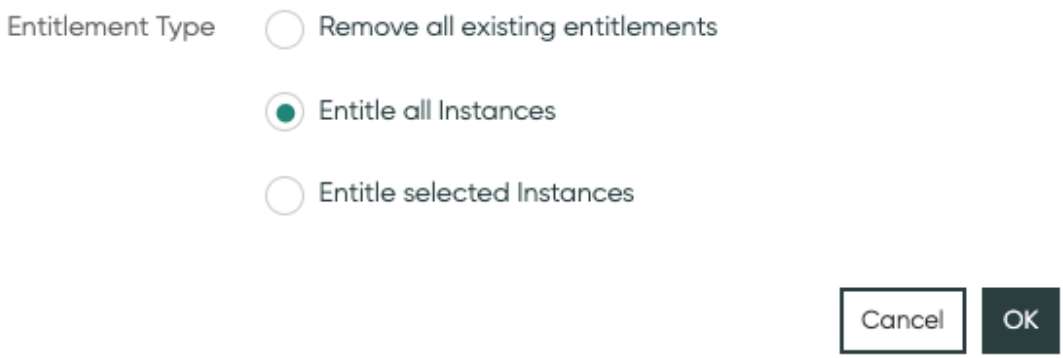


9. **Optional:** Alternatively, to manage your entitlement for the application on other ServiceNow AI Platform instances, follow these steps.

   a. If the Manage Entitlement button is not displayed, click the Performance Analytics for Vulnerability Response application on the Product List to display it.

   b. With the Eligible tab selected, click **Manage Entitlement**.

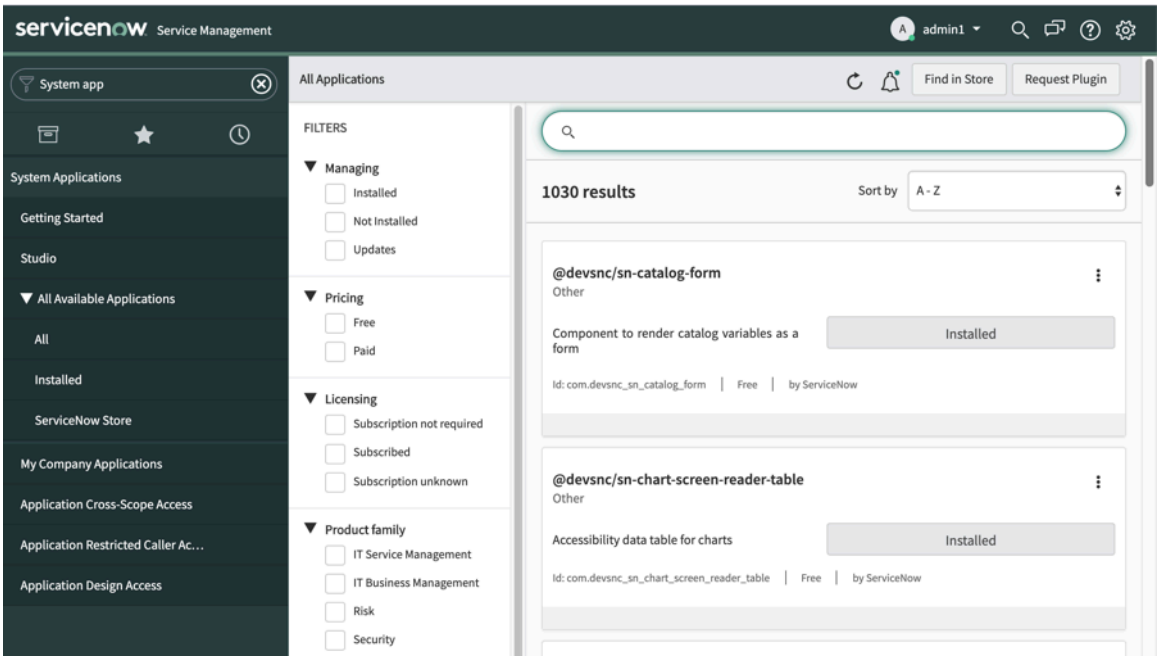
   c. In the Manage Entitlements for Vulnerability Response dialog that is displayed, choose one:



   d. Click **OK** or **Cancel** to continue.
   You are ready to activate plugins and install the application on your ServiceNow AI Platform instance(s).

10. Log in to the ServiceNow AI Platform instance that you want to install the Vulnerability Response application on.
11. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



12. From the applications listed, locate the Performance Analytics - Content Pack - Vulnerability Response (sn_vul_analytics) application and click **Install**.

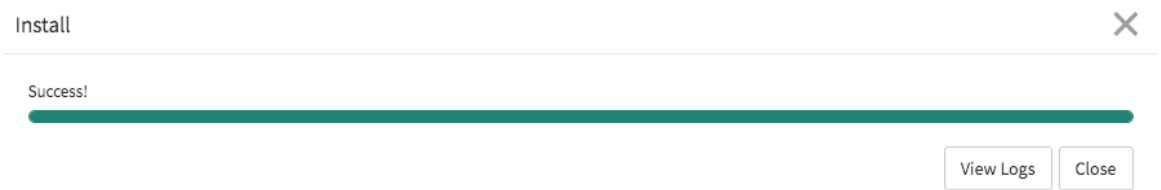
    Note: If you are updating to a new version, select the version you want from the choice list.

    and click **Update**.
    The Application installation dialog is displayed. Any dependencies that will be installed automatically with the application are also displayed.

13. **Optional:** If you want demo data, select the Load demo data check box and click **Install**.

    Note: If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Workaround to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.

    This installation may take some time. A message is displayed in the Install dialog after the application is successfully installed.



14. Click **Close**.

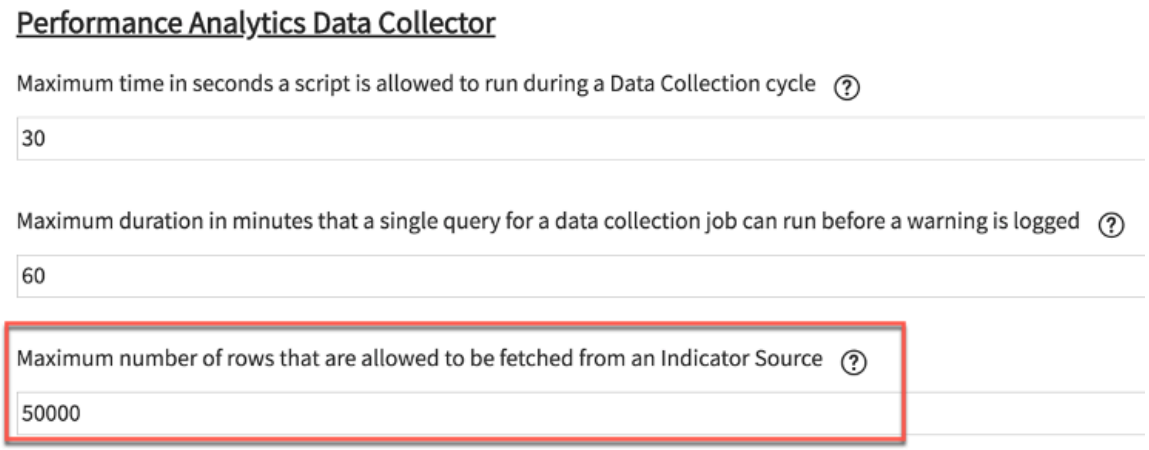
15. **Optional:** If you anticipate a large number of active vulnerable items in your environment, you may prefer to change the default setting for the maximum number of collected records, enable scheduled jobs, and set collection times during off-hours.
    To change these and other settings for the application after it is installed, follow these steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **All** > **Performance Analytics** > **Admin console**.

b. On the Advanced Configuration tile, click the **Performance Analytics Properties** link.

c. On the Admin Console [Performance Analytics] page, scroll to the Performance Analytics Data Collector section.
The default setting (50,000 records) is displayed for the Maximum number of rows that are allowed to be fetched from an Indicator Source.

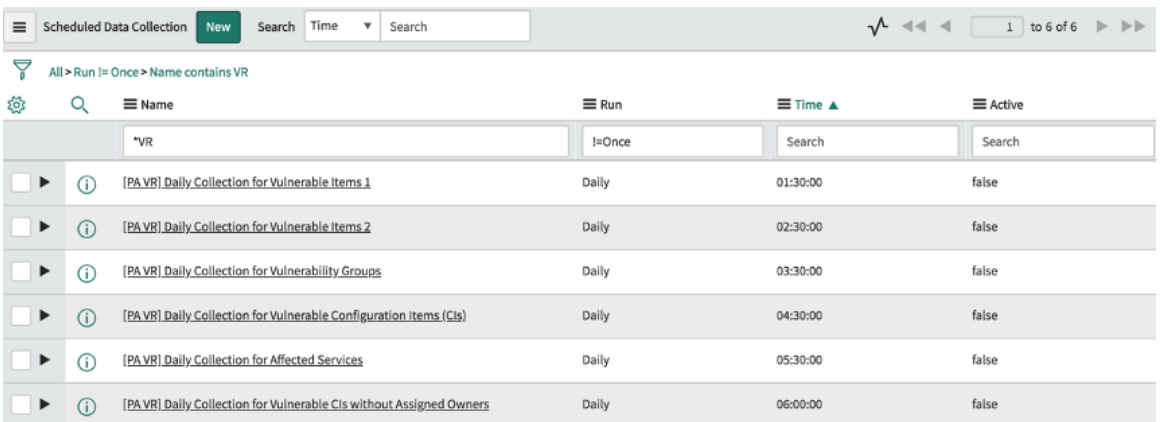


d. You may prefer to increase this number to a value that is roughly 20% more than the total number of active vulnerable items (VIs) you anticipate in your environment.

e. Click **Save**.

f. To activate scheduled jobs, navigate to **Performance analytics** > **Data Collector** > **Jobs**.
The Scheduled Data Collection list is displayed. In the Active column, the scheduled jobs listed in the Application column for Performance Analytics - Content Pack - Vulnerability Response by default are disabled (`false`).

Note: a scheduled job for historical data collection is not displayed on the list of jobs. For large sets of data, you may prefer to start collecting data and trends over time by enabling your daily jobs when you are setting up the Performance Analytics for Vulnerability Response application.

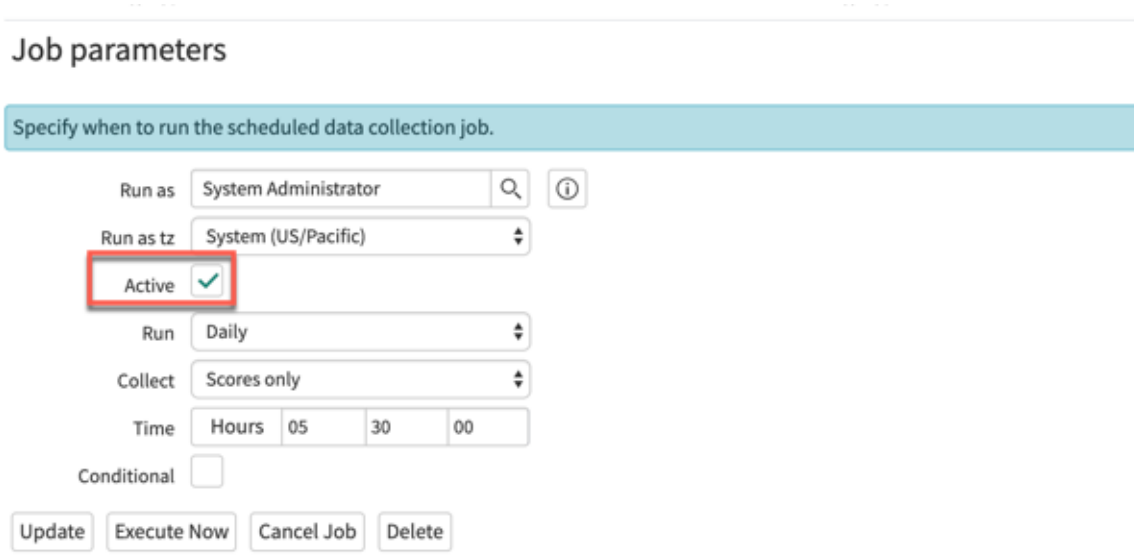


g. In the Name column, click a link to open a PA_VR job record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

h. If fields are not editable, click the **here** link to edit them.

i. In the Job parameters section, click the Active check box to schedule a job.
The Time fields are displayed.



j. Enter the start time for the job.
If you anticipate a large volume, you may prefer to set collection times during off-hours. If you anticipate 10 million active VIs or greater in your environment, contact your ServiceNow® implementation partner for more information on setting up your data collection environment.

For more information about the indicators used for data collection, see View the Performance Analytics indicators for Vulnerability Response [PA].

k. After you have enabled all the jobs you want, click **Update**.
The Scheduled Data Collection list is displayed. For more information, see Performance Analytics properties.

What to do next

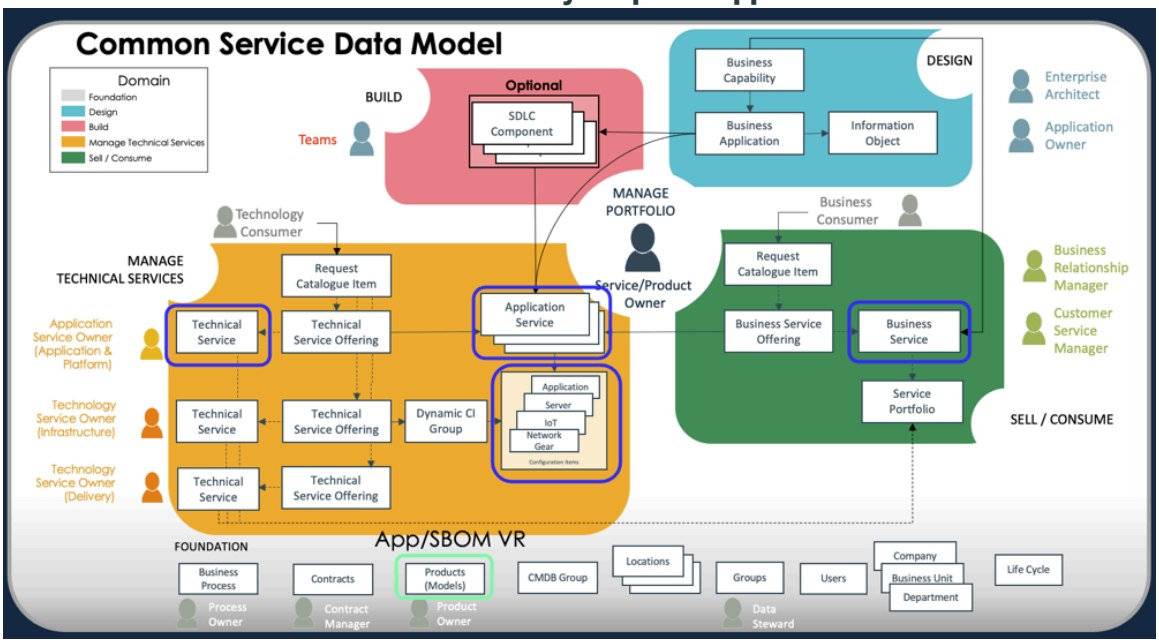
Navigate to **Vulnerability Response** > **Overview** to view the dashboard.

Vulnerability Response applications and CSDM tables

The Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications manage (contribute data to) CSDM tables. These applications also use data from CSDM tables that other applications generate. Several ServiceNow products, therefore, benefit from and add value to these Security Operations applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The CSDM data framework and Vulnerability Response applications



CSDM tables referenced by Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications

As assets are imported from third-party vulnerability scanners (integrations), they are brought into Vulnerability Response and represented in specific tables:

- Host Vulnerability Response Discovered Items.
- Cloud and Container Vulnerability Response discovered images
- Application Vulnerability Response Discovered Applications (product model)

As part of the Security Operations CMDB configuration item (CI) look up, a search is performed to match a (CI) record from imported data with existing records in the CMDB.

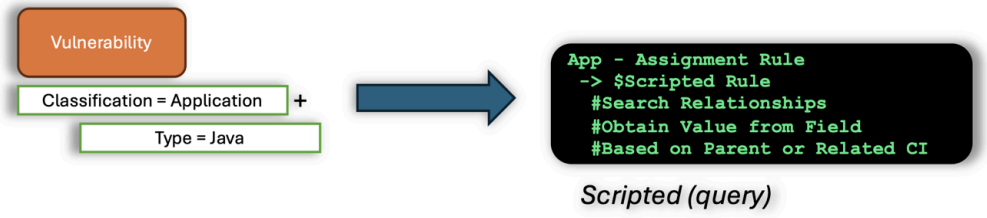
Each specific CI Record may contain non-discoverable attributes, for example, Support Group, or Classification, that are populated on the CI that can be used as input for vulnerable item assignment Rules. These attributes might be populated from Common Service Data Model (CSDM) synchronizations based on upstream Technical Service Offerings.

If you want to leverage related CSDM objects for Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications, you need to use scripted rules.

For example, to automatically assign vulnerable items for remediation using vulnerable item assignment rules, you might create a rule that leverages configuration item Classification values as they are updated on imported vulnerability entries. For this case, you need a scripted rule to query the target value you want from the related CSDM object.

Below is an example of a scripted query that you might use to see if a CI has Java and is tied to a vulnerability entry.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications reference the following tables. Refer to the CSDM data framework and Vulnerability Response applications image for more information.

- The Product Model [cmdb_model] table (referenced by Application Vulnerability Response and Software Bill of Materials).
- The Application Model [cmdb_application_product_model] table (referenced by Application Vulnerability Response and Software Bill of Materials).
- The Configuration Item [cmdb_ci] table.
- The Business Service [cmdb_ci_service_business] table.
- The Service [cmdb_ci_service] table.
- CMDB Group [cmdb_group] table.
- Dynamic CI Group [cmdb_ci_query_based_service] table.

CSDM tables used by Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications

1. Product Model [cmdb_model] table (used by Application Vulnerability Response and Software Bill of Materials).
2. Application Model [cmdb_application_product_model] table (used by Application Vulnerability Response and Software Bill of Materials).
3. The Configuration Item [cmdb_ci] table.
4. Business Application [cmdb_ci_business_app] (used by Application Vulnerability Response and Software Bill of Materials).
5. Business Service [cmdb_ci_service_business].
6. Technical service [cmdb_ci_service_technical].

Note:

When you upload Software Bill of Materials files, the SBOM applications try to match any Product Model and Business Applications you upload to those that already exist in your CMDB. You can link application services or business applications to a product model.

Products that add value to Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications

Using the Vulnerability Response applications with the following ServiceNow products can benefit your organization.

Third-party vulnerability scanners and integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Imported vulnerabilities from the National Vulnerability Database (NVD) and detection data from third-party scanners are reconciled with the assets in your CMDB. When an imported vulnerability matches an existing asset, a vulnerable item is created. Vulnerable items are grouped automatically into tasks for remediation, risk-scored with business context, prioritized and assigned to appropriate teams for remediation. For more information and a list of integrations see Vulnerability Response integrations.

The CWE Comprehensive 2000 and NVD Integrations

Imported data from the NIST National Vulnerability Database (NVD) and Common Weakness Enumeration (CWE) integrations is used to enrich the vulnerability data in your instance and help you decide whether to escalate remediation for a vulnerability, vulnerable item, or remediation task. See Understanding the NVD integrations and Configure and run the scheduled job for updating CWE records for more information.

Products that benefit from integration with Software Bill of Materials

Security Posture Control

Security Posture Control enables cybersecurity teams to get visibility into their complete enterprise asset inventory and determine their overall security posture. Policies in SPC can help you detect assets with vulnerability that you import with the Vulnerability Response applications to help you locate security tool coverage gaps.

Governance, Risk, and Compliance

Connect security and IT with an integrated risk program offering continuous monitoring, prioritization, and automation.

DevOps

Protect your environments from potentially harmful components during software development cycles with GitHub Actions that you initiate from your GitHub environment. Upload SBOM files to the ServiceNow AI Platform from your GitHub repositories.

Create or edit Vulnerability Response assignment rules

After you complete your initial assessment of assignment rules using Setup Assistant, you can create rules to automatically assign vulnerable items based on filter conditions. These rules assign vulnerable items as they are imported or manually created.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

The base system ships with one vulnerability assignment rule, **Assign to CI support group**, which assigns vulnerable items to the same assignment group as the CI support group. This rule can be modified using filter conditions or you can create a new rule. With assignment rules, you define the condition(s) of assignment and the order of execution. Once a VI matches a rule condition, the assignment lookup stops.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Assignment Rules**.
2. Open the **Assign to CI support group** rule or click **New**.
3. If **New**, fill in the fields on the form, as appropriate.

Vulnerability Assignment Rule

Field	Description
Name	Name of the group rule.
Active	Indicates whether the assignment rule is active.
Execution order	Order in which the rules are evaluated. High priority rules, items that need special handling, where risk is critical, or a VI should be handled by regulatory compliance, to be run first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign VIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.
Description	Description of the assignment rule.
Condition	
Preview	Shows how many results this query will return.
Condition fields	Conditions that must be met. **Note:** To make Rapid7 InsightVM asset tags available for use in the Condition filter for Assignment Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations. Case sensitivity for the search text you enter in the condition builder is not supported on this record or form.
New Criteria	Adds more condition filter fields to choose from.
Assign using	To automate the assignment of groups created based on this rule, choose one of the options available. ○ User group: Select a user group from the lookup table. ○ User group field: Select a user group field from the drop-down menu. ○ Script: Create or edit a script. **Note:** Creating or edit a script requires ServiceNow expertise.

4. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

New or updated rules are evaluated on the next import.

Note:

The reapply feature requires a baseline application of the rules. Once your rules are created, if you haven't already done so, activate the *Reapply all vulnerability assignment rules* scheduled job to execute, at your convenience. It applies all the rules to all Open VIs except those manually assigned. Depending on how many active VIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

If you haven't run this scheduled job, when you try to use the **Apply Changes** button on the Assignment Rules form, you will have to do it then. Reapplying assignment rules does not regroup the vulnerable items.

Create a Vulnerability Response assignment rule using ML

Use the following script to create a catch-all assignment rule for vulnerable items that uses ML recommendations from Predictive Intelligence to automatically assign them for remediation.

Before you begin

The Vulnerability Assignment Recommendations for Vulnerability Response application must be installed and activated. This application is available on the ServiceNow Store.

A classification solution must be defined, active, and trained. You use this model to help you predict the appropriate assignment group for vulnerable items (VI)s in cases when your assignment rules did not find a correct match for the intended recipients.

This rule might help you reduce the number of unassigned VIs after other assignment rules have already completed.

See Install Vulnerability Assignment Recommendations for Vulnerability Response and Create and train a solution definition for Vulnerability Response for more information.

Role required: sn_vul.vulnerability_admin

About this task

You might prefer to perform this task only if you have advanced coding experience, or you have in-depth knowledge about the ServiceNow AI Platform, its Predictive Intelligence features, and how assignment rules work.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Assignment Rules**.
2. Select **New**.
3. Fill in the fields on the form, as appropriate.
   See Create or edit Vulnerability Response assignment rules for more information about these fields.
4. From the Assign using choice list, select **Script**.
5. In the editor, copy and paste the following script.

```
    /*
    * Catch-all assignment rule using ML recommendation
    * NOTE: Requires Vulnerability Assignment Recommendations
for Vulnerability Response
    * Classification Solution must be active and trained
    */
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
    var ARU = new sn_vul.AssignmentRecommendationUtils();
    ARU.initialize();

    var viPredictionObj =
 ARU.getPredictionsForVI(vulnerableItemSysId);
    /*
    *returns object containing array of predictions
    *payload structure:
    *
    {
        "predictions": [
            {
                "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
                "name": "Windows Server support ",
                "confidence_score": "57.54"
            },
            ...
        ],
        "exception": ""
    }
    */
    var viPredictionArray = viPredictionObj['predictions'];
    var topPredictionObj = viPredictionArray.shift();

    return topPredictionObj['sys_id'];
}
```

6. Select **Submit**.

What to do next

Review Vulnerability Response assignment rules overview for more general information about assignment rules and the *Reapply all vulnerability assignment rules* scheduled job.

Create a Vulnerability Response assignment rule for service support

Use the following script to create a rule that assigns vulnerable items for remediation based on the business services they impact.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

You might prefer to perform this task only if you have advanced coding experience, or you have in-depth knowledge about the ServiceNow AI Platform and how assignment rules work.

With this rule, VIs are assigned according to how closely they match to the business services listed in your CMDB. If no related services, departments, or support groups are matched, VIs are assigned to the Vulnerability Analyst group.

This rule might help you reduce the number of VIs that are incorrectly assigned or remain unassigned after other assignment rules have already completed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Assignment Rules**.
2. Select **New**.
3. Fill in the fields on the form, as appropriate.
   See Create or edit Vulnerability Response assignment rules for more information about these fields.
4. From the Assign using choice list, select **Script**.
5. In the editor, copy and paste the following script.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related
 Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
    var ci = vitGR.getValue('cmdb_ci');
    var defaultAssignmentGroup = 'Vulnerability Analyst';
    var defaultGR = new GlideRecord('sys_user_group');
    defaultGR.get('name', defaultAssignmentGroup);
    var defaultAssignmentGroupID = defaultGR.sys_id;

    var maxSizeValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_b
y_CI_max_size", 1000);
    var maxDepthValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_b
y_CI_max_depth", 10);
    var customValues = {
        "maxDepth": maxDepthValue,
        "maxSize": maxSizeValue
    };
    var ciu = new global.CIUtils();
    var services = ciu.servicesAffectedByCI(ci, customValues);
    var svc = new GlideRecord("cmdb_ci_service");
    var hasSvc = false;
    if (services && services.length > 0) {
        svc.addQuery("sys_id", "IN", services.join(",")); //
 returns the service with highest business criticality.
 Implement alternate logic here.
        svc.addNotNullQuery("busines_criticality"); // typo
 intended
        svc.orderBy("busines_criticality");
        svc.setLimit(1);
        svc.query();
        hasSvc = svc.next();
    }
    if (!hasSvc) {
        // If there are no services it should be assigned to a
 default assignent group
        return defaultAssignmentGroupID;
    } else {
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
        var serviceAssignmentGroup =
 hasSvc.getValue('support_group'); //Also consider
 managed_by_group, assignment_group, change_control
        return !gs.nil(serviceAssignmentGroup) ?
 serviceAssignmentGroup : defaultAssignmentGroupID; //Return
 the Service assignment group if it is not empty, return the
 default assignment group otherwise.
    }
}
```

6. Select **Submit**.

What to do next

Review Vulnerability Response assignment rules overview for more general information about assignment rules and the *Reapply all vulnerability assignment rules* scheduled job.

Create or edit Vulnerability Response remediation task rules

After you complete your initial assessment of remediation task rules using Setup Assistant, you can create rules to automatically group vulnerable items based on filter conditions. These rules automatically group vulnerable items as they are imported or manually created. Use the filter to limit the vulnerable items grouped by this rule, such as selecting all vulnerable items with exploits.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task

The base system ships with one remediation task rule, **Vulnerability**, which groups vulnerable items by vulnerability and assignment group (from **Assignment Rules**). You can reapply the rules from the form or list view. For some sample entries, Vulnerability Response remediation task rule examples.

This rule can be modified as follows:

By using filter conditions and Group by choices.

By default, remediation tasks use **Assignment Rules**, when available, as part of their filter criteria.

Note: If no assignment rules exist, you can select a group using the **User group** field.

Starting with version 18.0 of Vulnerability Response, the **Vulnerability** remediation task rule is deactivated in Vulnerability Response for new implementations.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Remediation Task Rules**.
2. Open the rule or click **New**.
3. If **New**, fill in the fields on the form, as appropriate.

Remediation Task Rule

Field	Description
Name	Name of the task rule.
Active	Indicates whether the task is active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Description of the rule.
Case sensitive	Determines whether a condition is case sensitive or not. **Note:** The default value is case insensitive.
Condition	Optional filter conditions for the rule. **Note:** To make Rapid7 InsightVM asset tags available for use in the Condition filter for Remediation Task Rules, you must run the Rapid7 InsightVM Asset List integration before the other Rapid7 InsightVM integrations. By default, (**Case sensitive** check box disabled), the search text you enter in the condition builder on task rules records and forms is not case-sensitive. You have the option to enable case-sensitive searches on task records and forms.
Group by (up to six condition sets are available)	
Group vulnerable items from	The table the rule uses to group VIs. You can have up to six filters. Choices are: ○ Vulnerable Item [sn_vul_vulnerable_item] ○ Vulnerable Item → Configuration Item [cmdb_ci] ○ Vulnerable Item → Vulnerability [sn_vul_third_party_entry] **Note:** If you choose an extended table, the **Using field** is applied only for vulnerable items that use that extended table.
Using field	Field on the table that the rule uses to group VIs.
Assignment	
Assign remediation tasks by	When automatically assigning remediation tasks, the Assignment choice is used in addition to the **Group By** choices to group the vulnerable items. New tasks are created, as needed, to ensure that each vulnerable item is placed in a task with a matching assignment group set. To automate the assignment of tasks created based on this rule, choose one of the options available. ○ Group by field: If you selected any user group field from the **Using field** values in the **Group by**section, they appear in the drop-down menu. ○ User Group: Use the lookup list to select a static user group.

Note: If you change your mind about any of the **Group by** settings, the **Clear group by fields** related link resets the **Group by** fields on the form.

When a group rule is deleted, from the form or list view, you have the option to delete all **Open** groups created by that rule. Groups not in the **Open** state are excluded.

For some sample entries, see Vulnerability Response remediation task rule examples.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define fields and weights for the risk rule for Vulnerability Response Risk Calculators

Customize the parameters and weights for the risk rule so that you can generate risk scores that use the vulnerability and asset data that are unique to your organization. By selecting the fields that are included in the risk rule, you can define an effective risk scoring framework.

Before you begin

Additionally, you can use attributes in the configuration_item [cmdb_ci] in the Configuration Management Database (CMDB) to help you create logic for your Vulnerability Response risk calculators. If, for example, you determine that CIs that are external-facing in your organization are more vulnerable and might require immediate remediation, you can assign attributes such as *Internet Facing* for these CIs. This attribute, and others, are listed in the Common Service Data Model release notes for the Orlando family release. For current information and guidance on the CMDB, see the following topics:

- Common Service Data Model conceptual model
- CMDB schema model

Role required: sn_vul.manage_risk_score_configuration

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Calculators**.
2. On the Vulnerability Calculators page, select **Default Risk Calculator**.
3. Navigate to **Vulnerability Calculator page** > **Vulnerability Calculator Rules tab** > **Default Risk Rule**.
4. **Optional:** In the Risk Calculator Criteria section of the Vulnerability Risk Rule page, set the weight for each criterion according to its importance in the overall risk score calculation.
5. To deactivate the rule, you must clear the **Active** check box.
6. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
7. On the form, fill in the fields.

Risk rule field form

Field	Description
Choose reference table	Table that you use to define the risk score weightage. You can select one of these options: ○ **Vulnerable Item**: Add fields that are directly dot-walkable from the vulnerable item (VI). ○ **Vulnerable Item - Configuration Item**: Add dot-walkable fields that are part of the base table extensions, such as the Hardware table. These fields aren't part of the base table (cmdb_ci). ○ **Vulnerable Item - Vulnerability**: Add dot-walkable fields that are part of the tables that extend the base table, for example, Third-party Entry. These fields aren't part of the Vulnerability Entry base table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Vulnerable Item Reference Table**: Add fields that are a part of the Related tables (m2m) or tables that have a reference to the vulnerable item. These fields aren't directly dot-walkable from the VI. ○ **Configuration Item Reference Table**: Add fields that are a part of the Related tables (m2m) of cmdb_ci or tables that have a reference to cmdb_ci. These fields aren't directly dot-walkable from the VI. ○ **Vulnerability Reference Table**: Add fields that are a part of the Related tables (m2m) of sn_vul_entry or tables that have a reference to sn_vul_entry. These fields aren't directly dot-walkable from the VI. ○ **Custom Conditions**: Use this option to assign weights to the rule by evaluating the condition. For example, the Internet-facing filter determines if a configuration item (CI) is external or internal.
Table	Field that appears only when one of the following options is selected from the Choose reference table: ○ **Vulnerable Item -> Configuration Item** ○ **Vulnerable Item -> Vulnerability** ○ **Vulnerable Item Reference Table** ○ **Configuration Item Reference Table** ○ **Vulnerability Reference Table**
Field	Field to be used for risk score calculation for this rule.
Aggregation	Field that appears only when a reference table is selected from the Choose reference table. Select the minimum or maximum value to be considered for calculations when Field is selected from the Related tables (m2m).
Weight	Weightage of this field within the risk rule. The value must be an integer from 0 through 100.
Define Value Weightage	Component to assign weights to each field value. For numeric fields, field values can be defined as a range (for example, 1–5). The weights must be integer between 0–100. **Note:** This field doesn't appear if the Custom Conditions option is selected from the Choose reference table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Condition table	Field that appears only when Custom conditions is selected from the Choose reference table. Select a condition from the list.
Field name	Field that appears only when Custom conditions is selected from the Choose reference table. Enter a name for the risk criteria.
Condition	Field that appears only when Custom conditions is selected from the Choose reference table. Preview the items in this table that match the defined conditions.

8. Select **Submit**.
9. In the Rule page, activate and reapply the rule to reevaluate the risk score on the active vulnerable items.

Note: Starting with version 23.0 of Vulnerability Response, in case of:

- **Default Risk Calculator** rule: Whenever the risk score on a vulnerable item (VIT) changes, the following details are documented in the Notes section of the VIT:
  - Calculator group name
  - Calculator name
  - Field values that have a weightage greater than 1 and their risk score contribution.
  - Final risk score
- **Vulnerability Severity** risk rule: Whenever the risk score is updated on a VIT, the **Notes** section is updated with the following details:
  - Calculator group name
  - Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, select any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If **Template** is selected, the risk score is updated according to the specified condition in the rule. If **Script** is selected, you can either add or update the existing script.

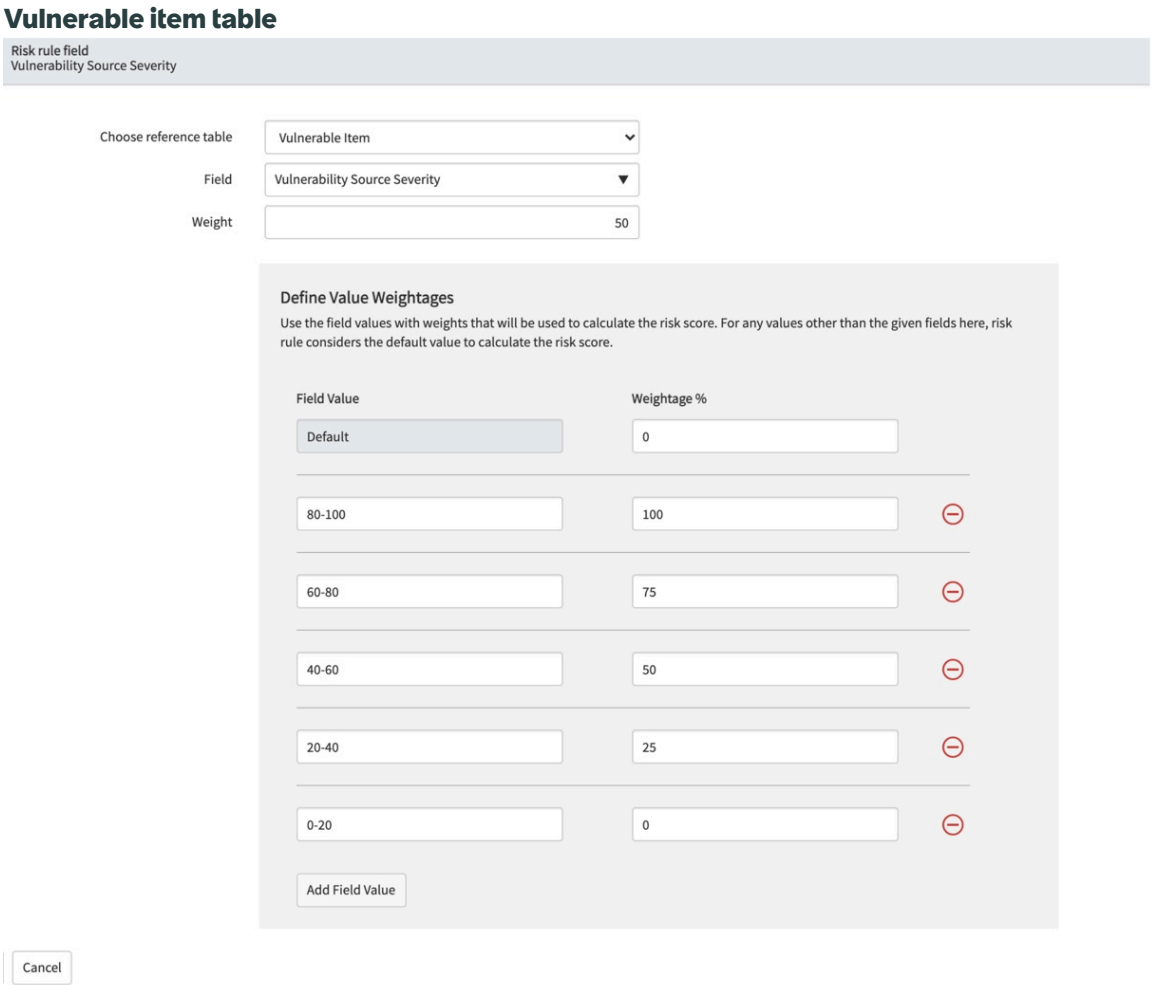
Example:
Example 1: Add a source severity as a criterion for a risk rule.

Use case: Third-party vendors, like Qualys and Tenable, provide their own scores. These scores are populated in the **Source Severity** field on the sn_vul_entry table. Use this field for risk score calculations. To use this score to compute the risk score, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Vulnerable item**.
5. From the Field list, select **Vulnerability.Source Severity**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
7. In the Define Value Weightage section, add field values, and assign a weight to them.



8. Select **Submit**.

Example 2: Add a business criticality as a criterion for a risk rule.

Use case: Let's assume your organization has many business services. The configuration item (CI) LINUX-SF-6381 is being used by the following services:

Criticality of the business services

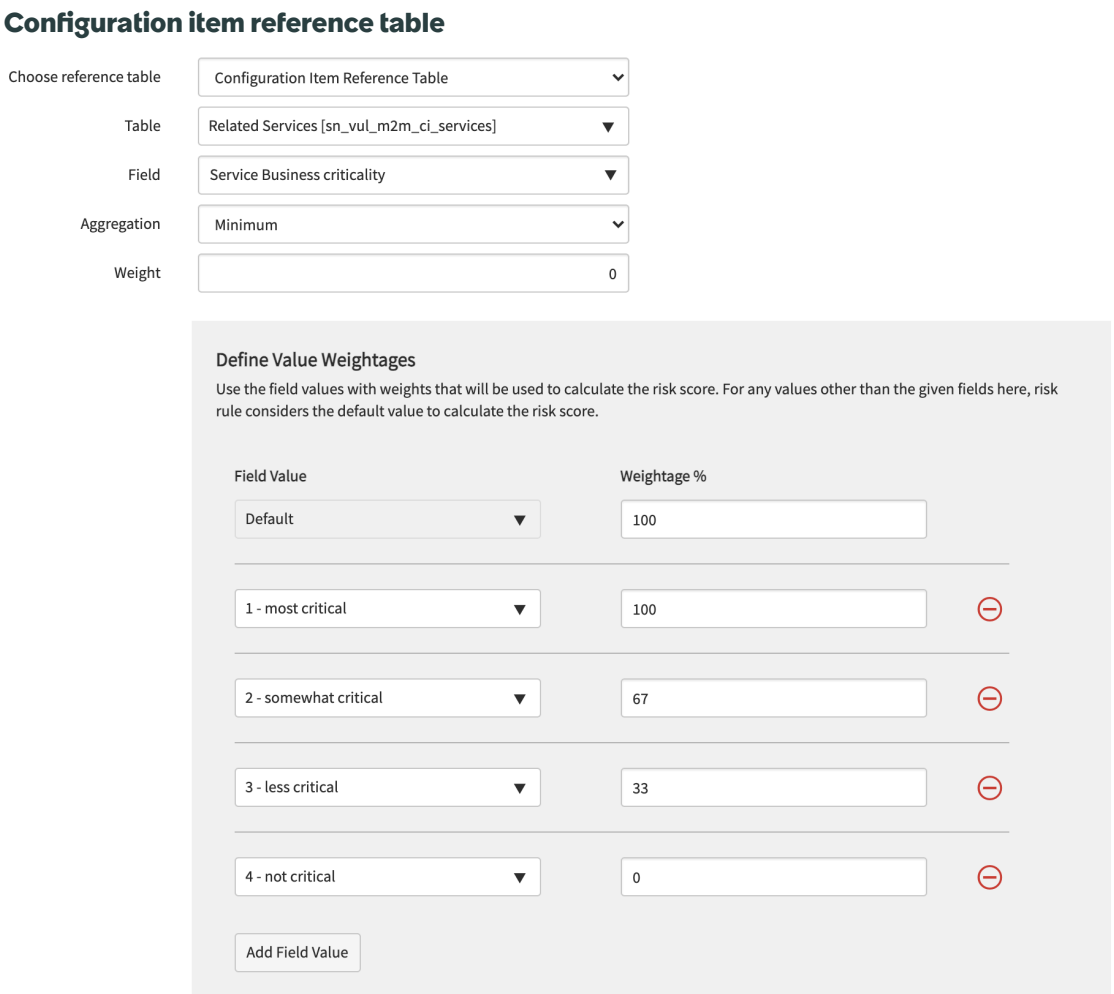
Business service	Criticality
Cloud Management	1 - Most critical
E-Commerce	2 - Somewhat critical
Client services	3 - Less critical
Travel and Expense	4 - Not critical

The mapping between the CI and services is stored in the Related Services [sn_vul_m2m_ci_services] table. When a vulnerability is found in the asset LINUX-SF-6381, a vulnerable item (VI) is created. You can use the value of the business criticality from the affected

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

services to compute the risk score for this VI. To use the criticality value of these services to compute the risk score, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Configuration Item Reference Table**.
5. From the Table list, select **Related Services [sn_vul_m2m_ci_services]**.
6. From the Field list, select **Service.Business criticality**.
7. In the **Aggregation** field, select **Minimum** to retrieve the most critical service for this use case (**1- Most critical** value) or Maximum to retrieve the least critical service for this use case (**4 – Not critical** value) for this use case.
8. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
9. In the Define Value Weightages section, add field values, and assign a weight to them.



10. Select **Submit**.

Example 3: Add a conditional criterion to the risk calculator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

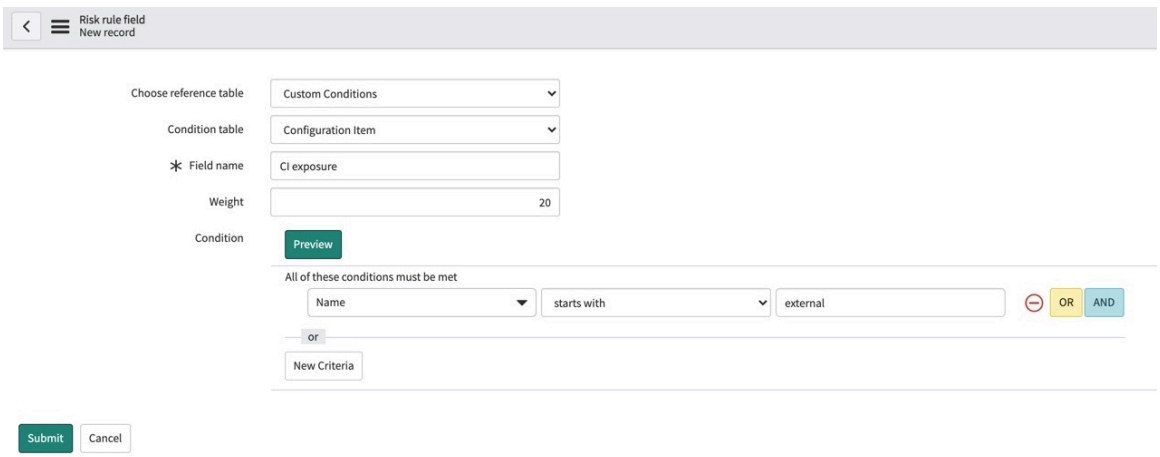
Let's assume that an organization has multiple configuration items (CIs), of which only a few can be accessed by an external user. Users can add risk score weightages for these outward-facing CIs.

Note: You can identify these CIs by their name. The names start with 'external'.

To add a conditional criterion to the risk rule, do the following:

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, select **Add criteria**.
4. From the Choose reference table list, select **Custom conditions**.
5. From the Condition table list, select **Configuration item**.
6. In the **Field name** field, enter the name **CI Exposure**.
7. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
8. In the **Condition** field, select **Name** > **starts with** and enter the value **external**.

Custom conditions for the new risk rule



9. Select **Submit**.

Note: Adding conditional criteria to your risk rule might degrade performance.

Related topics

Vulnerability Response calculators and vulnerability calculator rules

Create a Vulnerability Response calculator

Filtering within Vulnerability Response

Vulnerability Response Rollup Calculators

After your initial assessment of risk calculators in the Setup Assistant, use the vulnerability rollup calculators to configure how the cumulative risk score is computed for remediation tasks and imported vulnerabilities.

Use the vulnerability rollup calculators to configure how the cumulative risk score is computed for remediation tasks and imported vulnerabilities. The following rollup calculators are shipped with the base system:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- *Remediation Task Rollup*: Rolls up the risk scores for all vulnerable items in a remediation tasks, to provide an overall risk score for the entire group of vulnerable items.
- *Patch Update Rollup*: Rolls up the risk scores for all vulnerable items with same patch update, to provide an overall risk score for the patch update.
- *Organization Risk Score Rollup*: Rolls up the risk scores for all host vulnerable items, application vulnerable items, container vulnerable items and configuration issues in an organization, to provide an overall risk score for the entire organization in unified dashboard.

  Note: Starting with v22.0 of Vulnerability Response, you can configure rollup weights for organizational score. Also, individual roll-up calculators have been removed.

- *Vulnerable Item Rollup*: Rolls up the risk scores for all host vulnerable items in an organization, to contribute to the overall risk score of the entire organization for unified dashboard.
- *Vulnerability Entry Rollup*: Rolls up the risk scores for all vulnerable items with the same vulnerability entry, to provide an overall risk score for the vulnerability entry.
- *Rollup EPSS Scores from NVD to TPEs*: Rolls up the EPSS scores for all vulnerable items/ CVEs listed on the NVD table to existing TPEs, to provide an overall probability of the vulnerability being exploited.
- *Remediation Effort Rollup*: Rolls up the risk scores for all the records in a remediation effort, to provide an overall risk score for the remediation effort.

Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Rollup Calculator**.

Configure the rollup calculator to specify how much weight to give each of those computed values in setting the cumulative risk score. The higher the weight, the more that value is used to determine the rolled up risk score in the vulnerability or remediation tasks.

Note: When **Include deferred** is selected, all deferred vulnerable items are included in the rollup calculation for the remediation tasks. Be sure that you understand the impact on the total calculation before selecting this option.

Rollup calculators run the scheduled job, **Rollup VI values to vulnerability, Remediation Task (RT), and VI count on RT**, every 15 minutes to pick up changes and roll up the details and risk scores to remediation tasks and vulnerabilities. These scheduled jobs also calculate cumulative values for the number of VIs, maximum risk score, remediation target date, and status for remediation tasks.

Note: Calculated values for vulnerability entries do not include remediation target data.

The risk score is calculated when:

- The risk score, remediation target, remediation status, or vulnerability changes on the vulnerable items.
- The vulnerable item state changes to Open, Deferred, Closed, or changes from Closed or Deferred.
- Vulnerable items are deleted.
- Vulnerable items are added or removed from the remediation task.

Vulnerability rollup calculator example: Consider a remediation task VUL324567, which has the following vulnerable items:

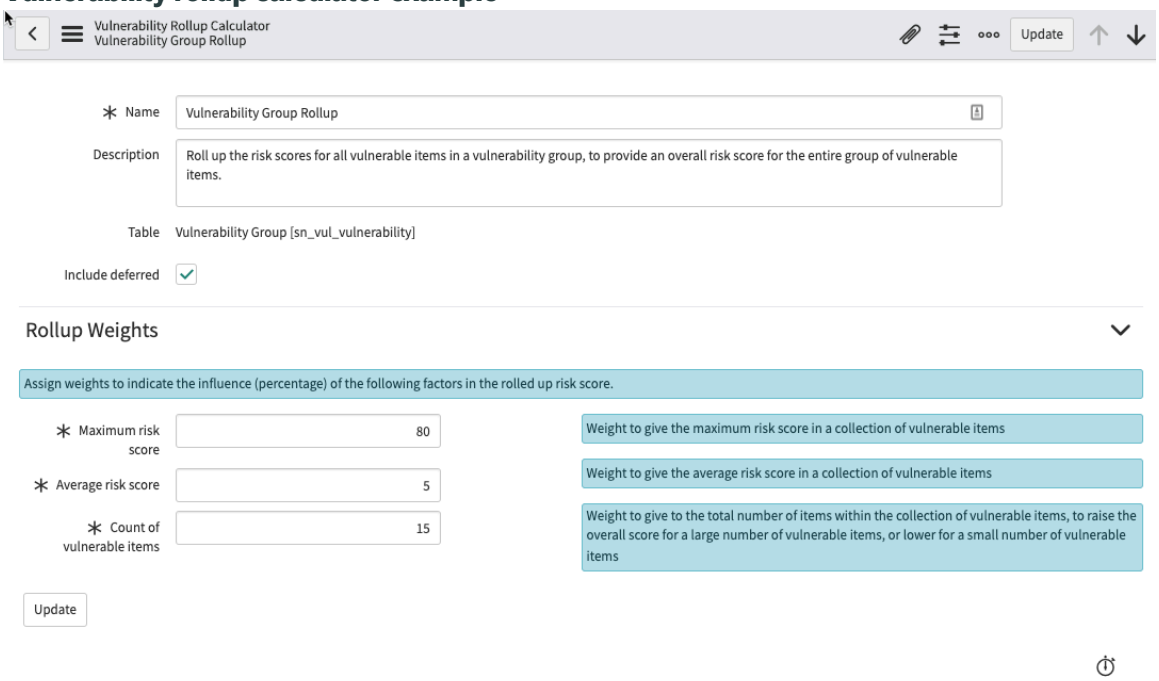
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- VIT1001 with risk score of 30
- VIT1002 with risk score of 40
- VIT1003 with risk score of 50

Also, consider the following weights in the vulnerability rollup calculator:

- Maximum risk score: 80
- Average risk score: 5
- Count of vulnerable items: 15

Vulnerability rollup calculator example



In the Vulnerability rollup calculator example, the formula for determining the remediation task **Risk Score** is:

(**Maximum risk score**/100) * 80 + (**Average risk score** /100) * 5 + (factor * 15)

The factor is determined as follows:

VI count	Factor
<10	0.2
10-100	0.4
101-1000	0.6
1001-10000	0.8
> 10000	1

So, for the remediation task, VUL324567:

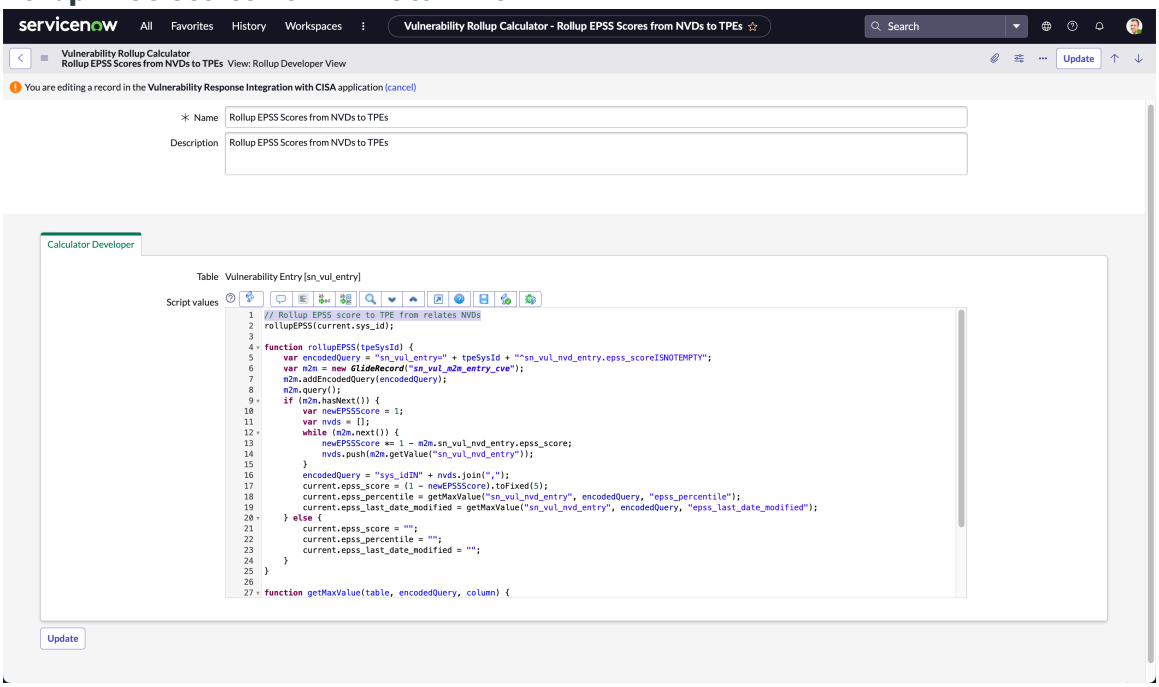
- Average risk score is 40
- Maximum risk score is 50

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- 50 (Maximum risk score)
- Factor is 0.2

The **Risk Score** would be 45 [(50/100) * 80 + (40/100) * 5 + 0.2 * 15 = 40 + 2 + 3 = 45]

Rollup EPSS Scores from NVDs to TPEs



EPSS Rollup calculator - Example

For example, consider an organization with 100 vulnerabilities, each with a 5% chance of being exploited. The question of great interest to a network defender might be: what is the probability that at least one of those vulnerabilities will be exploited, and therefore what is my overall threat? The probability of at least one event occurring is simply the complement (opposite) of no events occurring, that is:

```
P(at least one exploited vulnerability) = 1 - P(no
 vulnerabilities are exploited)
```

Where, the probability of no vulnerabilities is the linear product of each vulnerability not being exploited. In this example, since each vulnerability has a 5% chance of being exploited, they each have a 95% chance of not being exploited. And since there are 100 of them, we can write this as:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) =
 1 - P(one vuln not exploited)^100 = 1 - 0.95^100 = 0.994
```

Which says that the probability of at least one of the vulnerabilities being exploited is 99.4%.

Important: To modify the *Rollup EPSS Scores from NVD to TPEs*, you need to switch the Form context menu view to **Rollup Developer View** from the **Default view**.

Create or edit a Vulnerability Response remediation target rule

Set up remediation target rules after completing your initial assessment in the Setup Assistant. Vulnerability managers can set up a remediation target rule at the vulnerable item level to drive the remediation of high-risk vulnerabilities in a timely manner. When the remediation date for a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerable item is approaching, the system sends a notification to the users or groups specified in the rule.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Remediation Target Rules**.
2. Select **New**.
3. On the remediation target rule form, enter the required details.
   For a full description of each field, see Remediation target rule fields.
4. Select **Submit**.

Result

This rule goes into effect during the next run of the scheduled job *Evaluate remediation targets* or when using the **Apply Changes** button on the Remediation Target Rules list view. The same is true when an existing rule is updated. For more information on the scheduled job and **Apply Changes**, see Vulnerability Response remediation target rules.

Related topics

Assign the Vulnerability Response persona roles using Setup Assistant

Manage persona and granular roles for Vulnerability Response

Recalculate a remediation target date

The remediation target (RT) date defines when a finding must be remediated. Recalculation verifies that RT dates stay accurate and reflect the latest risk rating updates. When a finding's risk rating changes, the system can recalculate RT dates using the most recent update date, helping maintain accurate SLAs and avoid outdated or overdue target dates.

Before you begin

Note: By default, recalculation applies only to findings that aren't overdue. To include overdue findings in the recalculation, enable the *sn_sec_cmn.evaluate_targetmissed_records* system property.

Role required: admin

Procedure

1. Navigate to **Security Exposure Management** > **Administration** > **Remediation Target Rules**.
2. Open an existing rule to make updates.

   If you need to create a new rule, select **New**.

   For instructions, see Create or edit a Vulnerability Response remediation target rule.
3. Choose how the system should recalculate the remediation target (RT) date when the risk rating changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- In Workspace, this option appears in the Recalculate target date section
- In Classic view, use the **Target recalculation method** field.

Choice	Description
Default calculation	Retains the existing RT date. The recalculated date isn't applied.
Recalculate from risk change date	Updates the Remediation Target date to: Field change time + Target (days) based on the new risk rating.
Recalculate from risk change date and al ways set to earliest target date	Compares the existing RT date with Field change time + Target (days) and applies the earlier date.
Recalculate from risk change date and set to earliest target date only when risk rating increases	If the risk increases: Compares the existing RT date and the recalculated RT date and ap plies the earliest date. If the risk decreases: Applies Field change time + Target (days) without comparison.

4. Select **Save**.

What to do next

For more information on remediation target rules, see:

- Vulnerability Response remediation target rules
- Create or edit a Vulnerability Response remediation target rule
- Examples of recalculating a remediation target date

Examples of recalculating a remediation target date

The following examples show how the system recalculates the remediation target date based on different rule selections and risk rating changes.

Note: By default, SLAs define the remediation window for each risk level:

- Low risk: 30 days
- Medium risk: 15 days
- High risk: 10 days

Target from (date)	Field change time	Initial risk (Target (days)) → New risk (Target (days))	Existing RT date	Recalculated RT date	What happens
Default calculation					
Feb 1	Feb 10	Medium (15 days) → High (10 days)	Feb 16 (retained)	Feb 20	The recalculated RT date isn't applied. The system keeps

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Target from (date)	Field change time	Initial risk (Target (days)) → New risk (Target (days))	Existing RT date	Recalculated RT date	What happens
					the original RT date: Target from (date) + Target (days) → Feb 1 + 15 = Feb 16.
Recalculate from risk change date					
Feb 1	Feb 10	Medium (15 days) → High (10 days)	Feb 16	Feb 20 (applied)	Uses the recalculation formula: Field change time + Target (days) → Feb 10 + 10 = Feb 20.
Recalculate from risk change date and always set to earliest target date					
Feb 1	Feb 10	Medium (15 days) → Low (30 days)	Feb 16 (applied)	Mar 12	Compares the existing RT date (Feb 16) with the recalculated date (Feb 10 + 30 = Mar 12) and selects the earliest date → Feb 16.
Recalculate from risk change date and set to earliest target date only when risk rating increases					
Feb 1	Feb 10	Low (30 days) → High (10 days)	Mar 3	Feb 20 (applied)	Because the risk increased, the system compares the existing RT date (Mar 3) with the recalculated date (Feb 20) and applies the earlier date → Feb 20.
Feb 1	Feb 10	High (10 days) → Low (30 days)	Feb 11	Mar 12 (applied)	Because the risk decreased, no comparison is performed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Target from (date)	Field change time	Initial risk (Target (days)) → New risk (Target (days))	Existing RT date	Recalculated RT date	What happens
					The system sets RT date to: Field change time + Target (days) → Feb 10 + 30 = Mar 12.

Configure installed third-party integrations using the Setup Assistant

Configure Vulnerability Response to work with each of your installed third-party application deployments.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Setup Assistant** > **Integration Configuration**.
2. Select **Scanner Integrations** to configure installed third-party application deployments.
3. If Solution Management for Vulnerability Response is installed, you can select **Solution Integrations** to configure your vulnerability solution providers.

Configure installed solution integrations for Vulnerability Solution Management using Setup Assistant

After you install the Vulnerability Solution Management application, you can configure your vulnerability solution providers using Setup Assistant.

Before you begin

Roles required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin
Use the following sections to supplement the instructions and prompts provided in Setup Assistant for installed solution integrations for Solution Management for Vulnerability Response.

- Verify you have already installed Vulnerability Solution Management and the solution integrations you want before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
- Verify you have any third-party account credentials available. They are required to edit some solution integrations.
- See Install the Solution Management for Vulnerability Response application for more information before you configure installed solutions.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations**.

   The Microsoft Security Response Center Solution Integration requires an API key and URL from the Microsoft Security Response Center to configure it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Entering the API key is optional for MSRC. To obtain the MSRC key, you must have a Microsoft ID from a live.com, outlook.com, or Microsoft.com email account, a phone number registered with Microsoft, or a Skype login.

2. Enter the URL.
   The URL in Setup Assistant for MSRC is `https://api.msrc.microsoft.com`.
3. Click **Finish**.
4. **Optional:** You can execute imports on-demand by clicking **Execute Now** on the configuration page after you enter your credentials.
5. The Red Hat Solution Integration is also available.
   It does not require an API key.
6. In Setup Assistant, to the right of the Red Hat Solution Integration, click **Edit**.
7. Verify the URL in Setup Assistant for RHSI is `https://access.redhat.com/hydra/rest`
8. **Optional:** You can execute imports on-demand by clicking **Execute Now** on the configuration page.
9. Click **Finish** followed by **Mark as Complete** to complete the configuration.
   A check mark is displayed in the Setup Assistant for Solution Integrations when you have completed the configuration.

Configure the MS TVM Vulnerability Integration using Setup Assistant

Configure the Vulnerability Response integration with Microsoft Threat and Vulnerability Management (MS TVM) application, after you install it using the Setup Assistant.

Before you begin

In addition to the instructions and prompts that are provided in Setup Assistant for the Vulnerability Response integration with Microsoft Threat and Vulnerability Management integration, do the following actions:

- Verify that you have already installed the application before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
- See Preparing for the Microsoft Threat and Vulnerability Management Vulnerability Integration for more information before you configure the Microsoft Threat and Vulnerability Management integration for Vulnerability Response.
- Verify that you have MS TVM account credentials available. To obtain these credentials, see Set up Microsoft Azure for the MS TVM integration.

Roles required: System Admin (admin) for installation, Vulnerability Admin (sn_vul.vulnerability_admin) or sn_vul.admin (deprecated), and Configure Integration (sn_vul_msft_tvm.configure_integration) for configuration

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.

   The Microsoft Threat & Vulnerability Management tile is displayed.

   MS TVM is a multi-source integration, which means that you can have multiple deployments of the same third-party integration. The settings from your original third-party integration are used as a template for the settings of each new integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

2. To configure the Microsoft Threat and Vulnerability Management integration, click **Edit**.
3. On the form, fill in the fields.

Account Credentials form

Field	Description
Name	Name of the instance.
TVM region	Region close to your server location. Use the server nearest to your location for optimal performance of the API.
Authentication type	Method to verify the identity. User authentication controls the visibility of specific assets to specific users. MS TVM exports the device groups that are entitled for this user. The default value is Application.
Tenant ID	Tenant identity of your organization.
Client ID	Client identity that is generated after registering MS TVM in Microsoft Azure.
Username	User that has access to the complete device group. This field appears only when User is selected from the Authentication type.
Password	Password for the username that has access to the complete device group. This field appears only when User is selected from the Authentication type.
Client secret	Client secret that is generated after registering the MS TVM application. This field appears only when Application is selected from the Authentication type.

4. To save your changes and proceed to the first integration form, click **Next**.
   The Vulnerabilities Import Configuration form is displayed.
5. Enable or disable the vulnerabilities import, determine the initial start date for the vulnerabilities that you want imported, and schedule when the MS TVM Vulnerabilities import should run.
   If you want to import all the vulnerabilities, leave the initial start date blank.
   a. To import data on-demand, click **Import Vulnerabilities Now**.
   b. To see the integration record, click **Advanced Settings**.
6. To save your changes and proceed to the first integration form, click **Next**.
   The Recommendations Import Configuration form is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Enable or disable the recommendations import and determine the schedule when the MS TVM Vulnerabilities import should run.
   a. To import data on-demand, click **Import Recommendations Now**.
   b. To see the integration record, click **Advanced Settings**.
8. To save your changes and proceed to the first integration form, click **Next**.
   The Machines Import Configuration form is displayed.
9. Enable or disable the Machines Import, determine the initial start date for the machines that you want imported, and schedule when the MS TVM Machines import should run.
   If you want to import all the machines, leave the initial start date blank.

   Note: Machine tags are imported by default and used for organizing and tracking the machines listed in the MS TVM environment.

   a. To display the default configuration item (CI) lookup rules, click **CI Lookup rules**. CI Lookup Rules define how machine data from third-party sources are used to identify Configuration Items (CI)s in the ServiceNow AI Platform CMDB. You have the option to add lookup rules or modify the default CI lookup rules on this page. For more information, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.
   b. To import data on-demand, click **Import Machines Now**.

      Note: Machines that have the status as onboarded in MS TVM are retrieved by the ServiceNow application.

   c. To see the integration record, click **Advanced Settings**.
10. To save your changes and go to the first integration form, click **Next**.
    The Machine Vulnerabilities Import Configuration form is displayed.
11. Enable the following integrations and determine the initial start date for the vulnerabilities that you want imported.

Machine Vulnerabilities Import Configuration form

Integration	Description
Microsoft TVM Machine Vulnerabilities Delta Import	Retrieves vulnerabilities that have been updated during the full vulnerability import, including new, fixed, and updated vulnerabilities. You can only import delta data for the past 14 days.
Microsoft TVM Machine Vulnerabilities Full Import	Retrieves all the open vulnerabilities. Due to the high volume of data import, you can schedule it to run weekly.

Note:

Run the machines import before the Machine Vulnerabilities integration. Else, VIs are not created for the missing machines.

12. To save your changes and complete the configuration in Setup Assistant, click **Finish**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

If you want to activate a vulnerable item grouping in the classic environment, navigate to > **Vulnerability Response** > **Administration** > **Remediation Task Rules** > **Microsoft TVM Recommendation**.

In the form that is displayed, select the **Active** option to activate it. Alternatively, select **New** to create a new rule.

For more information, see Vulnerability Response remediation tasks and remediation task rules overview.

Configure the Qualys Vulnerability Integration using Setup Assistant

After you have installed the Qualys application, configure it using the Setup Assistant.

Before you begin

Use the following sections to supplement the instructions and prompts provided in Setup Assistant for configuration of the Qualys Vulnerability Integration.

- Verify you have already installed the application before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
- See Preparing for the Qualys Vulnerability Integration for more information before you configure the Qualys Vulnerability Integration.
- Verify you have any third-party account credentials available. They are required to edit some third-party applications.

Roles required: System admin (admin) for installation, Vulnerability Admin (sn_vul.vulnerability_admin) or sn_vul.admin (deprecated) for configuration.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.
   The installed integrations are displayed.
2. Click **Edit** to the right of the Qualys Vulnerability Integration you want to configure.
3. In the Account Credentials form, enter your Qualys Cloud Platform credentials.
   Your credentials are required to configure it.
4. Use the following notes as a guide as you continue with the configuration.
   - The **Advanced Settings** link points you to the Qualys Integration record. You can add parameters that are supported by the Qualys product for your scheduled queries to help you filter the vulnerability data you import. See Set additional filter parameters for Qualys imports for more information.
   - If you have upgraded from an earlier version of Vulnerability Response with a version of the Qualys Vulnerability Integration you've already configured, that version, with its configuration settings preserved, is still available.

     Under Import Settings in Host Detection Configuration for the Qualys Vulnerability Integration, there is an option to view fixed Qualys vulnerability detection records. If enabled, this permits you to create vulnerable items from detection records in a fixed status (state=**Fixed**). For more information on vulnerable item detections, see Vulnerability Response vulnerable item detections from third-party integrations.

     You can activate the **Lookup By Network Partition** check box on the Host Detection Configuration page to include the network partition identifier in the IP address lookup. See

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Update configuration items with the network partition identifier for the Qualys Vulnerability Integration for more information.

All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Remediation Task Rules. They are displayed in the Discovered Item form.

Note: The Qualys Host List integration should be run prior to creating Assignment or Remediation Task Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

Qualys **Asset Tags** are stored in the Host Tags module under the Qualys Vulnerability Integration.

- The Qualys Vulnerability Integration supports multi-source. You can have multiple deployments of the same third-party integration. To add another integration, on the Scanner Integrations page, click **Add Integration**.

  The settings from your original third-party integration are used as a template for the settings of each new integration.

  Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

  Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

- You can execute imports on-demand by clicking **Execute Now** on a configuration page.

5. Click **Finish** to complete the configuration in Setup Assistant.

Configure the Tenable Vulnerability Integration using Setup Assistant

After you have installed the Vulnerability Response Integration with Tenable application, configure it using the Setup Assistant.

Before you begin

Use the following sections to supplement the instructions and prompts provided in Setup Assistant for the Vulnerability Response Integration with Tenable integration.

- Verify you have already installed the application before you begin. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
- See Preparing for the Tenable Vulnerability Integration for more information before you configure the Tenable for Vulnerability Response.
- Verify you have any third-party account credentials available. They're required to edit some third-party applications.

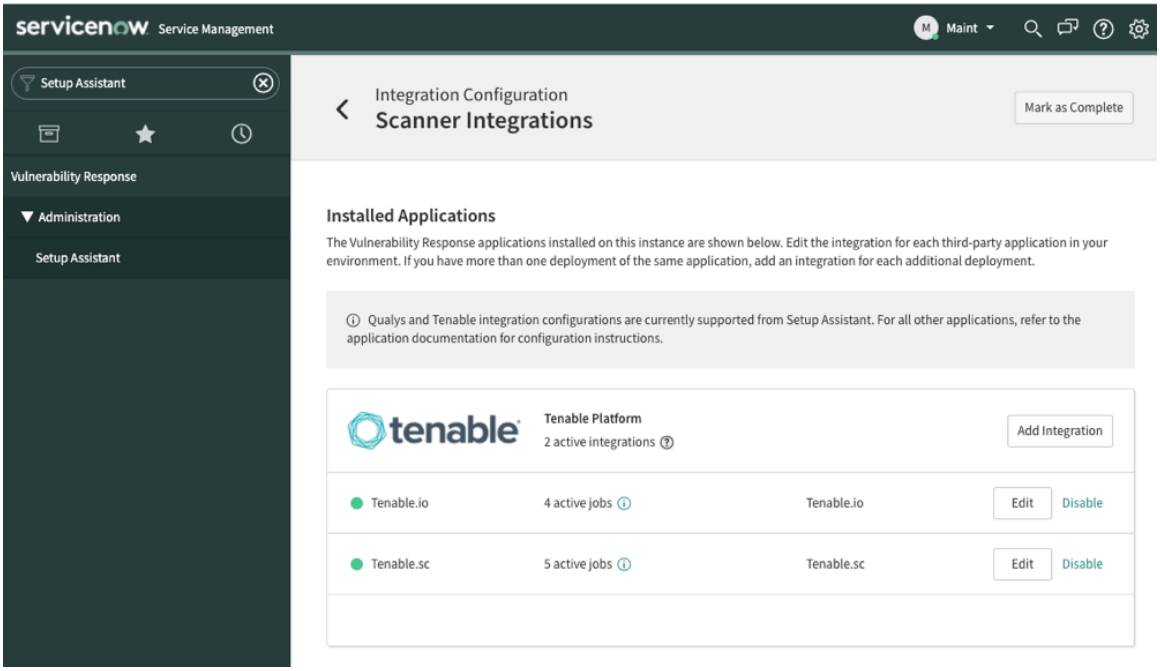
Roles required: System Admin (admin) for installation, Vulnerability Admin (sn_vul.vulnerability_admin), or sn_vul.admin (deprecated), and Configure Integration (sn_vul_tenable.configure_integrations) for configuration.

Procedure

1. If not displayed, navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.

   The Tenable.io, Tenable.sc, and Tenable.cs integrations are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Tenable is a multi-source integration, and you can have multiple deployments of the same third-party integration. The settings from your original third-party integration are used as a template for the settings of each new integration.

Note: If you delete the original vulnerability integration, you have to select another integration to use as your template. Consider disabling the integration instead of deleting it. Integrations created from disabled templates are disabled by default.

Data from each third-party integration is uniquely identified and available in a single instance of Vulnerability Response.

2. To the right of the Tenable integration you want to configure, select **Edit**.
3. In the Account Credentials form, fill in the fields.

   - Tenable.io requires Administrator access with a permission attribute greater than or equal to 64.

     Note: Starting with v3.8 of Vulnerability Response Integration with Tenable, accessing Tenable.io no longer needs administrator privileges. A basic user with a permission attribute equal to 16 can also access the product.

   - Tenable.sc requires Security Analyst or Manager access.
   - Tenable.cs requires a token with access to the Tenable CS Platform Generate token.

   a. Select your Tenable product.

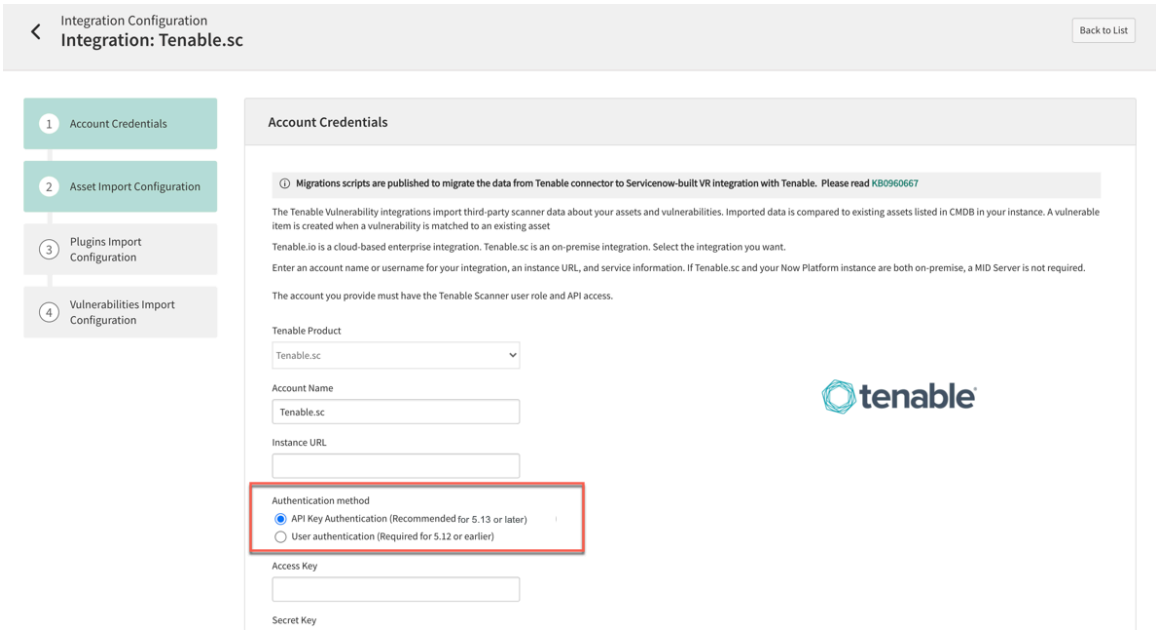
   b. Enter your Tenable account name.

   c. In the Instance URL field, enter the URL for your Tenable platform.

   d. Select an authentication method (in case of Tenable.cs, proceed to step f).

   Based on your version of Tenable.sc, you have two options for authentication:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



i. Starting with v5.13 of Tenable.sc, select **API Key Authentication**. Enter your Tenable Access and Secret Keys.

ii. Prior to v5.13, User authentication is supported by your ServiceNow AI Platform® instance and is required. Enter your ServiceNow AI Platform user name and password.

Only API key authentication is supported for Tenable.sc. Enter your Tenable Access and Secret Keys.

e. **Optional:** Select a MID Server.

(Optional) If your ServiceNow AI Platform instance and your Tenable.sc application aren't in the same location, choose a configured MID Server from the list. For more information, see MID Server.

- Starting with v15.0 of Vulnerability Response and v3.0 of the Tenable Vulnerability Integration, you have the option to enable the *Async_request* parameter as described in Data retrieval settings for the Tenable Vulnerability Integration. If you want to make synchronous calls, some configuration with Tenable is required. Contact the Tenable product for help. This parameter once activated is applicable for all the integrations of Tenable.sc and there's a 30-second timeout. To view the fix scripts, navigate to **System Definition** > **Fix Scripts**.

- (Optional) For existing customers, a fix script is available if you're using asynchronous calls.

If your ServiceNow AI Platform instance and your Tenable.sc application are both on-premise, although not required, you have the option to select a configured MID Server from the list.

Note: Whether you choose to employ a MID Server or not, the integrations time out after five minutes, and a message is displayed when there's no response from the server.

If you get a timeout error, in Setup Assistant verify that you have entered the correct credentials and URL.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

f. Enter the API token.

Note: If you get an error for invalid credentials in the Setup Assistant, verify that you have entered the correct credentials and URL.

4. Select **Next** to save your changes and proceed to the first integration form.
In case of Tenable.io and Tenable.sc, the Asset Import Configuration form is displayed. In case of Tenable.cs, the Container Asset Import Configuration form is displayed.

Note: The Container Asset Import Configuration form is visible only if Container Vulnerability Response is installed.

5. On this form, activate or deactivate the Asset Import Integration, determine the initial start date for the assets you want imported, and schedule when the Tenable asset import should run.

For Tenable.io

- Assets Integration can be used with the Tenable.io Compliance Results and Compliance Results Backfill Integration to import secure configuration assessment data about your assets into the Configuration Compliance application.
- Version 12.2 of the Configuration Compliance application is required on your instance if you wish to import and view this secure configuration assessment data.

  See Configuration Compliance imported data for more information about what data is imported with these integrations and where it's posted.

- The Tenable.io Compliance Results and Compliance Results Backfill Integrations aren't activated by default. If you activate them, you might prefer to use the default schedule settings provided. See the steps listed below for how to locate and activate integrations for the Tenable Vulnerability Integration.
- You can initiate a rescan on-demand for vulnerable items for the Tenable.io product from your instance. The Tenable.io Template Integration and the Tenable.io Scan Credential Integration are required to be activated prior to initiating rescans.

By default, these integrations are deactivated. When you enter your credentials for Tenable.io, all Tenable.io integrations are automatically activated. To manually activate or deactivate these integrations:

a. Navigate to **Tenable Vulnerability Integration** > **Administration** > **Integrations**.

b. On the list that is displayed, locate the Tenable.io integration records you want.

c. Open each record and select the **Active** check box to activate the integration.

d. Select **Update** to save your changes.

e. Return to the Setup Assistant to continue with your configuration for the Tenable Vulnerability Integration with Vulnerability Response.

- For the Tenable.io integration, you also have the option to activate and deactivate the import of asset tags. Asset tags are imported by default and used for organizing and tracking the assets listed in your CMDB in the Tenable.io environment.
- For both the Tenable.io and Tenable.sc products, if you select **Enable Lookup By Network Partition** under Lookup By Network Partition, you can create individual CIs using the Identification and Reconciliation engine (IRE) for your assets that have the same IP address. See Update configuration items with the network partition identifier for the Tenable Vulnerability Integration and Creating CIs for Vulnerability Response using the Identification and Reconciliation engine for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For Tenable.io and Tenable.sc at the top of the screen next to the Asset Import link, select the **CI Lookup rules** link to display the default configuration item (CI) lookup rules. CI Lookup Rules define how asset data from third-party sources are used to identify Configuration Items (CI)s in the ServiceNow AI Platform CMDB. You have the option to add lookup rules or modify the default CI lookup rules on this page. For more information, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.
- Select **Import Assets Now** to import data on-demand.
- The **Advanced Settings** link points you to the Asset Integration record. Starting with v3.3, You can add parameters that are supported by the Tenable.io product for your scheduled queries to help you filter the vulnerability data you import with the Tenable.io Assets, and the Fixed and Open Vulnerabilities Integrations. See Set additional filter parameters for Tenable.io imports for more information.

6. Select **Next** to save your changes and proceed to the next form.

   Note: In case of Tenable.io and Tenable.sc. For Tenable.cs Host Vulnerabilities Import Configuration form is displayed, continue from step 9 for further Tenable CS configuration.

   The Plugins Import Configuration form is displayed.

7. On the Plugin Import Configuration form, enable, or disable the Plugins (Third-party Vulnerability Entries) Import determine the initial start date for the plugins you want imported, and schedule when the Tenable Plugins import should run.

   If you want to import all the plugins, vulnerabilities, and assets, leave the initial start date empty.

   - Select **Import Plugins Now** to import data on-demand.
   - The **Advanced Settings** link points you to the Plugins Integration record.
   - For the vulnerabilities import, you can schedule and set severity levels for Tenable.io for the vulnerabilities that you want ingested. Determine a date so only the vulnerabilities created or updated starting with a specific date are imported.
   - For the Tenable.sc integration, you can determine a query filter and a date so only the vulnerabilities created or updated starting with a specific date are imported.

8. Select **Next** to save your changes and proceed to the next form.
   The Vulnerabilities Import Configuration form is displayed. Enable or disable the integration and determine the initial start date for the vulnerabilities you want imported.

   For the Tenable.io product:

   - Import only the vulnerabilities and associated VIs that match the conditions you choose with the Severity filter.
   - For the Tenable.io assets integration, *`Last Scan Time`* is imported and updated only for assets that have vulnerabilities.
   - Enable the **Fixed Vulnerabilities** option to view VIs for fixed detection records. If this flag is enabled in Setup Assistant, new VIs are created for detections in the **Fixed** state that don't exist in your instance. When enabled, this feature may negatively impact your ingestion performance.
   - The **Advanced Settings** link next to Import Filters points you to the Vulnerabilities Integration record.
   - Select the **Import Schedules** link at the top to configure how often vulnerabilities are ingested and enable the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For the Tenable.sc product:

- Import only the vulnerabilities and associated VIs that match the condition filters set by a Tenable Query in the Tenable platform. See Tenable documentation for more information about Tenable queries.

  The Tenable query filter that you select in the Setup Assistant also applies to the Tenable.sc Assets Integration. Only the assets with the vulnerabilities that match the conditions of the query filter are imported.

- Enable the **Fixed Vulnerabilities** option to view VIs for fixed detection records. If this flag is active in Setup Assistant, new VIs are created for detections in the **Fixed** state that don't exist in your instance. When active, this feature may negatively impact your ingestion performance.
- To include the network partition identifier in the IP address lookup, select the **Enable Lookup By Network Partition** check box from the **Lookup By Network Partition** section. For more information, see Update configuration items with the network partition identifier for the Tenable Vulnerability Integration.
- Select **Import Schedules** at the top to configure how often vulnerabilities are ingested and enable the integration.
- The **Advanced Settings** link next to Import Filters points you to the Vulnerabilities Integration record.
- The ServiceNow® Tenable.sc Scan Credential Integration is enabled (`Active`) automatically from within the Setup Assistant in your instance when you configure the Tenable.sc Vulnerabilities integrations (Tenable.sc Open and Fixed Vulnerabilities Integrations).

  This Integration imports and updates scanner credentials from the Tenable.sc product in your instance. This integration runs weekly to import and securely store your Tenable credentials data. Navigate to **Tenable Vulnerability Integration** > **Integrations** > **Tenable.sc Scan Credential Integration** to view more information about the Scan Credential Integration.

9. Select **Next** on Container Asset Import Configuration step.
   The Host Vulnerabilities Import Configuration form is displayed. Enable or disable the integration.
   - Import only the vulnerabilities and associated VIs that match the conditions you choose with the Severity filter.
   - The Advanced Settings link next to Import Filters points you to the Vulnerabilities Integration record.
   - Select the Import Schedules link at the top to configure how often vulnerabilities are ingested and enable the integration.
   - At the top of the screen next to the Import Schedules link, select the CI Lookup rules link to display the default configuration item (CI) lookup rules. CI Lookup Rules define how asset data from third-party sources are used to identify Configuration Items (CI)s in the ServiceNow AI Platform CMDB. You have the option to add lookup rules or modify the default CI lookup rules on this page. For more information, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

10. **Note:** This step is only for Tenable.cs Product.

    Select Next to save your changes and proceed to the next form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Import only the container vulnerabilities and associated CVIs that match the conditions you choose with the Severity filter.
- The Advanced Settings link next to Import Filters points you to the Vulnerabilities Integration record.
- Select the Import Schedules link at the top to configure how often vulnerabilities are ingested and enable the integration.
- Container Vulnerabilities Import Configuration is seen only if Container Vulnerability Response is installed.

Container Vulnerabilities Import Configuration form is displayed. Enable or disable the integration.

11. Select **Finish** to save your changes and complete the configuration in Setup Assistant.

What to do next

(Optional) Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Calculators** > **Default Risk Calculator** > **Tenable Risk Rule** to enable the Tenable Risk Rule.

In the Vulnerability Calculator Rule form that is displayed, select the Active check box to enable it.

The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response. The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with the new default risk calculator. This risk rule is deactivated by default. By enabling the Tenable risk calculator rule, the imported VPR values are used to calculate the Risk Score for vulnerable items. The default weight distribution for this risk calculator: VPR = 70%, Asset=15%, and Business Criticality=15%. Enabling this Tenable Risk Calculator rule may impact your data ingestion performance.

See Vulnerability Response calculators and vulnerability calculator rules

Setting up vulnerability solution providers

Set up vulnerability solution providers by following the checklist and then configuring the providers in the Setup Assistant.

Prepare solution integration checklist

Use the Setup Assistant to prepare for implementing a solution intelligence integration for all the vendors that support the Common Vulnerability Reporting Framework (CVRF) or Common Security Advisory Framework (CSAF) data format.

Preparing the Common Vulnerability Reporting Framework (CVRF) solution integration

Use the Setup Assistant to prepare for implementing a solution intelligence integration for all the vendors that support the Common Vulnerability Reporting Framework (CVRF) data format.

Before you begin

To integrate with the vendors that provide the solutions, ensure you perform the tasks in the following checklist. You can print the checklist and verify the items listed are completed before you install the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist

Task	Description
Dependent applications ☐	Verify that the following applications are installed from the ServiceNow Store: • Vulnerability Solution Management: For more information about installing Vulnerability Solution Management, see Install Vulnerability Response third-party applications using Setup Assistant and Install the Solution Management for Vulnerability Response application. • Vulnerability Response: For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 16.1 of Vulnerability Response or later.
Third-party account credentials ☐	Verify you have any third-party account credentials available. They are required to edit some solution integrations.
Vendor authentication ☐	Verify that you have authenticated the vendors for import of solutions using the APIs. For more information on how to authenticate vendors, see Configure Connection and Credential aliases. If you do not want to configure an API-based vendor, you can skip this step.
Customization of flow and flow action ☐	If you want to configure an API-based vendor other than Cisco, then you must customize the flow and flow action for extracting a unique key and CVRF URL from the response of an advisory. **Note:** Publishing CVRF URL is not standard across vendors. To customize the flow for vendors other than Cisco, see Configure a Common Vulnerability Reporting Framework vendor other than Cisco. You can skip this step if they do not want to configure vendors other than Cisco. By default, the flow for Cisco has been shipped with the application.
Roles ☐	Verify that you have an admin group or user who can manage the integration. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles.

Preparing the Common Security Advisory Framework (CSAF) solution integration

Use the Setup Assistant to prepare for implementing a solution intelligence integration for all the vendors that support the Common Security Advisory Framework (CSAF) data format.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

To integrate with the vendors that provide the solutions, ensure you perform the tasks in the following checklist. You can print the checklist and verify the items listed are completed before you install the application.

Integration preparation checklist

Task	Description
Dependent applications ☐	Verify that the following applications are installed from the ServiceNow Store: • Vulnerability Solution Management: For more information about installing Vulnerability Solution Management, see Install Vulnerability Response third-party applications using Setup Assistant and Install the Solution Management for Vulnerability Response application. • Vulnerability Response: For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 16.1 of Vulnerability Response or later.
Third-party account credentials ☐	Verify you have any third-party account credentials available. They are required to edit some solution integrations.
Vendor authentication ☐	Verify that you have authenticated the vendors for import of solutions using the APIs. For more information on how to authenticate vendors, see Configure Connection and Credential aliases for the Common Security Advisory Framework (CSAF). If you do not want to configure an API-based vendor, you can skip this step.
Customization of flow and flow action ☐	If you want to configure an API-based vendor other than Red Hat, then you must customize the flow and flow action for extracting a unique key and CSAF URL from the response of an advisory. **Note:** Publishing CSAF URL is not standard across vendors. To customize the flow for vendors other than Red Hat, see Configure a Common Security Advisory Framework vendor other than Red Hat. You can skip this step if they do not want to configure vendors other than Red Hat. By default, the flow for Red Hat has been shipped with the application.
Roles ☐	Verify that you have an admin group or user who can manage the integration. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure vulnerability solution providers

After you install the Vulnerability Solution Management application, configure the vulnerability solution providers by using the Setup Assistant.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration**.
2. Click **Solution Integrations**.
3. Under Installed Solutions section, fetch data by using either a URL, an API, or an import.
   - To fetch data by using a URL or API, click **Add Integration**.
   - To fetch data by uploading a Common Vulnerability Response Framework (CVRF) or Common Security Advisory Framework (CSAF) file, click **Import File**.

What to do next

Depending on which format you want to import the data in, you can perform one of the following tasks:

- For CVRF:
  - If you want to import a CVRF file, see Import Common Vulnerability Reporting Framework data through file import.
  - If you want to import CVRF data using the APIs, see Import Common Vulnerability Reporting Framework (CVRF) data through CVRF URL.
  - If you want to import CVRF data through advisories, see Import Common Vulnerability Reporting Framework data from advisories.
- For CSAF:
  - If you want to import a CSAF file, see Import Common Security Advisory Framework data through file import.
  - If you want to import CSAF data using the APIs, see Import Common Security Advisory Framework (CSAF) data through CSAF URL.
  - If you want to import CSAF data through advisories, see Import Common Security Advisory Framework data from advisories.

Common Vulnerability Reporting Framework (CVRF)

The Common Vulnerability Reporting Framework (CVRF) offers a standardized framework for the creation of vulnerability report documentation. It's an XML-based language that simplifies the sharing of crucial security-related information among diverse stakeholders across multiple organizations. By utilizing the CVRF format, information exchange and processing can be expedited.

Import Common Vulnerability Reporting Framework data through file import

Import a CVRF file to view data in the CVRF format. Importing is a one-time activity.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Once imported, a queue entry is created with an attachment, which gets parsed when the entry is processed. The data is then populated in the respective tables. Before parsing the CVRF data, a scanner-mapping record is created based on configuration. Then, the scanner-mapping data is transformed to vendor-mapping data.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Vulnerability Response Framework**.
2. Click **Import File**.

   Note: You can upload only one XML file at a time with a maximum file size of 1 GB.

3. In the **Name** field, enter a unique name for the integration.
   The scheduler is created with this name.
4. In the **Vendor** field, enter the name of the vendor.
   The **Source** field of the solutions is populated with the vendor name.
5. Click **Finish**.

Result

An import queue is created. Click the link in the info bar to view the queue entries for the vendor along with the related list. You can also view the status of the job.

After the data is imported to the CVRF format, the data is processed in the following way:

1. When the queue gets processed, the file is parsed with a dedicated data source.
2. Once the processing gets completed, the application log is updated.
3. Once the CVRF XML file is parsed, it populates the following tables in the ServiceNow® Vulnerability Response application.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

You can see the detailed information related to errors or exceptions in the Application logs.

Configure Connection and Credential aliases

Configure Connection and Credential aliases to authenticate vendors. In advisory parsing, third-party vendors are authenticated.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

Procedure

1. Create OAuth authentication.
   See Create an endpoint for clients to access the instance.
2. Create a Connection and Credential alias.
   See Create a Connection and Credential alias.
3. Create a Connection.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Click the name of the newly created Connection and Credential Alias.

b. Under the **Connections** tab, click **New**.

c. If the authentication type is OAuth, select the Application Registry Profile created in step 1 as **OAuth Entity Profile**.

d. Create a record in Connections from the related list of the record.

e. In the **Credential** field, select the credential record created in step 3d.

f. In the **Connection URL** field, enter the URL of the vendor.

g. Click **Submit**.

Configure a Common Vulnerability Reporting Framework vendor other than Cisco

Configure a Common Vulnerability Reporting Framework (CVRF) vendor other than Cisco with API support.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Connection & Credential** > **Connection & Credential Aliases**.
2. Create a record with the vendor-supported authentication type.
   For more information on how to authenticate a vendor, see Configure Connection and Credential aliases.
3. Navigate to **All** > **Vulnerability Response** > **Flow Designer**.
4. Duplicate the flow called "Advisory Parsing".

   Note:
   - If any of the actions needs to be changed, copy the action and use it in the new flow.
   - Update the pagination-related logic as per the vendor

5. If the date range parameter logic is not the same as Cisco, copy the action **Update Pagination Parameters** and make changes as required for the vendor.
6. Navigate to **All** > **Vulnerability Response** > **Enrichment Data Mappings**.
7. Create a record as per Cisco by changing the **Property key** value as per the vendor.
   This logic is for mapping required fields from an advisory payload to a ServiceNow table.
8. Map the following API tags from API Payload.
   These tags need to be mapped with details to be filled in the Enrichment Data Mapping table. By default, the Cisco-specific mapping is shipped.

   Note: You need to create a record if you need to configure multiple vendors that publish advisories.

Advisory payload tag	Column from table sn_vul_cvrf_solution_integration	Description
CVRF URL	cvrf_url	Tag name that contains the CVRF URL.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Advisory payload tag	Column from table sn_vul_cvrf_solution_integration	Description
Advisory ID (Unique key for response)	Id	Tag name that contains a unique identifier.
Last modified date	last_modified_date	Tag name that contains the date when the record was last updated.
securityAdvisoryIntegrationSysId	integration	Refers to the integration scheduled job sysId, which creates the vulnerability solution records.

9. Based on the response format, change the logic of parsing by copying the action **Retrieve List** from the Advisory Parsing flow.

Import Common Vulnerability Reporting Framework data from advisories

Import CVRF data from advisories by configuring the vendor URL with import type as API.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

About this task

When the integration runs, the advisories are fetched. The CVRF URL and advisories ID are extracted from the payload. The REST API calls are made for each CVRF URL, and data is parsed and stored in the sn_vul_solution table.

Procedure

1. Navigate to **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Vulnerability Response Framework**.
2. Click **Add Integration**.
3. On the form, fill in the fields.

Import solution advisories form

Field	Description
Import type	Option to select the import type. Select **API**.
Name	Unique name for the integration.
Vendor	Name of the vendor. **Note:** The **Source** field of the solutions is populated with the Vendor name.
Connection alias	Option to select an authenticated credential. **Note:** The sys_alias table stores credentials and the base URL for advisories.
Schedule	Frequency at which the data must be updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Day	Day of the week when you want the data to get updated.
Time	Time of the week when you want the data to get updated.
API Configuration	
Flow	Option to select the flow. The flow gets triggered when the scheduler gets executed. The flow takes care of parsing advisories and extracts the CVRF URL and stores those details in the update tables. You can copy the existing flow and edit as required. For example, you can make changes related to pagination.
Flow action	Option to select the flow action. Flow actions take care of the sliding window capability. You can update the flow actions and add the query parameter directly to the action by dragging.
Mapping Table	Option to select the mapping table. The record of the Enrichment Data Mapping Table is used for extracting the CVRF URL and Advisory ID from the payload of advisories.
Advisories from response	Option to enter the tag name from the payload of advisories from where the list of advisories can be extracted.
Filter Criteria	
Time range parameters	Option to select the time range for the request and the date format for API calls. Start Date/End Date Request parameter is the parameter name used for start date and end date during API calls. For example, StartDate, start_date, endDate, end_date.
Date format	Option to enter the date format, such as, `mm/dd/yyyy`. The date format is the format that the API needs for filtering. Formats that are not supported by GlideDate do not work.
Initial range in days	Enter the days for which the data must be fetched when the scheduler is first executed. For subsequent runs, the sliding window mechanism is followed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If you do not want to select a time range, select **No Parameters**.
Scanner mappings	
Scanner Source	Option to select the source of the third-party entry (TPE).
Vulnerability column	Option to select the keyword.
Keywords	Option to enter the keyword for searching the selected vulnerability column.

4. Click **Finish**.

Import Common Vulnerability Reporting Framework (CVRF) data through CVRF URL

Import CVRF data by configuring the vendor URL in the Setup Assistant.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

About this task

When the integration runs, data is fetched from the URL that gets parsed. Data is then stored in the sn_vul_solution table with source as the vendor name.

Note: Oracle directly publishes the CVRF URL for providing solutions. Thus, if you want to configure the integration for importing Oracle data, then ensure you have the CVRF URL for Oracle and follow the following steps.

Procedure

1. Navigate to **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Vulnerability Response Framework**.
2. Click **Add Integration**.
3. On the form, fill in the fields.

Import CVRF form

Field	Description
Import type	Type of import. Select **URL**.
Name	Unique name for the integration.
Vendor	Name of the vendor. **Note:** The **Source** field of the solutions is populated with the Vendor name.
URL	URL from which you want to fetch the solution data in the CVRF format.
Schedule	Frequency at which the data must be updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If the status tag of CVRF shows "FINAL", then the field is automatically set to **On Demand** to prevent unnecessary runs.
Day	Day of the week when you want the data to get updated.
Time	Time of the week when you want the data to get updated.

4. Click **Finish**.

Troubleshooting Common Vulnerability Reporting Framework data import

Troubleshooting actions can help resolve common issues when importing CVRF data in the Vulnerability Response application.

Issue	Action
Integration run duration is long	If the integration runs for a longer period than expected, then do the following: 1. Navigate to the sn_vul_ds_import_q_entry table. 2. Group by the **Status** field. You can see the entries, which are in the Completed, In progress, or In queued states.
Integration failed in API-based import	If the integration fails in API-based import, do the following: 1. Navigate to **Flow Designer**. 2. Open the flow that was selected in the configuration. **Note:** In the case of Cisco, open the Advisory Parsing flow. 3. Click **Executions**. 4. Open the latest execution or the execution that must be debugged. 5. Check the flow in each stage.
Integration failed in API-based import with a timeout error	If integration fails in an API-based import due to timeout in the advisory parsing flow, then do the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issue	Action
	1. Increase the timeout by opening `sys_properties.LIST`. 2. In the Name column, search for `sn_vul.CVRFFlowTimeout (inMiliSeconds)`. **Note:** Time is in milliseconds. 3. Open the record and update the value with a large number. 4. Save the record and rerun the integration.
Integration failed with error 'Scanner mapping to vendor-mapping data transformation is in progress'	Check if the integration fails during the URL or API-based import, with the following error:`Scanner mapping to vendor-mapping data transformation is in progress. Data will be populated only after the transformation is completed. Try to execute after some time.` If you have this error, then wait for some time and execute the integration again.
Import queue not getting created during file import	During a file import, sometimes the import queue does not get created. This failure means that the transformation that maps scanner-mapping data to vendor-mapping data is in progress. The queue entry is created once the process gets completed.

Common Security Advisory Framework (CSAF)

When used with Vulnerability Solution Management, the Common Security Advisory Framework (CSAF) enables automation security notifications through a machine-readable JSON format.

The CSAF lets you integrate with any solution intelligence vendor using the solution management framework to import the intelligence data. The CSAF security notifications can be one of the following types.

- Security Advisories
- Vulnerability Exploitability Exchange (VEX)
- Security Incident Response
- Informational Advisory

The CSAF only supports the file imports, URL imports, and API imports of security advisories from vendors.

Import Common Security Advisory Framework data through file import

Import a CSAF file to view data in the CSAF format. Importing is a one-time activity.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Once imported, a queue entry is created with an attachment, which gets parsed when the entry is processed. The data is then populated in the respective tables. Before parsing the CSAF data, a scanner-mapping record is created based on configuration. Then, the scanner-mapping data is transformed to vendor-mapping data.

Scanner mapping isn't applicable for National Vulnerability Database (NVD) based vulnerabilities, which are vulnerabilities with a Common Vulnerability Entry (CVE) in the NVD database.

If you only have one highest superseding solution and it rolls down to the vulnerable items, then the preferred solution gets populated. When there are multiple vendor solutions included in one NVD entry, the preferred solution isn't populated because there's more than one highest superseding solution. In this case, you must manually select a solution. For third-party vulnerabilities, the preferred solution gets populated only if you add the corresponding scanner mapping.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Security Advisory Framework**.
2. Select **Import File**.

   Note: You can upload only one JSON file at a time with a maximum file size of 15 MB.

3. In the **Name** field, enter a unique name for the integration.
   The scheduler is created with this name.
4. In the **Vendor** field, enter the name of the vendor.
   The **Source** field of the solutions is populated with the vendor name.
5. Select **Finish**.

Result

An import queue is created. Select the link in the info bar to view the queue entries for the vendor along with the related list. You can also view the status of the job.

After the data is imported to the CSAF format, the data is processed in the following way:

1. When the queue gets processed, the file is parsed with a dedicated data source.
2. Once the processing gets completed, the application log is updated.
3. Once the CSAF JSON file is parsed, it populates the following tables in the ServiceNow® Vulnerability Response application.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

You can see the detailed information related to errors or exceptions in the Application logs.

Configure Connection and Credential aliases for the Common Security Advisory Framework (CSAF)

Configure Connection and Credential aliases to authenticate vendors. In advisory parsing, third-party vendors are authenticated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

Procedure

1. Create OAuth authentication.
   See Create an endpoint for clients to access the instance.
2. Create a Connection and Credential alias.
   See Create a Connection and Credential alias.
3. Create a Connection.
   a. Select the name of the newly created Connection and Credential Alias.
   b. Under the **Connections** tab, select **New**.
   c. If the authentication type is OAuth, select the Application Registry Profile created in step 1 as **OAuth Entity Profile**.
   d. Create a record in Connections from the related list of the record.
   e. In the **Credential** field, select the credential record created in step 3d.
   f. In the **Connection URL** field, enter the URL of the vendor.
   g. Select **Submit**.

Configure a Common Security Advisory Framework vendor other than Red Hat

Configure a Common Security Advisory Framework (CSAF) vendor other than Red Hat with API support.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Connection & Credential** > **Connection & Credential Aliases**.
2. Create a record with the vendor-supported authentication type.
   For more information on how to authenticate a vendor, see Configure Connection and Credential aliases for the Common Security Advisory Framework (CSAF).
3. Navigate to **All** > **Vulnerability Response** > **Flow Designer**.
4. Duplicate the flow called "Advisory Parsing".

   Note:
   - If any of the actions needs to be changed, copy the action and use it in the new flow.
   - Review the page_index_key and page_size_key parameters as per the vendor API.
   - Update the pagination-related logic as per the vendor

5. If the date range parameter logic is not the same as Red Hat, copy the action **Update Pagination Parameters** and make changes as required for the vendor.
6. Navigate to **All** > **Vulnerability Response** > **Enrichment Data Mappings**.
7. Create a record as per Red Hat by changing the **Property key** value as per the vendor.
   This logic is for mapping required fields from an advisory payload to a ServiceNow table.
8. Map the following API tags from API Payload.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These tags need to be mapped with details to be filled in the Enrichment Data Mapping table. By default, the Red Hat specific mapping is shipped.

Note: You need to create a record if you need to configure multiple vendors that publish advisories.

Advisory payload tag	Column from table sn_vul_cvrf_solution_integration	Description
CSAF URL (Resource URL pointing to CSAF Payload)	cvrf_url	Tag name that contains the CSAF URL.
Advisory ID (Unique key for response)	Id	Tag name that contains a unique identifier.
Last modified date	last_modified_date	Tag name that contains the date when the record was last updated.
csaf (Static Value)	advisory_format	Advisory format value for CSAF payloads. Note that this is a static value applicable for all of the CSAF Integrations.
securityAdvisoryIntegrationSysId	integration	Refers to the integration scheduled job sysId, which creates the vulnerability solution records.

9. Based on the response format, change the logic of parsing by copying the action **Retrieve List** from the Advisory Parsing flow.

Import Common Security Advisory Framework data from advisories

Import CSAF data from advisories by configuring the vendor URL with import type as API.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

About this task

When the integration runs, the advisories are fetched. The CSAF URL and advisories ID are extracted from the payload. The REST API calls are made for each CSAF URL, and data is parsed and stored in the sn_vul_solution table.

Scanner mapping isn't applicable for National Vulnerability Database (NVD) based vulnerabilities, which are vulnerabilities with a Common Vulnerability Entry (CVE) in the NVD database.

If you only have one highest superseding solution and it rolls down to the vulnerable items, then the preferred solution gets populated. When there are multiple vendor solutions included in one NVD entry, the preferred solution isn't populated because there's more than one highest superseding solution. In this case, you must manually select a solution. For third-party vulnerabilities, the preferred solution gets populated only if you add the corresponding scanner mapping.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Security Advisory Framework**.
2. Select **Add Integration**.
3. On the form, fill in the fields.

Import solution advisories form

Field	Description
Import type	Option to select the import type. Select **API**.
Name	Unique name for the integration.
Vendor	Name of the vendor. **Note:** The **Source** field of the solutions is populated with the Vendor name.
Connection alias	Option to select an authenticated credential. **Note:** The sys_alias table stores credentials and the base URL for advisories.
Schedule	Frequency at which the data must be updated.
Day	Day of the week when you want the data to get updated.
Time	Time of the week when you want the data to get updated.
API Configuration	
Flow	Option to select the flow. The flow gets triggered when the scheduler gets executed. The flow takes care of parsing advisories and extracts the CSAF URL and stores those details in the update tables. You can copy the existing flow and edit as required. For example, you can make changes related to pagination.
Flow action	Option to select the flow action. Flow actions take care of the sliding window capability. You can update the flow actions and add the query parameter directly to the action by dragging.
Mapping Table	Option to select the mapping table. The record of the Enrichment Data Mapping Table is used for extracting the CSAF

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	URL and Advisory ID from the payload of advisories.
Advisories from response	Option to enter the tag name from the payload of advisories from where the list of advisories can be extracted.
Filter Criteria	
Time range parameters	Option to select the time range for the request and the date format for API calls. Start Date/End Date Request parameter is the parameter name used for start date and end date during API calls. For example, StartDate, start_date, endDate, end_date.
Date format	Option to enter the date format, such as, `mm/dd/yyyy`. The date format is the format that the API needs for filtering. Formats that are not supported by GlideDate do not work.
Initial range in days	Enter the days for which the data must be fetched when the scheduler is first executed. For subsequent runs, the sliding window mechanism is followed. **Note:** If you do not want to select a time range, select **No Parameters**.
Scanner mappings	
Scanner Source	Option to select the source of the third-party entry (TPE).
Vulnerability column	Option to select the keyword.
Keywords	Option to enter the keyword for searching the selected vulnerability column.

4. Select **Finish**.

Import Common Security Advisory Framework (CSAF) data through CSAF URL

Import CSAF data by configuring the vendor URL in the Setup Assistant.

Before you begin

Role required: sn_vul.vulnerability_admin, sn_vul.admin (deprecated), or admin

About this task

When the integration runs, data is fetched from the URL that gets parsed. Data is then stored in the sn_vul_solution table with source as the vendor name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The URL can either be a direct CSAF payload, which contains the advisory details, or a Resource-Oriented Lightweight Information Exchange (ROLIE) Feed URL. In either case, the payload is parsed accordingly and the solution records are created. Complete the following steps for CSAF URL import.

You can also import vulnerability solutions from CSAF Aggregators or Trusted Providers through a URL import that supports ROLIE Feed. These vulnerability solutions are automatically mapped to the correct vendor and vulnerable items (VITs) based on the Common Vulnerabilities and Exposures (CVEs).

Scanner mapping isn't applicable for National Vulnerability Database (NVD) based vulnerabilities, which are vulnerabilities with a Common Vulnerability Entry (CVE) in the NVD database.

If you only have one highest superseding solution and it rolls down to the vulnerable items, then the preferred solution gets populated. When there are multiple vendor solutions included in one NVD entry, the preferred solution isn't populated because there's more than one highest superseding solution. In this case, you must manually select a solution. For third-party vulnerabilities, the preferred solution gets populated only if you add the corresponding scanner mapping.

Procedure

1. Navigate to **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Configuration** > **Solution Integrations** > **Common Security Advisory Framework**.
2. Select **Add Integration**.
3. On the form, fill in the fields.

Import CSAF form

Field	Description
Import type	Type of import. Select **URL**.
Name	Unique name for the integration.
Single vendor	Select this option if you are importing CSAF from one vendor.
Vendor	Name of the vendor. This field is only available if you select **Single Vendor**. **Note:** The **Source** field of the solutions is populated with the Vendor name.
Multi Vendor	Select this option if you are importing CSAF from multiple vendors.
Aggregator	A trusted provider whose solution you can import.
URL	URL from which you want to fetch the solution data in the CSAF format.
Schedule	Frequency at which the data must be updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If the status tag of CSAF shows "FINAL", then the field is automatically set to **On Demand** to prevent unnecessary runs.
Day	Day of the week when you want the data to get updated.
Time	Time of the week when you want the data to get updated.
Scanner Mappings **Note:** The Scanner Mappings section is optional for CSAF.	
Scanner source	Option to select the source of the third-party entry (TPE).
Vulnerability column	Option to select the keyword.
Keywords	Option to enter the keyword for searching the selected vulnerability column.

4. Select **Finish**.

Troubleshooting Common Security Advisory Framework data import

Troubleshooting actions can help resolve common issues when importing CSAF data in the Vulnerability Response application.

Issue	Action
Integration run duration is long	If the integration runs for a longer period than expected, then do the following: 1. Navigate to the sn_vul_ds_import_q_entry table. 2. Group by the **Status** field. You can see the entries, which are in the Completed, In progress, or In queued states.
Integration failed in API-based import	If the integration fails in API-based import, do the following: 1. Navigate to **Flow Designer**. 2. Open the flow that was selected in the configuration. **Note:** In the case of Red Hat, open the Advisory Parsing flow. 3. Select **Executions**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issue	Action
	4. Open the latest execution or the execution that must be debugged. **5.** Check the flow in each stage.
Integration failed in API-based import with a timeout error	If integration fails in an API-based import due to timeout in the advisory parsing flow, then do the following: **1.** Increase the timeout by opening `sys_properties.LIST`. **2.** In the Name column, search for `sn_vul.CVRFFlowTimeout (inMiliSeconds)`. **Note:** Time is in milliseconds. **3.** Open the record and update the value with a large number. **4.** Save the record and rerun the integration.
Integration failed with error 'Scanner mapping to vendor-mapping data transformation is in progress'	Check if the integration fails during the URL or API-based import, with the following error:`Scanner mapping to vendor-mapping data transformation is in progress. Data will be populated only after the transformation is completed. Try to execute after some time.` If you have this error, then wait for some time and execute the integration again.
Import queue not getting created during file import	During a file import, sometimes the import queue does not get created. This failure means that the transformation that maps scanner-mapping data to vendor-mapping data is in progress. The queue entry is created once the process gets completed.

Additional Vulnerability Response setup and configuration tasks

To help you with remediation, you can perform these additional administrative setup tasks as part of your configuration outside of the basic setup. You perform these tasks outside of the Setup Assistant.

You can use the default reporting supplied with Vulnerability Response to oversee your security posture. You can edit those reports if they do not suit your environment, or use them as templates to create your own.

If the Performance Analytics for Vulnerability Response application is installed, you can create reports, responsive dashboards, and more. See Getting Started with reports for more information.

Email notifications increase productivity and smooth workflow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With Software Exposure Assessment, look up the publisher, product name, and version number in Software Asset Management (SAM Foundation) to determine your exposure to vulnerable software.

Visibility into vulnerability libraries can provide flexibility with grouping and remediation tasks.

Configure Exception Management to help you when your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception.

For more additional setup tasks, refer to the topics that follow this overview.

Quick start tests for Vulnerability Response

Validate that Vulnerability Response still works after you make any configuration change such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

The test execution property is disabled by default to prevent running tests on a production system. Run tests only on development, test, and other non-production instances. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production. See Run the Automated Test Framework (ATF) test suite for Vulnerability Response for more information about setting up and running the test suite for Vulnerability Response.

Vulnerability Response quick start tests require activating the Vulnerability Response application (sn_vul) and loading the demo data.

Vulnerability Response tests

Test	Description	Release version
VR: Create Remediation Target Rule	Create a Remediation Target Rule.	Madrid
VR: Create Vulnerability Group Rule	Create a Vulnerability Group Rule.	Madrid
VR: Create Vulnerable Item via Form	Determine whether a user can successfully create a vulnerable item from the Vulnerable Item form.	Madrid
VR: Vulnerability Group Life Cycle	Determine whether a user can successfully resolve a vulnerability group.	Madrid
VR: Vulnerable Item life cycle	Determine whether a user can successfully move a vulnerable item through its life cycle, and also determine whether a closed vulnerable item can be reopened.	Madrid
VR: Rollup Calculator	Determine whether the rollup risk calculator can provide an overall risk score for an entire group of vulnerable items using the scores for	New York

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response tests (continued)

Test	Description	Release version
	all the vulnerable items in a vulnerability group.	
VR: Vulnerability Response Assignment Rules	Determine whether a sample set of assignment rules can successfully auto-assign vulnerable items to an assignment group for remediation.	New York
VR: Vulnerability Calculators	Test the vulnerability calculators.	New York
VR: CI Lookup - Qualys	Create a new lookup rule with method "field_matching" called "Lookup By Network Adapter" for Qualys. Determine whether a configuration item is successfully matched in the Discovered Item table by network adapter and IP address with the new lookup rule.	Orlando
VR: Create Normal and Emergency Change Request	Determine whether the user can successfully create normal and emergency change requests from a vulnerability group.	Orlando
VR: Split Vulnerability Group	Determine whether the user can successfully split a vulnerability group.	Orlando
VR: Update VG state when a CHG is cancelled.	Determine whether the State field on a vulnerability group successfully transitions when a change request that is associated with the vulnerability group is cancelled.	Orlando
VR: Update VG state when a CHG transitions to Review.	Determine whether the State field on a vulnerability group successfully transitions when a change request that is associated with it moves to the Review state.	Orlando
VR: CI Lookup - Rapid7	Test CI lookup using the existing Rapid7 Vulnerability Integration lookup rule, **IP Address**.	Orlando

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response tests (continued)

Test	Description	Release version
VR: CI lookup - Qualys	Test CI lookup by creating a new lookup rule for the Qualys Vulnerability Integration	Orlando
VR: Exception Approval Workflow for VI	Create an exception request and verify that the approval process is working.	Orlando
VR: False Positive Approval Workflow for VI	Create a false positive exception request and verify that the approval process is working.	Orlando
VR: Application Vulnerability Response (AVR)	Determine whether your rules and calculators are working correctly. Verify that updates are working.	Orlando
Remediation target rules: VI import test	Tests VR remediation target rules during import.	Paris
VR: Classification Rule	A sample classification rule that automatically classifies a vulnerability.	Tokyo

Related topics

Quick start tests

Run the Automated Test Framework (ATF) test suite for Vulnerability Response

Run the Automated Test Framework (ATF) test suite after you install or upgrade the Vulnerability Response application.

Before you begin

Confirm a successful installation and that your instance works as designed.

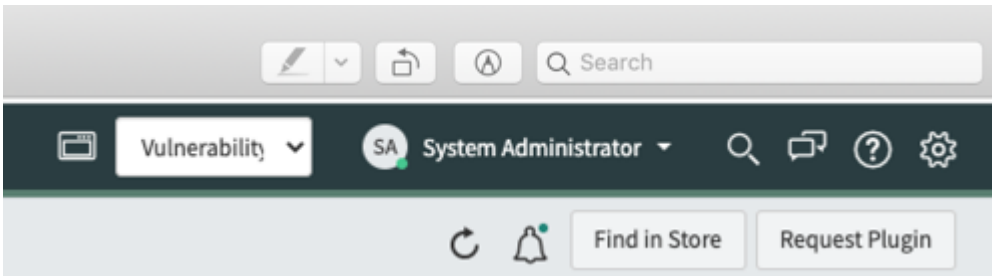
The test execution property is disabled by default to prevent running tests on a production system. Run tests only on development, test, and other non-production instances. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production.

- Verify you installed demo data when you installed Vulnerability Response. Demo data is required to run the Vulnerability Response test suite.
- To enable the test, follow these steps:
  1. Navigate to **All** > **Automated Test Framework (ATF)** > **Administration** > **Properties**.
  2. If not selected, select the **Enable test/test suite execution** check box.
  3. Click **Save**.
  4. If the scope is not set to **Vulnerability Response** in the header, or the scope is not displayed in the header, click the settings icon at the top of the page in the browser window  .
  5. In the System Settings window, click **Developer**.
  6. If not selected, click **Show application picker in header** and close the window.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. In the list that is displayed next to `System Administrator`, click **Vulnerability Response** for the field.

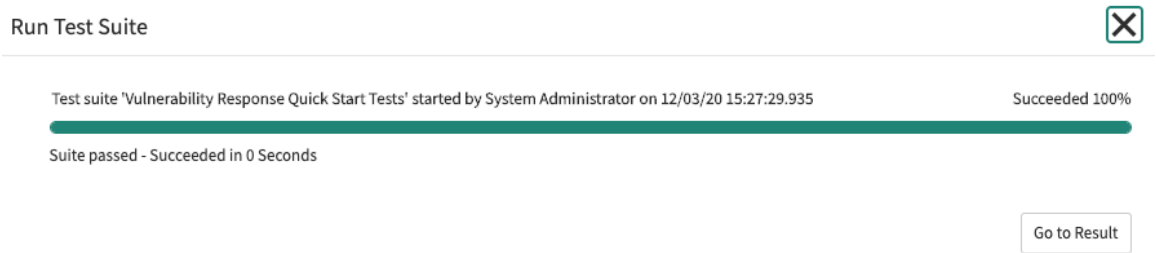
   The field is displayed as shown in the following image.



Role required: admin or atf_test_admin

Procedure

1. Navigate to **All** > **Automated Test Framework (ATF)** > **Suites**.
2. From the Test Suites list, locate **Vulnerability Response Quick Start Tests**.
3. Select it to open the record.
4. In the open record, select the **Active** check box.
5. Click **Update**.
6. If the **Run Test Suite** button is not displayed, refresh your screen, open the record again and click **Run Test Suite** to start the test.
   After a few moments, the Run Test Suite dialog indicates a successful test. Click **Go to Result** for more



   information.

What to do next

Congratulations! You can continue with your configuration of Vulnerability Response.

For more information about automated tests for Vulnerability Response and automated tests, tests suites, and creating automated tests, see Automated Test Framework (ATF).

Install Vulnerability Assignment Recommendations for Vulnerability Response

Install Vulnerability Assignment Recommendations so that you can reduce the time that you spend on identifying owners for vulnerability findings that are unassigned or incorrectly assigned. This application is available as a separate subscription in the ServiceNow Store.

Before you begin

Before you run the Vulnerability Assignment Recommendations feature of Vulnerability Response in your ServiceNow AI Platform® instance, you must first download and install the Vulnerability Assignment Recommendations for Vulnerability Response application. Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. For more information, see Activate a ServiceNow Store application.

Roles required: admin

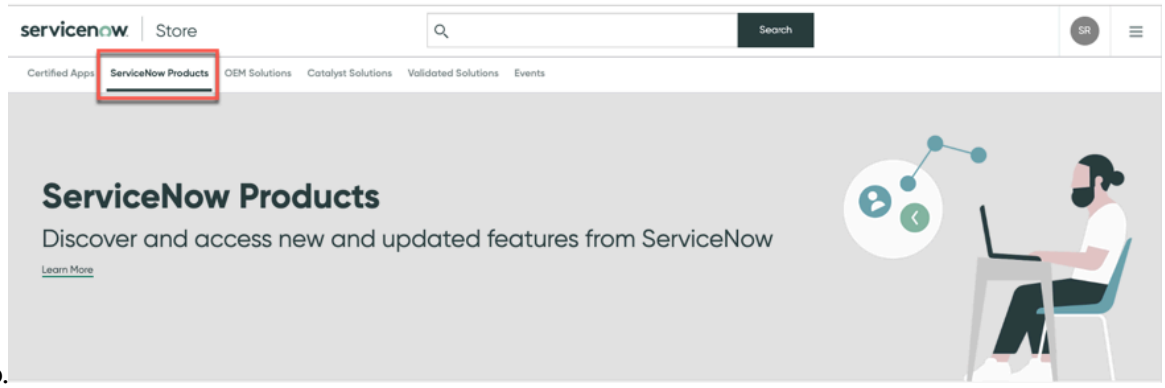
Setup tasks	Action
Verify that the Vulnerability Response application is installed and activated.	Navigate to **All** > **System Applications** > **All Applications** > **Installed in your instance**. Vulnerability Response is shown in this list if it is installed. If the application is not installed and activated, see Install Vulnerability Response.
Verify that the Predictive Intelligence application is installed and activated.	Navigate to **System Applications** > **All Applications** > **Installed in your instance**. Predictive Intelligence is shown in this list if it is installed. If the application is not installed and activated, see Install Predictive Intelligence.
Verify that you have the required ServiceNow roles for your instance.	Check that you have these required roles for installation and verification of expected results: • vulnerability_admin: Required to enable and configure Vulnerability Assignment Recommendations. You can also use it to view and select assignment recommendations for vulnerable items and remediation tasks. • ServiceNow admin: Required to install applications.

Procedure

1. Navigate to the ServiceNow Store.
2. Click **Log In** and enter your HI credentials.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To view the available ServiceNow products, click the ServiceNow **Products** tab.



4. To view all the associated applications that you are entitling for Vulnerability Assignment Recommendations, click the Vulnerability Response product.

   The page lists all the applications that you are eligible for if you opt-in. For information on an application, click the link for the application.

5. To verify that you have entitlement to Vulnerability Assignment Recommendations, click **Opt-in**.
6. To agree to the terms and conditions, at the prompt, select the check box and click **Accept**.
   A message appears that indicates you have successfully opted-in for the application.
7. Skip to step 10 to install the application on your ServiceNow AI Platform instance.
8. **Optional:** If you want to manage your entitlement for the Vulnerability Assignment Recommendations application on other ServiceNow AI Platform instances, click **Manage Entitlement**.

   Note:

   If the **Manage Entitlement** button is not displayed, click the Vulnerability Assignment Recommendations application on the Product List to display it.

   a. Choose an option.

   b. Click **OK** or **Cancel** to continue.
   You are ready to activate plugins and install the application on your ServiceNow AI Platform instances.
9. Log in to the ServiceNow AI Platform instance that you want to install the Vulnerability Assignment Recommendations application on.
10. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
11. From the applications listed, locate the Vulnerability Assignment Recommendations application (sn_vul_recom) and click **Install**.
    The Application installation dialog box is displayed and any dependencies that are installed are displayed.
12. **Optional:** If you want demo data, select the **Load demo data** check box and click **Install**.

    Note: If you do not select the **Load demo data** check box, demo data is not available to install from the Application Manager later. For information on how to install or reinstall demo data after the initial installation, see the Workaround to install demo data if application is already installed [KB0722909] article in the Now Support Knowledge Base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This installation may take some time. A message is displayed in the Install dialog box after the application and its dependencies are successfully installed.

13. Click **Close**.
14. To configure Vulnerability Assignment Recommendations, see Configure Vulnerability Assignment Recommendations for Vulnerability Response.

Configure Vulnerability Assignment Recommendations for Vulnerability Response

Enable Vulnerability Assignment Recommendations to reduce the time that you spend on identifying the owners for vulnerability findings that are unassigned or incorrectly assigned.

Before you begin

Role required: sn_vul.manage_assignment_recom_config

About this task

This application is not enabled by default.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Assignment Recommendations**.
2. Select **Enable Assignment Recommendations**.
   The **Predictive Intelligence solution definition field** appears. The default value is **Vulnerable Item Assignment**.
3. Click **Save**.

Create and train a solution definition for Vulnerability Response

Create and train a solution definition model for Vulnerability Response by using Predictive Intelligence. You can use this model to predict the assignment group for a vulnerable item (VI) or remediation task (RT) based on existing data.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Predictive Intelligence** > **Classification** > **Solution Definitions**.
2. On the Classification Definitions form, click **Vulnerable Item Assignment**.
   This is the default solution definition.

   Note:

   - The default Training Frequency is 30 days. This means that every 30 days, the model retrains automatically using the VI dataset that matches the configured filter condition.
   - Fields from the Vulnerable Item table can be used for training. The default solution definition trains on two VI fields: **Vulnerability.Summary** and **Configuration item.Name**. You can customize the fields used for training, depending on which fields you find helpful for predicting vulnerability ownership in your organization.

3. To create and train the classification solution, see Create and train a classification solution.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can also create and train a similarity or a clustering solution. For more information, see:

- Create and train a similarity solution.
- Create and train a clustering solution.

4. Click **Update & Retrain**.

Note: To configure advanced settings for ML solutions, see Configuring advanced settings for your ML solutions.

Create a Vulnerability Response calculator

A vulnerability calculator is a pre-defined formula to calculate a target field when certain criteria are met. Calculators, which calculate the vulnerable item **Risk Score**, can contain **Risk Rules**.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Note: You may notice performance degradation when running vulnerability calculators that contain scripts.

Order your rules to run the simplest rules first and only run scripts on the items that cannot be handled with a condition and template value or a risk rule.

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Vulnerability Calculators**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Vulnerability calculator form

Field	Description
Name	The name of the vulnerability calculator.
Table	Auto-filled with the name of the vulnerable item table.
Application	Auto-filled with Vulnerability Response.
Target field	Field to calculate.
Description	Text description of the calculator.
Active	Turn the calculator on or off.

4. Right-click in the header to **Save**.
   The **Vulnerability Calculator Rules** section appears.
5. Create a rule for the calculator by clicking **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For the **New Risk Rules** form (only available when the **Target field** is **Risk Score**) see step 10.

6. Fill in the fields, as appropriate.

Vulnerability Calculator Rule form

Field	Description
Name	Name of the calculator rule.
Order	The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Calculator	Auto-filled with the calculator parent.
Active	By default the **Active** check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.
Advanced view	When selected, scripted conditions and scripted values can be selected from **Condition type** and **Value type**.

7. Fill in the fields in the **When this condition is met** tab, as appropriate.

When this condition is met tab

Field	Description
Name	Name of the calculator rule.
Order	The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Calculator	Auto-filled with the calculator parent.
Active	By default the **Active** check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to vulnerable items created in the system.
Advanced view	When selected, select scripted conditions and scripted values from **Condition type** and **Value type**.
Condition type	Available when you select the **Advanced view**. Choices include: ○ Filter: Uses filter conditions. ○ Filter group: See create a new filter group to define the calculator criteria. ○ Script: Script condition used to determine when to apply this calculator. **Note:** Before you write scripts for determining when to apply the calculators, return to the **Vulnerability Calculators** list. Explore the vulnerability calculator records shipped with the base system.
Condition	Defines basic filter conditions for determining whether to use the calculator or not.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Selecting either the **Filter group** or **Script** condition types, hides this field. Case sensitivity for the search text you enter in the condition builder is not supported on this record or form.

8. Click the **Set these values** tab and fill in the fields on the form, as appropriate.

Set these fields tab

Field	Description
Value type	Available when you select the **Advanced view**. Choices include: ○ Template: Define the values to set on each field. ○ Script: Used to set the values on each field.
Script values	Available if you selected the **Script** value type. Defines what values to apply the calculations to.
Template	Select the fields and values you want to use for the calculator. Selecting either the **Script** value type, hides this field.

9. When you have completed all entries, click **Submit**.

Note: When you edit an existing calculator, and you want to update all existing scores, you can use the **Reapply Calculator** button. It runs through all active vulnerable items (VIs), and if that calculator would be used to set its value, recalculates the value for those VIs. Since reapplying a calculator can take a long time, a scheduled job handles it.

10. For the **New Risk Rules** form, fill in the fields as appropriate.

Set each weight according to the percentage of the result that should come from that value. For any data that your scanner does not provide, or for data that should not be part of the risk score, set the weight to zero.

You can add, delete, or update the fields. You can also configure the weightage percentage for the field values. For more information, see Define fields and weights for the risk rule for Vulnerability Response Risk Calculators.

As you update the weights, scenarios display the weights remaining, as well as anticipated **Risk Score** results.

Field	Description
Name	Name of the calculator rule.
Order	The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Calculator	Auto-filled with the calculator parent.

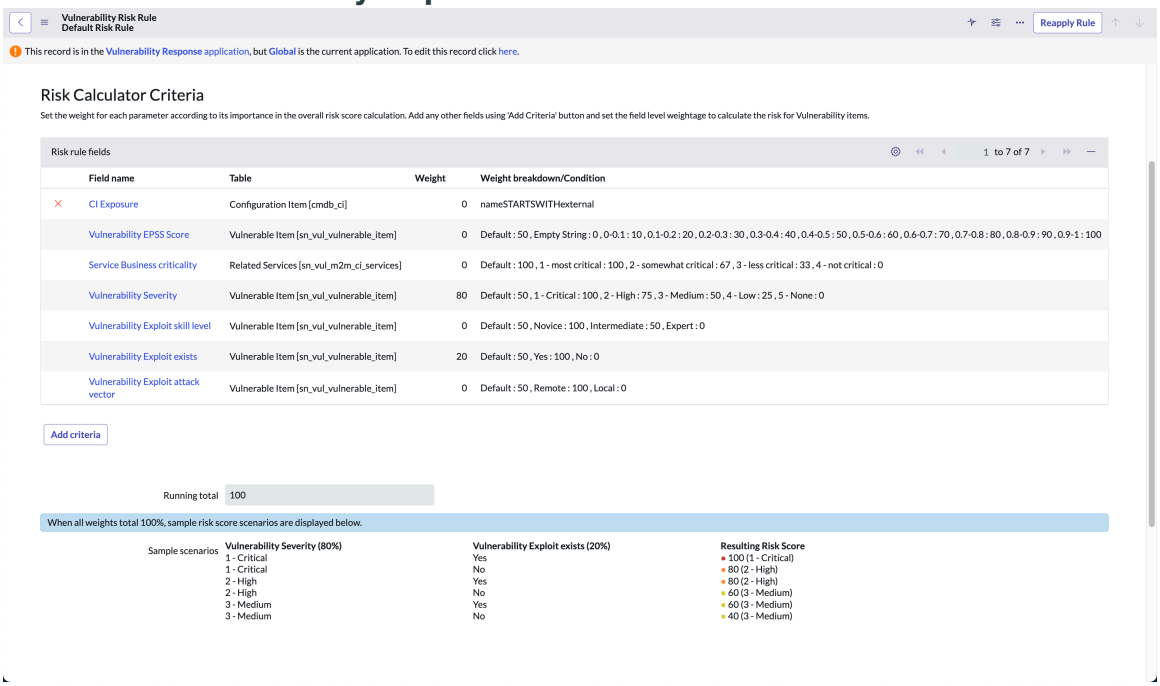
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	By default the **Active** check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.
Condition	Defines basic filter conditions for determining whether to use the calculator. Selecting either the **Filter group** or **Script** condition types, hides this field.
Weights	
Vulnerability Severity	Percentage of the result that comes from severity.
Vulnerability EPSS Score	Probability of the vulnerability being exploited. By default, the weight of this criteria is zero. If you want to use this for your risk score calculation, set an appropriate weight against this criteria.
Exploit exists	Percentage of the result that comes from the existence of an exploit. If this information is not present in your vulnerabilities, set the weight to zero.
Exploit skill level	Percentage of the result that comes from the skill level required by the exploit. If this information is not present in your vulnerabilities, set the weight to zero.
Exploit attack vector	Percentage of the result that comes from where the attack is targeted. If this information is not present in your vulnerabilities, then set weight to zero.
Service Business criticality	Percentage of the result that comes from business criticality. If you have not linked your CIs to business services, then set weight to zero.
CI Exposure	Percentage of the result that comes from whether the CI is internet-facing. If the weight is non-zero, a condition filter appears to define which CI are internet-facing. Set the filter to select your Internet-facing configuration items. You can preview which records match the condition.
Running total	Auto-computed percentage totals. When this value reaches 100, the Scenario preview shows you sample risk scores in different scenarios.
Risk score scenarios	When all weights total 100%, risk score scenarios display, providing a preview of the risk score in some of the possible scenarios.

You can add or remove criteria, and adjust the weight of each criteria using the Embedded list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk Rule CI for Vulnerability Response v20.x



11. Click **Submit**.

Disable the default vulnerability calculator if not used

If you do not use vulnerability calculators, disable the default calculator, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Calculators**.
2. Open the relevant calculator.
3. Clear the **Active** check box to deactivate the calculator.
4. Click **Update**.

Create, enable, or, modify Vulnerability Response auto delete rules

You can create, enable, or, modify the delete vulnerability item (VI) and remediation task (RT) delete rules. Use auto delete to remove older records from the VI and RT tables.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- admin: modify the auto delete rules
- sn_vul.vulnerability_admin or sn_vul.admin (deprecated): view the auto-delete module

About this task

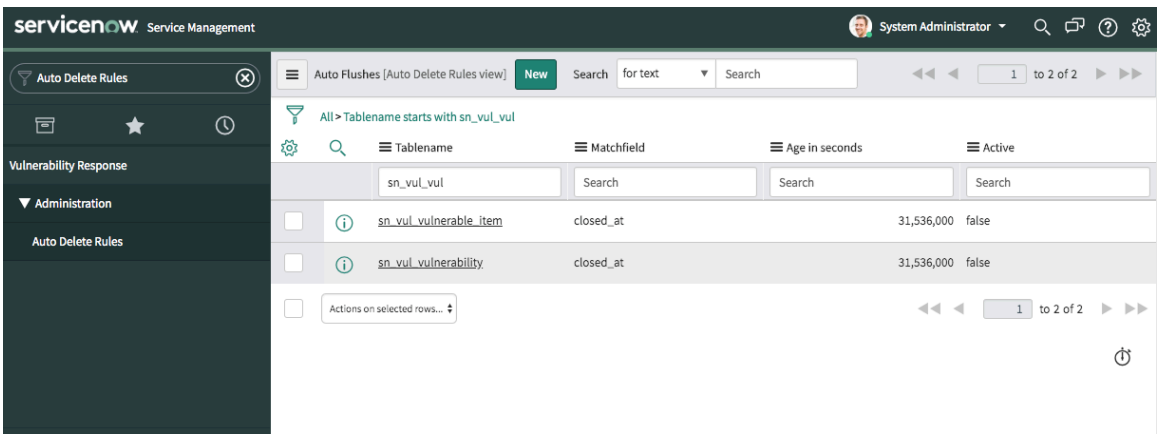
Over time, a large amount of closed records are likely to accumulate in the VI and VUL tables in your instance. Many of these records may have been closed for more than 365 days but have not been removed. Use auto delete rules to remove many of these older, closed records. Removing these records not only significantly reduces the number of records in the VI and VUL tables, deleting them also helps you maintain high performance.

Although auto delete targets records by default that have been closed for 365 days, the very first run may attempt to purge too many records in a single transaction. Depending on the size of your environment, you may prefer to stagger the deletion process to limit the scope of the query. For example, you might start your first run for closed records that are older than 450 days. After that run is completed, you might work your way down by smaller increments (425, 400, 375) until you have reduced the number of records that are older than 365 days.

There are two rules supplied with your ServiceNow AI Platform® that automatically delete closed records that meet specified conditions along with any records that refer to them. One rule deletes vulnerable items, and the other rule deletes remediation tasks. By default, these auto delete rules are disabled so that you are required to activate them manually prior to deleting any records. You can choose the two pre-configured rules that are provided with your instance, or, you can create your own.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Auto-Delete Rules**.
   The list view is displayed.



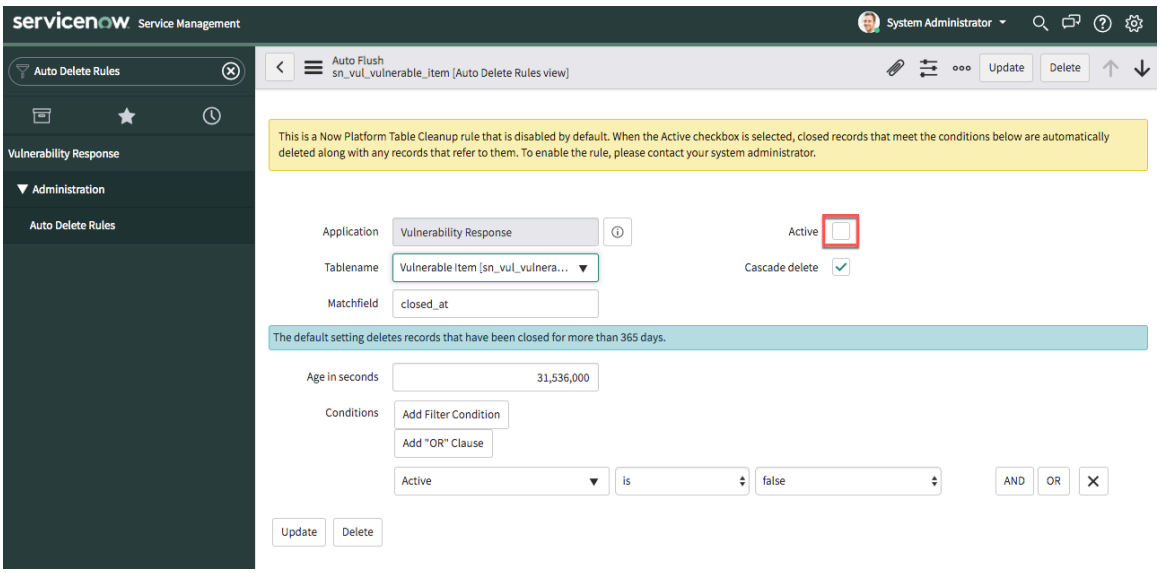
2. To edit, select the delete rule for vulnerable items (sn_vul_vulnerable_item) or the rule for remediation tasks (sn_vul_vulnerability).
3. To create a new rule, click **New**.
4. Fill in or edit the fields on the form, as appropriate.

Field	Description
Application	Name of the application in which records are being deleted. The default value is Vulnerability Response.
Tablename	Name of the table for which the rule is being applied.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Matchfield	Field for which the system monitors the duration.
Active	Option for activating the rule. Once activated, the record can be deleted.
Cascade delete	Option to delete all matching records, plus any records referring to them. If this option is not selected, only matching records are deleted, but not the records that refer to them.
Age in seconds	Age of the vulnerability record to be deleted. For both VI and RT rules, the age is 365 days. This age is displayed in seconds.
Conditions	Filter conditions defining the records in the VI and RT (VUL) tables to which the rules apply.

5. Select the **Active** check box to activate a rule.



Once the rule is activated, the hourly platform function, **Auto flush**, deletes those records from the table for which the rule is activated.

If your environment has millions, or tens of millions, of records that match your delete criteria, you may want to consult with ServiceNow customer support prior to enabling the auto delete rules to help you delete records using a phased process.

Add vulnerability significance charts to the Vulnerability Response homepage

You can add vulnerability significance definition charts and other visualizations to the Overview.

Before you begin

- Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.
- The Vulnerability Analytics plugin must be activated.

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Overview**.
   Some reports are added to the dashboard by default. For more information about these reports, see Using the default Vulnerability Response dashboards.
2. Near the dashboard header, click the card view icon **Add content** to open the dialog box to add more widgets.
3. From the lists in the **Add Widgets** dialog box, select **Reports** to display more Vulnerability Response reports.

Content	Options
Remediation Task Details	**Treemap** > **Vulnerability Significance** > **Vulnerability Significance**
Vulnerability Significance score report	**Performance Analytics** > **Score** > **Services with Vulnerability Significance**
Vulnerable Entry	**Reports** > **Vulnerable Entry** > **Vulnerabilities by Impact, Score, Week**
Remediation Task	**Reports** > **Remediation Task** > **Remediation Task by Time to Remediate Status**
Remediation Task Item	**Reports** > **Remediation Task Item** > **New Vulnerable Items**
Vulnerability Integration Run	**Reports** > **Vulnerability Integration Run** > **Last 30 Days Qualys Duplicates, New VIs, Results, Updated VIs, Qualys Integration Runs**
Vulnerable Item	**Reports** > **Vulnerable Item** > **An extensive list of vulnerable item filters including open Qualys VIs.**.

4. Click the location on the screen you want to add the gauge.
5. Close the **Add content** box.

Define Vulnerability Response email notifications

Set up email notifications to share useful information about important updates and activities such as approval and rejection of false-positive requests. Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Email Templates**.
2. Select **New**.

   For detailed instructions on creating email notifications, see Create an email notification.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result

Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the links open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for the users with the roles, sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin.
- Links open in the IT Remediation Workspace for the users with the role, sn_vul.remediation_owner.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Define Vulnerability Response email templates

Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Email Templates**.
2. Select **New**.

   For detailed instructions for creating email templates, see Construct an email message with a template.

Create or edit remediation target notifications

Vulnerability administrators can edit the remediation target notification or add new ones, specifying when to send the notification, who receives the notification, and what content is in the notification.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Notifications**.
2. Select the remediation target notification record or select **New**.
3. Fill in fields on the form, as appropriate.
   For more information on the form fields, see Create an email notification.
4. Select **Preview Notification** to view the message.

Result

Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for the users with the roles, sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin.
- Links open in the IT Remediation Workspace for the users with roles, sn_vul.remediation_owner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Configure the Vulnerability Exposure Assessment

Assess the zero-day (current day) exposure of your assets to vulnerable software with the Vulnerability Exposure Assessment application.

Important: You can perform the exposure assessment by Common Vulnerabilities and Exposures (CVE) and software to leverage the additional capabilities in the Vulnerability Assessment Workspace. For more information, see Explore the Vulnerability Assessment workspace.

Role required: admin

Compatibility and system requirements

The Vulnerability Response application is available on the ServiceNow Store. The Software Asset Management (SAM) Foundation application [com.snc.asset_management] is installed as part of the Vulnerability Response application. To verify that the SAM Foundation application is installed on your instance, navigate to **System Applications** > **All Available Applications** > **All** and search for `com.snc.asset_management`. If the application isn't installed, select **Install**. For more information on SAM Foundation, see Software Asset Management Foundation plugin.

Since the Vulnerability Exposure Assessment application requires access to the asset data on your ServiceNow AI Platform® instance, the asset management applications must have data to reference. The Software Discovery Models table [cmdb_sam_sw_discovery_model] and the Software installations [cmdb_sam_sw_install] require data.

The Vulnerability Exposure Assessment application also works with either the SAM Foundation or the SAM Pro ServiceNow AI Platform® applications. The SAM Pro application is not part of the core Vulnerability Response product from the ServiceNow Store and requires a separate subscription.

Note: The SAM Pro application is required only for the Content Library which can yield better results.

Starting with v23.0 of Vulnerability Response, if you have the Pro or Enterprise subscription, you will be redirected to the **Exposure Assessment** page in the Workspaces based on your role upon clicking the **Exposure Assessment** link in the **All** menu:

Accessing Exposure assessment page in the workspaces

Role	Workspace
Vulnerability Manager	Vulnerability Manager Workspace
Event Manager [sn_vul_analyst.vul_event_manager] or Emergency Response [sn_vul_analyst.emergency_response]	Vulnerability Assessment Workspace

To avoid being redirected to the workspaces and remain on the Classic Exposure Assessment page, set the **Link Type** to *List of Records* in the Link type tab on the Module - Exposure Assessment page. You can access the Module - Exposure Assessment page by selecting the **Edit Module** icon next to the **Exposure Assessment** link in the **All** menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With the vulnerability write role [sn_vulnerability_write], you can view the Exposure Assessment module and create and edit exposure assessment records on-demand for vulnerable software in your instance with the Vulnerability Response application.

Related topics

Assess your exposure to vulnerable software

Configure Exception Management for Vulnerability Response

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to a vulnerable item (VI) or remediation task (RT) that cannot be remediated according to the policy.

Before you begin

Limit the duration of an exception requested and add a questionnaire to the exception or false positive request using the Vulnerability Response module. By default, an exception is requested using the ServiceNow® Vulnerability Response module. You can also request an exception using the GRC: Policy and Compliance Management integration.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.manage_exception_configuration

About this task

If Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

If you add a questionnaire, it’s sent to the person raising the exception or false positive request. You can either use the default questionnaire or create one based on your requirements.

It’s useful for the exception approver to understand the reason for requesting the exception.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Management**.
2. On the Exception Management Configuration form, select how you want to manage an exception by selecting an option from the **Manage exceptions using** list.
   You can select either Vulnerability Response or GRC: Policy and Compliance Management. You must activate the GRC plugin to use GRC: Policy and Compliance Management to request an exception. Changing the configuration doesn’t impact the existing data.
3. If you selected the Vulnerability Response option, enter the following information:

Settings for VR Exception Management form

Field	Description
Duration	Period for which an exception can be requested.
Unit	Unit of time for the specified period.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Enable questionnaire to request exception	Option to add a questionnaire to the exception request being raised.
Questionnaire to request exception	Displays the questionnaire selected by you to request an exception. The **Exception Questionnaire** is displayed by default. **Note:** This field appears only when you select the **Enable questionnaire to request exception** check box.
Questionnaire for compensating control	Displays the questionnaire that a remediation owner must answer for risk reduction requests. Starting from v20.0 of Vulnerability Response, you can set questionnaire for risk reduction requests. The **Compensating Control Questionnaire** is selected by default. **Note:** This field appears only when you select the **Enable questionnaire to request exception** check box.
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Questionnaire to mark false positive	Displays the questionnaire selected by you to mark as false positive. The questionnaire for false positive request is displayed by default. **Note:** This field appears only when the **Enable questionnaire to mark false positive** check box is selected.

If you have customized the existing questionnaire and upgrade to v20.0, then this customized questionnaire appears for risk reduction request instead of the default **Compensating Control Questionnaire**.

4. If you selected the GRC: Policy and Compliance Management option, enter the following information:

Settings for VR Exception Management form

Field	Description
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Questionnaire to mark false positive	Displays the questionnaire selected by you to mark as false positive. The questionnaire for false positive request is displayed by default.

5. To configure questionnaires based on conditions for exception and false-positive requests:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In the VR Questionnaire Configuration section, select **New**.

b. In the Questionnaire Configuration - New Record form, fill in the fields and select **Submit**.
For more information on the Questionnaire Configuration form fields, see Questionnaire Configuration form fields.
The created questionnaire appears in the VR Questionnaire Configuration section of the Settings for VR Exception Management form.

For example, if you want to configure questionnaire for false-positive requests for critical vulnerable items, then select the **False positive for vulnerable items** approval rule, provide the condition as `Risk rating is 1 - Critical` and select the desired questionnaire in the Questionnaire Configuration form.

6. Select **Save**.

Add an exception approver

Add users to the approver groups so that you can request an exception.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.exception_approver

About this task

Upto Vulnerability Response v14.0, an exception request for a vulnerable item or remediation task is approved using the default two-level approval workflow. The request must be approved by two levels of approvers.

Note: Upto Vulnerability Response v14.0, if there's no first-level approver, an exception can't be requested. However, starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. In the Name column, search for **Exception**, and click **Exception Approver - Level 1**.

   Note: Starting from Vulnerability Response v12.8.1, you can use the system properties provided in the base system for exception approvals via workflow in the System Properties [sys_properties] table. So, when an exception or false positive request is raised via workflow, it's sent for approval to the group IDs defined in the system property. Navigate to **All** > **System Properties** and select *sn_vul.exception_approver_L1*, *sn_vul.exception_approver_L2*, or *sn_vul.false_positive_approver_group* to change the property value.

3. On the Group Exception Approver - Level 1 form, click the Group Members related list.
4. Click **New** to create a list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. On the form, fill in the fields.

User form

Field	Description
User ID	Unique identifier for the user.
First name	User's first name.
Last name	User's last name.
Title	User's job title. Enter a title or job description, or select one from the list.
Department	User's department.
Password	Password assigned to the user. This password can be permanent or temporary.
Password needs reset	Option to enable the user to reset the password to ensure security.
Locked out	Option to lock the user out of the instance and terminate all the user's active sessions. The system prevents users with the admin role from locking themselves out.
Active	Option to make this user active. Only you can see an inactive user in these areas: ○ Lists of users ○ Selection list on reference fields (magnifying glass icon) ○ Auto-complete list that appears when you type into a reference field
Web service access only	Option to designate this user as a non-interactive user.
Internal Integration User	Option to designate this user as an internal integration user.
Email	User's email address.
Language	User's preferred language.
Calendar integration	Calendar used to manage the work schedule. For example, Outlook.
Time zone	Time zone for this user's location.
Date format	User's preferred format for dates.
Business phone	User's business phone.
Mobile phone	User's mobile phone.
Photo	Photo that you can upload by clicking on **Click to add...**.

6. Click **Submit**.
7. Repeat steps 1–5 to create an Exception Approver - Level 2.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The approver must navigate to **Vulnerability Response** > **My Approvals** and approve requests.

Note: To approve an exception for GRC: Policy and Compliance Management, see Policy and Compliance Management optional setup.

Configure approval rules for Exception Management

Starting with Vulnerability Response v15.0, use the flow designer to approve exception requests for exception management, exception rules, and false positive management. If you are deploying Vulnerability Response (VR) for the first time, the flow designer is enabled by default.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

If you are an existing VR user, the default option is workflow.
If you have deployed Vulnerability Response v15.0 or later, the value of the system property *sn_vul.flow_designer_activation* is set to true. This means that the flow designer is enabled by default.

If you are already using Vulnerability Response prior to v15.0, the value of this system property is set to false. You can activate the flow designer by changing the value to true.

Note: You cannot revert to using the workflow after activating the flow designer. For a detailed comparison between the workflow and flow designer, see Exception management workflow versus flow designer.

To use the flow designer, create rules using the Approval Rules module. Using this module, you can configure approval rules for each of the following exception management workflows.

- Exception request for remediation tasks
- Exception request for vulnerable items
- Exception rule
- False positive for remediation tasks
- False positive for vulnerable items

Note: You can also define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow. For information on configuring approval levels, see Create approval levels for Exception Management.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Approval Rules**.
2. On the Approval Rules page, select the group for which you want to set the approval rule.
3. On the form, fill in the fields.

Approval Rule form

Field	Description
Name	Approval configuration name.
Table	Table on which the rule is applied.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Application	Default value is Vulnerability Response.
Rule type	Specifies the rule type. For example, exception management, false positive or exception rule.
Active	Enabled by default, signifying that the approval rule is in use.
Description	Short description of the approval rules.
Approval expiry (days) Starting from v21.0 of Vulnerability Response	Date until when the approver can approve the request.
Notify approver (days) Starting from v21.0 of Vulnerability Response	Date after which the approver is notified to take action.

4. Select **Update**.
   In the Approval Configurations tab, there are two levels of approvers set up by default. You can select a rule to define the conditions based on different use cases within a rule. For more information, see Create configurations for an approval rule.

   Note: In each configuration page, you can create multiple approval levels. For more information, see Create approval levels for Exception Management.

Example:
Based on different use cases, you can define different approval processes for the same vulnerabilities found on different configuration items.

Create configurations for an approval rule

Define the conditions to filter out matching vulnerable items, remediation tasks, or exception rules for an approval level.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
In the Approval Configurations module, you can configure multiple levels of approval for different configurations. Define condition-based rules, with each rule containing multiple levels of approval.

Note: Use the Approval rules module to configure approval rules for the exception management workflows. For information on configuring approval rules, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Approval Rules**.
2. Select an approval rule and navigate to the **Approval Configurations** tab.
3. Select a configuration.
4. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approval Configuration form

Field	Description
Name	Approval configuration name.
Approval rule	Contains the table and type details for the approval rule.
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 is run before a configuration with an order entry of 200.
Active	Enabled by default, signifying that the approval configuration is in use.
Description	Short description of the approval configuration levels.

5. Set a condition for the vulnerable items or remediation tasks in one of the following ways:

Field	Description
Condition	Identifies the matching vulnerable items or remediation tasks.
Advanced condition	Script that defines the condition for the vulnerable items or remediation tasks. **Note:** This field appears when you select the **Advanced** check box.

6. Select **Update**.
   You can define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow. For information on configuring approval levels, see Create approval levels for Exception Management.

Example:
You can define different approval paths for:

- Example 1: Different types of vulnerabilities or configuration items (internet facing or internal).
- Example 2: Deferral and risk reduction requests when a remediation owner raises these requests concurrently for host vulnerable items (VITs) or remediation tasks (VUL).

  The Change Approval column holds the deferral state change approval records. When you set a condition on the Change approval column using the condition builder, the deferral approval record is considered but not the risk reduction approval record. So, to set the condition on the risk reduction state change approval record, use the **Advanced condition** field.

  For the **Exception request for vulnerable items** approval rule, the **Request for risk rating from Medium to Low** approval configuration is shipped with the base system. This configuration is set to false by default. You can use this configuration to set an approval path for the risk reduction requests from Medium to low. You can also update the script in this configuration so that it is applicable for various risk rating changes in the risk reduction requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request for risk rating from Medium to Low configuration:

```
function evaluate() {
    var gr = new GlideRecord("sn_vul_change_approval");
    gr.addQuery("sys_id", approval);
    gr.addQuery("current_value", "3 - Medium");
    gr.addQuery("desired_value", "4 - Low");
    gr.query();
    if (gr.next()) {
        return true;
    }
    return false;
}
evaluate();
```

Set the preceding configuration to true with lowest order and set the **Default configuration - Exception request for VI** configuration to true.

Result: When a remediation owner raises a deferral and risk reduction requests concurrently from the IT Remediation Workspace, the deferral approval requests are redirected to the approvers defined in the **Default configuration - Exception request for VI** and the risk reduction approval requests are redirected to the approvers defined in the **Request for risk rating from Medium to Low** configuration.

Create approval levels for Exception Management

Define the levels of users and user groups that are going to approve the exception requests.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Approval Rules**.
2. Select an approval rule and navigate to the **Approval Configurations** tab.
3. Select a configuration.
4. In the Approver Levels section, select an approver level.
5. On the form, fill in the fields.

Approver Level form

Field	Description
Name	Approval level name.
Required approval	Select how many approvals are required for the selected level: ○ One approver required ○ All users must approve
Active	Enabled by default, signifying that the approval level is in use.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 runs before a configuration with an order entry of 200.
Approval rule	Contains the table and type details for the approval rule.
Approval configuration	Contains the approval configurations.
Assign using	Select an option from: ○ User and user group ○ Approval table field ○ Script
Groups	Approver level group consisting of multiple users. The user must have one of the following roles: ○ sn_vul.exception_approver: For exception management and exception rules ○ sn_vul.false_positive_approver: For false positive
Users	Edit the users listed in the groups.

6. To save the changes, select **Update**.

Note: Prior to v15.0, the workflow process is functional if there are users only in Exception level 1. However, starting from v15.0, there must be at least one user in each level.

Prior to v15.0, in the workflow, if there was no user in the second level, the vulnerability item or vulnerable group was deferred. However, v15.0 onwards, if there is no user in the second level, the approval request is automatically rejected.

Example:
There can be different approval levels for vulnerabilities for Linux and Windows servers.

Exception management workflow versus flow designer

Starting with Vulnerability Response v15.0, if you are deploying Vulnerability Response (VR) for the first time, the flow designer for approving exception requests in exception management is enabled by default. If you are an existing VR user, the default option is workflow.

Note: Starting with Vulnerability Response v19.0, only flow designer is supported for new customers. If you are an existing user and upgrade to Vulnerability Response v19.0, then both flow designer and exception management workflow are supported.

Workflow versus flow designer

Considerations	Workflow	Flow designer
Version	Prior to v15.0 of Vulnerability Response.	Starting from v15.0 of Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Workflow versus flow designer (continued)

Considerations	Workflow	Flow designer
Default option	Default option if you are an existing VR user.	Default option for new VR users starting from v15.0.
Setting the approval process	Exception management includes exception and false positive requests along with exception rules.	Includes defining various levels and adding different approvers for different use cases. Easier to implement than the workflow. Exception management includes exception and false positive requests along with exception rules.
Upgrading to flow designer	You can upgrade to flow designer from workflow. However, existing requests can only be approved using the workflow.	Flow designer is enabled by default.
System property *sn_vul.flow_designer_activation*	If you have been using the workflow for exception management prior to v15.0, the system property is set to false. To activate the flow designer, set this property to true. **Note:** You cannot revert to using the workflow after activating the flow designer.	If you are using VR for the first time for v15.0 or later, the system property value is set to true by default.
Approval rules module	After setting the system property to true, the **Enable module approval rules** scheduled job runs within 24 hours. This scheduled job enables the **Approval rules** module. To activate this module instantly, run this job manually.	If you have deployed VR for the first time from VR v15.0, this module is available by default.
Approval levels	Provides the option to set only two levels of approvers.	Provides multiple options such as setting any number of configurations, approver levels, and dynamically adding approvers for each rule.

Add a false positive approver

Only users added to the False Positive Approver group can approve false positives for vulnerable items (VIs) and remediation tasks (VULs). Granting a false positive is a single-level approval process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Note:

Starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > > **User Administration** > **Groups**.
2. In the **Name** column, search for **False Positive** and click the option.
3. On the Group form, navigate to **Group members** > **New** (or **Edit**).
4. On the User form, create a record by entering the user details, and click **Submit**.
   All roles are granted to the user. The selected users are added to the Group Members list. These members can approve requests to mark VIs or remediation tasks as false positive. Once approved, the state of the record is updated to Closed and it is reopened only on the specified date.

Configure questionnaire for risk reduction

Starting with Vulnerability Response v20.0, you can customize risk reduction request's questionnaire for a set of filtered vulnerable items or remediation tasks.

Before you begin

Role required: admin

About this task

The **Questionnaire for compensating controls for vulnerable items** and **Questionnaire for compensating controls for vulnerable group** approval rules are shipped with the base system.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Management**.
2. On the Settings for VR Exception Management form, select the Enable questionnaire to request exception check box.
3. To configure questionnaires based on conditions for risk reduction requests:

   a. In the VR Questionnaire Configuration section, select **New**.

   b. On the Questionnaire Configuration - New Record form, select the **Questionnaire for compensating controls for vulnerable groups** or **Questionnaire for compensating controls for vulnerable items** approval rule and provide the condition.

   c. Select the desired questionnaire and select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on the Questionnaire Configuration form fields, see Questionnaire Configuration form fields.
The created questionnaire appears in the VR Questionnaire Configuration section of the Settings for VR Exception Management form.

4. Select **Save** on the Settings for VR Exception Management form.

View Vulnerability Response SLAs for remediation tasks

To ensure that vulnerable items are processed correctly, you can define a Service Level Agreement (SLA) for Vulnerability Response remediation tasks.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
The SLA definitions in this list are a subset of the platform SLA list, specific to Vulnerability Response.

For detailed instructions, see Create an SLA definition.

If you are tracking the time it takes to remediate VIs, you might prefer to use Vulnerability Response remediation target rules. Remediation target rules define the expected time frames for remediating vulnerable items (VI) specifically within the context of Vulnerability Response, whereas SLAs might provide a time frame for remediating the vulnerability itself.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **SLA Definitions**.
2. Click on a definition.
   Task SLAs are shown in the related lists of **Remediation Tasks**.

Configure watchdog

Use the watchdog configuration page to create new or update existing watchdogs with conditions that you want to specify. You can enable the notification for each watchdog, and get notified when the conditions are met.

Before you begin
Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **All** > **Security Operations** > **WatchDog** > **Configuration**.
2. Select the watchdog you want to implement.
3. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Watchdog integration form

Field	Description
Name	Name of the watchdog.
Active	Set the check box to *true* to enable the watchdog.
Condition type	Choose from Filter or Script.
Advanced condition	This field appears only when Script is selected from Condition type.
Table	Select table to run the watchdog condition.
Condition	Condition to evaluate the watchdog.
Notify	Check box to notify the groups or users if the watchdog condition is met.
Users	List of users to be informed if the watchdog condition is met.
Groups	Group to be informed if the watchdog condition is met.
Watch log	
Watchdog	Reference to the watchdog table.
Count	Number of records that meet the watchdog criteria.
Notes	Additional notes for the watchdog logs.

4. Select **Update**.

Configure maximum rows in related list

Control the number of rows that appear in related lists to reduce load time and improve readability and performance across Vulnerability Response (VR), Configuration Compliance (CC), Cloud Vulnerability Response (CVR), and Application Vulnerability Response (AVR). The related lists display associated records, such as affected CIs, findings, or remediation tasks so that you can quickly access relevant details without leaving the form.

Before you begin

Role required: sn_vul_cmn.admin

Procedure

1. Navigate to **All** > **sys_properties.LIST**.
2. Search for and open the property: *sn_vul_cmn.related_list.set_max_row*
3. In the Value field, enter one of the following:
   - Positive integer: Displays that number of rows in each related list.
   - Negative integer: Invalid input or value is ignored.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Empty (no value): Displays all rows.

  Note: Displaying more than 100 rows affects the performance.

4. Select **Update** to apply the changes.

Result

After you update the system property, the following related lists will reflect the configured row limit:

In Classic UI

- Affected CIs
- Image Findings
- Potential Duplicate Items
- Potential Solutions
- Preferred Solutions
- Remediation Tasks
- Vulnerable Items

In Workspace UI

- Potential Solutions
- Affected CIs
- Affected Applications
- Affected Docker Images

Advanced Vulnerability Response configuration tasks

The following setup tasks require coding or advanced ServiceNow expertise and are not considered part of the basic configuration.

You might prefer to perform these tasks only if you have advanced coding experience or you have a expert knowledge of the ServiceNow AI Platform.

Create domain-separated imports for an integration

If you require imported data to be in a specific domain, the user assigned to run the integrations must belong to that domain.

Before you begin

Role required:
import_admin and the configure integration role for your specific integration, for example, sn_vul.configure_r7_integration or sn_vul_tenable.configure_integration.

About this task

This set of tasks requires coding or advanced ServiceNow expertise.

The import queues contain data attachments that the scheduled jobs (integrations) process. In a domain-separated environment, you must match the scheduled job with the correct import queue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Create a domain.
2. For every domain you create, create a user and assign the user to that domain.

   Think of this user as a **run_as** placeholder for the domain in your vulnerability integration. It is the equivalent to the **VR.System** user in the global domain. This user needs access to data sources, transform maps, and vulnerability data.

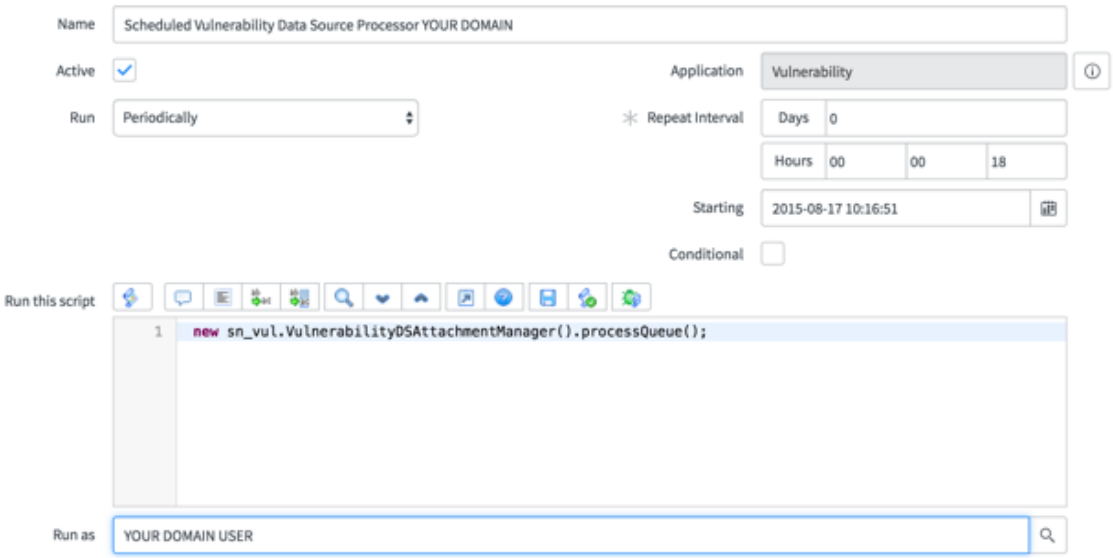
   Note: Do not use this user for any other purpose.

3. Create a scheduled job in each domain.
   For more information on additional precautions and settings, see Additional settings for domain separation.

   a. Navigate to **All** > **System Definition** > **Scheduled Jobs**.

   b. Copy **Scheduled Vulnerability Data Source Processor** into the domain.

   c. To identify the scheduled job, append the domain to the name.



   d. In the **Run as** field, change the **run_as** user to the user you created in the Step 2.

   Starting from v20.1 of Vulnerability Response, the following script changes are shipped with the base system.

4. **Note:** Edit the following UI action so that the integration runs in the **run_as** user domain.

   Edit the **Execute Now** UI action in the **Qualys Host Detection Integration** integration job to add this code block to the top of the file.

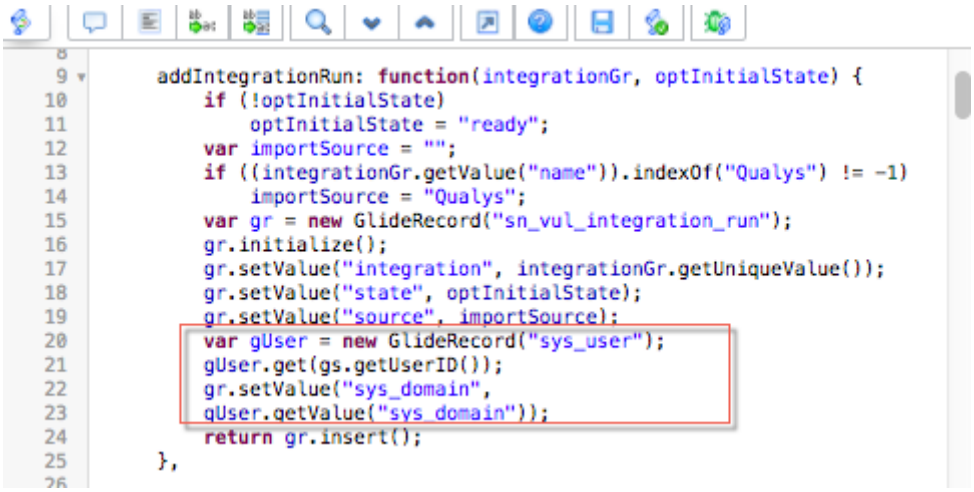
   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

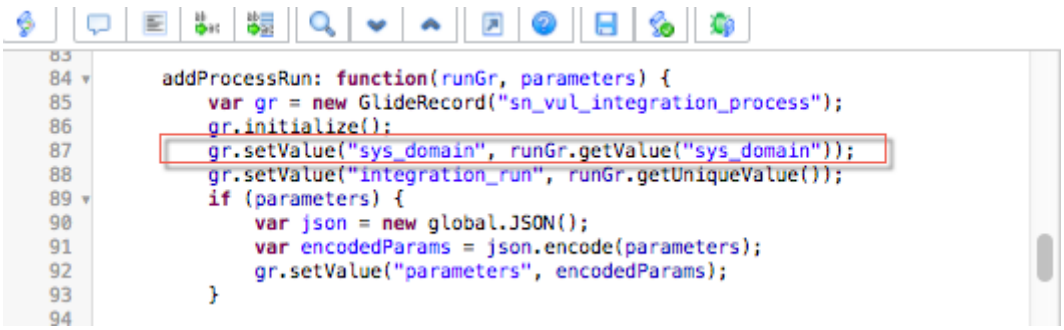
5. **Note:** Edit the following script includes so that integration run in the **run_as** user domain.

   Edit the **VulnerabilityIntegrationUtils** script include method **addIntegrationRun** to add the highlighted code



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Edit the **VulnerabilityIntegrationUtils** script include method, **addProcessRun** to add the highlighted code in the following image.
   addProcessRun code



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Edit the **VulnerabilityIntegrationUtils** script include method, **copyProcess** to add the highlighted code in the following image.
   copyProcess code

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Script

```
_copyProcess: function(intProcGr, isProcessErrored) {
    var copy = new GlideRecord('sn_vul_integration_process');
    copy.initialize();
    copy.setValue('integration_run', intProcGr.getValue('integration_run'));
    copy.setValue('parameters', intProcGr.getValue('parameters'));
    copy.setValue('state', 'new');
    copy.setValue('notes', '');
    copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
    if (isProcessErrored) {
        copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
        var nextRetryDueOn;
        if (intProcGr.getValue('next_retry_due_on') != '')
            nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
        else
            nextRetryDueOn = new GlideDateTime();

        var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
        var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
        nextRetryDueOn.addSeconds(nextRetryDelay * 60);
        if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
            copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
    } else
        copy.setValue('retries', intProcGr.retries + 1);

    copy.insert();
    return copy;
},
```

8. Edit the **DataSourceVulnReportRefreshProcessor** script include method **_processFromDataSourceGroups** to change this original code:
   Original _processFromDataSourcesGroups code

```
_processFromDataSourceGroups: function(payload, fileName) {
    var gr = new GlideRecord("sn_vul_int_data_src");
    gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
    gr.orderBy("ds_group_number");
    gr.orderBy("last_used");
    gr.query();
    var lastGroup;
    if (gr.getRowCount() == 0) {
        throw new Error("There are no data sources to provide data to.");
    }
    while (gr.next()) {
        var thisGroup = gr.getValue("ds_group_number");
        if (lastGroup == thisGroup && lastGroup !== undefined) {
            continue;
        } else {
            var ds = new GlideRecord("sys_data_source");
            if (!ds.get(gr.sys_data_source + ""))
                continue;

            var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
            mgr.queueItem(ds.getUniqueValue(), fileName, payload,
this.integrationProcessGr.getUniqueValue());
            gr.setValue("last_used", new GlideDateTime().getValue());
            gr.update();
            lastGroup = thisGroup;
        }
```

   To:

   Edited _processFromDataSourcesGroups code

```
            var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
            mgr.queueItem(ds.getUniqueValue(), fileName, payload,
this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
            gr.setValue("last_used", new GlideDateTime().getValue());
            gr.update();
            lastGroup = thisGroup;
```

9. Edit the **VulnerabilityDSAttachmentManager** script include method, **queueItem** to add the following highlighted code blocks
   queueItem

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if(optDomain){
            gr.setValue("sys_domain", optDomain);
    }
    var sysId = gr.insert();
```

_getNext

```
_getNext: function() {
    // First go through the retries, if any
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    var sysDomainUser = gUser.getValue("sys_domain");
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "RETRY");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.orderBy("queued_on");
    gr.query();
    if (gr.next()) {
        return gr;
    }

    // Then handle the regular queued items
    gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "QUEUED");
    gr.orderBy("queued_on");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next()) {
        return gr;
    }
```

_processQueueEntry function

```
_processQueueEntry: function(entry) {
    var schedGrId = this._getScheduledImportSet(entry.data_source);
    if (gs.nil(schedGrId)) {
        return;
    }

    var dataSourceGr = new GlideRecord("sys_data_source");
    if (!dataSourceGr.get(entry.data_source)) {
        gs.warn("Non existent data source - marking as complete");
        entry.setValue("status", "COMPLETE");
        entry.setValue("processing_notes", "Data source does not exist, could not process.");
        entry.update();
        return;
    }

    try {
        this._deleteDataSourceAttachments(entry.data_source);
        if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
            gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue entry " + entry.sys_id);
            throw "Attachments not deleted";
        }
        var attachmentApi = new GlideSysAttachment();
        attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
        var schedGr = new GlideRecord("scheduled_import_set");
        schedGr.get(schedGrId);
        schedGr.setValue("data_source", entry.data_source);
        schedGr.setValue("run_as", gs.getUserID());
        schedGr.update();
```

At this point, you are ready for domain-separated imports.

Note: If you have multiple deployments of a Vulnerability Response or Application Vulnerability Response integration, repeat this process for each deployment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create and support multiple domains in the background jobs framework

Background jobs in vulnerability response products are designed to run for long periods of time to perform multiple processes on your records. The background job processors are shipped with the base system that run via the system user and create records in the global domain.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Domain Admin** > **Domains**.
2. Create a domain.

   For more information on how to create a domain, see Create a domain.

   For every domain created, create a user and assign the user to the domain. Suppose this user as a run_as placeholder for the domain. It's the equivalent of VR.System user in the global domain. This user needs access to vulnerability data.

3. Change the run_as of the scheduled jobs *`Scheduled Background Job Manager`*, and *`Close the parent background job`*.

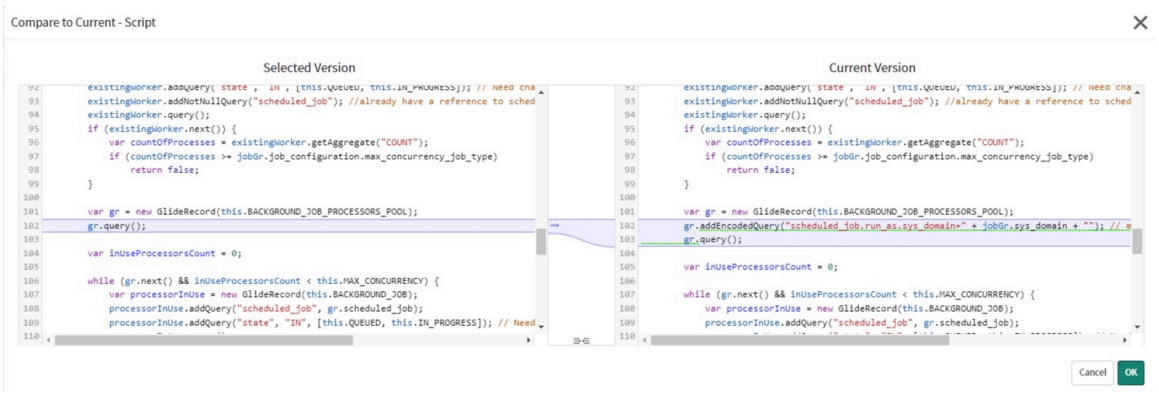
   If you have multiple domains created, duplicate this job and change run_as user accordingly. You may also want to keep a copy of the preceding jobs with the run_as user of the global domain in an inactive mode.

   Ten processor jobs (for example, *`Background job processor 10`*) are shipped with the base system. Change the run as of these jobs to the domain-separated user. If multiple domains are present, then two jobs per domain are sufficient, but these jobs can also be duplicated if necessary. Keep two processor jobs with run_as user in the global domain.

   Starting from v20.0 of Vulnerability Response, the following script changes are shipped with the base system.

4. Modify the script include *`BackgroundJobManager`*, and add the following line as shown in the following image.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" +
 jobGr.sys_domain + "");
```



Note: Trigger the on-demand reapply of any rules from the correct domain.

Create a Vulnerability Response CI lookup rule

The **CI Lookup Rules** module contains rules that are used to find the matching record for host information received during third-party vulnerability integration imports. The host

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

information is matched with the discovered items, unmatched configuration item classes, and the Configuration Management Database (CMDB).

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.vulnerability_admin

About this task

Creating CI lookup rules requires advanced ServiceNow and Vulnerability Response expertise. Rather than modifying one of the existing lookup rules, consider copying it and modifying the copy. When you are satisfied that the new rule does what you want, deactivate the original.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Procedure

1. Navigate to **All** > **Security Operations** > **CMDB** > **CI Lookup Rules**.
2. Click **New**.
3. On the form, fill in the fields.

CI lookup rule form

Field	Description
Name	Name of the rule.
Lookup method	Method used for matching. Choices are: ○ **Script**: Pre-built (IP address, DNS name, and so on) or custom script. ○ **Field matching**: Search on table or field in the CMDB.
Type	Type used with the Script **Lookup method**.
Order	Order of precedence for the rule. Rules with the lowest order are evaluated first.
Active	Check box for whether the rule is active or disabled.
Source	Source used as input to this rule.
Source field	Source field used as input to this rule. Select any field, but it is treated as a string value.
Condition	Condition based on which the CI lookup rule is applied. This condition depends on the attribute from the third-party scanner. **Note:** The asset attribute is a part of the payload. It is received from the third-party scanner. See the Discovered Items table for payload examples.
Script	Editable sample script, based on the **Type**, is shown. Implement the custom script following the comments included in the template of the default function.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

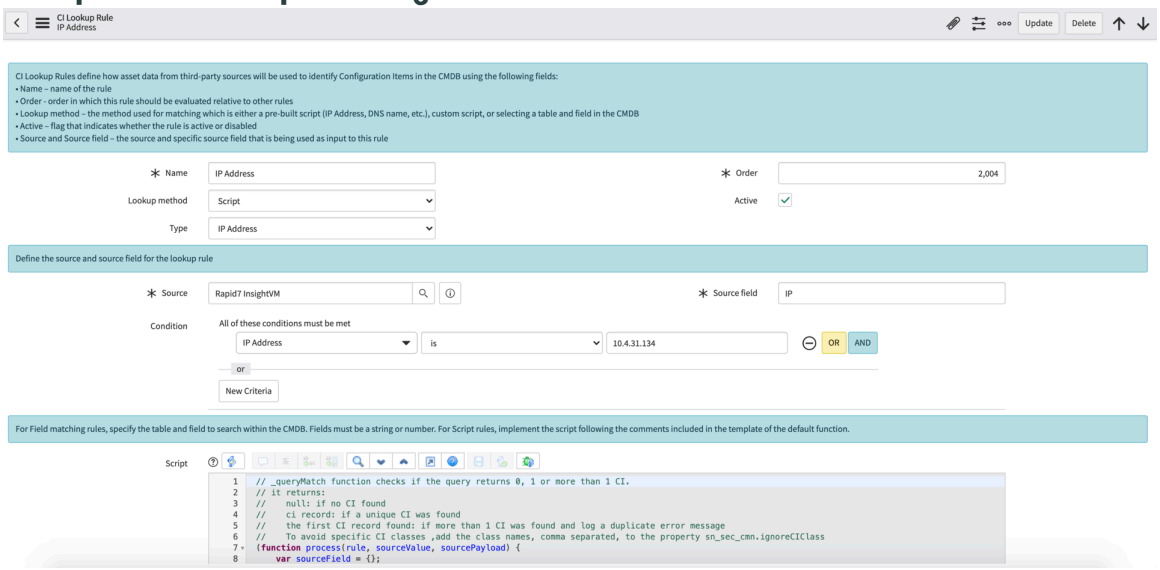
Field	Description
	Note: The process function has three parameters: *rule*, *sourceValue*, and *sourcePayload*
Search on table	Table to search within the CMDB. Used with field matching **Lookup Method**.
Search on field	Field that contains information that can be used to locate a CI. Used with the field matching **Lookup method**. This field may be on the CI record, or on a related record, such as a network adapter.

4. Click **Submit**.

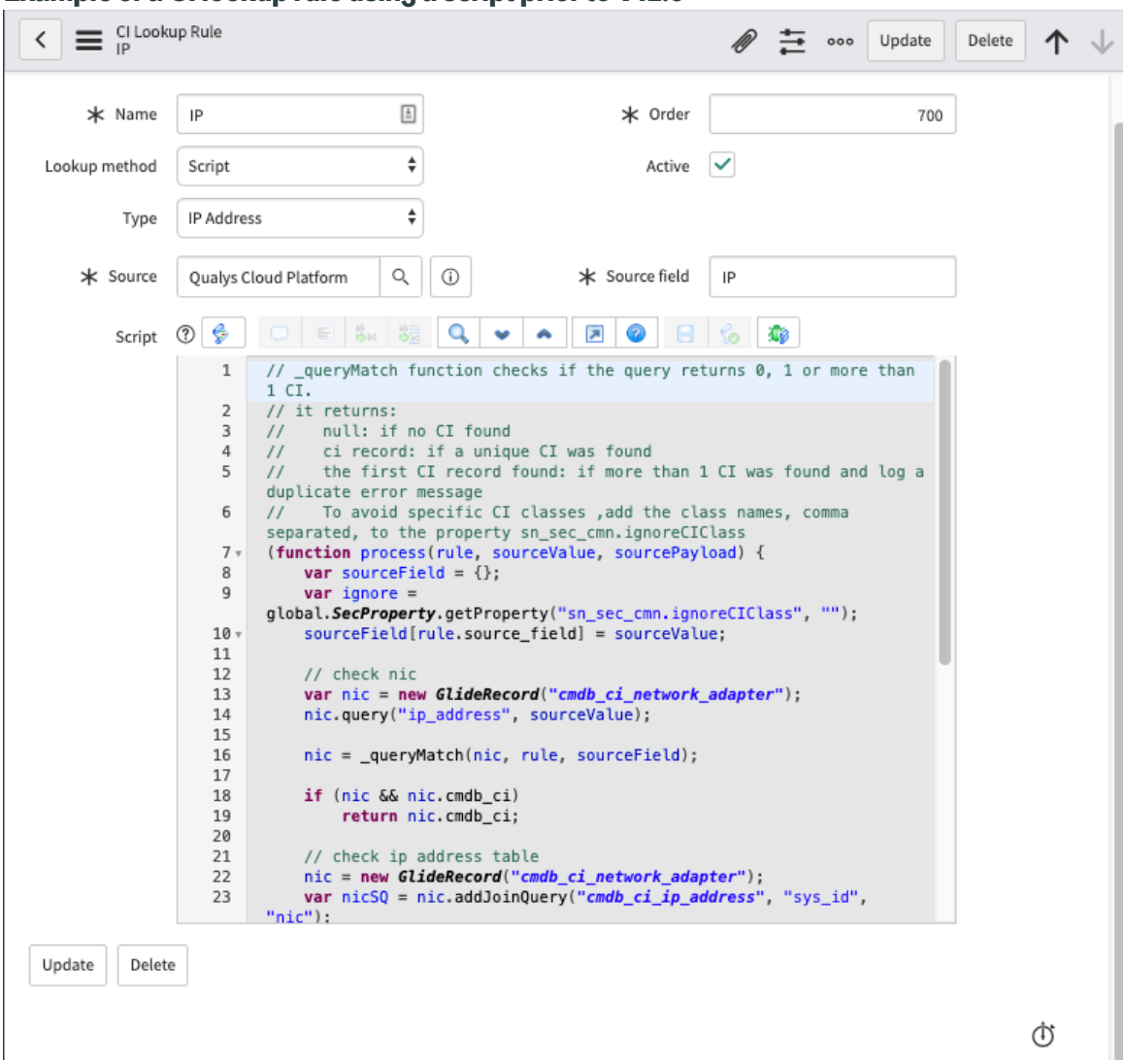
For more information implementation information for CI Lookup Rules see, Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example of a CI lookup rule using a condition builder for V12.0



Example of a CI lookup rule using a script prior to V12.0



Related topics

Vulnerability Response vulnerable item form fields

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ignore CI classes

To ignore some configuration item (CI) classes, for example Load Balancer [cmdb_ci_lb], when running CI Lookup Rules, set the **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*] system property.

Before you begin

Role required: admin

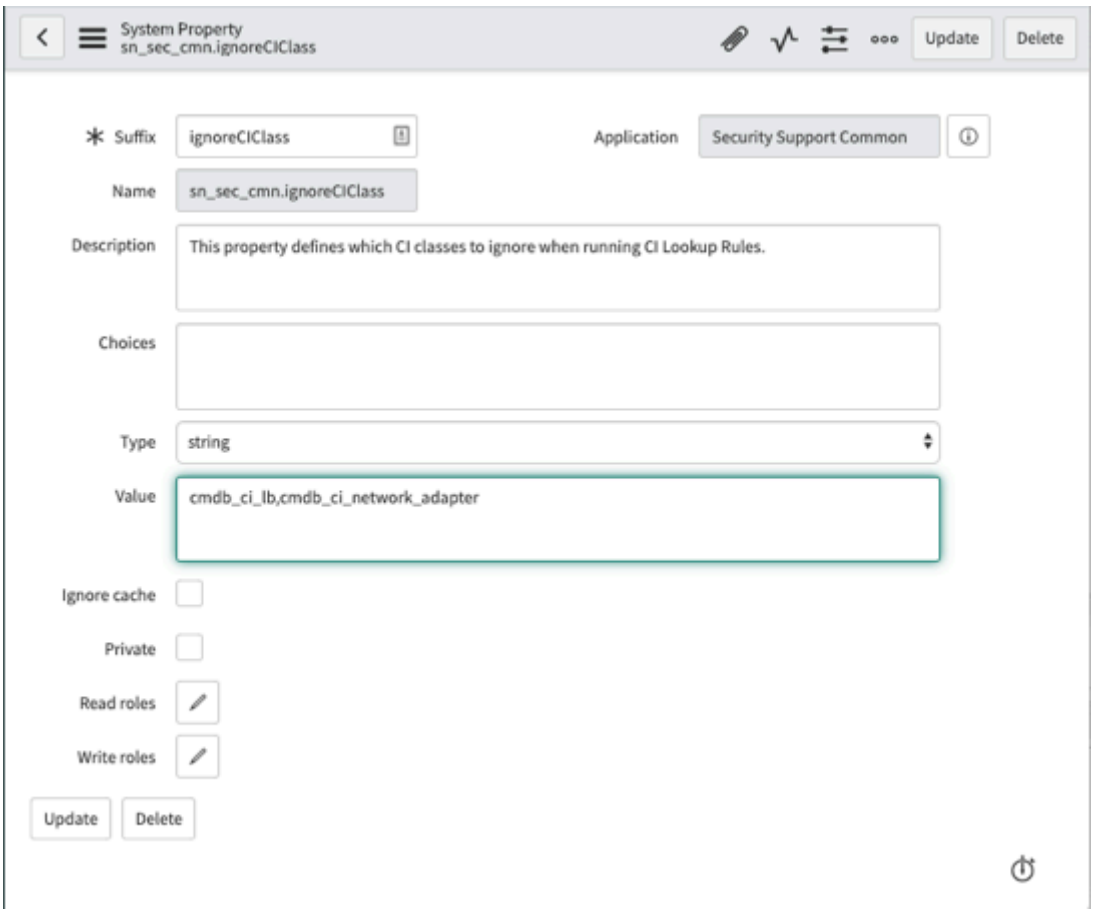
Note:

The **ignoreCIClass** system property is available starting with Vulnerability Response v9.0, however, the property functionality is not available upon upgrade from any previous version.

If you have upgraded from any Security Operations application, prior to version 9.0, see KB0788209 for instructions on how to enable this functionality.

Procedure

1. Enter `sys_properties.list` in the left navigation bar.
2. Click **Enter**.
3. In the **Search** menu, under **Name** enter `sn_sec_cmn.ignoreCIClass`.
4. In the **Value** text box, enter the CI classes to exclude in a comma-separated list.



5. Click **Update**.
   This list is used by CI Lookup Rules during the next import. Vulnerable items created during import are not associated to a CI of any type listed in the **Value** field of the `sn_sec_cmn.ignoreCIClass` system property.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Filter decommissioned CIs

Filter decommissioned configuration items (CIs) while running the CI lookup rules. To filter decommissioned CIs when running the Security Operations CMDB CI lookup rules, set the **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] system property to true.

Before you begin
Role required: admin

About this task
The default value of the system property is true. This property is only applicable for CI lookup rules in Vulnerability Response and it does not impact the IRE lookup logic.

Procedure
1. Enter `sys_properties.list` in the left navigation bar.
2. Select **Enter**.
3. In the **Search** menu, under **Name** enter `sn_sec_cmn.filterOutDecommissionedCI` to filter the decommissioned CIs.
4. In the **Value** text box, enter the value true or false.
   The default value is true.
5. Select **Update**.
   This value is used by CI Lookup Rules during the next import. The `sn_sec_cmn.filterOutDecommissionedCI` system property filters out the decommissioned CIs while running these lookup rules.

Auto-promote CIs

Edit the JSON string in the **autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] system property so your configuration item (CI) lookup rules auto-promote all the Security Operations CMDB CIs to matching entries in the [cmdb_ci] table.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
The system property type is 'string' and requires you enter a JSON string. This property is activated by default and promotes matching CIs while running the CI lookup rules.

Custom-written lookup scripts might return child table records from the script. For this property, the *`_autoPromoteCI`* function in the *`CIIdentify Script Include`* takes the CI returned by the lookup script and automatically traverses the relationships to arrive at the *`cmdb_ci`* entry and return it.

To override the auto-promotion logic, that is, to add or update new CI classes, add the JSON object in the Value field in the [**sn_sec_cmn.autoPromoteFields**] system property.

Procedure
1. Enter `sys_properties.list` in the left navigation bar.
2. Select **Enter**.
3. Locate the [**sn_sec_cmn.autoPromoteFields**] system property and select the record to open it.

   Default string:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. In the **Value** text box, edit the string using the default pairing format.
5. Select **Update**.
   This value is used by CI Lookup Rules during the next import.

Detection key configurations for Vulnerability Response

Use configurable detection keys to choose between Asset ID and Configuration Item, with validations, UI controls, and a schedule job to update existing detections.

The Detection Key Configuration provides you with greater control over how vulnerability detections are uniquely identified within the system. Previously, the detection key relied exclusively on the **asset ID**. Now, you can choose between:

- **Asset ID (Discovered Item Source ID)**
- **Configuration Item (CI)**

This flexibility helps align detection logic with internal asset management practices, especially when CI-level tracking is required.

Additionally, the following updates have been added:

- A new **Configure Detection Granularity** module.
- A new **Configuration Item** column on the Detection Key table.
- Editable detection key fields with controlled access.
- Validation checks to preserve data integrity during in-progress jobs.
- Schedule jobs to apply updated detection keys to existing detection records.

Run detection key configuration

Use the revised detection key to update the existing detections and vulnerable item records.

Before you begin

Role required: sn_vul.vulnerability_admin can modify detection key configurations and apply changes to existing detection records.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Configure Detection Granularity**.
2. Open a detection key configuration record.
   The Configuration Item (CI) field is available. The Asset ID and Configuration Item fields are editable, while all other fields can't be edited.
3. Select **Configuration Item**, de-select **Asset ID** to switch to CI-based detection.
4. If both Asset ID and CI are selected, the system displays an error message.
   - The record moves to a **Pending state**.
   - An info message appears, notifying that changes are made but not yet applied to existing detections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select **Apply Changes**.
   For the following cases, the detection key can't be modified:
   - If the integration for the respective scanner or the CI lookup rules job is running, then detection key can’t be modified.
   - If the detection key has been updated and the scheduled job is run to update the detections with the new key, configurations can't be modified until the job is completed.
   - If the detection key update job is running, then the integration for that particular scanner will not run.
6. The scanner for which the detection keys are changed:
   - Fixing the detections for updated key for Qualys
   - Fixing the detections for updated key for Rapid7
   - Fixing the detections for updated key for Tenable

   All existing detection and vulnerable item records are updated using the revised detection key. New detections generated by integrations use the new detection key fields.

Configure the vulnerable item key

Configure the granularity of the vulnerable item (VI) key in the Vulnerability Response application to define what makes a vulnerable item (VI) in your organization.

Before you begin

Role required: admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Key terms:

Configuration item (CI)

An existing asset listed on your CMDB.

Vulnerability

A record of a known vulnerability imported from the National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE), or third-party integrations with Vulnerability Response.

Vulnerable item

A vulnerable item is created when an imported vulnerability matches a configuration item in your CMDB.

Detection

A single, distinct occurrence of a vulnerability as reported by the scanners of your third-party integrations. Detections are imported and displayed on both the detection and the vulnerable item records in your instance. Also referred to as a Vulnerable Item Detection.

By default, a vulnerable item is a unique combination of a configuration item (CI), a vulnerability, and an integration instance. To create vulnerable items with more granularity, add unique ports from vulnerable item detections to help you manage remediation of vulnerabilities at the level you feel is most effective for your organization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you want to create vulnerable items with more granularity, configure the vulnerable item key so that it includes port. When Include port is enabled, vulnerable items are created by unique ports from vulnerable item detections.

Starting from Vulnerability Response V17.1, you can identify and remediate Rapid7 vulnerabilities by adding proof as the VI key. For more information, see Adding proof to Rapid7 vulnerable item keys.

Choose an option from the following table to enable the Include port option.

Three scenarios for enabling the Include port option with the VI key for the first time

If...	Description
One or more of the following conditions is true: • You are upgrading from a version of Vulnerability Response prior to v10.0 that did not support vulnerable item detections. • You are a new customer and you have no Vulnerability Response data (vulnerable items or vulnerable item detections) in your ServiceNow AI Platform® instance. • You have already deleted all your vulnerable item records and related data in your instance and you are ready to build all your Vulnerability Response data starting with a fresh import to include VIs distinguished by unique port.	Enable Include Port. After Include port is enabled, imported detections create vulnerable items that include VIs distinguished by unique port starting with the next import.
Both conditions are true: • You have v10.0 or later of Vulnerability Response and you have existing Vulnerability Response data (vulnerable items or vulnerable item detections) in your instance that you want to preserve. • You want to start creating new vulnerable items to include VIs distinguished by unique port.	Enable Include port. Your existing detections and their associated vulnerable items will be preserved. After Include port is enabled, new detections create new vulnerable items that include VIs distinguished by unique port starting with the next import.
Both conditions are true: • You have v10.0 or later of Vulnerability Response. • You have existing Vulnerability Response data (vulnerable items or vulnerable item detections), but you do not want to preserve your existing data, because you prefer to build your vulnerability data starting from a fresh import and you want to include VIs distinguished by unique port.	1. Delete all your vulnerable item records and related data from your instance. 2. Enable Include port. After Include port is enabled, new detections create new vulnerable items that include VIs distinguished by unique port starting with the next import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If the Include port option is enabled, more than one vulnerable item may be created for a configuration item. For example, if a vulnerability exists for two ports on a configuration item, ports 80 and 443, two unique VIs are created, one for each port starting with the next import.

Note: Be sure you want to create VIs to include VIs by unique ports before you enable this feature. Once you enable the VI key to include port, you must first delete your Vulnerability Response data before you can disable Include port and return to importing vulnerability data using the default VI key granularity, that is, where VIs are created for port but not distinguished by a unique port. For more information about deleting your vulnerability data, See Delete all your vulnerable item records and related data in Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Configure VI granularity**.

   The Last Updated field displays the date the VI key was last configured.

2. Click the Include Port check box to enable it.
3. Click **Save**.
   The Confirmation dialog is displayed.

   If you have no vulnerable item detection records in your instance, both vulnerable item detections and vulnerable items are created by unique port starting with your next import.

   If you have existing vulnerable item detections and vulnerable items in your instance, existing detections and associated vulnerable items will be preserved. New detections create new vulnerable that include VIs distinguished by unique port starting with the next import.

What to do next

Verify vulnerable items by port are displayed on the vulnerable item detection and vulnerable item records. For more information, see View Vulnerability Response vulnerable item detection data.

Adding proof to Rapid7 vulnerable item keys

Add proof as a vulnerable item (VI) key for the Rapid7 VIs. Including the proof for specific vulnerabilities enables the Rapid7 scanner integration to create VIs for each proof received from Rapid7.

A VI key is the combination of vulnerability, configuration item (CI), and integration instance. Splitting detections into different VIs based on proof creates multiple VIs. You can assign the vulnerabilities to the appropriate remediation owners.

For example, there might be two detections with the same vulnerability and CI, but with different proofs, leading to the creation of one VI. Starting from Vulnerability Response V17.1, you can identify and remediate vulnerabilities by adding proof as the VI key.

You can add the proof as a VI key in the following way:

Navigate to **All** > **Vulnerability Response** > **Administration** > **Configure VI granularity** and select the option to include proof.

Use case: Including proof in VI key for existing VIs or splitting existing VIs based on detection proof

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To create VIs based on proof, you can use the R7 log4j vulnerabilities. For example, you can use one of the multiple R7 log4j vulnerabilities such as `R7 - apache - log4j - core - cve - 2021 - 44228`, `R7 - amazon_linux - cve - 2021 - 44228`, or `R7 - amazon - linux - ami - 2 - cve - 2021 - 44228`.

If all the detections in a VI have the same proof, then the existing VI is updated to include 'Proof in the VI Key (external_id)'. If there are multiple detections with different proofs, then the existing VI is closed. The detections are split across the new VIs with 'Proof in the VI Key (external_id)'.

Note:

If you provide the vulnerability ID, the existing VIs are split based on the proof. The new vulnerabilities for this vulnerability ID also have proof as one of the VI keys.

Delete all your vulnerable item records and related data in Vulnerability Response

Permanently remove all Vulnerability Response data (vulnerable items or vulnerable item detections) and related data and records from the from the Vulnerability Response application in your ServiceNow AI Platform® instance.

Before you begin

Delete vulnerable item detection records, vulnerable items, vulnerability groups, and any related records in the Vulnerability Response application from your instance. Use this process to clean out your instance to import data with a fresh start from your third-party integrations, or, as a prerequisite to returning the vulnerable item (VI) key configuration to its default setting. For more information on configuring the VI key, see Configure the vulnerable item key.

Note: This action deletes all the vulnerable item records and any related data from your instance. This data once deleted cannot be retrieved. It also requires you to suspend data import and disable your active third-party integrations with Vulnerability Response.

Deleting your vulnerable item data with this process prior to changing the VI key configuration is required. Removing all data ensures that all your vulnerable items and vulnerable item detections are mapped and updated with the most current data starting with the next Import.

Verify the following conditions apply prior to deleting your data:

- You have v10.0 or later of Vulnerability Response installed. For more information, see Vulnerability Response vulnerable item detections from third-party integrations.
- You want to disable Include port and return the VI key configuration to its default setting.
- You have existing vulnerable items and vulnerable item detections but do not want, or need to update and keep them.
- You have determined you want to remove all existing Vulnerability Response data and related records to clean up your instance.

Role required: sn_vul.vulnerability_admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Integrations**.
2. Record all of the active integrations that are displayed.

   All of the active integrations listed with scheduled jobs are disabled prior to deleting all of your vulnerable items and related data so that no new data is imported during the data removal. Recording this list helps you activate your integrations after the delete is completed.
3. Review the How to delete Existing Vulnerability Response Data for Reimport article in the HI Knowledge Base.
4. If a warning message is displayed that prevents you from writing to the Active column, to disable active integrations, follow these steps.

   a. In the Name column click an item to open the record.

   b. If you cannot edit the Active check box, click the **here** link to edit the record.

   c. Click the **Active** check box to disable the integration and the cancel the next scheduled job.

   d. Click **Update** to save your changes and return to the list.

   e. Verify you have disabled any active integrations from the Integrations list.
   After you disable an integration, it is no longer displayed on the active integrations list. To view a list inactive integrations, and locate all the integrations you disabled after you delete all your vulnerability data, in the Active column at the top, enter `=false`.
5. Continue with the steps in the KB article for deleting your existing vulnerability data.
6. After you have confirmed that all data is successfully deleted, navigate to **Vulnerability Response** > **Administration** > **Configure VI granularity**.
7. On the form:
   - If you deleted data because you prefer to build your vulnerability data to include port from a fresh import, enable Include port and click **Save**.
   - If you deleted data because you want to return the VI key to its default setting, disable Include port and click **Save**.

   For more information, see Configure the vulnerable item key.

Filtering within Vulnerability Response

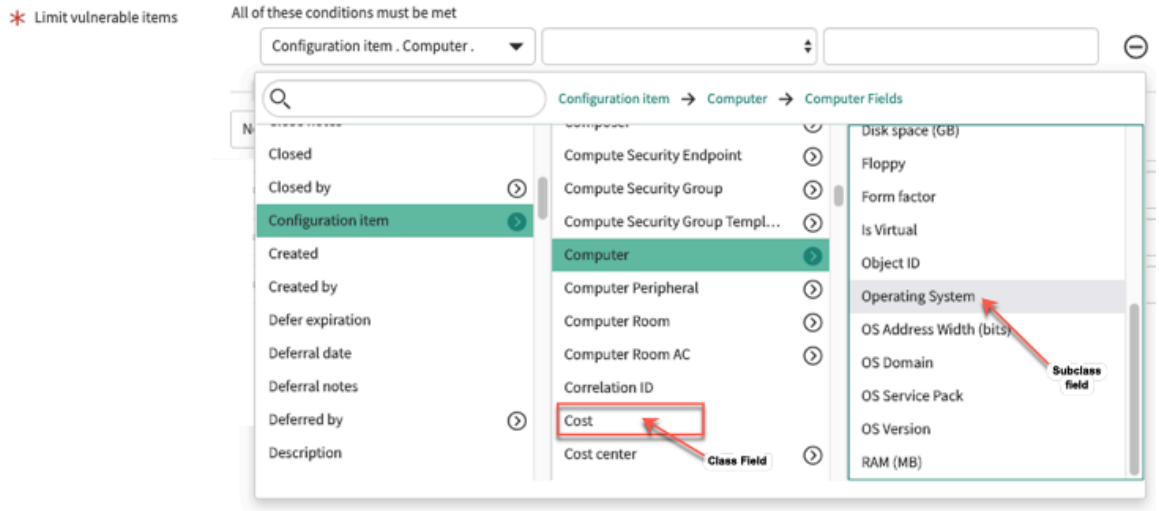
Remediation Task Rules, Calculators, and Assignment Rules use conditions during import, created using the **Condition builder**. Changes to their criteria can affect performance since each record is evaluated using these filters.

The rules and calculators shipped with the base system are optimized for performance. Editing or creating rules or calculators takes care and may require both ServiceNow and Vulnerability Response expertise.

Avoid filtering based on subclass fields

Some tables support extension. An example of that is the CMDB CI [cmdb_ci] table. Tables like cmdb_ci_hardware and cmdb_ci_computer extend this table. If you filter based on a field that is not on the parent table, that filter can be expensive to construct and evaluate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



For example, filtering on **Configuration Item** > **Cost** would not adversely affect performance because **Cost** is a class field, and not a subclass field, of **Configuration Item**.



Configuration Item > **Computer**, however, is a subclass requiring a dot-walk to another field, in this case, **Operating System**. This process can take many milliseconds which adds up quickly, when millions of vulnerable items are being imported, and affect performance.



Note: Using the [contains] condition is like a wild card search and can cause performance impact. Using [is], wherever possible, is more efficient.

Severity mapping for Vulnerability Response

Vulnerability Response ships with National Vulnerability Database (NVD) to normalized ServiceNow severity mapping. ServiceNow third-party integrations provide severity mappings upon installation. These maps can be adjusted by changing the fields in existing maps.

Rapid7 Vulnerability Integration Severity Mapping

Normalised_Severity

Calculate normalised_severity on third-part entry using the severity coming from **sn_vul_nvd_entry** table. This is set using Business Rules for Lookup normalized severity on **sn_vul_entry** table.

Source_severity

Data from the **severity_score** table is mapped to **source_severity** table while the **Rapid7 Vulnerability Integration- API** is running.

Priority

This field is empty.

Qualys Vulnerability Integration Severity Mapping

Normalised_Severity

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Calculate normalised_severity on third-part entry using the severity coming from **sn_vul_nvd_entry** table. This is set using Business Rules for Lookup normalized severity on **sn_vul_entry** table.

Source_severity

Data from the **SEVERITY_LEVEL** is mapped to the **source_severity** table while the **Qualys Knowledge Base Integration** is running.

Priority

Data for the Priority field is obtained from **SEVERITY table** and mapped to **priority** table while **Qualys Host Detection Integration** is running using the Business Rule mapped to Qualys Data.

Note: Business Rules run in the background and checks the priority for Qualys and accordingly maps the Priority. So, to map Qualys data, BR is responsible.

Tenable.io Vulnerability Integration Severity Mapping

Normalised_Severity

Calculate normalised_severity on third-part entry using the severity coming from **sn_vul_nvd_entry** table. This is set using Business Rules for Lookup normalized severity on **sn_vul_entry** table.

Source_severity

Data from **risk_factor** table is mapped to **source_severity** table while the **Tenable.io Plugin Integration** is running.

Priority

Data from **severity_id** is mapped to **source_severity** while the **Tenable.io Open Vulnerabilities Integration** is running.

VPR

Data from **score** is mapped to **Source_risk_score** while **Tenable.io Plugin Integration** is running.

Data from **Calculated from score** is mapped to **Source_risk_rating** while **Tenable.io Plugin Integration** is running.

Tenable.sc Vulnerability Integration Severity Mapping

Normalised_Severity

Calculate **normalised_severity** on third-part entry using the severity coming from sn_vul_nvd_entry table. This is set using Business Rules for Lookup normalized severity on **sn_vul_entry** table.

Source_severity

Data for **riskFactor** table is mapped to **source_severity** while the **Tenable.io Plugin Integration** is running.

Priority

Data from **severity** received as **"severity": { "id": "0", "name": "Info", "description": "Informative" }** is mapped to **source_severity** while the **Tenable.io Open Vulnerabilities Integration** is running.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

VPR

Data from **vprScore** is mapped to **Source_risk_score** while **Tenable.io Plugin Integration** is running.

Data from **Calculated from vprScore** is mapped to **Source_risk_rating** while **Tenable.io Plugin Integration** is running.

TVM Severity Mapping

Normalised_Severity

Calculate normalised_severity on third-part entry using the severuty coming from **sn_vul_nvd_entry** table. This is set using Business Rules for Lookup normalized severity on **sn_vul_entry** table.

Source_severity

Data from **severity** table is mapped to **source_severity** while **Microsoft TVM Vulnerability(CVE) Integration** is running.

Priority

This field is empty.

Create a Vulnerability Response severity map

Vulnerability Response severity mapping transforms third-party source severity fields to recognizable fields in Vulnerability Response.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

Vulnerability Response ships with National Vulnerability Database (NVD) to normalized ServiceNow severity mapping. ServiceNow third-party integrations such as the Qualys Vulnerability Integration provide severity mappings upon installation. These maps can be adjusted by changing the fields in existing maps.

Creating or editing a severity map is intended only for customized or non-standard third-party mappings in your environment.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Normalized Severity Mapping**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field mapping

Field	Description
Source	The name of the source for the severity mapping.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source value	The source severity value.
Target value	The target severity value. Choices are: ○ 1- Critical ○ 2 - High ○ 3 - Medium ○ 4 - Low ○ 5 - None

4. Repeat Step 3 for each source severity level.
5. Click **Submit**.

Define service classifications for Vulnerability Response reporting and related lists

Bring more focus to reporting and related lists in Vulnerability Response by defining service classifications. In addition, reducing the number of requested service classifications can improve the performance of Vulnerability Response data gathering.

Before you begin
Role required: admin

Note:

Editing system properties requires both ServiceNow and Vulnerability Response expertise.

Procedure

1. Enter `sys_properties_list.do` in the left navigation bar.
2. Click **Enter**.
3. In the **Search** menu, under **Name** enter `sn_vul.service_classifications`.
4. Open the *`sn_vul.service_classifications`* system property.
5. In the **Value** text box, enter the comma-separated list of the service classifications you want.

   Note: When this setting is empty, all services are listed.

   Examples:

   To see Business Services, Technical Services and Application Services and exclude Service Offerings, Shared Services, and unclassified services, set the value to: **Business Service,Technical Service,Application Service**.

   To see Application Services, set the value to: **Application Service**.

6. Click **Update**.
   The data in each report and vulnerable item related list is filtered by service classification during the next run of the nightly performance analytics job.

Audit selected fields in the vulnerable items table

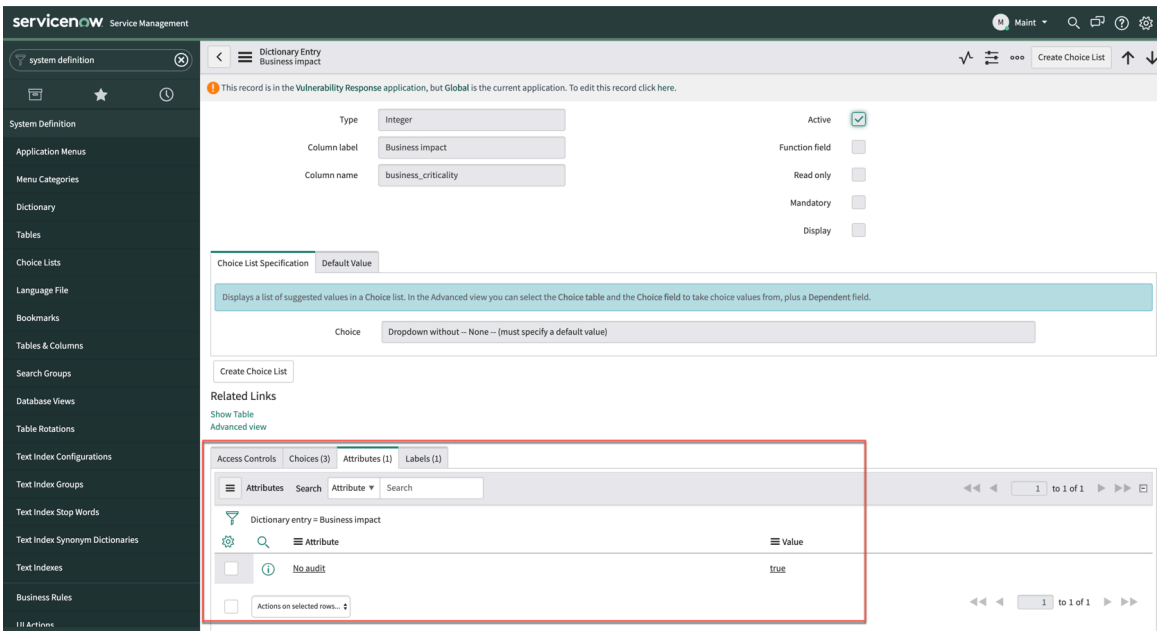
Enable auditing for fields you specify in the Vulnerable Item [sn_vul_vulnerable_item] table. This method of auditing is useful when you want to audit fields that you cannot audit by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
The sn_vul_vulnerable_item table is auditable by default. Fields that have the no_audit attribute set to true are not auditable. For more information about auditing tables, see Enable auditing for a table.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **System Definition** > **Tables** and search for the sn_vul_vulnerable_item table.
   The list of dictionary entries for the table is displayed.
2. To enable auditing for a field, click the name of the entry.
   The Dictionary Entry page for that entry is displayed.



3. Navigate to **Attributes** > **No audit**.
   The Dictionary Attribute page is displayed.
4. To remove the no audit=true attribute, click **Delete**.
   Auditing for this field is enabled.

Vulnerability Response background job framework configuration

Define the background job framework in your ServiceNow AI Platform® instance. These configuration changes can help you improve performance by reducing the amount system resources used to run your background jobs.

What can you edit in the background job framework

With the Background job configuration module, you have the following setting options in the framework:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can define the number of background jobs that run concurrently for Vulnerability Response processes.
- For long jobs that run in the background and process large amounts of data, you can create partitions to process data in smaller chunks.
- You can cancel a job.

Why configure the background job framework

Background jobs in your ServiceNow AI Platform® are designed to run for long periods of time to perform multiple processes on your records in Vulnerability Response. These jobs were previously based on business rules that run asynchronously. There is no limit to the number of these jobs that can run in the background in your instance so that the large amounts of records that are impacted by these jobs can be processed. When multiple jobs that take a long time to complete, run concurrently in the background, the system resources used to run your scheduled jobs are impacted, which in turn, might negatively impact your performance.

Configuring the background job framework can help you improve your performance by reducing the amount system resources used to run your background jobs.

Key terms

Job capability

Describes the particular jobs. For example, a particular job might include the following capabilities:

- The job can be run in parallel with another job of the same type.
- The job can be partitioned.
- The job can be canceled while running.

Concurrency

Refers to jobs or pieces of jobs that run in parallel.

Partition

Partitions are pieces of jobs that can be split up so that they can be processed in parallel to achieve better performance. Usually refers to jobs with long run times.

Job configuration

Refers to the settings for a particular scheduled job.

Scheduled job

Scheduled Jobs are automated pieces of work that can be performed at a specific time or on a recurring schedule.

System resources

Refers to the amount of system resources you must support a given number of background jobs and scheduled jobs in your environment.

System property

System properties store configuration information that rarely or never changes. Each time you change or add a system property, the system flushes the cache to keep all nodes in the cluster synchronized. This cache flush impacts performance.

Business rule

A business rule is a server-side script that runs when a record is displayed, inserted, updated, or deleted, or when a table is queried. Business rules accomplish tasks

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

like automatically changing values in form fields when certain conditions are met, or creating events for email notifications and script actions.

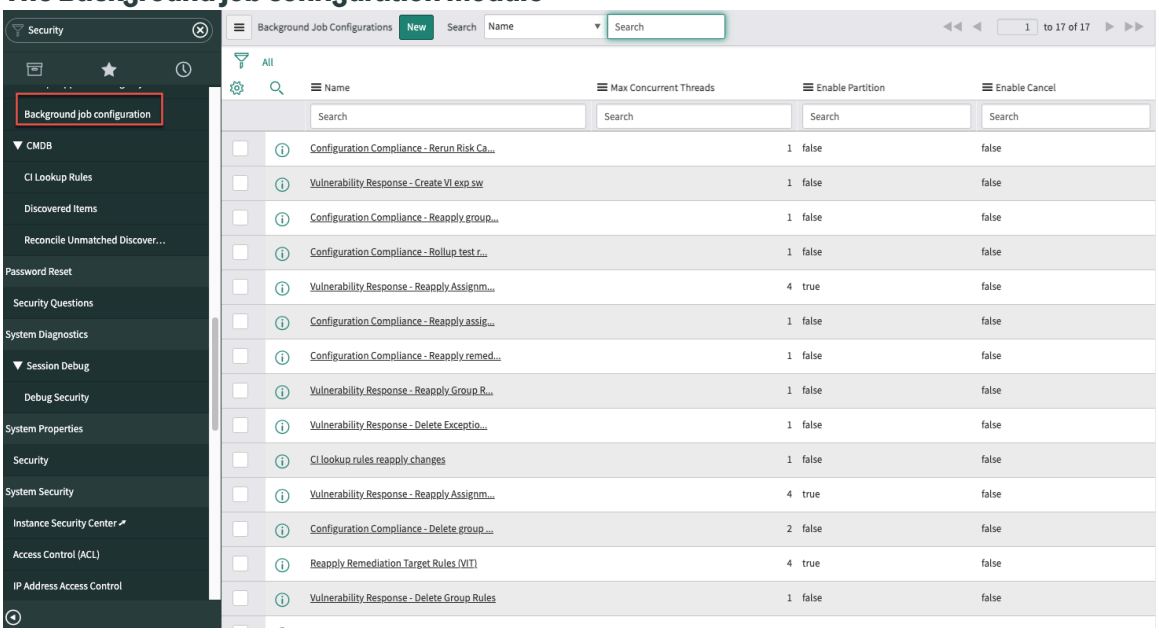
Use case for defining the background job framework

For example, the background job that applies remediation target rules for vulnerable item records (VITs) and Application Vulnerability Response vulnerable item records (AVITs) simultaneously processes large amounts of records with multiple tasks.

Depending on the size of the import and the number of records you have in your environment, this job might use a large amount of your available system resources and take a long time to successfully complete. System maintenance jobs or other scheduled jobs might run more slowly.

The Background job configuration module, jobs are listed by name and a unique Configuration ID. On these records, you can define how many tasks you want to run concurrently for a given background job. You can also set the job to process partitions of data so the tasks complete more quickly and easily and use less of your system resources. You can also cancel a job if you determine it is running too long.

The Background job configuration module



For more information about the required steps to define the background job configurations, see Define background job configurations in Vulnerability Response.

Define background job configurations in Vulnerability Response

Define how many tasks you want to run concurrently for a given background job. You can also set the job to import partitions of data so the tasks complete more quickly and easily and use less of your system resources. You can also cancel a job if you determine it is running too long.

Before you begin

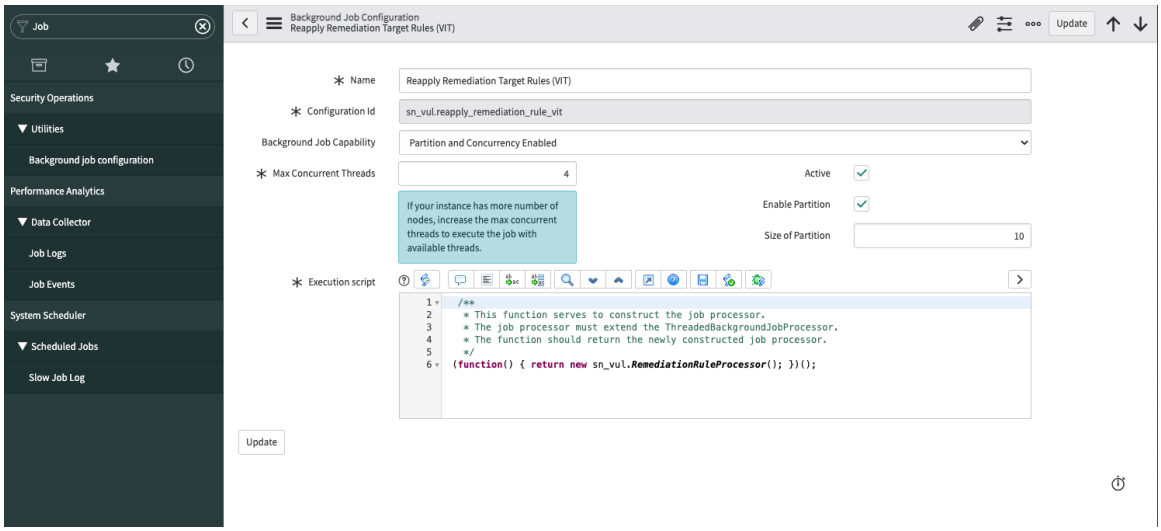
Role required: sn_vul.vulnerability_admin or Vulnerability managers with the sn_sec_cmn.manage_background_job granular role

See the section below the steps for an example.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Operations** > **Background Job Configurations**.
2. In the Name column, click a record to open it.
3. Edit the fields.



Field	Description
Name	Name of the job.
Configuration ID	Read-only. Unique ID used to identify the job.
Background Job Capability	Choose one. ○ Partition and Concurrency Enabled - A job with a long run time can be split up, and the job can be run in parallel with another job of the same type. ○ Concurrency Enabled - The job can be run in parallel with another job of the same type. ○ Cancel Enabled - The job can be can celed. ○ Concurrency and Cancel Enabled - The job can be run in parallel with another job and be canceled. ○ Partition, Concurrency, and Cancel En abled - A job with a long run time can be split up, the job can be run in parallel with another job of the same type, and the job can be canceled. ○ None The displayed value indicates if a job sup ports partitioning, concurrency, and cancella tion.
Max Concurrent Threads	This field is displayed only if concurrency is supported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Enter the maximum number of jobs you want this configuration to run in parallel. The number of scheduled jobs supported by your instance is by default 10. You can lower this value if you believe you might use, or have lower system resources available to run your background jobs.
Active	Enable or disable the job If a job is disabled, you cannot create jobs of this type. Any existing jobs in the queue will not be processed.
Enable Partition	This field is displayed only if partitioning is supported. This option permits you to limit and define the number of items this job can process at one time. The Size of Partition field is also displayed. If you leave this field disabled, background jobs that support partitioning process all the items in your instance with this job.
Size of Partition	This field is displayed only if partitioning is supported. Default is 10,000 items. Enter a value for the number of items per data chunk you want this job to process. This option is available for jobs that process large numbers of records such as VIs, remediation tasks, test results, and test result groups.
Execution script	Displays the job processor that is used to run this job. A default method for jobs that support partitioning is provided.
Enable Cancel	This field is only displayed if job cancellation is supported. This option is supported for jobs that process discovered items and reapply CI rules.

4. Click **Update** to save your changes.
   See the following example for how to verify results for your configuration changes.

   There are two Remediation target rules job configurations that are included with the application, one for vulnerable items, one for application vulnerable items:

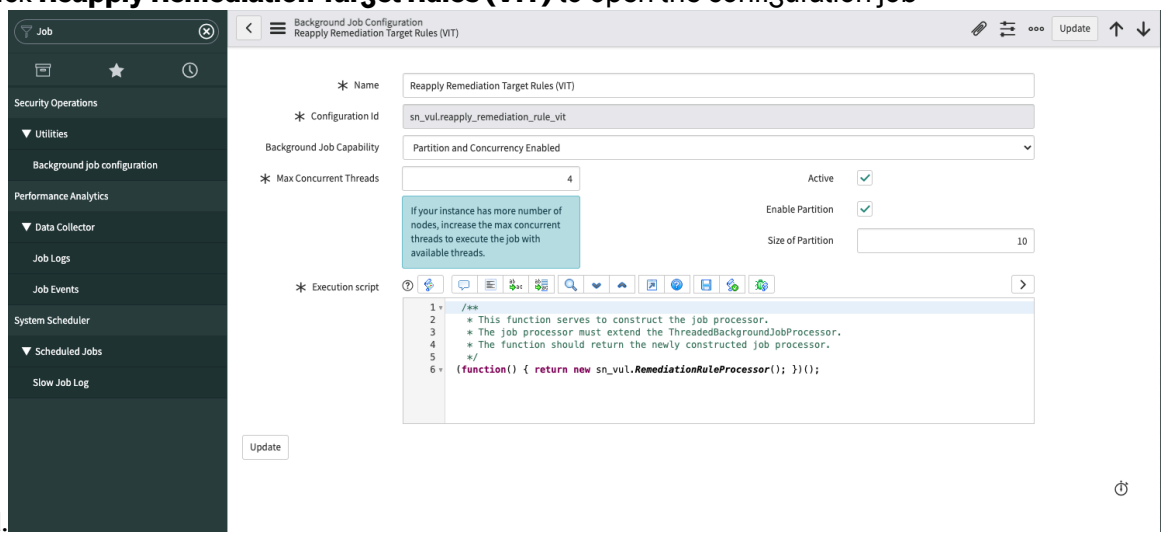
   - Reapply Remediation Target Rules (VIT)
   - Reapply Remediation Target Rules (AVIT)

   Assume that you change to your remediation target rules and want to reapply them without using most your available system processing resources. To help you limit the processing

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

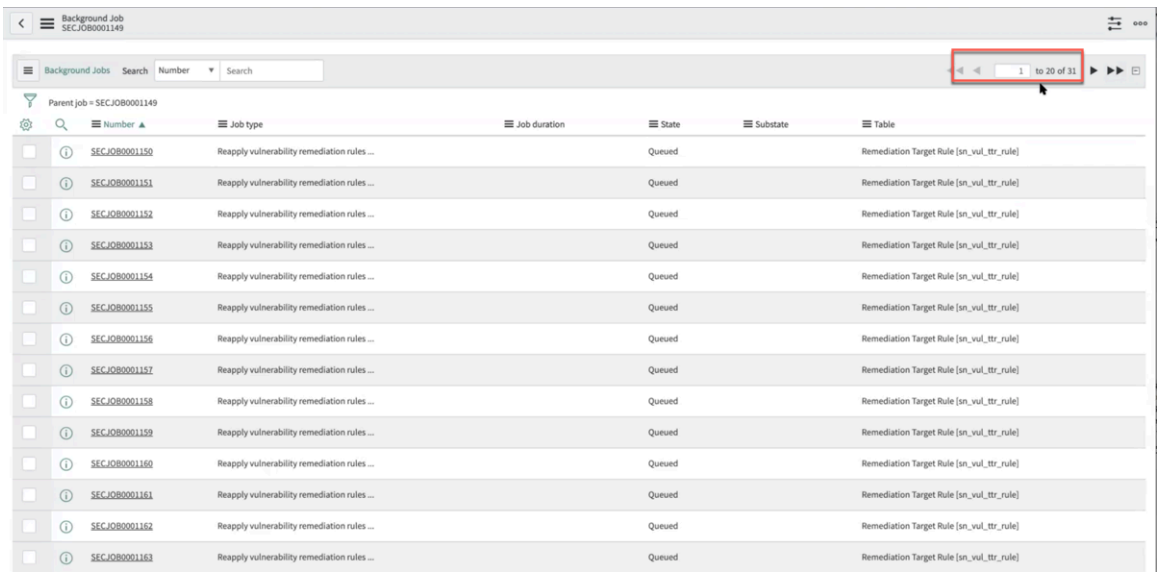
resources, you can control the number of background jobs you run and the number of items you process per job in the Background Job Configurations module.

5. To define these settings, navigate to **Security Operations** > **Background Job Configurations** and click **Reapply Remediation Target Rules (VIT)** to open the configuration job record.



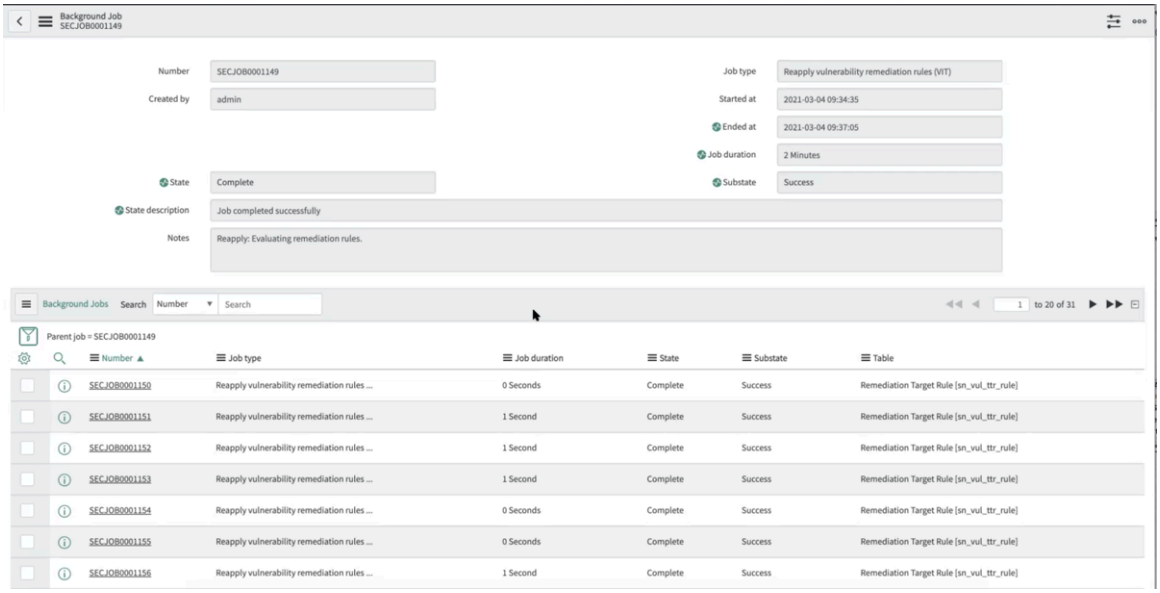
For the sake of the example, say you know you have just over 300 VIs.

6. On the open configuration job record, change the Partition size value from **4** to **10**.
7. Navigate to **Vulnerability Response** > **Remediation Target Rules**, locate the Reapply vulnerability remediation rule you changed, select the record from the list and click **Apply Changes** to reevaluate your target rules for your existing VIs.
The Reapply vulnerability remediation rules (VIT) job is queued.
8. Click the **View status** link to view the Background job record and verify that the jobs are queued, as shown in the following image.
For this example, 31 jobs are created to process target rules for 307 VIs (maximum of 10 items per job). These jobs are child jobs of the primary background job. The child jobs process the records sequentially.



When all the jobs successfully complete, the fields are updated on the Background Job record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Navigate to your vulnerable items and verify they reflect your new rule change.

Advanced parallel processing for background jobs in Vulnerability Response

With this advanced setting, control the total number of background jobs that are being processed parallel, regardless of the job type.

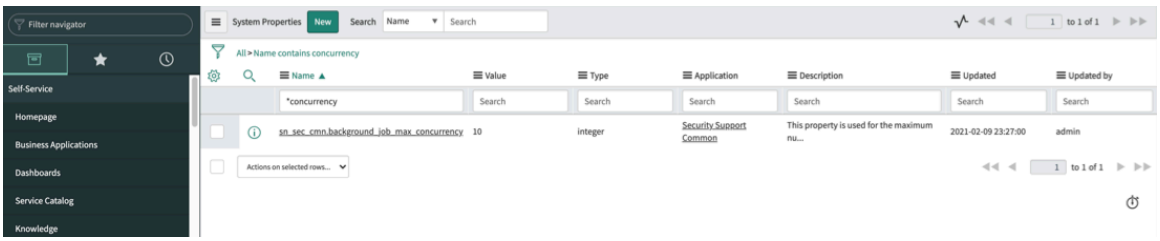
Before you begin

Role required: sn_vul.vulnerability_admin, or Vulnerability managers with the sn_sec_cmn.manage_background_job granular role

Note: This procedure requires advanced programming knowledge.

Procedure

1. In the Filter navigator, enter **sys_properties.list** and locate the *sn_sec_cmn.background_job_max_concurrency* system property.



2. Click it to open the record.

By default, the *sn_sec_cmn.background_job_max_concurrency* system property executes a maximum of 10 background jobs in parallel.

If your instance has a low number of nodes, you can reduce this value in the system property. For example, say you have seven assignment rules on your Group rules list. On the Reapply Assignment rules job configuration record, three jobs are set for the Max concurrent threads. Your concurrency value for your framework is 10, but your system is a single node instance, so you can process two partitioned jobs from your Reapply Assignment Rules job concurrently. If you set the Maximum Max concurrent threads to one Assignment rules job record, all the Reapply Assignment Rules job type will be processed sequentially.

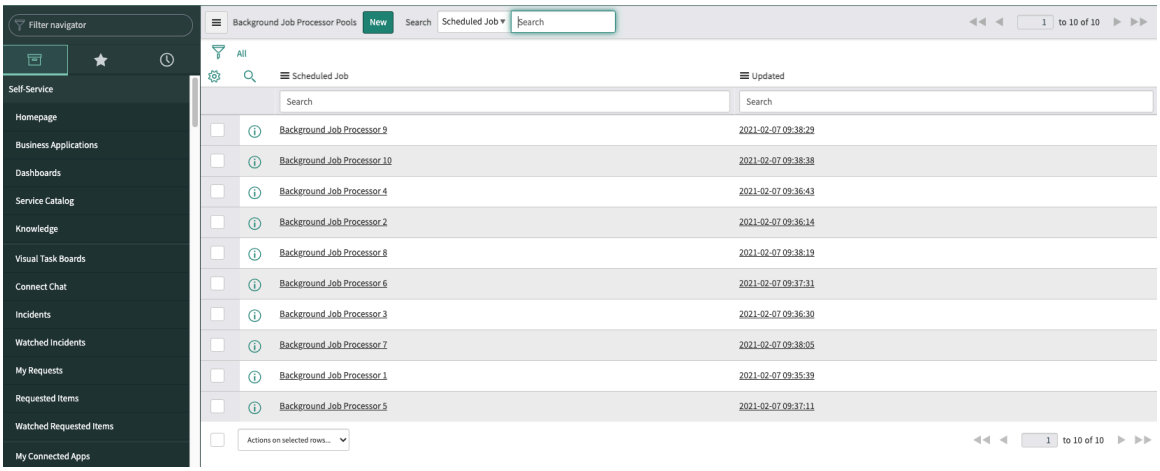
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Conversely, if your instance has more nodes, you can increase this value, but you also must add more scheduled jobs to make this change.

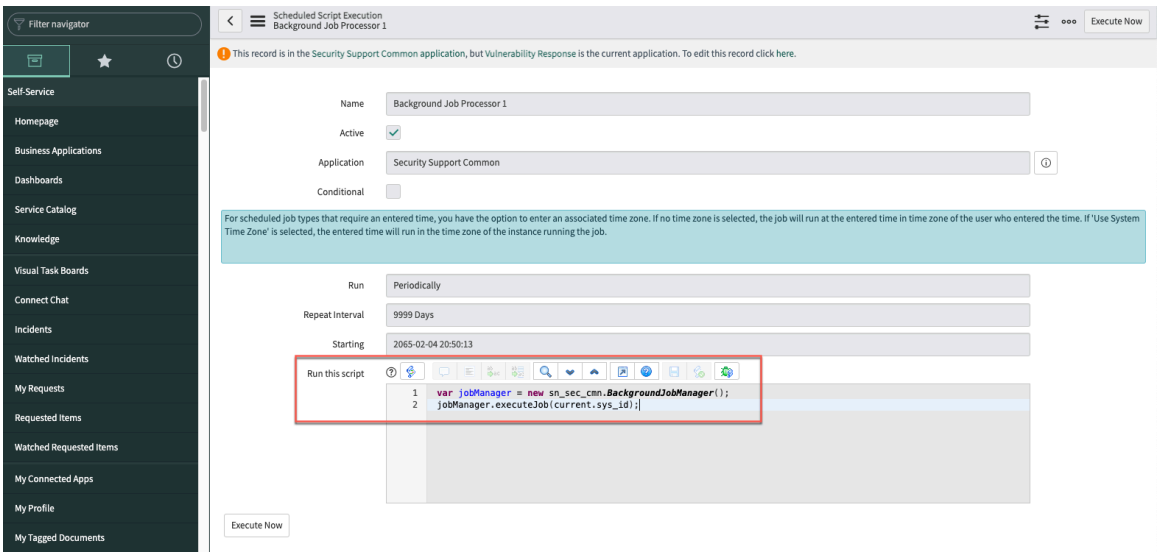
To increase the number of scheduled jobs, duplicate a scheduled job as many times as you need to match the value that you increased your system property by. For example, by default, there are 10 scheduled jobs. So, if you want 20 jobs, you must duplicate a job 10 times.

The ten scheduled jobs that are included with the ServiceNow AI Platform® for processing are displayed in the sn_sec_cmn_background_job_processor_pool table.

3. In the Filter navigator, enter **sn_sec_cmn_background_job_processor_pool.list**



4. Click a job to copy and duplicate it as many times as you need so that the number of jobs matches the value that you increased your system property by.



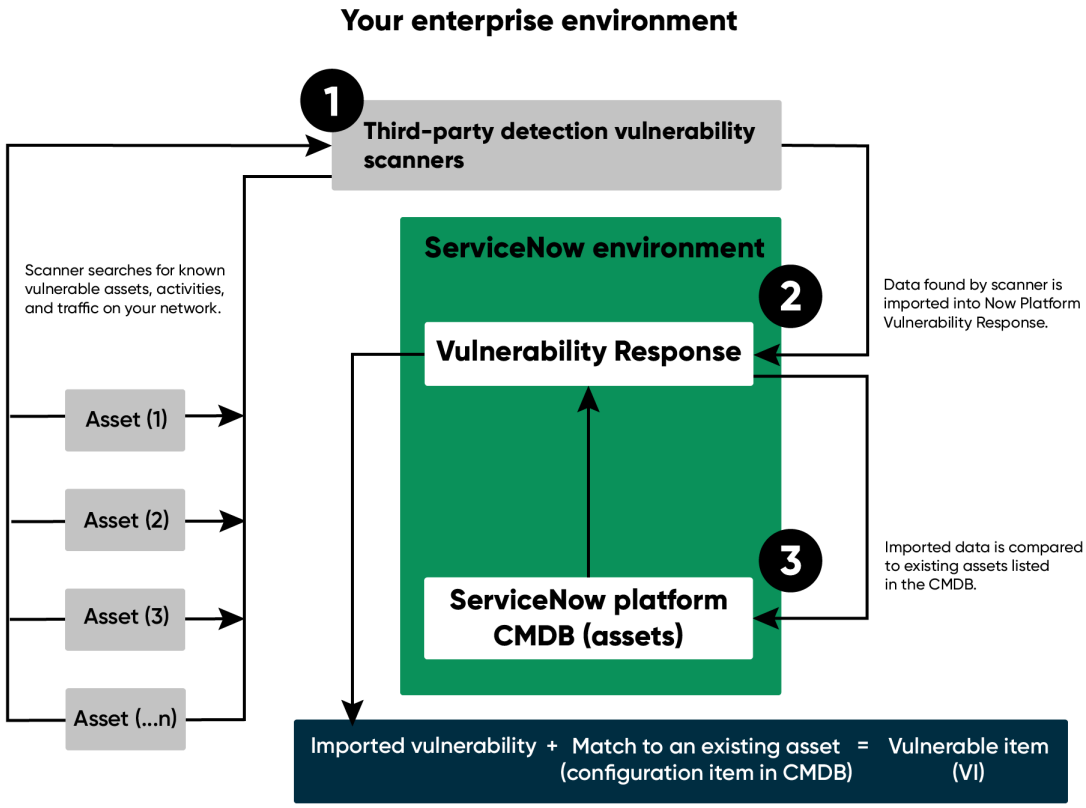
5. After the scheduled job is defined, add a reference by clicking **New** on the sn_sec_cmn_background_job_processor_pool list for the job you copied.

Vulnerability Response integrations

Vulnerability Response includes support for third-party integrations. Included in this section are some basic guidelines for developing your own integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Third-party integrations



Imported vulnerabilities from the National Vulnerability Database (NVD) and detection data from third-party scanners are reconciled with the assets in your CMDB. When an imported vulnerability matches an existing asset, a vulnerable item is created. Vulnerable items are grouped automatically into tasks for remediation, risk-scored with business context, prioritized and assigned to appropriate teams for remediation.

Note:

Third-party integrations are treated separately. If more than one third-party integration application is in use in your environment there is no vulnerable item (VI) deduplication across integrations. For example, VI deduplication between Rapid7 and Qualys is not available.

However, mismatches in detection count between a third-party scanner (for example, Qualys) to VIs in your ServiceNow instance are expected, since we dedupe across IPs, ports and so on.

For information about third-party integrations supported by Application Vulnerability Response see, Integrating Application Vulnerability Response with other applications

- CISA Known Exploit Vulnerability (KEV) Integration
- Understanding the Microsoft Threat and Vulnerability Management Vulnerability integration
- Understanding the HCL BigFix patch orchestration integration with Vulnerability Response
- Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM
- Understanding the NVD integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Qualys Vulnerability Integration
- Understanding the Rapid7 Vulnerability Integration
- Shodan Exploit Integration
- Understanding the Tenable Vulnerability Integration
- Microsoft Security Response Center Solution Integration

  The Microsoft Security Response Center Solution Integration is available with Vulnerability Solution Management. For information on the installation and configuration of the Microsoft Security Response Center Solution Integration and the Red Hat Solution Integration, see Install the Solution Management for Vulnerability Response application. You can configure, edit, schedule, and launch on-demand the Microsoft Security Response Center Solution Integration and the Red Hat Solution Integration from within the Setup Assistant.

Additional notes for integrations

If multiple deployments are supported for an integration, see Create domain-separated imports for an integration.

- You can install, configure, schedule, and launch on-demand many of the integration applications from within Setup Assistant.
- You can install the Rapid7 Vulnerability Integration application from Setup Assistant, but configuration is not supported for this integration from within the Setup Assistant. See Install the Rapid7 Vulnerability Integration for more information.
- The Tenable for Vulnerability Response application by Tenable is created and maintained by Tenable. See their documentation at Tenable for Vulnerability Response.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Starting from VR v17.1, the following integration process state names have been updated:

State name prior to V17.1	State name V17.1 onwards
Processing	Retrieving

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State name prior to V17.1	State name V17.1 onwards
WaitComplete	Waiting/Processing

Note: You can view the attachments that are downloaded and processed. When the status of the integration run is `waitcomplete`, it displays the percentage of integration that is complete.

Manually created integrations

You can add other integrations that are not available as ServiceNow Store applications, as needed. See Manually create a vulnerability integration for more information.

Vulnerability Response applications and CSDM tables

The Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications manage (contribute data to) CSDM tables. These applications also use data from CSDM tables that other applications generate. Several ServiceNow products, therefore, benefit from and add value to these Security Operations applications. See Vulnerability Response applications and CSDM tables for more information.

Understanding the NVD integrations

The NVD integrations use data imported from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) product to help you determine the impact and priority of flaws in your code. Run this integration as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The NIST NVD collects both Common Vulnerabilities and Exposures (CVE) and Common Platform Enumeration (CPE) data and makes that data available to the ServiceNow AI Platform®. It easily integrates with Vulnerability Response to map CVE and CPE vulnerabilities enriching the data in your instance.

Important: There's a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

After it's installed, the NIST National Vulnerability Database Integration-API (CVE only) integration is invoked automatically as a scheduled job and runs daily. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Tip: Activation of this plugin on production instances may require a separate license.

Available versions

Release version	Release Notes
Vulnerability Response Integration with NVD v1.2	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Initial import of vulnerability data with the NVD and CWE integrations

1. Perform an initial import of CWE data with the CWE Comprehensive 2000 Integration.

   See Configure and run the scheduled job for updating CWE records. You perform CWE updates **On Demand** from the integration record by default, and, you must configure it.

   Note: Schedule the CWE update to run prior to the NVD database update. The default day for the NVD update is **Weekly** on **Monday**.

2. Verify the Vulnerability Response Integration with NVD application is installed and an initial data import from either the NIST National Vulnerability Database Integration - API (CVE only) or the NIST National Vulnerability Database Integration - API (CVE and CPE) is successful.

   For CPEs, verify an initial data import from the NIST National Vulnerability Database Integration - API (CPE only) is successful.

   Activation of this plugin on production instances may require a separate license. After the plugin is installed, the NIST National Vulnerability Database Integration - API (CVE only) is activated by default. It runs daily. See Install the Vulnerability Response Integration with the NIST National Vulnerability Database for more information.

3. Third-party libraries are updated as scheduled jobs. Refer to your integration documentation at Vulnerability Response integrations for more information about third-party integrations.

Understanding imported vulnerability data and vulnerable items

In your ServiceNow AI Platform instance, each imported vulnerability is represented by a vulnerability entry in the source libraries of third-party scanner products like Qualys, for example. The vulnerable items (VI)s that are imported and updated in your instance are references to third-party libraries, such as the Qualys library. A third-party library can, in turn, reference back to the NVD.

For example, when you ingest third-party vulnerability data from a product like Qualys, you're ingesting VIs that reference a QID (Qualys Identifier). In the case of Qualys, that QID in turn references a CVE from the NVD library. When you click that QID in a remediation task or vulnerable item record in the Vulnerability Response application, and you've run the NVD and CWE integrations to ingest data, you are viewing current, enriched vulnerability data that lets you see the relationships that exist between your VIs and CVEs, CWEs, and CPEs.

Before you run a third-party scanner product like Qualys that has its own library, you must first install and run, at a minimum, the NIST National Vulnerability Database Integration- API (CVE only) integration (also includes CISA-related details), CWE Integration to ingest vulnerability data. These NVD and CWE data imports enrich your Vulnerability Response or Application Vulnerability Response data prior to importing data with a third-party product.

For more information about managing the NVD, CWE, and third-party libraries and viewing them, see Importing data with the NVD and CWE integrations and managing third-party libraries and View Vulnerability Response vulnerability libraries.

After you verify the successful NVD import, to further enrich your vulnerability data, Configure and run the scheduled job for updating CWE records.

Perform the NVD and CWE imports prior to importing vulnerability data with a third-party product. Third-party libraries are updated as scheduled jobs. Refer to your integration documentation at Vulnerability Response integrations for more information about third-party integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Locating the NVD integrations

To view the NVD integrations, navigate to **Vulnerability Response or Application Vulnerability Response** > **Administration** > **Integrations**.

The following integrations are included in the base system.

Note: Only the NIST National Vulnerability Database Integration - API (CVE only) integration is active, by default.

NVD integrations

Integration	Description
NIST National Vulnerability Database Integration - API (CVE only)	Retrieves only NIST NVD vulnerability data (CVE). By default, this integration is automatically set to run daily.
NIST National Vulnerability Database Integration-API (CPE only)	Retrieves CPE data from NIST NVD. This integration is inactive by default. Activate this integration if you want to capture CPE data that includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. This information is stored in Vulnerable Software. This integration is set to run daily and is inactive by default. To activate this integration, see Activate the NIST National Vulnerability Database–API (CPE only).
NIST National Vulnerability Database Integration-API (Unmapped CPE)	Retrieves CPE data associated with fetched CVE from NIST NVD. This integration is inactive by default. Activate this integration if you want to capture CPE data that includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. This information is stored in an NVD vulnerability entry record related list. This integration is set to run On Demand and is inactive by default. To activate this integration, see Activate the NIST National Vulnerability Database–API (Unmapped CPE).

Important: The "NIST National Vulnerability Database Integration-API (CVE and CPE)" integration is deprecated.

For integration run statuses see, View the (National Vulnerability Database) NVD integration import run status.

Preparing for the NVD integrations

A successful integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The NVD integrations assume that you are familiar with the NIST National Vulnerability Database (NVD).

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Note: Before running the NVD integrations, make any necessary configuration changes based on your requirements.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Configure and run the scheduled job for updating CWE records

Data imports from the CWE further enrich the vulnerability data in your instance. Use Common Weakness Enumeration (CWE) records downloaded from the CWE database for reference when deciding whether a vulnerability must be escalated. Run this integration as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product.

Before you begin

Roles required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Note: Schedule the CWE update to run prior to the NVD database update. The default day for the NVD update is **Weekly** on **Monday**.

Update common weakness records from the Common Weakness Enumeration database on a regularly scheduled basis. You can also update the default script or write your own scripts, as needed.

Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations page.

- If you have the admin role, you can add repositories to the scheduled job.
- If you have sn_vul.vulnerability_read, you can execute the scheduled job.
- If you have sn_vul.vulnerability_write, you can edit the details of the scheduled job.

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.
2. Select the **CWE Comprehensive 2000 Integration** scheduled job.
3. Modify the fields, as needed.

Vulnerability Integration form

Field	Description
Name	Name of the scheduled job.
Active	Whether the scheduled job is active. If you do not want the job to run for a specific time period, you can set up the parameters you want to use and deactivate the job.
Run	Frequency you want the job to run. Subsequent fields are displayed or hidden based on your setting in this field. **Note:** The CWE update is **On Demand** by default. Set to a scheduled period that is prior to your NVD updates. Choices include: ○ Daily: Choose a **Time** ○ Weekly: (most common choice) Choose a **Day** and**Time** ○ Monthly: Choose **Day** and **Time** ○ Periodically: Choose a **Repeat interval**, **Starting** date and time ○ Once: Choose a **Starting** date and time
Day	The day you want the scheduled job to run. If you selected **Weekly** in the **Run** field, this field displays the days of the week. If you selected **Monthly** in the **Run** field, this field displays the days of the month. **Note:** Schedule the CWE update to run prior to the NVD database update. The default day for the NVD update is **Weekly** on **Monday**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Time	The time you want the scheduled job to start. **Note:** Schedule the CWE update to run prior to the NVD database update. The default time for the NVD update is 01:00:00
Integration script	The script for pulling data from the data sources specified in the **Data Sources** related list.
Source integration	[Read only]
Source Instance	[Read only]
Application	[Read only] The name of the application for which you are running the scheduled job.
Repeat Interval	The number of days and hours before the scheduled job runs again. This field appears when **Periodically** is selected in the **Run** list.
Starting	The date and time to start the periodic updates. This field appears when **Periodically** is selected in the **Run** list.
Conditional	The check box to add conditional parameters.
Condition	The conditions to run the schedule job. This field appears when **Conditional** check box is selected.
Report processor strategy	The strategy for pulling data and processing the scheduled job. ○ To pull data from the data sources in the **Data Sources** related list using the script in the **Integration script** field, select **Data Source Attachment**. ○ To select a custom processor in the **Report Processor script** field, select the **Custom Report Processor**.
Report processor	The script to be executed when the scheduled job runs. This field appears when **Custom Report Processor** is selected in the **Report processor strategy** list.
Processor factory script	The script to build the report processor. This field appears when **Custom Report Processor** is selected in the **Report processor strategy** list.

4. Right-click in the header to **Save** your changes.
5. To run the scheduled job immediately, click **Execute Now**.
   You are returned to the Vulnerability Integrations view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To watch the progress of the import, select the **CWE Comprehensive 2000 Integration** scheduled job again and select the **Vulnerability Integration Runs** tab.

   See View Vulnerability Response vulnerability libraries to see the imported entries.

Install the Vulnerability Response Integration with the NIST National Vulnerability Database

Before you run the integration on your instance, the installation and configuration steps must be completed so the NIST National Vulnerability Database (NVD) product properly integrates with Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application isn't installed and activated see, Install Vulnerability Response.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns users to the Vulnerability Manager in Vulnerability Response or the App-Sec Manager group in Application Vulnerability Response. For information on Group roles in Vulnerability Response see, Manage persona and granular roles for Vulnerability Response. For information on group roles in Application Vulnerability Response see Application Vulnerability Response user groups and roles. • The Vulnerability Manager or App-Sec Manager oversees configuration and verifies expected results.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Before running the NVD integrations, make any necessary configuration changes based on your requirements.

There's a configured run-as user for each integration record. The default value for this user is **VR.System**. Don't change this value.

Procedure

1. Log in to the instance you want to install the NVD integrations on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Vulnerability Response Integration with NVD application.
4. Select the application tile.
   Detailed information about the application you're installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Select **Request App** and enter your Now Support login credentials.
6. Select **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and select **Validate Instance**.
8. Select **Request**.
   You'll receive an email with detailed installation instructions.
9. Navigate to **All** > **System Applications** > **Applications** > **All**.
10. Locate the application, select it, and select **Install**.
    Your application is automatically installed on your instance.

What to do next

After initial installation, for modifications refer to Optional NVD integration modification and activities.

Activate the NIST National Vulnerability Database–API (Unmapped CPE)

To ingest Common Platform Enumeration (CPE) data for fetched Common Vulnerabilities and Exposures (CVE) data, you can perform a full data import with an on-demand scheduled job.

Before you begin

The National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (Unmapped CPE) integration captures (CPE) data that includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. This information is stored in an NVD vulnerability entry record related list.

Role required: sn_vul.vulnerability_admin or App-Sec Manager

Procedure

1. Navigate to **All** > **Vulnerability Response or Application Vulnerability Response** > **NVD** > **Integrations**.
2. Select the NIST National Vulnerability Database Integration–API (Unmapped CPE) integration.
3. Select the **Active** check box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The integration is pre-configured to run on demand. By activating the integration, it will automatically run after the NIST NVD Integration-API (CVE only) integration. Changing any other integration parameter requires both ServiceNow and Vulnerability Response and expertise and could result in incomplete data.

a. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.

b. Select NIST National Vulnerability Database Integration–API (Unmapped CPE) Integration.

c. Select the **Integration Details** tab.
Regardless of the **Import since** field's value, CPEs for all the retrieved CVEs are retrieved.

4. Select **Execute Now** to perform an initial full support integration run.
After the initial import is complete, scheduled imports of delta data resume. For integration run statuses, see View the (National Vulnerability Database) NVD integration import run status.

Activate the NIST National Vulnerability Database–API (CPE only)

To ingest Common Platform Enumeration (CPE) data, you can perform a full data import with a daily scheduled job.

Before you begin

The National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (CPE only) integration captures (CPE) data that includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name. This information is stored in a vulnerable software table.

Role required: sn_vul.vulnerability_admin or App-Sec Manager

Procedure

1. Navigate to **All** > **Vulnerability Response or Application Vulnerability Response** > **NVD** > **Integrations**.
2. Select the NIST National Vulnerability Database Integration–API (CPE only) integration.
3. Select the **Active** check box.

- The integration is pre-configured to run daily. Changing any other integration parameter requires both ServiceNow expertise and could result in incomplete data.
- Activating this integration will automatically activate NIST National Vulnerability Database Integration- API (CVE only) and NIST National Vulnerability Database Integration- API (Unmapped CPE) integrations and will set its run field to on demand.
- Additionally, a successful integration run of NIST National Vulnerability Database Integration- API (CPE only) will automatically trigger NIST National Vulnerability Database Integration- API (CVE only). And successful completion of NIST National Vulnerability Database Integration- API (CVE only) will automatically trigger NIST National Vulnerability Database Integration- API (Unmapped CPE).

Note: The Import since date field in the NIST National Vulnerability Database Integration - API (CPE only) Integration is empty by default. Keep it empty to fetch data of the last 357 days.

To retrieve historical data during your initial import from the NVD scan, set a start date in the NIST National Vulnerability Database Integration- API (CPE only) Integration record.

a. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.

b. Select NIST National Vulnerability Database Integration–API (CPE only) Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select the **Integration Details** tab.

d. Set the **Import since** field's value to the earliest date you want to retrieve.
Each successful import resets this date to the selected day's date and time.

4. Select **Execute Now** to perform an initial full support integration run.
After the initial import is complete, scheduled imports of delta data resume. For integration run statuses, see View the (National Vulnerability Database) NVD integration import run status.

Optional NVD integration modification and activities

Configure optional modifications specifically for the NVD integrations.

Note: Changing other NVD integration settings, other than the ones listed here, requires advanced ServiceNow and Vulnerability Response expertise and is beyond the scope of the product documentation.

Perform a manual NVD integration import

If your initial import failed, or you don't want to wait for the scheduled initial import, you can perform a full data import independent of the daily or weekly scheduled job.

Before you begin

Note: The NIST National Vulnerability Database Integration- API (CPE only) and the NIST National Vulnerability Database Integration-API (Unmapped CPE) integrations are inactive by default. See Activate the NIST National Vulnerability Database–API (CPE only) and Activate the NIST National Vulnerability Database–API (Unmapped CPE) for more information.

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Vulnerability Response or Application Vulnerability Response** > **Administration** > **Integrations**.
2. Choose and integration, for example, the NIST National Vulnerability Database Integration - API (CVE only) integration.
3. Select **Execute Now**.

   Note: If the NIST National Vulnerability Database Integration-API (Unmapped CPE) Integration is activated, associated CPE data is stored in the Vulnerable Software related list of the NVD vulnerability entry. See Vulnerability Response vulnerability form fields.

4. For integration run statuses see, View the (National Vulnerability Database) NVD integration import run status.

View the (National Vulnerability Database) NVD integration import run status

Use the **Vulnerability Integration Runs** related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin

To view the NVD integration import run status:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Vulnerability Response and the Vulnerability Response integration with NVD integration application must be installed and configured.
- The NVD integration imports must be running. The NIST National Vulnerability Database Integration-API (CVE only) integration runs by default.

> **Note:** The NIST National Vulnerability Database Integration-API (CPE only) and the NIST National Vulnerability Database Integration-API (Unmapped CPE) integrations are inactive by default. See Activate the NIST National Vulnerability Database–API (CPE only) and Activate the NIST National Vulnerability Database–API (Unmapped CPE) for more information.

Role required: sn_vul.vulnerability_admin or App-Sec Manager

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error.

To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it's also older than one hour. The last record processed being older than an hour indicates that the import queue entry is stuck, and it's timed out to prevent any further delays in processing.

> **Note:** The **Last Record Processed** field is updated based on what is defined in the following system properties:
>
> - *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
> - *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. If you aren't using the NVD integration run status chart, Navigate to **All** > **Vulnerability Response or Application Vulnerability Response** > **Administration** > **Integrations**.
2. Select a **link** for an integration.
3. Select the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.

   Trouble?

   The most common causes for a failed run include:

   - Network interruption.
   - An issue in the data transfer resulting in corrupted data during the transform.

   If you encounter any of these conditions, select **Execute Now**, and rerun the integration.

Related topics

Vulnerability Response vulnerability form fields

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add CVEs to third-party entries

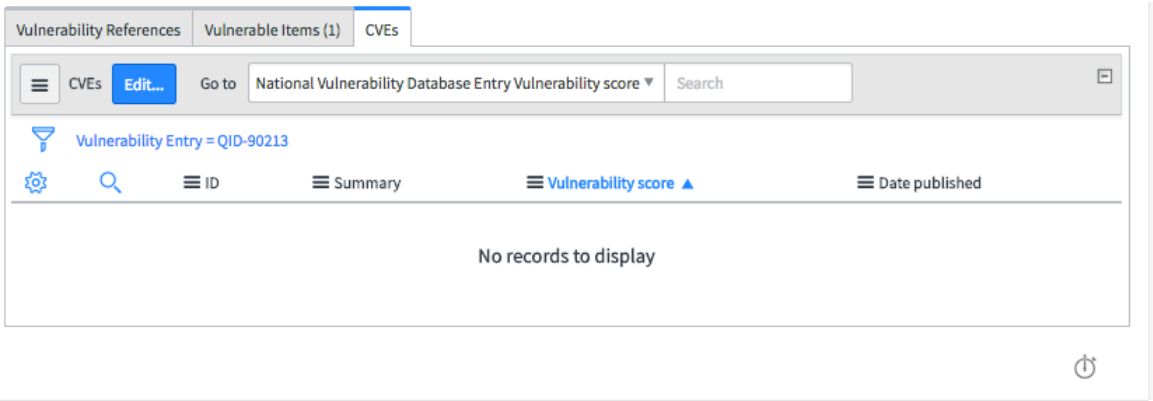
Common Vulnerability and Exposure (CVE) information can be related to a single third-party vulnerability. It is usually added during a third-party integration import however, you can add multiple CVEs (vulnerabilities) manually.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Libraries** > **Third-Party**.
2. Open a record.
3. Click on the **CVEs** related list tab.



4. Click **Edit**.
5. Choose which CVEs to add.

   Note: You can use condition filters to refine the CVE collection.

6. Click **Save**.

Related topics

Vulnerability Response vulnerability form fields

View Vulnerability Response vulnerability libraries

You can view vulnerability data imported from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-parties to decide whether to escalate a remediation task.

Before you begin

Role required: sn_vul.remediation_owner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Libraries**.

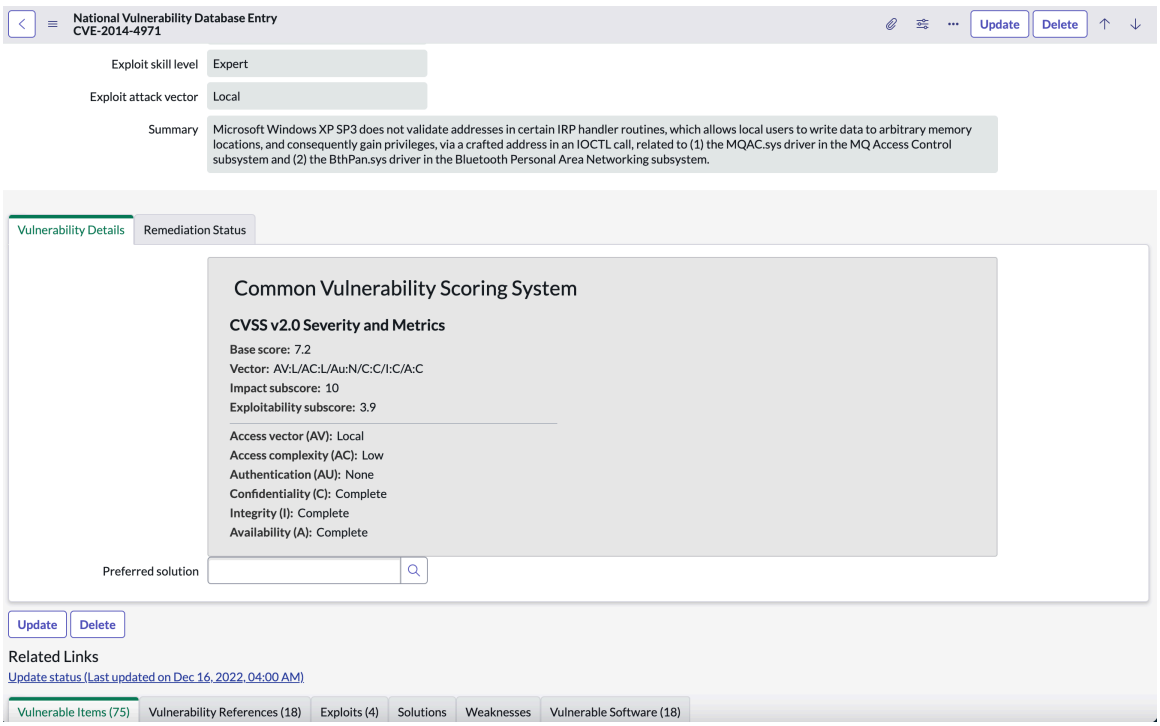
   For information on specific fields, see Vulnerability Response vulnerability form fields.

   The following libraries are available:

Libraries	Description
NVD	List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics including exploits.
CWE	List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations screen, it is for reference only.
Third-party	List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs.

2. Choose a library to view vulnerabilities.
3. Click a link in the list to open a record.

   A CVE record in the National Vulnerabilities Database Entries library. More information is available in the **Related Links**. After a data import, you can pick a vulnerability and explore its relationships to vulnerable items, exploits, possible solutions, potential patches, and any references to KB Articles in the HI Knowledge Base. If Vulnerability Solution Management is installed, you can view a preferred solution on NVD records if one is available.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CISA Known Exploit Vulnerability (KEV) Integration

The Vulnerability Response integration with the CISA Known Exploited Vulnerabilities (KEVs) catalog ingests data to help you effectively prioritize and remediate these vulnerabilities.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

CISA enables urgent and prioritized remediation of actively exploited vulnerabilities for government agencies and corporations.

About CISA

Cybersecurity & Infrastructure Security Agency (CISA) is a U.S. Cybersecurity & Infrastructure Security Agency that publishes a report on the most exploited vulnerabilities. It easily integrates with Vulnerability Response to map Common Vulnerabilities and Exposures (CVE) vulnerabilities enriching the data in your instance. This information is then rolled up to the Third-Party Vulnerability Entries table. The earliest due date is considered for the roll-up to the vulnerable items.

Note: The **CISA Exists** check box for CVEs retrieved by CISA.

Values retrieved from the CISA integration:

- CVE ID
- Due date
- Date added
- Vendor/Project
- Product
- Known ransomware (starting from v21.0 of Vulnerability Response, a new field **Known To Be Used in Ransomware Campaigns** is ingested from the CISA Known Exploited Vulnerabilities (KEVs) catalog. It's indicated by the flagging of the **Known ransomware** field on the National Vulnerability Entry database table. The flag is set at the Common Vulnerabilities and Exposures (CVE) level and rolled up to the third-party entry (TPE).

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Scheduled jobs

The CISA Integration is invoked automatically as a daily scheduled job. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Available versions

Release version	Release Notes
Vulnerability Response v16.5, v18.0 Vulnerability Response Integration with CISA v1.0, v1.2	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing the CISA integration

To view the CISA integration, navigate to **Vulnerability Response** > **Administration** > **Integrations** > **CISA Known Exploit Vulnerability Integration**.

The following integrations are included in the base system.

Note: Only the CISA Integration is active, by default.

CISA integration

Integration	Description
Cybersecurity & Infrastructure Security Agency (CISA) Integration	Retrieves CISA vulnerability data (CVE) and enriches the existing vulnerability data. This integration is set automatically to run daily.

To view data in third-party vulnerabilities, see View Vulnerability Response vulnerability libraries.

Preparing for the CISA integration

A successful integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The CISA Known Exploited Vulnerability integration assumes that you are familiar with the Cybersecurity & Infrastructure Security Agency (CISA).

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

Note: Before running the CISA integration, make any necessary configuration change based on your requirements.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install the ServiceNow® Vulnerability Response Integration with CISA application

Before you run the integration on your instance, the installation and configuration steps must be completed so the Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerability advisor integrates with Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.
Verify that the Vulnerability Response Integration with NVD application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application is not installed and activated see, Install the Vulnerability Response Integration with the NIST National Vulnerability Database.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns users to the Vulnerability Manager in Vulnerability Response. For information on Group roles in Vulnerability Response see, Manage persona and granular roles for Vulnerability Response. • The Vulnerability Manager oversees configuration and verifies expected results.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Log in to the instance you want to install the Vulnerability Response Integration with CISA on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Vulnerability Response Integration with CISA application.
4. Select the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Select **Request App** and enter your Now Support login credentials.
6. Select **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and select **Validate Instance**.
8. Select **Request**.
   You will receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and then select **Install**.
    Your application is automatically installed on your instance.

What to do next

Note: No configuration is required for the CISA integration.

Understanding the Exploit Prediction Scoring System (EPSS) integration

Overview of the EPSS integration with Vulnerability Response.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview

The Exploit Prediction Scoring System (EPSS) integration imports EPSS data related to common vulnerabilities and exposures (CVEs) from First.org to prioritize and remediate vulnerabilities. For more information see, https://www.first.org. The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

Data imports from the EPSS integration, further enrich the NVD data in your instance. If NVD records are not present, then it will create a placeholder in the CVE table and add EPSS details in the same table. Run this integration as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product.

Important: There is a configured run-as user for each integration record. The default value for this user is VR.System. Do not change this value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Initial import of data with the EPSS integration

1. Perform an initial import of EPSS data with the First.org EPSS Integration. For more information, see Configure and run a scheduled job to update CVE records with EPSS data.

   Important: You perform EPSS updates **Daily** from the integration record by default, and you must configure it if you want it to run as a scheduled job.

2. Third-party libraries are updated as scheduled jobs. For more information, see Importing data with the NVD and CWE integrations and managing third-party libraries.

   Important: It is recommended to perform NIST National Vulnerability Database Integration - API (CVE only) integrations before EPSS.

Perform the EPSS imports prior to importing vulnerability data with a third-party product. Third-party libraries are updated as scheduled jobs. Refer to your integration documentation at Vulnerability Response integrations for more information about third-party integrations.

Important: The following integration is included in the base system. The integration is active by default.

After the initial run, base system scheduled jobs run the integrations automatically in order. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

On activation of the EPSS integration, the EPSS Score, EPSS Percentile, and EPSS Last Modified fields are added to the Vulnerability Entries table. For existing CVEs these fields are auto-updated on successful completion of the initial import job. If there are new CVEs that are added to the Vulnerability Entries table after the completion of the EPSS scheduled job, the newly added CVEs will indicate their source as EPSS. The scores are rolled up to existing TPEs from CVEs from the NVD table, using the base system *`Rollup EPSS score from NVD to TPEs calculator`*. You can also modify the calculator. For more information, see Vulnerability Response Rollup Calculators.

Related topics

Create a Vulnerability Response calculator

Configure and run a scheduled job to update CVE records with EPSS data

Customize the base system scheduled job to update CVE records with EPSS data.

Before you begin

Important: You need to download and activate the Vulnerability Response Integration with CISA (com.snc.vulnerability.cisa) plugin to enable the EPSS integration.

Following are the list of new fields added in NVD table to store EPSS data.

- EPSS Score
- EPSS Percentile
- EPSS Last Modified

Note: Configure the list view or form view as per the requirement to view newly added fields.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Data imports from the EPSS integration, further enriches the NVD data in your instance. If NVD records are not present, then it will create a placeholder in the CVE table and add EPSS details in the same table. Run this integration as part of your initial setup of Vulnerability Response and post to importing vulnerability data into your instance.

Note: By default, the First.org EPSS Integration is in **Active** state. The base system scheduled job is configured, by default, to run daily.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.
2. Find and select First.org EPSS Integration.
3. Modify the fields, as needed.
4. Right-click on the header to **Save** your changes.
5. Select **Execute Now**, to run the scheduled job immediately.
   You are returned to the Vulnerability Integrations view.
6. Select **First.org EPSS** > **Vulnerability Integration Runs tab** to view the progress of the import.
   On successful completion of the scheduled job, the EPSS scores, percentile, and the last modified EPSS score timestamps are updated on the CVEs.

What to do next

- See Add EPSS Score condition in Risk calculator Business Rule.
- See View Vulnerability Response vulnerability libraries to see the imported entries.

Add EPSS Score condition in Risk calculator Business Rule

Modify Business Rule to add EPSS score condition to Risk Calculator.

Before you begin

Note: The following procedure is required for the EPSS updates on vulnerabilities to roll down to the vulnerable items.

Role required: sn_vul.manage_risk_score_configuration

Procedure

1. Navigate to **All** > **System Definition** > **Business Rule**.
2. Search for **Set recalculate flag**.

   Note: There are two *`Set recalculate flag`* business rules. You can use either of them.

3. Navigate to the **When to run** tab.
4. Select **Add "OR" Clause** and select `EPSS Score` from **choose field** and `changes` from **Choose operator** field.
5. Select **Update**.

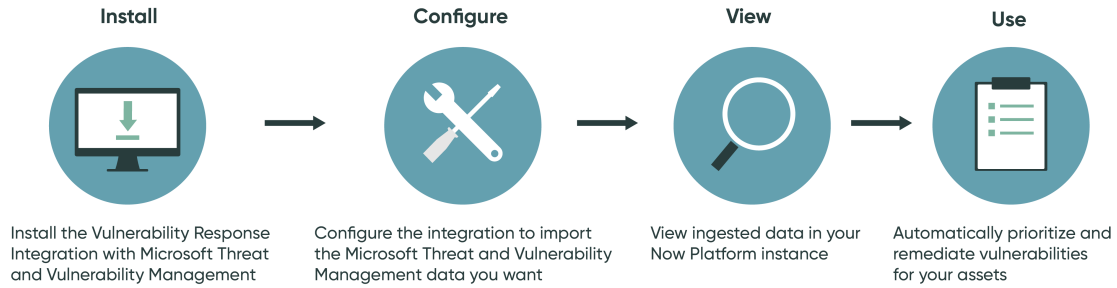
Understanding the Microsoft Threat and Vulnerability Management Vulnerability integration

The Vulnerability Response integration with Microsoft Threat and Vulnerability Management (MS TVM) application uses data imported from MS TVM to help you prioritize and remediate

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerabilities for your assets. The application is available with a separate subscription from the ServiceNow Store.

You can use the MS TVM Vulnerability integration to import third-party scanner data about your assets and vulnerabilities. You can then view reports about vulnerabilities and vulnerable items on the Vulnerability Response dashboards.



Available versions

Release version	Release notes
Vulnerability Response Integration with MS TVM v2.2	For more information about released versions of the Vulnerability Response application, compatibility, and schema changes, see the Vulnerability Response Compatibility Matrix and Release Schema Changes [KB0856498] article in the HI Knowledge Base.

Domain separation and MS TVM

Import vulnerability integration data to a specified domain by assigning a user in that domain to run the integrations. To create domain-separated imports for the MS TVM Vulnerability Integration, see Create domain-separated imports for an integration.

Terms and key features of the integrations

Vulnerable items and vulnerabilities

A vulnerable item is created in your ServiceNow AI Platform instance when:

- An imported vulnerability from a third-party scanner is matched to an existing asset (configuration item) in your CMDB). The MS TVM product refers to these matches as vulnerabilities.
- An imported vulnerability from a third-party scanner is not matched to an existing asset in your CMDB. In this case, an unmatched configuration item (CI) is also created with a vulnerable item.

  Use the Identification and Reconciliation Engine (IRE) to create CIs in two new classes when an existing CI can't be matched with a host. Otherwise, unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine.

Third-party vulnerability entries

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Third-party vulnerability entries are imported from third-party scanners such as MS TVM and are listed in the Third-Party Vulnerability Entries table in your ServiceNow AI Platform instance. Also, National Vulnerability Database entries (CVEs) are imported from MS TVM. The exploit information that is associated with both these types of entries comes from MS TVM. This exploit information can be used for risk calculation.

Note: A third-party vulnerability is retrieved only for vulnerabilities that do not have a CVE assigned to them. MS TVM can add a temporary name for the vulnerability, for example, TVM - XXXX - XXXX. This name is updated after a CVE ID is assigned.

Configuration item (CI)

CIs are the existing assets that are listed in your CMDB.

Discovered item

Discovered items are the assets that are ingested from the MS TVM machine import that match existing CIs in your CMDB.

If a match is not found, a CI is created in the Unmatched CI class of the CMDB. Enable the CMDB CI Class Models plugin, the Identification and Reconciliation Engine (IRE) creates CIs by using new classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. If the original, unmatched CI is reclassified, the discovered item records are updated to reflect that state. Discovered items give you visibility into how assets are identified and mapped to CIs in the CMDB.

CI lookup rules

When data is imported from MS TVM, Vulnerability Response automatically uses machine (asset) data to search for matches in the CMDB. CI lookup rules are used to identify CIs and to add them to VI records when VIs are created.

Instance

An instance refers to multiple accounts of MS TVM. Each account can be an instance in the MS TVM application.

Integration

An integration is a scheduled job that retrieves information from a third-party source, such as the integration of the MS TVM machines.

Deployment

When an integration supports multi-source, a single integration existence is referred to as a deployment of your integration. A deployment refers to the integrations and products across your environment. For example, you might have multiple deployments of MS TVM in your environment.

The MS TVM integration also includes the following key features:

- You can identify the assets across your environment and update the CIs on your existing discovered items, vulnerable items, and detection records to give you more details about your vulnerabilities.
- You can schedule when you want the jobs to run for all the MS TVM integrations. You can also execute scheduled jobs on-demand.
- You can group vulnerable items.
- You can configure CI lookup rules to define how the asset data from third-party sources is used to identify CIs in your CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required ServiceNow AI Platform roles

The integration tasks require the following roles in your ServiceNow AI Platform instance.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

admin

The system admin uses Setup Assistant to install the MS TVM application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant.

sn_vul.vulnerability_admin

Once assigned, the vulnerability admin completes the configuration of the MS TVM integrations in Setup Assistant. This role has complete access to the Vulnerability Response application and its records. The vulnerability admin configures all Vulnerability Response applications and rules for installed third-party integrations.

sn_vul_msft_tvm.configure_integration

This role contains the `sn_vul_msft_tvm.read_integration` granular role. Users with this role can configure the#Vulnerability Response Integration with the Microsoft Threat and Vulnerability Management application.

sn_vul_msft_tvm.read_integration

Users with this role can only view the#Vulnerability Response Integration with the Microsoft Threat and Vulnerability Management application records.

Vulnerability Response group

By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically.

MS TVM integrations

Multi-source is supported for all the MS TVM integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You also install and configure the Vulnerability Response Integration with the MS TVM application from Setup Assistant.

To view the MS TVM integrations, navigate to **Microsoft TVM Vulnerability Integration** > **Administration** > **Integrations**. Vulnerability Response provides integrations with MS TVM end points to import the data according to the scheduled time intervals. The following integrations are included in the base system.

MS TVM integrations

Run sequence	Schedule	Integration	Description
1	Daily	Microsoft TVM Recommendations Integration	Retrieves a list of all the actionable security recommendations to remediate the vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM integrations (continued)

Run sequence	Schedule	Integration	Description
2	Daily	Microsoft TVM Vulnerability (CVE) Integration	Retrieves a list of the national vulnerability database entries and third-party vulnerability entries, as well as their exploit information.
3	Daily	Microsoft TVM Machines Integration	Retrieves all asset (machine) data, including machine tags, from the Microsoft TVM and processes it in your instance.
4	Weekly **Note:** After installation, this integration is run automatically after the machines import.	Microsoft TVM Machines Vulnerabilities Integration (Full Import)	Retrieves all the open vulnerabilities on all the assets.
5	Daily	Microsoft TVM Machines Vulnerabilities Integration (Delta Import)	Retrieves all the information that has changed in the full vulnerability import of the organization, including the new, fixed, and updated vulnerabilities.

Vulnerable items are grouped into remediation tasks according to the group rules that you set and are assigned for remediation based on your assignment rules. For more information, see Vulnerability Response remediation tasks and remediation task rules overview and Vulnerability Response assignment rules overview.

CI lookup rules

When data is imported from MS TVM, Vulnerability Response automatically uses machine (asset) data to search for matches in the Configuration Management Database (CMDB). CI lookup rules are used to identify CIs and add them to VI records when VIs are created. For more information on how CI lookup rules work, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

Note: Once you remove a rule, you can't recover it. Instead of removing an existing rule, you should disable it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following MS TVM lookup rules are shipped with the base system:

- MAC_ADDRESS
- FQDN
- IP

Note: You can use multiple values for the IP_ADDRESS and MAC_ADDRESS of an asset. A CI lookup rule considers all values for matching.

Discovered items

You can see the CIs that were detected during an import from the MS TVM Machines integration.

Note: The default filter for this list is set to `Unmatched`. You can view all discovered items from an import by removing the filter.

For more information, see Discovered Items.

Machine tags

Machine tags, also known as host tags, are used for organizing and tracking the assets in your organization. You assign tags to your machines.

All machine tags are imported as part of the MS TVM Machines integration. Machine tags are generally used for filtering in Vulnerability Response assignment rules and vulnerability group rules. The tags are displayed in the Discovered Item form.

Note: Run the MS TVM Machine integration before you create Vulnerability Response assignment or remediation task rules in the Vulnerability Response application so that all tags are available for these rules before vulnerable items are imported and grouped. Also note the following points about tags:

- Tag storage is not case sensitive. If a Paris tag is created, then a PARIS tag cannot be stored in the Machine tag table. `Paris` and PARIS are considered to be the same machine tag by the system. Whichever tag is imported first is the tag that is stored and recognized.
- Using machine tags as a group key in a remediation task rule may have unexpected results. Group keys are columns in the remediation tasks table, whereas machine tags are intended for use only in the condition builder.
- Machine tags are controlled by the global system property sn_vul.import_host_tags. This property is set to `true` by default. Disabling tags disables them across all ServiceNow AI Platform® instances.

What to do next

After you download the Vulnerability Response integration with Microsoft Threat and Vulnerability Management from the ServiceNow® Store, installation and configuration are supported by Setup Assistant in Vulnerability Response. For more information, see Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant.

Preparing for the Microsoft Threat and Vulnerability Management Vulnerability Integration

You can prepare for the ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability integration by performing setup tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin using a checklist

To install and configure the Vulnerability Response Integration with the MS TVM application, you can print the following checklist and verify the items listed are completed before you install the application and import vulnerability data into your ServiceNow AI Platform® instance.

Integration preparation checklist

Task	Description
☐	Verify that you have one of the following sets of information: • ClientSecret, ClientId, and TenantId for your MS TVM account • Username, Password, ClientId, and TenantId for your MS TVM account. To obtain this information, see Set up Microsoft Azure for the MS TVM integration.
☐	If not already installed and activated, install the Vulnerability Response application before you install the third-party application. For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 14.0 of Vulnerability Response or later.
☐	If you don't already have the application on your instance, get entitlements and download the Vulnerability Response integration with MS TVM application to your ServiceNow AI Platform® instance. See .
☐	Estimate the number of vulnerable items that you expect to import. Verify that your instance can accept the number of vulnerable items that you expect to import. An undersized instance can lead to long load times. If you don't know the size of your instance, or if you need assistance, contact ServiceNow® Technical Support.
☐	Verify that you have the following groups or users to manage the integrations and to remediate vulnerable items: **admin** Uses Setup Assistant to install the Vulnerability Response integration with the MS TVM application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant. **sn_vul.vulnerability_admin** Completes the configuration of the MS TVM integration. This role has complete access to the Vulnerability Response (VR) application and its records. This admin configures all VR applications and rules and configures third-party integrations. **sn_vul_msft_tvm.configure_integration**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist (continued)

Task	Description
	Configures the MS TVM Vulnerability Integration. This role contains the sn_vul_msft_tvm.read_integration granular role. **sn_vul_msft_tvm.read_integration** Views (reads) records of the MS TVM Vulnerability Integration. **Vulnerability Response group** By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance before you use Setup Assistant. For more information, see Create a user group. Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.
☐	Install the Vulnerability Response integration with NVD and run the NIST National Vulnerability Database Integration - API (CVE only).
☐	To promote improved performance for your first import, you can disable certain features, rules, or jobs in your instance. • Disable vulnerability calculators if you do not use them. These calculators, plus any that you have defined, run every time a vulnerable item record is created or updated. For more information, see Disable the default vulnerability calculator if not used. • During the initial import of records, certain notification-related business rules can cause many notifications to be generated, which could impact the performance of the ingestion.

You are ready to Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant.

Set up Microsoft Azure for the MS TVM integration

Set up your account in the Microsoft Azure portal to access the Microsoft Threat and Vulnerability Management (MS TVM) API remotely. You need this account so that you can access the MS TVM tenant to gather information for machines, vulnerabilities, and security recommendations.

Before you begin

Role required: Microsoft Azure portal administrator.

About this task

Complete the following setup tasks in your Microsoft Azure portal before you install the ServiceNow® application for this integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To verify that you have access to the most current content, see the Microsoft doc website. If you haven't created an application ID for OAuth 2.0 authentication in the Microsoft Azure portal, follow the steps in this procedure.

Procedure

1. Log in to the Microsoft Azure portal by using your Azure portal administrator credentials.
2. In the left navigation panel on the Home pane, click **Azure Active Directory**.
3. In the Overview pane, click **App Registrations (Preview)**.
4. In the App registrations (Preview) pane, click **New Registration**.
   The Register an application form is displayed.
5. On the form, fill in the fields.

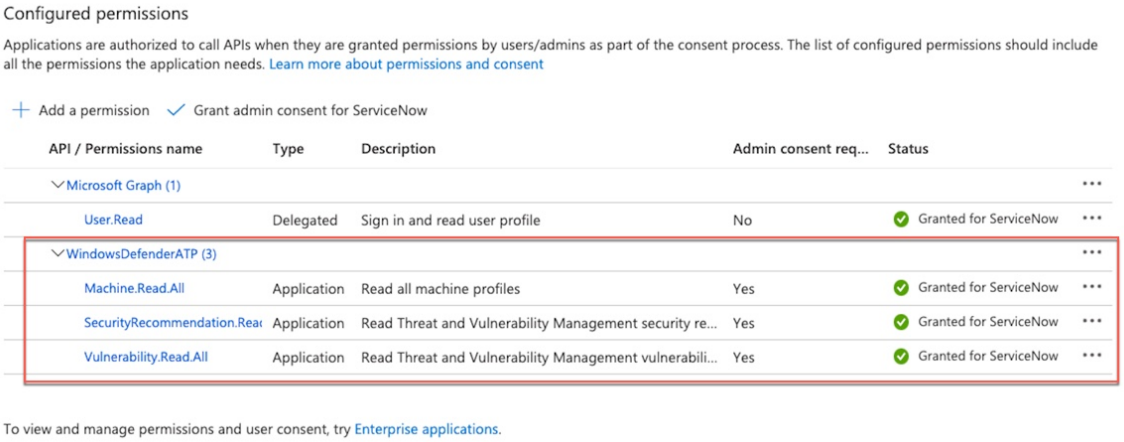
Register an application form

Field	Description
Name	Name for the application. In this example, `ServiceNow MS TVM Integration` is entered.
Supported account types	For this account, in Supported account types, click **Accounts in this organizational directory only (ServiceNow only - Single tenant)**.
Redirect URL (optional)	If you enter a value for this field, it is not used by the integration.

6. Click **Register**.
   The Application (client) ID and Directory (tenant) ID are created. Enter these values on the configuration page in the **Client ID** and **Tenant ID** fields during the configuration step in the ServiceNow VR-TVM integration Setup Assistant. This step was described in Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant.
7. When you see the Application (client) ID displayed in the ServiceNow MS TVM Integration pane, click **View API Permissions**.
8. Navigate to **Request API permissions** > **APIs my organization uses**, and then click **Windows Defender ATP**.
9. In the ServiceNow MS TVM Integration - API permissions pane, click **Add a Permission**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Provide read access to machines, vulnerabilities, and security recommendations.



11. Click **Grant Admin Consent for <your organization name>**.

Note: To authenticate as an application from a ServiceNow instance, do the following actions:

a. Navigate to **Servicenow MS TVM Integration** > **Certificates & Secrets**, and then click **New Client secret**.

b. On the form, fill in the fields.

Client secrets form

Field	Description
Description	Name of the application.
Expires	Date of expiry.

c. Click **Add**.

The **Value** field is populated with the new client secret, which is your new password.

Note: You will need this password when you are configuring the integration in your ServiceNow AI Platform instance. For more information, see Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant.

d. Save this password in a secure location. After you leave this page, this password is not available.

You have successfully created an application ID for authentication in the Microsoft Azure portal.

What to do next

You are ready to set up your ServiceNow AI Platform® instance for the integration.

Install and configure the Vulnerability Response Integration with the MS TVM application using Setup Assistant

Install and configure the Vulnerability Response integration with the Microsoft Threat and Vulnerability Management (MS TVM) application so that you can use the data that is imported from MS TVM to prioritize and remediate vulnerabilities for your assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Before you run the ServiceNow® Microsoft Threat and Vulnerability Management Vulnerability Integration, you must download the Vulnerability Response Integration with Microsoft Threat and Vulnerability Management application from the ServiceNow Store and install and configure it using the Setup Assistant in the Vulnerability Response application.

Before you install the MS TVM application, verify you have completed all the items in the Preparing for the Microsoft Threat and Vulnerability Management Vulnerability Integration checklist. For information on setting up your Microsoft Azure account, see Set up Microsoft Azure for the MS TVM integration.

Roles required: admin for initial assignment of the sn_vul.vulnerability_admin role and installing the Microsoft Threat and Vulnerability Management application in Setup Assistant. Vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin (deprecated) to configure the application in Setup Assistant after it is installed.

About this task

Perform the following procedure before you install and configure the MS TVM Integration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration application Installation**.

   After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the **Microsoft Threat and Vulnerability Management** tile and click **Install**.

   The Vulnerability Response Integration with Microsoft Threat and Vulnerability Management application that you downloaded from the ServiceNow Store is installed.

3. Follow the prompts in the Setup Assistant to continue with the installation.
   For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation in Setup Assistant, navigate to **Integration Configuration** > **Scanner Integrations** in Setup Assistant to continue with the configuration. For more information to supplement the prompts that are provided in Setup Assistant, see Configure the MS TVM Vulnerability Integration using Setup Assistant.

Data retrieval settings for the Microsoft Threat and Vulnerability Management Integration

You can use data retrieval settings to help you determine the type and scope of data that you want to import from the ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability integration to your ServiceNow AI Platform® instance.

Data retrieval settings help you to control the data that you want to import. You can set the values of these filters in integration instances. To view the integration instances, navigate to **Microsoft Threat and Vulnerability Management Vulnerability Integration** > **Integration Instances** and click your MS TVM integration.

On the Integration Instance page, click the **Integration Instance Parameters** to display a list of parameters, or click the **Vulnerability Integrations** tab for a schedule, REST details, integration details, data sources, and integration run information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data retrieval settings and filters for the MS TVM integrations in your ServiceNow AI Platform instance

The following settings are available for the MS TVM integrations in your ServiceNow AI Platform instance. These and other configuration settings are displayed on the Integration Instance page of your ServiceNow AI Platform instance. You may prefer to leave these settings in their default settings for the first few integration runs.

MS TVM.

vi_size_limit

Defines the number of vulnerable item records to include in the result set from the MS TVM Machine Vulnerabilities integration. This setting must be in the int32 format. The default value is 2,000.

vulnerabilities_size_limit

Defines the number of vulnerability records to include in the result set from the MS TVM Vulnerability (CVE) integration. This setting must be in the int32 format. The default value is 2,000.

recommendations_size_limit

Defines the number of vulnerability records to include in the result set from the MS TVM Recommendations Integration. This setting must be in the int32 format. The default value is 2,000.

asset_size_limit

Defines the number of vulnerability records to include in the result set from the MS TVM Machines integration. This setting must be in the int32 format. The default value is 2,000.

machine_filter

Filters the machines that are coming from MS TVM. This filter is applied to the MS TVM Machines integration. The default value is to bring in machines where onBoardingStatus is onBoarded.

REST messages for the Microsoft Threat and Vulnerability Management Vulnerability Integration

You can use the REST messages for the ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability Integration to make calls to the MS TVM API.

MS TVM access token

You can also use the REST messages for the MS TVM access token to retrieve the access token from the MS TVM API so that you can authenticate REST API requests. Changes to the record method of the REST message impact the authentication requests made to MS TVM.

MS TVM integration

You can use the REST message for the MS TVM integration to retrieve information from MS TVM. Changes to the record method of the REST message impact the requests made to MS TVM to retrieve information. REST messages contain the following REST methods.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

REST methods

REST method	Description of method
GET vulnerabilities	Retrieves vulnerability and exploit information from MS TVM.
GET Software Vulnerabilities by Machine	Retrieves all the open vulnerabilities.
GET recommendations	Retrieves the list of all actionable security recommendations that affect the organization.
GET machines	Retrieves the collection of assets.
GET Software Vulnerabilities changes by Machine	Retrieves all the information that has changed in the full vulnerability import of the organization, including new, fixed, and updated vulnerabilities.

Data transformation for the Microsoft Threat and Vulnerability Management Vulnerability Integration

After you identify the data that you want to import, the data is retrieved from the ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) application, processed through a set of data sources, and transformed in your instance.

During installation, normalized severity maps are installed in the Normalized Severity Mapping module. These maps transform imported Microsoft third-party vulnerability severity levels to standard severity levels for processing in your instance. For information about creating severity maps, see Create a Vulnerability Response severity map.

MS TVM Machines Import

The data from the imported machines is first loaded into the MS TVM Machines Import [sn_vul_msft_tvm_machines_import] table.

The MS TVM Machines Transform is used to transform the imported machines information.

Note: Changes to this transform map alter how data from the MS TVM Machines import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and search for **Microsoft TVM Machines Transform**.

The following table lists the transform map fields by integration.

MS TVM Machines transform map fields

Source field	Target field	Description
u_id	source_id	Unique ID for assets. This ID maps to the source_id of the discovered item record.
u_ipaddresses.macAddress	mac_address	MAC Address that is mapped from the API to the host mac address field of the cmdb_ci record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM Machines transform map fields (continued)

Source field	Target field	Description
u_ipaddresses.ipAddress	ip_address	IP Address field that is mapped to the IP address field of the cmdb_ci record.
u_lastseen	last_scan_date	Field that maps to the last_scan_date field on the discovered item record.
u_machinetags		Tags that are saved in sn_sec_cmn_host_tag. The mapping from tags to assets is saved in sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	os	Field that maps to the os field on the cmdb_ci record.
u_computerdnsname	fqdn	Field that maps the dnsname field from the API to the fqdn field on the cmdb_ci record.

The following transform scripts are run during the transformation process.

MS TVM Machines transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation).	Script that is used to initialize the values in the scope variable (sn_vul_msft_tvm) for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to update values in the host and verify whether the host exists. Based on the results, this script modifies the values in the scope variable (sn_vul_msft_tvm). This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of CIs created, updated, and ignored. This script is for internal use and should not be modified or deleted.

The MicrosoftTVMMachinesProcessor script include is called from the onBefore transform script. It takes the output from the Microsoft TVM machines' integration and transforms it into a CI. Any changes to this script include may alter the transformation of the Microsoft TVM machines' data in the CI and Discovered item table.

MS TVM Vulnerabilities integration

The imported vulnerabilities data is first loaded into the Microsoft TVM CVE (Vulnerabilities) Import [sn_vul_msft_tvm_vulnerabilities_import] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Changes to this transform map alter how data from the MS TVM Vulnerabilities import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and search for the **Microsoft TVM Vulnerabilities Transform**.

The following table lists the transform map fields by integration.

Microsoft TVM Vulnerabilities transform map fields

Source field	Target field	Description
u_id	id	Maps to the ID column of the sn_vul_entry record.
u_severity	source_severity	Maps the Severity field to the severity. The default value is 5.
u_publishedon	date_published	Maps the u_publishedon field to the published date.
u_publicexploit	public_exploit	Maps the u_publicexploit provided by the scanner to the public exploit column in the vulnerability entry table.
u_cvssv3	v3_base_score	Maps the cvssv3 score to the v3 base score in the vulnerability entry record.
u_description	summary	Maps the description to the summary field in the vulnerability entry record.
u_exploitinkit	malware_kit	Maps the u_exploitinkit field to the malware kit in the Exploit table.
u_exploittypes	type	Maps the exploit type to the type in the Exploit table.
u_exploitverified	is_exploit_verified	Maps the u_exploitverified field to the verified exploit in the Exploit table.
u_exploituris	exploit_links	Maps the u_exploituris field to the exploit links in the Exploit table.

The following transform scripts are run during the transformation process.

When the script is run	Purpose
onStart (when an import set has started transformation).	Script that is used to initialize the values in the scope variable (sn_vul_msft_tvm) for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to create or update the values in the NVD or the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the script is run	Purpose
	This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the values of the new items that were created and the items that have been updated and ignored. This script is for internal use and should not be modified or deleted.

MS TVM Recommendations import

The imported recommendation data is first loaded into the MS TVM Recommendations Import [sn_vul_msft_tvm_recom_import] table.

Note: Changes to this transform map alter how the data from the MS TVM Recommendations import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and search for **MS TVM Recommendation Transform**.

The following table lists the transform map fields by integration.

MS TVM Recommendation transform map fields

Source field	Target field	Description
u_recommendedvendor	recommended_vendor	Maps the u_recommendedvendor field to the Vendor column.
u_weaknesses	weaknesses	Maps the u_weaknesses field to the Weaknesses column.
u_exposedmachinescount	src_exposed_machines_cnt	Maps the u_exposedmachinescount field to the Exposed machines count column.
u_status	status	Maps the status to the Status field in the recommendation record.
u_productname	product_name	Maps the u_productname field to the Product name in the recommendation record.
u_nonproductiv_impactedassets	non_prod_impacted_assets	Maps the u_nonproductiv_impactedassets field to the Impacted assets column in the recommendation record.
u_activealert	active_alert	Maps the u_activealert field to the Active alert column in the recommendation record.
u_recommendedversion	recommended_version	Maps the u_recommendedversion field to the Recommended

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM Recommendation transform map fields (continued)

Source field	Target field	Description
		version column in the recommendation record.
u_totalmachinecount	total_machine_count	Maps the u_totalmachinecount field to the Total machine count column in the recommendation record.
u_exposureimpact	exposure_impact	Maps the u_exposureimpact field to the Exposure impact column in the recommendation record.
u_recommendationname	recommendation_name	Maps the u_recommendationname field to the Recommendation name column in the recommendation record.
u_subcategory	subcategory	Maps the u_subcategory field to the Subcategory column in the recommendation record.
u_id	source_id	Maps the recommendation ID from MS TVM to the Source ID column.
u_remediationtype	remediation_type	Maps the u_remediationtype field to the Remediation type column in the recommendation record.
u_relatedcomponent	related_component	Maps the u_relatedcomponent field to the Related component column in the recommendation record.
u_recommendedprogram	recommended_program	Maps the u_recommendedprogram field to the Recommended program column in the recommendation record.
u_recommendationcategory	recommendation_category	Maps the u_recommendationcategory field to the Recommendation category column in the recommendation record.
u_publicexploit	public_exploit	Maps the u_publicexploit field to the Public exploit column in the recommendation record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM Recommendation transform map fields (continued)

Source field	Target field	Description
u_vendor	vendor	Maps the u_vendor field to the Vendor column in the recommendation record.
[Script]	integration_instance	Name of the instance from which the recommendation is imported.
[Script]	sys_domain	Domain in which this record is imported.

The following transform scripts are run during the transformation process.

MS TVM Recommendation transform map script

When the script is run	Purpose
onStart (when an import set has started transformation).	Script that is used to initialize the values in the scope variable (sn_vul_msft_tvm) for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to update values in the recommendations and verify whether the recommendations exist. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the values of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

MS TVM Machine Vulnerabilities import

The MS TVM Machine Vulnerabilities transform map is used to transform open and fixed vulnerabilities information that is imported from MS TVM.

Note: Changes to this transform map alter how data from the MS TVM Machine Vulnerabilities Import is processed.

To access the MS TVM Open and Fixed Vulnerabilities transform maps, navigate to **System Import Sets** > **Transform Maps** and search for the **MS TVM Machine Vulnerabilities Transform**.

The following table lists the transform map fields by integration.

MS TVM Machine Vulnerabilities transform map fields

Source field	Target field	Description
u_id	detection_key	Maps the u_id field to the Detection key column in the detection table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM Machine Vulnerabilities transform map fields (continued)

Source field	Target field	Description
u_diskpaths	proof	Maps the u_diskpaths field to the Proof column in the detection table.
u_registrypaths	proof	Maps the u_registrypaths field to the Proof column in the detection table.
u_recommendedsecurityupdateid	preferred_solution	Maps the u_recommendedsecurityupdateid field to the Preferred solution column in the vulnerable item table, if the solution exists with the same ID in the sn_vul_solution table.
u_recommendationreference	recommendation	Maps the u_recommendationreference field to the Recommendation column in the vulnerable item table.
u_cveid	vulnerability	Maps the u_cveid field to the Vulnerability column in the vulnerable item table.
u_status	source_status	Maps the u_status field to the Source status column in the detection table.
u_eventtimestamp	temporal_score	Maps the u_eventtimestamp field to the Last found column in the vulnerable item table.
u_lastseentimestamp	last_seen	Maps the u_lastseentimestamp field to the Last seen column in the vulnerable item table.
u_firstseentimestamp	first_seen	Maps the u_firstseentimestamp field to the First seen column in the vulnerable item table.
u_recommendedsecurityupdate	solution_summary	Maps the u_recommendedsecurityupdate field to the Solution

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MS TVM Machine Vulnerabilities transform map fields (continued)

Source field	Target field	Description
		summary column in the vulnerable item table.
u_recommendedsecurityupdateurl	solution_summary	Maps the u_recommendedsecurityupdateurl field to the Solution summary column in the vulnerable item table.

The following transform scripts are run during the transformation process.

When the script is run	Purpose
onStart (when an import set has started transformation).	Script that is used to initialize the values in the scope variable (sn_vul_msft_tvm) for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to check if the Vulnerability Entry and Detections exist. If not, these records are created in their respective tables. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to update the count of VIs and Detections as imported from MS TVM. This script is for internal use and should not be modified or deleted.

Integration run status chart for the Microsoft Threat and Vulnerability Management Vulnerability Integration

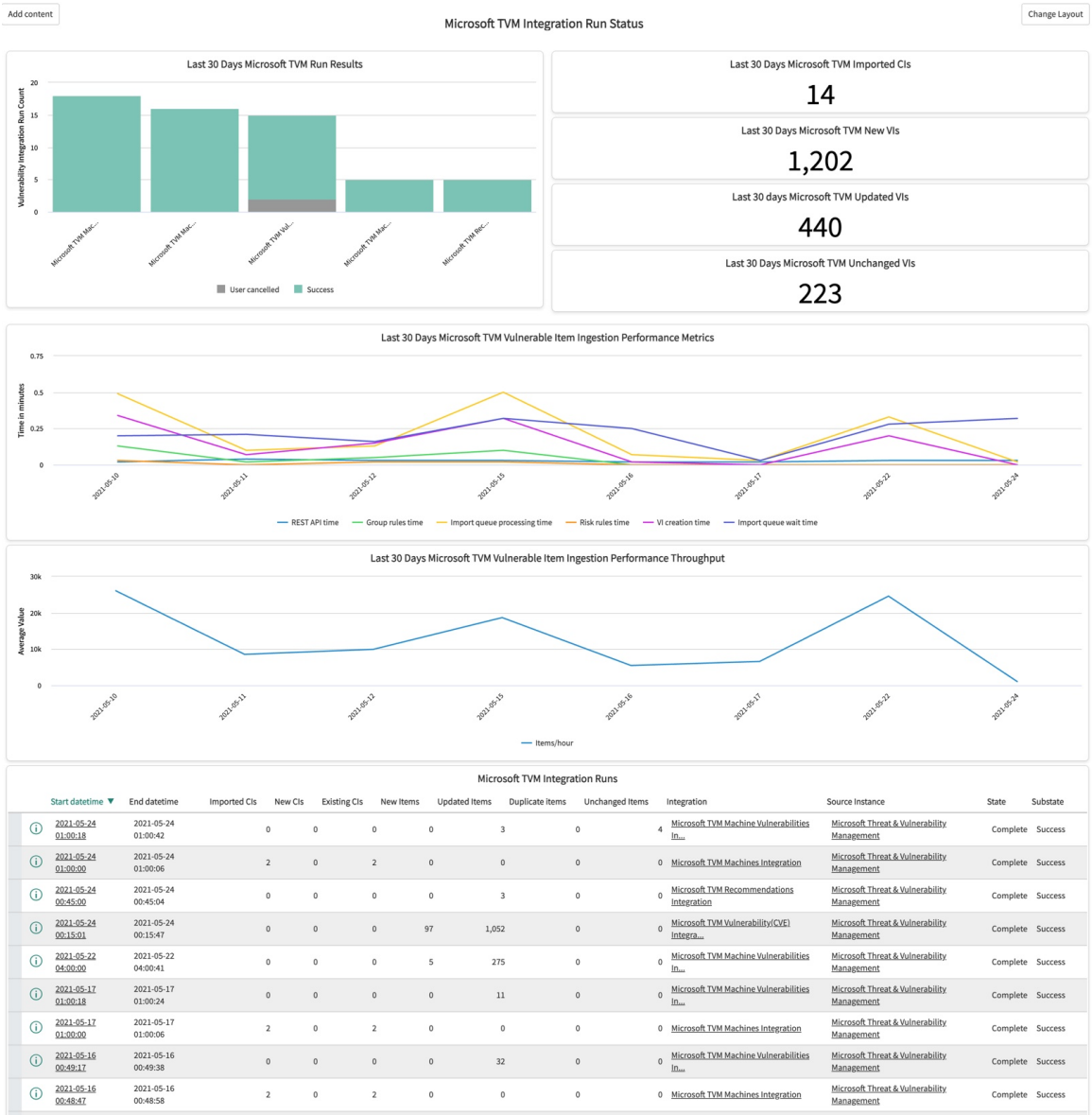
You can use the Microsoft Threat and Vulnerability Management (MS TVM) Integration Run Status module to provide you with a graphical view of the status of the MS TVM integration runs.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

In the chart, you can point to any part of the graph to display a summary of data that is specific to that part. If you click any part on the bar graph, a list opens to provide more detailed information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



MS TVM integration run status chart reports

Name	Description
Last 30 days Microsoft TVM Results	Number of integration runs that were completed for each integration. This report shows both the successful and failed runs. Each run is displayed as a bar in the graph.
Last 30 Days Microsoft TVM New VIs	Number of new vulnerable items that were imported in the last 30 days.
Last 30 Days Microsoft TVM Updated VIs	Number of updated vulnerable items that were imported in the last 30 days.
Last 30 Days Microsoft TVM Unchanged VIs	Number of duplicate vulnerable items that were imported in the last 30 days.
MS TVM Integration Runs	Integration run records in a list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	Note: V16.1: To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.
Last 30 Days Microsoft TVM Vulnerable Item Ingestion Performance Metrics	Daily performance metrics for vulnerable items compared for the last 30 days.
Last 30 Days Microsoft TVM Vulnerable Item Ingestion Performance Throughput	Daily vulnerable item ingestion throughput that was measured for the Microsoft TVM Host Detection integration for the last 30 days.
Last 30 days Microsoft TVM Imported CIs	Number of new configuration items that were imported in the last 30 days.

Verify the Microsoft Threat and Vulnerability Management integration import run status

Use the Microsoft Threat and Vulnerability Management (MS TVM) import run status to verify the success of your integration runs and to locate any issues.

Before you begin

This procedure makes the following assumptions:

- You have Vulnerability Response and the MS TVM Vulnerability Integration installed and configured.
- MS TVM Vulnerability Integration imports are scheduled and running.

Role required: sn_vul.vulnerability_admin

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Microsoft Threat and Vulnerability Management** > **Integrations**.
   a. Choose an integration.
   b. Click the Vulnerability Integration Runs related list.
2. Verify that the state of the imports is Complete, with the Substate as Success.
   The most common causes for a failed run are as follows:
   - Network interruption.
   - Bit decay in the data transfer resulting in corrupted data during the transform.
3. **Optional:** If you see one of these conditions that have caused a failed run, click **Execute now** and rerun the integration.

Split Microsoft TVM detections based on the vulnerability instance to split vulnerable items

ServiceNow® Vulnerability Response enables the splitting of detections from Microsoft Threat and Vulnerability Management (MS TVM) scanners, enabling the creation of a unique vulnerable item (VIT) for each detected vulnerability instance. This split enables the assignment of VITs to various remediation teams, enhancing the management and tracking of vulnerabilities.

Before you begin

Role required: admin

About this task

The Microsoft Threat and Vulnerability Management (MS TVM) scanner's payload contains detection data, with each path within the proof used to split the detections. The diskpath tag in the payload identifies the vulnerability's location, facilitating accurate identification and management of vulnerabilities according to their specific paths.

Procedure

1. In the Third-party Integrations table [sn_sec_int_integration], set the **Include proof in VI key** column value to true for Tenable.io and Tenable.sc.
2. Navigate to **All** > **Vulnerability Response** > **Administration** > **Configure VI granularity**.
3. On the Include port form, select the Include port check box and select the **click here** link.
4. On the Add proof to VI keys list, select **New**.
5. On the Add proof to the VI key- New record form, in the **Vulnerability** field, add the Microsoft Threat and Vulnerability Management (MS TVM) CVE for which you want to include the proof and select **Submit**.
   The selected vulnerability appears in the Add proof to VI keys list.

Example: Splitting detections from Microsoft Threat and Vulnerability Management (MS TVM) scanner

The following detection from Microsoft Threat and Vulnerability Management (MS TVM) scanner shows proof in the diskpath tag.

```
            "id": "329f3283
 fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-
2024-7528",
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
"deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

           "rbacGroupId":
     "rbacGroupName": "Unassigned",
      "deviceName": "ip-0a1409fd.secops.com",
       "osPlatform": "WindowsServer2019",
         "oVersion": "10.0.17763.5936",
       "osArchitecture": "x64",
        "softwareVendor": "mozilla",
       "softwareName": "firefox",
       "softwareVersion": "126.0.1.0",

            "cveId"; "CVE-2024-7528",
           #vulnerabilitySeverityLevel": "High",
        #recommendedSecurityUpdate":; "mfsa2024-33",

        "recommendedSecurityUpdateId": null,

           "recommendedSecurityUpdateUrl": null,
            "diskPaths": ['c: llprogram
files\lamazonlIcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\Icfn-bootstrap\\libsst-3.dll,

         "registryPaths":
           1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
lMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox
126.0.1 (x86 en-US)"


        #lastSeenTimestamp": "2024-08-28 19:36:07",

         "firstSeenTimestamp": "2024-08-06 20:32:34",

       "endOfSupportStatus": null,
          "endOfSupportDate": null,
      "exploitabilityLevel": "NoExploit",
          "recommendationReference": "va-_-mozilla-_-firefox",

         "cvssScore": 8.8,
      "securityUpdateAvailable": true,
         "cveMitigationStatus": null
```


Understanding the HCL BigFix patch orchestration integration with Vulnerability Response

You can manage patches and patch deployments for critical vulnerabilities for large groups of assets with the Vulnerability Response patch orchestration integration with the HCL BigFix product.

Patch orchestration with Vulnerability Response

Patch orchestration with Vulnerability Response uses scheduled imports from third-party solution integrations, patch vendors, and vulnerability scanners. Scanner detection data match the assets in your environment to vulnerabilities and to the patch updates that can fix them. Submit patch requests for approval, schedule patch updates to resolve vulnerable items, and monitor remediation progress all from records in the Vulnerability Response application in your ServiceNow AI Platform®.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response Patch Orchestration with HCL BigFix

When the Vulnerability Response Patch Orchestration with HCL BigFix integration application is used with the ServiceNow® Vulnerability Solution Management, Patch Orchestration, and Vulnerability Response applications, vulnerability managers and analysts can perform the following tasks:

- See more context and information about the types of patches and vendors' solutions (patches).
- View and monitor vulnerability and solution data, as well as vulnerability remediation progress from records in the Vulnerability Response Workspaces.

IT specialists and remediation owners can perform the following tasks:

- Deploy patches supported by the BigFix product for their Windows, CentOS, MAC, Oracle, and other assets at regular, scheduled intervals during off-hours to avoid work conflicts.
- Identify unpatched assets with vulnerabilities, or assets that or were not successfully updated by scheduled patches from imported detection data from third-party scanners.
- Schedule available patches from either the IT Remediation Workspace or from the classic environment for vulnerable, unpatched assets from patch update, remediation task, and discovered item records.

Key terms in the Vulnerability Response and BigFix applications

Configuration item (CI)

CIs are the existing assets that are listed in your#Configuration Management Database (CMDB). BigFix calls CIs, computers.

Computer groups

Terminology used in the BigFix product that refers to a group of assets.

Vulnerable item

An imported vulnerability that matches an existing asset in your CMDB.

Instance

A distinct account of the BigFix application. Each user account can be an instance in the BigFix application. This term also refers to a unique, secure web address for a ServiceNow AI Platform instance.

Integration

An integration is a scheduled job in the ServiceNow AI Platform that retrieves information from a third-party source, such as the integration with the BigFix machines.

Solution

There are two types of solutions in the context of this integration, potential and preferred. A potential solution is one that might address a vulnerability. Vulnerabilities often have many potential solutions. #A preferred solution matches the most effective solution for a specific, detected vulnerability.

Patch

Software updates that fix vulnerabilities. In the BigFix application, patches are called, Fixlets. For example, BigFix has Fixlets for Windows, CentOS, MAC, Oracle and other products.

Preferred patch

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Preferred patches are software updates that are intended to fix specific vulnerabilities. Patches, once deployed, map to the vulnerable items that are related to specific vulnerabilities and fix them.

Remediation task

Lists of vulnerable items in the Vulnerability Response application of actions that are required to fix vulnerabilities.

Deployment

Deployment for the purposes of this integration refers to when you apply, initiate, or schedule a patch to a machine. BigFix calls these deployments, actions. You can deploy (create actions) for the patches you downloaded from BigFix in your ServiceNow AI Platform. Navigate to discovered items, patches, or remediation tasks from individual records in Vulnerability Response. You can deploy patches with scheduled jobs to individual machines or to computer groups.

Deployment in the ServiceNow AI Platform can also refer to an integration that supports multi-source. A single integration existence is referred to as a deployment of your integration. A deployment refers to the integrations and products across your environment. For example, you might have multiple deployments of the BigFix Vulnerability integration in your environment.

Vulnerability Solution Management and the Vulnerability Response Patch Orchestration with HCL BigFix Integration

Solution management is provided by the Vulnerability Solution Management application, a ServiceNow AI Platform application that correlates your vulnerability findings with the breakdown of the solutions (patches) that remediates them. Identify the software patches from third parties for products and services, configuration updates, and other controls that have the highest impact for your organization. Along with third-party scanner information, the Solution Management for Vulnerability Response, Vulnerability Response, and the Vulnerability Response Patch Orchestration with HCL BigFix applications work together to roll preferred patches up from the solution, to the vulnerability, to the vulnerable item to help you fix and close vulnerabilities to your environment.

The Solution Management for Vulnerability Response, Vulnerability Response, and the Vulnerability Response Patch Orchestration with HCL BigFix Integration are all available in the ServiceNow® Store.

Required ServiceNow AI Platform roles

The integration installation, configuration, and remediation tasks require the following roles in your#ServiceNow AI Platform instance.

admin

Users with this role get entitlements for applications in the ServiceNow Store and downloads them to ServiceNow AI Platform instances.

sn_vul.vulnerability_admin

Users with this role activate applications in the ServiceNow AI Platform instance and completes the configuration of the Vulnerability Response application. This role has complete access to the Vulnerability Response (VR) application and its records. This admin user configures all VR applications, rules, and third-party integrations.

sn_vul_bigfix.configure_integration

Users with this role configure the BigFix Patch Orchestration Integration application. This role contains the sn_vul_bigfix.read_integration granular role.

sn_vul_bigfix.read_integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Users with this role can view (read only) the#ecords of the Vulnerability Response and the BigFix Patch Orchestration Integration application and patch orchestration data.

sn_vul_patch_orch.configure_patch

Users with this role can configure and apply patches.

sn_vul_patch_orch.read_patch

Users with this role can view (read only) patch information.

Approvers

Assign uses to the Approver level 1 and Approver level 2 approver groups if you want submitted patch requests approved prior to deployment.

For more information about assigning these roles using the Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about the Vulnerability Response roles in your ServiceNow AI Platform, see Vulnerability Response personas and granular roles.

CI lookup rules

When data is imported from the BigFix application,#he Vulnerability Response application automatically searches for matches in the#Configuration Management Database (CMDB) using machine (asset) data. CI lookup rules are used to identify CIs (assets) and add them automatically to vulnerable item (VI) records when VIs are created.

The following CI lookup rules are shipped with the base system and are used to identify CIs (assets) and add them to the Vulnerability Response application:

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

You can use multiple values for the IP_ADDRESS of an asset. A CI lookup rule considers all values for matching. For more information about how CI lookup rules and how they work, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

MID Server

The Vulnerability Response Patch Orchestration with HCL BigFix integration is an on-premises integration. It requires a standalone MID Server that is not part of a MID Server cluster. The MID server is required to runs scripts on remote machines from your instance in order to import data from the BigFix server. APIs for this integration are called using MID Servers that you set up in your ServiceNow AI Platform instance. See Prepare for the Vulnerability Response Patch Orchestration integration with HCL BigFix for more information.

Integrations and dependencies of the Vulnerability Response Patch Orchestration integration with HCL BigFix

The following product and dependency applications are required for the Vulnerability Response Patch Orchestration with HCL BigFix Integration. These applications are available in the ServiceNow® Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions of applications and dependencies required for the patch orchestration integration

To view patch orchestration data and available updates (patches) in the workspaces in Vulnerability Response, the following applications are required. All applications listed are available in the ServiceNow® Store. Some applications require separate subscriptions.

For more information about version compatibility with the required applications and family releases, refer to the KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes article in the HI Knowledge Base.

Application and release version
Vulnerability Response
Vulnerability Solution Management
Vulnerability Response Patch Orchestration application
Vulnerability Response Patch Orchestration with HCL BigFix application
Security Support Common
Security Support Orchestration
A supported third-party vulnerability scanner application

Vulnerability Response Patch Orchestration application tables

The Vulnerability Response Patch Orchestration application contains the following tables:

Table	Description
Patch Update [sn_vul_patch_orch_update]	Stores information about the patches that are available on distinct instances.
Device Update [sn_vul_patch_orch_m2m_src_ci_update]	Stores data about the deployed patches, along with deployment status, that are on displayed on discovered item records.
Collection [sn_vul_patch_orch_collection]	Stores collection data from distinct instances.
Device Collection [sn_vul_patch_orch_m2m_src_ci_collection]	Stores collections data about discovered items.
Patch Deployment [sn_vul_patch_orch_deployment]	Stores information about deployed patches about Collections and CIs.
Potential Patch [sn_vul_patch_orch_m2m_vuln_patch]	Stores data about patches and vulnerabilities that identify the patches that might be used to resolve a vulnerability.

Vulnerability Response patch orchestration integrations with HCL BigFix

The integrations developed by ServiceNow® engineering make up the orchestrated solution deployment with the BigFix product. The following integrations are included with the Vulnerability Response Patch Orchestration Integration with HCL BigFix application that you download from the ServiceNow® Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you install the integration application on your ServiceNow AI Platform instance, to view these integrations, navigate to **Integrations** > **BigFix Patch Orchestration Integration** > **Integrations**. The Vulnerability Response application processes data on scheduled time intervals imported by these integrations with BigFix endpoints.

Integration	Description
BigFix Collection Integration	• This integration is scheduled to run daily and runs first in the chained integration run. • Retrieves the computers and computer groups that make up the computer groups (configuration items) from the BigFix application.
BigFix Fixlet Integration	• When scheduled, this integration is triggered by the completion of the BigFix Collection Integration. You can also run it on-demand. • Retrieves information about all available fixlets (patches) from the BigFix server.
BigFix Device Fixlet Integration	• When scheduled, this integration is triggered by the completion of the BigFix Fixlet Integration. You can also run it on-demand. • Retrieves information about the fixlets that are currently on computers (assets) from the BigFix server.
BigFix Actions Integration	• When scheduled, this integration is triggered by the completion of the BigFix Device Fixlet Integration. You can also run it on-demand. • Retrieves information about the patches scheduled by the IT team in the BigFix server.

Prepare for the Vulnerability Response Patch Orchestration integration with HCL BigFix

Prepare for the integration by performing the following setup tasks.

Before you begin

Roles required: admin for installing the applications and assigning roles. Other roles are listed in the following table.

About this task

A successful integration requires planning and careful execution of pre-integration tasks.

You are ready to Install the Vulnerability Response Patch Orchestration with HCL BigFix application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. For a smooth installation and configuration of the Vulnerability Response Patch Orchestration with HCL BigFix application, follow the checklist provided.
2. You might prefer to print the following checklist and verify the items listed are completed before you install the application.

   After installation and configuration, import vulnerability and patch-related information into your ServiceNow AI Platform® instance.

Task	Description
☐	(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application. For more information about installing and activating the Vulnerability Response application, see, Install Vulnerability Response. This integration requires version 16.0 of Vulnerability Response or later.
☐	If not already installed, get entitlements and install and third-party scanner application to import vulnerability data. See Vulnerability Response integrations for more information about third-party scanners supported by Vulnerability Response. See .
☐	If not already installed, get entitlements and download the Vulnerability Response Patch Orchestration with HCL BigFix application to your ServiceNow AI Platform® instance. See .
	Obtain BigFix credentials. Verify you have any account names, passwords, and other service information required by your BigFix products so that you have access to them.
☐	Verify that you have groups or users to manage the integrations and remediate vulnerable items. **admin** The system admin gets entitlements, downloads, and installs the BigFix Patch Orchestration application and the other applications required for the integration. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in the Setup Assistant in Vulnerability Response or from the User Administration module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	sn_vul.vulnerability_admin Once assigned, the vulnerability admin completes the configuration of the BigFix integrations and the other third-party applications. This role has complete access to the Vulnerability Response (VR) application and its records. This role configures all VR applications, rules, third-party integrations, Vulnerability Response Patch Orchestration and Vulnerability Solution Management applications. **sn_vul_bigfix.configure_integration** Users with this role configure the BigFix Patch Orchestration Integration application. This role contains the sn_vul_bigfix.read_integration and connection_admin granular roles that permit the user to connect to the BigFix console and configure the integration instances in your ServiceNow AI Platform. **sn_vul_bigfix.read_integration** Users with this role can view (read only) the #ecords of the Vulnerability Response and the BigFix Patch Orchestration Integration application and patch orchestration data. **sn_vul_patch_orch.configure_patch** Users with this role can configure and apply patches. Patches requested by this user from Vulnerable item and Patch Update records are sent for approval if change management is active and approvers are assigned. **sn_vul_patch_orch.read_patch** Users with this role can view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces. **Approvers** Users assigned to the Approver level 1 and, optionally, Approver level 2, approver groups approve submitted patch requests. By default, patches are submitted to the the Approver level 1 group for approval prior to deployment. For more information about the approval process, see Patch orchestration with Vulnerability Response. For more information about setting up approvers and groups, see Assign the Vulnerability Response persona roles using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	The system admin performs the initial assignment of roles to users and groups for the integration. By default, the Vulnerability Response group is available. If not already created, you may prefer to create additional groups for remediation specialist and vulnerability analyst roles and add users with the User Administration module in your instance. See Create a user group.
☐	Verify you have enabled any features, rules, dependency plugins, or jobs in your instance required for the integration. ○ The Vulnerability Response Patch Orchestration with HCL BigFix is an on-premises integration that requires you to use a standalone MID Server. For more information about MID Servers in your instance, see MID Server. ○ Navigate to **System Applications** > **All Available Applications** > **All** and locate the plugin. If not installed in your instance, install and activate it.

What to do next

You are now ready to Install the Vulnerability Response Patch Orchestration with HCL BigFix application.

Install the Vulnerability Response Patch Orchestration with HCL BigFix application

Download the Vulnerability Response Patch Orchestration with HCL BigFix application from the ServiceNow® Store.

Before you begin

Roles required: admin for initial assignment of the sn_vul.vulnerability_admin role and installing the application. Vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin (deprecated)) to configure the Vulnerability Response Patch Orchestration with HCL BigFix and other applications after they are installed.

About this task

Before you install the application, verify you have completed all the items in the checklist in Prepare for the Vulnerability Response Patch Orchestration integration with HCL BigFix.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Procedure

1. Navigate to **All** > **System Applications** > **all Available Applications** > **All**.
2. Locate the **Vulnerability Response Patch Orchestration with HCL BigFix** application and click **Install**.

   This action installs the application you downloaded from the ServiceNow Store.
3. Alternatively, you can install applications from the Setup Assistant.
   For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

After you complete the installation, navigate to **All** > **BigFix Patch Orchestration Integration** > **Configuration** to continue with the configuration.

Configure the Vulnerability Response patch orchestration integration with HCL BigFix

After you have installed the application, configure it with your BigFix account information and validate your credentials.

Before you begin

Roles required: sn_vul.vulnerability_admin and sn_vul_bigfix.configure_integration

Procedure

1. Navigate to **BigFix Patch Orchestration Integration** > **Configuration**.
2. Fill in the fields with your BigFix information and credentials.

Field	Description
Integration instance	The name of the BigFix instance account you want to use, for example, `BigFix Patch management integration`.
Host name	Enter the URL for the BigFix host.
Username	Enter your BigFix account username.
Password	Enter your BigFix account password.
MID Server	Enter the name of the standalone MID Server from the list that you want to use. See Prepare for the Vulnerability Response Patch Orchestration integration with HCL BigFix for more information about MID Servers and set up tasks in your ServiceNow AI Platform®.

3. Click Save and Test Credentials.
   The status of your connection between BigFix and your ServiceNow AI Platform® instance#s displayed in the Validation Status Field. If you do not see a successful test, follow the prompts.
4. **Optional:** Domain separation is supported for this integration.
   You can add multiple configurations of to your instance. To add additional configurations:

   a. Navigate to **BigFix Patch Orchestration Integration Integration Instances**.

   b. Verify the application scope, `Vulnerability Response Patch Orchestration with HCL BigFix`, is displayed in the Application scope field.

   c. Click **New**.

   d. Fill in the form.

Field	Description
Name	Name for the integration instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Application	Vulnerability Response Patch Orchestration with HCL BigFix
Integration	[Read only] BigFix Patch management is the default.
Active	Default is activated (selected). If cleared, the instance is not active.

e. Click **Submit**.
Your new integration instance is displayed on the Integration Instances list.

f. Repeat steps 1-3 to configure your integration instance and test your credentials.

5. Set up approvals for patch requests.
By default, a system property [**sn_vul_patch_orch.patch_approval_required**] is activated so that when patch deployments are scheduled, they are submitted for review and approval to users assigned to the Level 1 - Patch update approval group.

If you want users with the sn_vul_patch_orch.configure_patch role to schedule patches without approval, you can deactivate the [**sn_vul_patch_orch.patch_approval_required**] property. You might prefer to leave approvals activated so that scheduled patches do not conflict with normal working hours.

Note: If you deactivate the approval system property, any user with the sn_vul_patch_orch.configure_patch role can schedule and deploy patches without review and approval.

As a user with the sn_vul.vulnerability_admin role, to deactivate the system property:

a. Navigate to **sys.properties.list**.

b. Locate **sn_vul_patch_orch.patch_approval_required** and click it to open the record.

c. In the Value field, type `false`.

d. Click **Update**.

6. If you do not deactivate this property, you must assign approvers for patch requests.
As a user with the sn_vul.vulnerability_admin role, follow these steps.

a. Navigate to **Vulnerability Response** > **Administration** > **Approval Rules**.

b. If the **Deploy patch update approval** Approval Rule is not displayed in the list, click **All** to the right of the green filter icon in the upper left of the screen to display the entire list.

c. From the list, click **Deploy patch update approval**.

d. On the record, with the Approval Configuration tab selected, click **Default Configuration Patch Update approval**.

e. On the record, click **Level 1 - Patch update approval**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

f. Add users in this group.

The users assigned to this group approve patch requests submitted by users with the sn_vul_patch_orch.configure_patch role. Navigate to **My Approvals** to view and process the requests.

7. Click**Update** to save your changes.
8. **Optional:** You can set up multi-level approvals so that more than one approval is required prior to the deployment of scheduled patch requests.

a. With the Default Configuration Patch Update approval record displayed, click **New**.

b. Fill in the fields.

Field	Description
Name	Approval level name, for example, **Level 2 - Patch update approval**.
Active	Activated by default, signifying that the approval level is in use.
Required approval	Select how many approvals are required for the selected level: ▪ One approver required ▪ All users must approve
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 runs before a configuration with an order entry of 200.
Role	Select a role for the group from the list.
Approval rule	Contains the table and type details for the approval rule.
Approval configuration	Contains the approval configurations.
Assign using	Select an option: ▪ User and user group ▪ Approval table field ▪ Script
Groups	Approver level group consisting of multiple users. The user must have one of the following roles that you specify.
Users	Edit the users listed in the groups.

c. Click **Submit** to save your edits.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing patch data for the Vulnerability Response patch orchestration integration with HCL BigFix

Patch data and patch rollup data, as well as vulnerability information and remediation status of your vulnerabilities, are displayed on records in your instance.

Viewing patch data in the Vulnerability Response Workspaces

Roles required:

- sn_vul_patch_orch.configure_patch role to configure and schedule patches
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces

In the IT Remediation Workspace, you can view patches:

- On the Home view, where you can click scorecards to view records for Preferred solutions on VIs, Vulnerable CIs, and Preferred Patches on VIs.
- On the List view, where you can view all Patch Update records (VPUs) from the Patches links, and the vulnerable items (VITs) that are assigned to you that have patches.

You can schedule patches from the following records:

- From Patch Update (VPU)
- Remediation task (RT)
- Discovered Item (SDI) records

In the Vulnerability Manager Workspace, you can view patches:

- From the Home view on watch topics, where you can view preferred and potential patches, Patch scheduled dates, and, if the patch has been downloaded all on the **Vulnerable Items** tab.
- From the List view on remediation efforts, where you can view patch data on VI records from the**Vulnerable Items** tab.

From the classic environment view, navigate to **All** > **Vulnerability Response** > **Patches**.

Patch Update records in the VR Workspaces and in the classic environment view

Patch data and patch rollup data and status are displayed on records in your instance.
Patch records are included as part of the patch orchestration feature of this integration with Vulnerability Response. View Patch (VPU) records in Vulnerability Response Workspaces from the List view in the IT Remediation Workspace. Patch Update records in both the classic view and Vulnerability Response Workspaces includes the following data:

- Vulnerability solution data and information from patch vendors imported by the Vulnerability Solution Management application.
- Source Remediation Status that includes the total number of devices that have the a given vulnerability that can be fixed by a patch and any devices that are missing updates.
- Remediation Status that includes % of VIs remediated and the total VIs that have a patch as a preferred patch.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Associated Devices, Vulnerable Items, Patch Deployments and Patch Requests on the Related Links on records in the class view. This data is displayed on tabs on records in the Vulnerability Response Workspaces.
- Patch Requests that remediation owners have submitted for approval.

State rollup on vulnerable item records

For more information about state rollup to records, see Patch data and state rollup for patch orchestration in Vulnerability Response.

Records that roll up active VI counts

To avoid rolling up all the patches to all the vulnerabilities, the scheduled job only picks up changes to the active VI count. These count changes and related data are rolled up to the following records in Vulnerability Response:

- VIT
- RT
- Vulnerability solution
- Patch Update

Viewing data for patches without solutions

For more information about viewing patches without solutions, see View patches without solutions in Vulnerability Response.

Patch data on the Vulnerability Response

The Vulnerability Management (PA) and CISO dashboards are included with a subscription with the Performance Analytics for the Vulnerability Response application. If you have a subscription for Performance Analytics, but do not have a patch orchestration integration installed, the remediation tab is displayed on the CISO dashboard, but it is not populated with data.

For the Vulnerability Management (PA) dashboard, navigate to **All** > **Vulnerability Response** > **Overview**. Click the **Remediation** tab and scroll to the bottom of the page to view Patch Updates data: patches scheduled and not scheduled, patches missing their target dates, and weekly counts.

For the CISO Dashboard, navigate to **All** > **Vulnerability Response** > **CISO Dashboard**. With the Overview tab selected, scroll to the bottom of the page to view Patch Coverage data: Criticality, patches scheduled and not scheduled, and patches missing their target dates.

For more information about the Vulnerability Response dashboards, see Using the default Vulnerability Response dashboards, Patch orchestration with the Vulnerability Response Workspaces, and Viewing patch orchestration data on the Vulnerability Response dashboards.

Schedule patches with the Vulnerability Response patch orchestration integration HCL BigFix

Schedule patches from Patch Update and Remediation task records in the Vulnerability Response application in your ServiceNow AI Platform instance.

Before you begin

Starting with version 16.1, you can schedule patches from the Vulnerability Response Workspaces or from the classic environment.

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul_patch_orch.configure_patch role to configure and schedule patches
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces

Procedure

1. In the Vulnerability Vulnerability Response Workspaces, as a user with the sn_vul.remediation_owner role, navigate to **All** > **Vulnerability Response** > **IT Remediation Workspace**.
2. On the Home page, click **Preferred patch on VIs**.
   The list of Patch Update records for the VIs with preferred patches that are assigned to you are is displayed.
3. Locate a record that you want to open and click to open it.
4. Alternatively, from the List view in the workspace, click **Patches** > **All** and locate a Patch Update record.
   The Patch Update record is displayed. You might prefer to review the data before you schedule a patch, because there might be other patches already scheduled.
5. Refer to the following table about the data displayed and what you can do.

Task	Description
Click a Related Items link	○ Overview - View details such as the patch update record number, the article and bul letin IDs, the release date and category of the update, the site name for the patch, Risk rating, Risk score, description, solution (if provided), and remediation status. ○ Associated Devices - The list of impacted configuration items affected by the patch and status. ○ Vulnerable items - The list of vulnerable items associated with the vulnerability and patch. ○ Patch Deployments - The names and infor mation related to deployments of this patch on assets or asset groups for this patch. ○ Patch requests - A list of patch requests al ready submitted for this patch. This is dis played.
Click a link to open a record	From lists displayed on opened records from the related items links, view more details, in cluding messages about missed targets. Once opened, records remain open as tabs until you close them.
Schedule Patch	When you are ready to schedule a patch or submit a request, click **Schedule Patch**. In the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	dialog that is displayed, fill in the fields. See the steps below for more details.
Add a work note or attach a file	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel. You can also upload a file.

6. Click **Schedule Patch**.
7. In the dialog, fill in the fields.

Field	Description
Select Target	
Assets	Choose one from the list to continue. `Com puter Group` is displayed by default. ○ Computer Group: Select this option if you want to choose a collection (a group of as sets) for this patch.#The groups are made up of the configuration items that are import ed from the BigFix application. ○ Computer List: Select this option if you want to choose individual computers (as sets) for this patch. You can see data about the manufacturer, location, class, when it was last updated, and the maintenance schedule on the dialog that is displayed. Click **Next** to continue.
Computer Group or Computer List	Depending on your selection for Assets, one of the fields is displayed. Choose from the lists.
Schedule	
Deployment Name	Enter a name for this patch deployment. This name helps you track your updates.
Deployment type	Choose one option from the list.
Deadline time	Set the value for the deadline time. This val ue is the time the patch is last available for de ployment.
Available time	Set the value for the time the patch becomes available.
Deployment time based on	Select a time zone from the list to base your deployment time window on.
Allow restart	Default is deactivated. Activate (select) this option to instruct the machines in the group

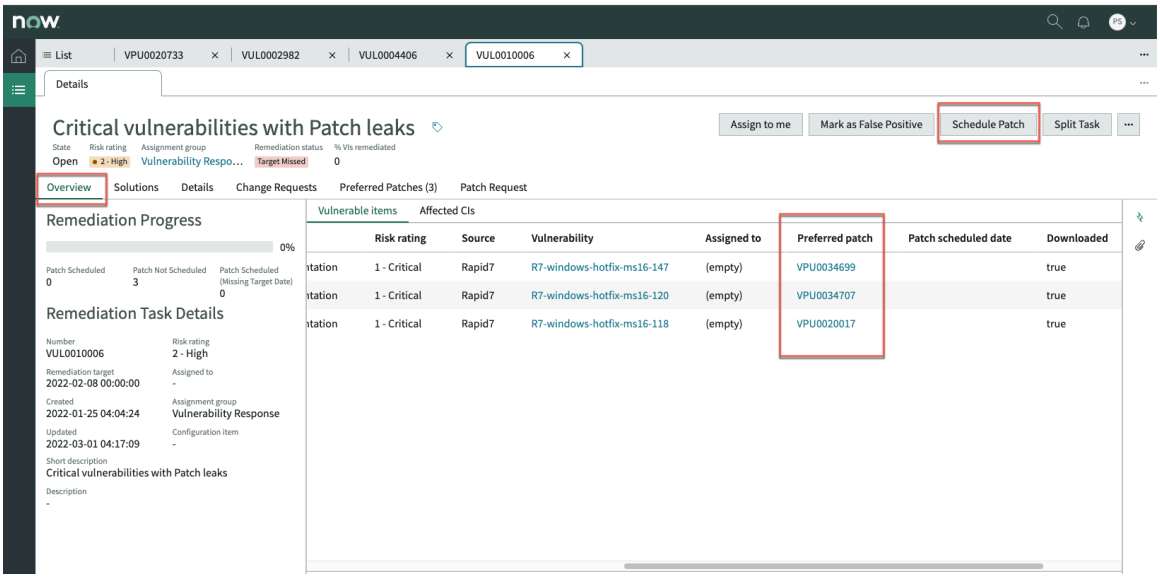
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	to restart automatically after the patch is suc cessfully completed.
Description	Add more text for about the patch. This infor mation is displayed on the Description field of the Patch Update records.

8. Click **Deploy**.
   The patch request is sent to for review. You can view the status of all your submitted requests from **Exception requests** > **My requests** from the List view.
9. Alternatively, you can schedule patches from remediation tasks (RT)s that are assigned to you or your group.

   Note: The option to schedule a patch from a remediation task record is available only if there are patches mapped to (associated with) the VIs in the task. These patches are displayed in the Preferred patch column if you scroll to the right of a remediation task records with the Overview tab selected.

   Remediation task with Preferred patches



10. Click **Schedule Patch** from the RT record and follow the steps listed above to schedule it in the dialog.
11. You can schedule patches for the steps listed previously in the classic environment.
    To locate these records, follow these steps.

    a. In the classic environment, navigate to **Vulnerability Response** > **Patches** > **All**.

    b. From the list that is displayed, locate a Patch Update record.

    c. For remediation tasks, navigate to **Vulnerability Response** > **Remediation Tasks** and locate a record.
    The track the remediation status on the Remediation Status tab. On the bottom of the record, patch data is displayed on the Related Links.

    d. Click Schedule Patch and fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Deployment Name	Enter a name for this patch deployment. This name helps you track your updates.
Patch update	Choose one from the available patches on the list.
Assets	Choose one: ▪ Computer Group: Select this option if you want to choose a collection (a group of assets) for this patch.#The groups are made up of the configuration items that are imported from the BigFix application. ▪ Computer List: Select this option if you want to choose individual computers (assets) for this patch. You can see data about the manufacturer, location, class, when it was last updated, and the maintenance schedule on the dialog that is displayed.
Start time and End time	Enter the start and end times for the time window. Enter when you want the patch to start its deployment, and last day the patch can be installed.

REST messages for the Vulnerability Response patch orchestration integration with HCL BigFix

The Vulnerability Response patch orchestration integration with HCL BigFix REST messages are used to make calls to the BigFix API.

BigFix login

You can also use the REST messages for the BigFix Login so that you can authenticate REST API requests. Changes to the record method of the REST message impact the authentication requests made to BigFix.

Parameter name	Value	Description
sourceType	cumulative	Indicates the source integration pulls data from. Used by code. Changes are not recommended.
sortDIR	desc	Indicates the sort direction for the data pulled from integration. Changes are not recommended.
sortField	severity	Indicates the field the data sort is based on. Changes are not recommended.
type	vuln	Indicates the type of data to be fetched from

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parameter name	Value	Description
		integration for the assets integration. Changes are not recommended.

BigFix integration

You can use the REST message for the BigFix integration to retrieve information from BigFix. Changes to the record method of the REST message impact the requests made to BigFix to retrieve information. REST messages contain the following REST methods.

REST methods

REST method	Description
GET Fetch Data	Retrieves the information from BigFix regarding one of the following based on the query provided: • Computer/Computer Groups • Fixlets • Relevant Fixlets on computers • Actions

Parameter name	Value	Description
url	Dynamic values based on user	Indicates the endpoint of the BigFix Console

BigFix deploy patch

You can use the REST message for the BigFix integration to schedule patches from your ServiceNow AI Platform® to BigFix. Changes to the record method of the REST message impact the requests made to BigFix to retrieve information. REST messages contain the following REST methods.

REST method	Description
POST Deploy Patch	Schedules the patch to BigFix console on single/multiple computers.

Parameter name	Value	Description
url	Dynamic values based on user	Indicates the endpoint of the BigFix Console.
title	Dynamic values based on user	Title of the deployment.
settings_tag	XML tag-named settings with values	Indicates settings that have different parameters and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parameter name	Value	Description
		are sent to BigFix while scheduling the patch.
computer_tag	XML tag-named computers with values	Indicates list of computers on which the patch is going to be scheduled.
site_name	Value from patch update	Name of the site where the Fixlet is present.
fixlet_id	Value from patch update	Id of the Fixlet.

Data transformation for the patch orchestration integration with HCL BigFix

Data is retrieved from the Vulnerability Response patch orchestration with HCL BigFix integration, processed through a set of data sources, and transformed in your ServiceNow AI Platform® instance.

BigFix Collection import

The data from the imported assets (computers and computer groups) are loaded into the BigFix Collection Import [sn_vul_bigfix_collection_import] table. The BigFix Computer and Computer Groups Import TM (transform map?) is used to transform the imported information.

Note: Changes to this transform map alter how data from the BigFix Collection import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and locate BigFix Computer and Computer Groups Import TM. The following table lists the transform map fields by integration.

BigFix Computer and Computer Groups import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script used to initialize the values in the scope variable [sn_vul_bigfix] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script used to create and update CIs based on CI Lookup Rules and collections as well as relation between them. Based on the results, this script modifies the values in the scope variable [sn_vul_bigfix]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of CIs created, updated, and ignored. This script is for internal use and should not be modified or deleted.

BigFix Fixlet import

The data from the imported fixlets are loaded into BigFix Fixlet Import [sn_vul_bigfix_patch_update_import] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

BigFix Fixlet Import TM is used to transform the imported information.

Note: Changes to this transform map alter how data from the BigFix Fixlet import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and locate the BigFix Fixlet Import TM.

The following table lists the transform map fields by integration.

BigFix Fixlet import transform map fields

Source field	Target field	Description
u_id	article_id	Unique Id of a fixlet in a site.
u_id	source_id	Unique Id of a fixlet in a site.
U_site_name	Sn_vul_bigfix_site_name	Site name in BigFix where the Fixlet relies.
U_display_name	Title	Title of the Fixlet.
[Script]	Bulletin_id	Source id of the solution.
[Script]	Sn_vul_solution	Solution based on the source id.
U_source	bulletin_source	Source vendor of the solution.
[Script]	Date_release	Release date of the fixlet.
U_category	Update_category	Category of the fixlet.
[Script]	Is_highest_supersedence	Boolean for if the fixlet is highest supersedence or not.
[Script]	Is_downloaded	Boolean of if the fixlet is downloaded or not.
[Script]	Integration_instance	Name of the instance from which the fixlet is imported.
U_source_severity	Source_severity	Severity of the fixlet.
U_applicable_count	Num_total	Total number of devices with missing fixlets.
[Script]	Last_modified	Last modified date of fixlet.

BigFix Fixlet import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_bigfix] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to update the values in the scope variable [sn_vul_bigfix]. This script

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

BigFix Fixlet import transform map script timing (continued)

Script	Description
	is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of fixlets created, updated, and ignored. This script is for internal use and should not be modified or deleted.

BigFix Device Fixlet Import

The data from the imported relevent fixlets on computers are loaded into the BigFix Device Fixlet Import [sn_vul_bigfix_device_patch_import] table.

BigFix Device Fixlet TM is used to transform the imported information.

Note: Changes to this transform map alter how data from the BigFix Device Fixlet import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and locate the BigFix Device Fixlet TM.

The following table lists the transform map fields by integration.

BigFix Device Fixlet transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_bigfix] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to Create and Update CIs based on CI Lookup Rules and collections as well as relation between them. Based on the results, this script modifies the values in the scope variable [sn_vul_bigfix]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of CIs created, updated, and ignored. This script is for internal use and should not be modified or deleted.

BigFix Actions Import

The data from the imported actions are loaded into the BigFix Actions Import [sn_vul_bigfix_deployment_import] table.

The BigFix Actions Import TM is used to transform the imported information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Changes to this transform map alter how data from the BigFix Actions import is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and locate the BigFix Fixlet Import TM.

The following table lists the transform map fields by integration.

BigFix Actions Import transform map fields

Source field	Target field	Description
u_id	source_id	Unique Id of an action.
U_name	name	Name of the action
[Script]	Sn_vul_bigfix_discovered_item	Reference of the discovered item on which the patch is deployed
U_status	status	Status of the action
[Script]	Sn_vul_patch_orch_update	Reference of the patch
U_apply_count	Count_success	Success count of action.
U_retry_count	retry	Retry count of the action.
[Script]	Deployment_time	Start time of the action.
[Script]	deadline	End time of the action.
[Script]	Source_created	Creation time of the action.
[Script]	Integration_instance	Name of the instance from which the action is imported.

BigFix Actions import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_bigfix] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to update the values in the scope variable [sn_vul_bigfix]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of actions created, updated, and ignored. This script is for internal use and should not be modified or deleted.

Example workflow for the Vulnerability Response patch orchestration integration with HCL BigFix

An example of how patch orchestration works with the HCL BigFix product.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Say, for example, your entire environment is patched once every three weeks. The most recent patching window was completed a week ago, but you want to apply a patch to fix a critical vulnerability that has recently become known. Due to the critical nature of this vulnerability, you cannot wait two more weeks for the next scheduled patch.

Roles required:

- sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin for the Vulnerability Manager Workspace.
- sn_vul.remediation_owner to view the IT Remediaiton Owner workspace.
- sn_vul_patch_orch.configure_patch role to configure and schedule patches.
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces.

About this task

As a vulnerability manager or analyst working in the Vulnerability Manager Workspace, you might consider creating watch topics, or editing existing watch topics to help you capture imported VIs with critical vulnerabilities. With the patch orchestration integration, you can also see the patches you want to use to fix and track these vulnerabilities. The following table lists a few samples with the conditions you might set for watch topics for patch orchestration. Use these examples to help you determine settings that work best for your environment. See Create a watch topic in the Vulnerability Manager Workspace for more information about setting up the watch topic.

Sample watch topics for patch orchestration in the Vulnerability Manager Workspace

Watch topic name	Description
Critical Vulnerabilities with Patch Leaks	`Risk rating is 1 - critical` AND `Reason is Patch Not Scheduled`
Critical Vulnerabilities with Patches Scheduled (missing SLA)	`Reason is Patch Scheduled (Missing Target Date)`
Critical Vulnerabilities with Patches Scheduled	`Risk rating is 1 - critical` AND `Patch scheduled date is not empty` AND `Reason is Patch Scheduled`

- As a vulnerability manager or analyst, after you create the watch topics and remediation efforts, you generate remediation tasks. From VI records and remediation tasks, you can drill down into the Detections tab and locate discovered item records that have the vulnerability you are tracking, along with the assets imported by the BigFix product.
- As a vulnerability analyst or admin, you can monitor the patch data associated with the vulnerability. You might also deploy a patch or multiple patches to a specific asset (configuration item) from a discovered item record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As an IT remediation specialist, you have options for how you address the vulnerability with a patch deployment.

- You can schedule the patch from a Patch Update record (VPU#).
- If vulnerable items (VI)s have preferred solutions mapped to them, and they are assigned to you or your groups, you can schedule the patches from a remediation task that has these vulnerable items.

Procedure

1. As an IT Remediation Specialist, in the IT Remediation Workspace, click the Home view.
2. From the home view, click the **Assigned remediation tasks** scorecard to view the records.

   For the sake of this example, you might check the Short description field on the remediation task (VUL#) for any text that relates to your critical vulnerability. Say, for example, you might know that your vulnerability manager has created a watch topic called, Critical vulnerabilities with Patch leaks to catch VIs (VIT#) with this critical vulnerability.

   With the record open, you can also review the VIs, the Preferred patches, and see if you or any of your group has already submitted any patch requests for approval.
3. If you have enough information, you might prefer to submit a request for a patch now from this remediation task.

   Note: If the VIs associated with the record do not have patches that are mapped to them, the **Schedule Patch** button is not available on the record.
4. Click **Schedule Patch** and fill out the fields in the dialog.
   For more information about how to schedule a patch, see Schedule patches with the Vulnerability Response patch orchestration integration HCL BigFix.
5. Alternatively, from the List view in the IT Remediation Workspace, you can click on the Remediation tasks, Vulnerable items, Solutions, and Patches links to view these records.

   In the case of this example, instead of a watch topic name, you might know the Article ID or the Bulletin ID and title of the patch. If so, you might want to check if any of the VIs with this vulnerability are assigned to you or to your groups. From Patch Update records, you can submit patch requests. From VI records, you can check for potential patches and open the associated remediation task if you want to submit a patch request.
6. If you don't have access to the workspaces, or you prefer to view data and schedule patches from the classic environment, follow these steps.

   a. Navigate to **All** > **Vulnerability Response** > **Patches** > **All**.

   b. Locate the Patch Update record you want.
   You might prefer to filter the records with `Critical` Risk Scores.

   c. Review the associated VIs and % VIs remediated fields on the Remediation Status tab.
   If the VIs have patches available, the **Schedule Patch** button is displayed in the upper right of the record.

   d. If you decide you want to submit a request, click **Schedule Patch**.
   For more information about how to schedule a patch, see Schedule patches with the Vulnerability Response patch orchestration integration HCL BigFix.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Alternatively, say you don't have the patch ID information, but you might check the Short description field on the remediation tasks that are assigned to your group for any text that relates to your critical vulnerability.

f. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**.

g. Locate the record you want and click it to open it.
On the open record, review the Remediation Status tab for VIs and % VIs remediated. Click the Related Links for VI records, Preferred Solutions, Preferred Patches, and Patch Requests.

> **Note:** If the VIs associated with the record do not have patches that are mapped to them, the **Schedule Patch** button is not available on the record.

h. Click **Schedule Patch** from the record if you want to submit a patch request.

Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM

Manage patches and patch deployments for the critical vulnerabilities on your assets with the Vulnerability Response integration with the Microsoft System Center Configuration Manager (SCCM) product.

Patch orchestration with Vulnerability Response

Patch orchestration with Vulnerability Response uses scheduled imports from third-party solution integrations, patch vendors, and vulnerability scanners. Scanner detection data match the assets in your environment to vulnerabilities and to the patch updates that can fix them. You submit patch requests for approval, schedule patch updates to resolve vulnerable items, and monitor remediation progress all from your ServiceNow AI Platform® instance.

Vulnerability Response patch orchestration with Microsoft SCCM

When the Vulnerability Response Patch Orchestration with the Microsoft SCCM application is used with the ServiceNow® Vulnerability Solution Management, Patch Orchestration, and Vulnerability Response applications, vulnerability managers and analysts can perform the following tasks:

- See more context and information about the types of patches and vendors' solutions (patches).
- View and monitor vulnerability and solution data, as well as vulnerability remediation progress from records in the Vulnerability Response Workspaces.

IT specialists and remediation owners can perform the following tasks:

- Deploy patches supported by the Microsoft SCCM product for their Windows, CentOS, macOS, Oracle, and other assets at regular, scheduled intervals during off-hours to avoid conflicts with work.
- Identify unpatched assets with vulnerabilities, or assets that or were not successfully updated by scheduled patches from imported detection data from third-party scanners.
- Schedule available patches from either the IT Remediation Workspace or from the classic UI for vulnerable, unpatched assets from patch update, remediation task, and discovered item records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key terms in the Vulnerability Response and Microsoft SCCM applications

Configuration item (CI)

CIs are the existing assets that are listed in your#Configuration Management Database (CMDB). Microsoft SCCM calls CIs, devices.

Collections and device collections

Terminology used in the Microsoft SCCM product that refers to a group of assets.

Vulnerable item

An imported vulnerability that matches an existing asset in your CMDB.

Instance

A distinct account of the Microsoft SCCM application. Each user account can be an instance in the Microsoft SCCM application. This term also refers to a unique, secure web address for a ServiceNow AI Platform instance.

Integration

An integration is a scheduled job in the ServiceNow AI Platform that retrieves information from a third-party source, such as the integration with the Microsoft SCCM machines.

Solution

There are two types of solutions in the context of this integration, potential and preferred. A potential solution is one that might address a vulnerability. Vulnerabilities often have many potential solutions. #A preferred solution matches the most effective solution for a specific, detected vulnerability.

Patches

Software updates that fix vulnerabilities. In the Microsoft SCCM application, patches are called, Patches. For example, Microsoft SCCM has patches for Windows, CentOS, MAC, Oracle and other products.

Preferred patch

Preferred patches are software updates that are intended to fix specific vulnerabilities. Patches, once deployed, map to the vulnerable items that are related to specific vulnerabilities and fix them.

Remediation task or, prior to v15.0 of Vulnerability Response, vulnerability groups

Lists of vulnerable items in the Vulnerability Response application of actions that are required to fix vulnerabilities.

Deployment

Deployment for the purposes of this integration refers to when you apply, initiate, or schedule a patch to a machine. You can deploy the patches you downloaded from Microsoft SCCM in your ServiceNow AI Platform by navigating to discovered items, patches, or remediation tasks from individual records in Vulnerability Response. You can deploy patches with scheduled jobs to individual machines or to computer groups.

Deployment in the ServiceNow AI Platform can also refer to an integration that supports multi-source. A single integration existence is referred to as a deployment of your integration. A deployment refers to the integrations and products across your environment. For example, you might have multiple deployments of the Microsoft SCCM Vulnerability integration in your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Solution Management and the Vulnerability Response patch orchestration integration with Microsoft SCCM

The Vulnerability Solution Management application is a ServiceNow AI Platform application that correlates your vulnerability findings with the breakdown of the solutions (patches) that remediate them. Identify the software patches from third parties for products and services, configuration updates, and other controls that have the highest impact for your organization. Along with third-party scanner information, the Solution Management for Vulnerability Response, Vulnerability Response, and the Vulnerability Response Patch Orchestration with Microsoft SCCM applications work together to roll preferred patches up from the solution, to the vulnerability, to the vulnerable item to help you fix and close vulnerabilities to your environment. The Solution Management for Vulnerability Response, Vulnerability Response, and the Vulnerability Response Patch Orchestration Microsoft SCCM integration applications are all available in the ServiceNow® Store.

Required ServiceNow AI Platform roles

The integration installation, configuration, and remediation tasks require the following roles in your#ServiceNow AI Platform instance.

admin

Users with this role get entitlements for applications in the ServiceNow Store and downloads them to ServiceNow AI Platform instances.

sn_vul.vulnerability_admin

Users with this role activate applications in the ServiceNow AI Platform instance and completes configuration of the Vulnerability Response application. This role has complete access to the Vulnerability Response (VR) application and its records. This admin user configures all VR applications, rules, and third-party integrations.

sn_vul_sccm.configure_integration

Users with this role configure the Microsoft SCCM Patch Orchestration Integration application. This role contains the sn_vul_sccm.read_integration granular role.

sn_vul_sccm.read_integration

Users with this role can view (read only) the#ecords of the Vulnerability Response and the Microsoft SCCM Patch Orchestration Integration application and patch orchestration data.

sn_vul_patch_orch.configure_patch

Users with this role can configure and apply patches.

sn_vul_patch_orch.read_patch

Users with this role can view (read only) patch information.

Approvers

Assign uses to the Approver level 1 and Approver level 2 approver groups if you want submitted patch requests approved prior to deployment.

For more information about assigning these roles using the Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

CI lookup rules

When data is imported from the Microsoft SCCM application,#he Vulnerability Response application automatically searches for matches in the#Configuration Management Database (CMDB) using Resource ID data. CI lookup rules are used to identify CIs (assets) and add them automatically to vulnerable item (VI) records when VIs are created. The following CI lookup rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

are shipped with the base system and are used to identify CIs (assets) and add them to the discovered items.

This lookup rule relies on the data brought in by the Service graph connector with SCCM. You must install and run the CMDB integration prior to running the SCCM integrations. If you have multiple installations of the SCCM server, you can configure the Service graph connector connection alias in the SCCM patch orchestration configuration page.

MID Server

The Vulnerability Response Patch Orchestration with Microsoft SCCM is an on-premises integration. It requires a standalone Windows MID Server that is not part of a MID Server cluster. The MID server is required to runs scripts on remote machines from your instance to import data from the SCCM server. APIs for this integration are called using MID Servers that you set up in your ServiceNow AI Platform instance. Prepare for the Vulnerability Response patch orchestration integration with Microsoft SCCM.

Integrations and dependencies of the Vulnerability Response Patch Orchestration with the Microsoft SCCM application

The following product and dependency applications are required for the Vulnerability Response Patch Orchestration with Microsoft System Center Configuration Manager (SCCM) integration. These applications are available in the ServiceNow® Store

Available versions of applications and dependencies required for the patch orchestration integration

To view patch orchestration data and available updates (patches) in the workspaces and the classic UI in Vulnerability Response, the following applications are required. All applications listed are available in the ServiceNow® Store. Some applications require separate subscriptions.

For more information about version compatibility with the required applications and family releases, refer to the KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes article in the HI Knowledge Base.

Application and release version
Vulnerability Response
Vulnerability Solution Management
Vulnerability Response Patch Orchestration application
Vulnerability Response Patch Orchestration with Microsoft SCCM application
Security Support Common
Security Support Orchestration
Service Graph connector with SCCM

Vulnerability Response patch orchestration application tables

The Vulnerability Response Patch Orchestration application contains the following tables:

Table	Description
Patch Update [sn_vul_patch_orch_update]	Stores information about the patches that are available on distinct instances.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Device Update [sn_vul_patch_orch_m2m_src_ci_update]	Stores data about the deployed patches, along with deployment status, that are on displayed on discovered item records.
Collection [sn_vul_patch_orch_collection]	Stores collection data from distinct instances.
Device Collection [sn_vul_patch_orch_m2m_src_ci_collection]	Stores collections data about discovered items.
Patch Deployment [sn_vul_patch_orch_deployment]	Stores information about deployed patches about Collections and CIs.
Potential Patch [sn_vul_patch_orch_m2m_vuln_patch]	Stores data about patches and vulnerabilities that identify the patches that might be used to resolve a vulnerability.

Vulnerability Response Patch Orchestration with Microsoft SCCM integrations

The integrations developed by ServiceNow® engineering make up the orchestrated solution deployment with the Microsoft SCCM product. The following integrations are included with the Microsoft SCCM Patch Orchestration Integration application that you download from the ServiceNow® Store.

After you install the integration application on your ServiceNow AI Platform instance, to view these integrations, navigate to **Integrations** > **SCCM Patch Orchestration Integration** > **Integrations**. The Vulnerability Response application processes data on scheduled time intervals imported by these integrations with Microsoft SCCM endpoints.

Integration	Description
Microsoft SCCM Collection Integration	• This integration is scheduled to run daily and runs first in the chained integration run. • Retrieves the device collections from the SCCM Collections.
Microsoft SCCM Device Collection Integration	• When scheduled, this integration is triggered by the completion of the SCCM Collection Integration. You can also run it on-demand. • This integration fetches the devices under each collection. This integration creates records in the discovered items table and Device Collection table.
Microsoft SCCM Patch Update Integration	• When scheduled, this integration is triggered by the completion of the SCCM Device Collection Integration. You can also run it on-demand. • Retrieves information from the SCCM server about the Patches that are either installed or missing on devices (assets).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
Microsoft SCCM Deployments Integration	• When scheduled, this integration is triggered by the completion of the Patch Update Integration. You can also run it on-demand. • Retrieves information about the patches scheduled by the IT team in the SCCM server.

Prepare for the Vulnerability Response patch orchestration integration with Microsoft SCCM

Prepare for the integration by performing the following setup tasks.

Before you begin

Roles required: admin for installing the applications and assigning roles. Other roles are listed in the following table.

About this task

A successful integration requires planning and careful execution of pre-integration tasks.

Procedure

1. For a smooth installation and configuration of the Vulnerability Response Patch Orchestration with Microsoft SCCM application, follow the checklist provided below.
2. You might prefer to print the following checklist and verify the items listed are completed before you install the application and import vulnerability and patch-related information into your ServiceNow AI Platform® instance.

Task	Description
☐	(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application. For more information about installing and activating the Vulnerability Response application, see, Install Vulnerability Response. This integration requires version 16.1 of Vulnerability Response or later.
☐	If not already installed, get entitlements and install and third-party scanner application to import vulnerability data. See Vulnerability Response integrations for more information about third-party scanners supported by Vulnerability Response. See .
☐	If not already installed, get entitlements and download the Vulnerability Response Patch Orchestration with Microsoft SCCM application to your ServiceNow AI Platform® instance. See .

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
☐	Obtain Microsoft SCCM credentials. Verify you have any account names, passwords, and other service information required by your Microsoft products so that you have access to them.
☐	Verify that you have groups or users to manage the integrations and remediate vulnerable items. **admin** The system admin gets entitlements, downloads, and installs the Microsoft SCCM Patch Orchestration application and the other applications required for the integration. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in the Setup Assistant in Vulnerability Response or from the User Administration module. **sn_vul.vulnerability_admin** Once assigned, the vulnerability admin completes the configuration of the Microsoft SCCM integrations and the other third-party applications. This role has complete access to the Vulnerability Response (VR) application and its records. This role configures all VR applications, rules, third-party integrations, Vulnerability Response Patch Orchestration and Vulnerability Solution Management applications. **sn_vul_sccm.configure_integration** Users with this role configure the Microsoft SCCM Patch Orchestration Integration application. This role contains the sn_vul_sccm.read_integration and connection_admin granular roles that permit the user to connect to the SCCM console and configure the integration instances in your ServiceNow AI Platform. **sn_vul_sccm.read_integration** Users with this role can view (read only) the #ecords of the Vulnerability Response and the Microsoft SCCM Patch Orchestration Integration application and patch orchestration data. **sn_vul_patch_orch.configure_patch** Users with this role can configure and apply patches. Patches requested by this user from Vulnerable item and Patch Update records are sent for approval if change management is active and approvers are assigned. **sn_vul_patch_orch.read_patch**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	Users with this role can view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces. **Approvers** Users assigned to the Approver level 1 and, optionally, Approver level 2, approver groups approve submitted patch requests. By default, patches are submitted to the Approver level 1 group for approval prior to deployment. For more information about the approval process, see Configure the Vulnerability Response Patch Orchestration with Microsoft SCCM integration. For more information about setting up approvers and groups, see Assign the Vulnerability Response persona roles using Setup Assistant. The system admin performs the initial assignment of roles to users and groups for the integration. By default, the Vulnerability Response group is available. If not already created, you may prefer to create additional groups for remediation specialist and vulnerability analyst roles and add users with the User Administration module in your instance. See Create a user group.
☐	Verify you have enabled any features, rules, dependency plugins, or jobs in your instance required for the integration. ○ The Vulnerability Response Patch Orchestration with Microsoft SCCM is an on-premises integration that requires you to use a standalone Windows MID Server. For more information about MID Servers in your instance, see MID Server. ○ Navigate to **System Applications** > **All Available Applications** > **All** and locate the plugin. If not installed in your instance, install and activate it.

Install the Vulnerability Response Patch Orchestration with Microsoft SCCM application

Download the application from the ServiceNow Store.

Before you begin

Before you install the application, verify you have completed all the items in the checklist in Prepare for the Vulnerability Response patch orchestration integration with Microsoft SCCM.

Roles required: admin for initial assignment of the sn_vul.vulnerability_admin role and installing the application. Vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin (deprecated) to configure the Vulnerability Response Patch Orchestration Microsoft SCCM and other applications after they are installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to sub-production or development instances, it's not necessary to get entitlement proceed to Activate a ServiceNow Store application.

Procedure

1. Navigate to **All** > **System Applications** > **all Available Applications** > **All**.
2. Locate the **Vulnerability Response Patch Orchestration with Microsoft SCCM** application and click **Install**.

   This action installs the application you downloaded from the ServiceNow Store.
3. Alternatively, you can install applications from the Setup Assistant.
   For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation, navigate to **All** > **Microsoft SCCM Patch Orchestration Integration** > **Configuration** to continue with the configuration.

Configure the Vulnerability Response Patch Orchestration with Microsoft SCCM integration

After you have installed the application, configure it with your account information and validate your credentials.

Before you begin

Roles required: sn_vul.vulnerability_admin and sn_vul_sccm.configure_integration

Procedure

1. Navigate to **All** > **Microsoft SCCM Patch Orchestration Integration** > **Configuration**.
2. Fill in the fields with your Microsoft SCCM information and credentials.

Field	Description
Integration instance	The name of the Microsoft SCCM instance account you want to use, for example, `Microsoft SCCM Patch management integration`.
Host name	Enter the URL for the Microsoft SCCM host.
Username	Enter your Microsoft SCCM account username.
Password	Enter your Microsoft SCCM account password.
MID Server	Enter the name of the standalone MID Server from the list that you want to use. See Prepare for the Vulnerability Response patch orchestration integration with Microsoft SCCM for more information about MID Servers and set up tasks in your ServiceNow AI Platform®.

3. Click Save and Test Credentials.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The status of your connection between Microsoft SCCM and your ServiceNow AI Platform® instance#s displayed in the Validation Status Field. If you do not see a successful test, follow the prompts.

4. **Optional:** Domain separation is supported for this integration.
   You can add multiple configurations of to your instance. To add additional configurations:

   a. Navigate to **All** > **Microsoft SCCM Patch Orchestration Integration Integration Instances**.

   b. Verify the application scope, `Vulnerability Response Patch Orchestration with Microsoft SCCM`, is displayed in the Application scope field.

   c. Click **New**.

   d. Fill in the form.

Field	Description
Name	Name for the integration instance.
Application	Vulnerability Response Patch Orchestration with Microsoft SCCM
Integration	[Read only] Microsoft SCCM Patch management is the default.
Active	Default is activated. If cleared, the instance is not active.

   e. Click **Submit**.
   Your new integration instance is displayed on the Integration Instances list.

   f. Repeat steps 1-3 to configure your integration instance and test your credentials.

5. Set up approvals for patch requests.
   By default, a system property [**sn_vul_patch_orch.patch_approval_required**] is activated so that when patch deployments are scheduled, they are submitted for review and approval to users assigned to the Level 1 - Patch update approval group.

   If you want users with the sn_vul_patch_orch.configure_patch role to schedule patches without approval, you can deactivate the [**sn_vul_patch_orch.patch_approval_required**] property. You might prefer to leave approvals activated so that scheduled patches do not conflict with normal working hours.

   Note: If you deactivate the approval system property, any user with the sn_vul_patch_orch.configure_patch role can schedule and deploy patches without review and approval.

   As a user with the sn_vul.vulnerability_admin role, to deactivate the system property:

   a. Navigate to **All** > **sys.properties.list**.

   b. Locate **sn_vul_patch_orch.patch_approval_required** and click it to open the record.

   c. In the Value field, type `false`.

   d. Click **Update**.

6. If you do not deactivate this property, you need to assign approvers for patch requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As a user with the sn_vul.vulnerability_admin role, follow these steps.

a. Navigate to **All** > **Vulnerability Response** > **Administration** > **Approval Rules**.

b. If the **Deploy patch update approval** Approval Rule is not displayed in the list, click **All** to the right of the green filter icon in the upper left of the screen to display the entire list.

c. From the list, click **Deploy patch update approval**.

d. On the record, with the Approval Configuration tab selected, click **Default Configuration Patch Update approval**.

e. On the record, click **Level 1 - Patch update approval**.

f. Add users in this group.

The users assigned to this group approve patch requests submitted by users with the sn_vul_patch_orch.configure_patch role. Navigate to **My Approvals** to view and process the requests.

7. Click**Update** to save your changes.
8. **Optional:** You can set up multi-level approvals so that more than one approval is required prior to the deployment of scheduled patch requests.

a. With the Default Configuration Patch Update approval record displayed, click **New**.

b. Fill in the fields.

Field	Description
Name	Approval level name, for example, **Level 2 - Patch update approval**.
Active	Activated by default, signifying that the approval level is in use.
Required approval	Select how many approvals are required for the selected level: ▪ One approver required ▪ All users must approve
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 runs before a configuration with an order entry of 200.
Role	Select a role for the group from the list.
Approval rule	Contains the table and type details for the approval rule.
Approval configuration	Contains the approval configurations.
Assign using	Select an option:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	▪ User and user group ▪ Approval table field ▪ Script
Groups	Approver level group consisting of multiple users. The user must have one of the following roles that you specify.
Users	Edit the users listed in the groups.

c. Click **Submit** to save your edits.

Viewing patch data and patch data rollup for the Vulnerability Response Patch Orchestration integration with Microsoft SCCM

Patch data and patch rollup data, as well as vulnerability information and remediation status of your vulnerabilities are displayed on records in your instance.

Viewing patch data in the Vulnerability Response Workspaces

Roles required:

- sn_vul_patch_orch.configure_patch role to configure and schedule patches
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces

In the IT Remediation Workspace, you can view the patches:

- On the Home view, where you can click scorecards to view records for Preferred solutions on VIs, Vulnerable CIs, and Preferred Patches on VIs.
- On the List view, where you can view all Patch Update records (VPUs) from the Patches links, and the vulnerable items (VITs) that are assigned to you that have patches.

You can schedule patches from the following records:

- From Patch Update (VPU)
- Remediation task (RT)
- Discovered Item (SDI) records

In the Vulnerability Manager Workspace, you can view patches:

- From the Home view on watch topics, where you can view preferred and potential patches, Patch scheduled dates, and, if the patch has been downloaded all on the **Vulnerable Items** tab.
- From the List view on remediation efforts, where you can view patch data on VI records from the**Vulnerable Items** tab.

From the classic environment view, navigate to **All** > **Vulnerability Response** > **Patches**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Patch Update records in the VR Workspaces and in the classic environment view

Patch data and patch rollup data and status are displayed on records in your instance. Patch records are included as part of the patch orchestration feature of this integration with Vulnerability Response. View Patch (VPU) records in Vulnerability Response Workspaces from the List view in the IT Remediation Workspace. Patch Update records in both the classic environment and Vulnerability Response Workspaces include the following data:

- Vulnerability solution data and information from patch vendors imported by the Vulnerability Solution Management application.
- Source Remediation Status that includes the total number of devices that have a given vulnerability that can be fixed by a patch. Additionally, it also includes and any devices that are missing updates.
- Remediation Status that includes % of VIs remediated and the total VIs that have a patch as a preferred patch.
- Associated Devices, Vulnerable Items, Patch Deployments and Patch Requests on the Related Links on records in the class view. This data is displayed on tabs on records in the Vulnerability Response Workspaces.
- Patch Requests that remediation owners have submitted for approval.

State rollup on vulnerable item records

For more information about state rollup to records, see Patch data and state rollup for patch orchestration in Vulnerability Response.

Records that roll up active VI counts

To avoid rolling up all the patches to all the vulnerabilities, the scheduled job only picks up changes to the active VI count. These count changes and related data are rolled up to the following records in Vulnerability Response:

- VIT
- RT
- Vulnerability solution
- Patch Update

Viewing data for patches without solutions

For more information about viewing patches without solutions, see View patches without solutions in Vulnerability Response.

Patch data on the Vulnerability Response

The Vulnerability Management (PA) and CISO dashboards are included with a subscription with the Performance Analytics for the Vulnerability Response application. If you have a subscription for Performance Analytics, but do not have a patch orchestration integration installed, the remediation tab is displayed on the CISO dashboard, but it is not populated with data.

For the Vulnerability Management (PA) dashboard, navigate to **All** > **Vulnerability Response** > **Overview**. Click the **Remediation** tab and scroll to the bottom of the page to view Patch Updates data: patches scheduled and not scheduled, patches missing their target dates, and weekly counts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For the CISO Dashboard, navigate to **All** > **Vulnerability Response** > **CISO Dashboard**. With the Overview tab selected, scroll to the bottom of the page to view Patch Coverage data: Criticality, patches scheduled and not scheduled, and patches missing their target dates.

For more information about the Vulnerability Response dashboards, see Using the default Vulnerability Response dashboards, Patch orchestration with the Vulnerability Response Workspaces, and Viewing patch orchestration data on the Vulnerability Response dashboards.

Schedule patches with the Microsoft SCCM integration with Vulnerability Response

Schedule patches from Patch Update and Remediation task records in the Vulnerability Response application in your ServiceNow AI Platform instance.

Before you begin

Starting with version 16.1, you can schedule patches from the Vulnerability Response Workspaces or from the classic environment.

Roles required:

- sn_vul_patch_orch.configure_patch role to configure and schedule patches
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces

Procedure

1. In the Vulnerability Vulnerability Response Workspaces, as a user with the sn_vul.remediation_owner role, navigate to **All** > **Vulnerability Response** > **IT Remediation Workspace**.
2. On the Home page, click **Preferred patch on VIs**.
   The list of Patch Update records for the VIs with preferred patches that are assigned to you are is displayed.
3. Locate a record that you want to open and click to open it.
4. Alternatively, from the List view in the workspace, click **Patches** > **All** and locate a Patch Update record.
   The Patch Update record is displayed. You might prefer to review the data before you schedule a patch, because there might be other patches already scheduled.
5. Refer to the following table about the data displayed in the IT Remediation Workspace and what you can do.

Task	Description
Click a Related items link	○ Overview - View details such as the patch update record number, the article and bul letin IDs, the release date and category of the update, the site name for the patch, Risk rating, Risk score, description, solution (if provided), and remediation status. ○ Associated Devices - The list of impacted configuration items affected by the patch and status. ○ Vulnerable items - The list of vulnerable items associated with the vulnerability and patch.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	○ Patch Deployments - The names and infor mation related to deployments of this patch on assets or asset groups for this patch. ○ Patch requests - A list of patch requests al ready submitted for this patch.
Click a link to open a record	From lists displayed on opened records from the related items links, view more details, in cluding messages about missed targets. Once opened, records remain open as tabs until you close them.
Schedule Patch	When you are ready to schedule a patch or submit a request, click **Schedule Patch**. In the dialog that is displayed, fill in the fields. See the steps below for more details.
Add a work note or attach a file	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel. You can also upload a file.

6. Click **Schedule Patch**.
7. In the dialog, fill in the fields.

Field	Description
Step 1 Select Target	
Collection	Choose a collection (group of assets) from the list to continue. These are the collections imported from SCCM.
Step 2 Schedule	
Deployment Name	Enter a name for this patch deployment. This name helps you track your updates.
Deployment type	Choose one option from the list. ○ Required - this patch is a required update. ○ Available - this patch is not required, but available for deployment.
Deadline time	Set the deadline. This value indicates last day the patch can be installed.
Available time	Set the value for the time the patch first be comes available for deployment.
Deployment time based on	Select a time zone from the list to base your deployment time window on.

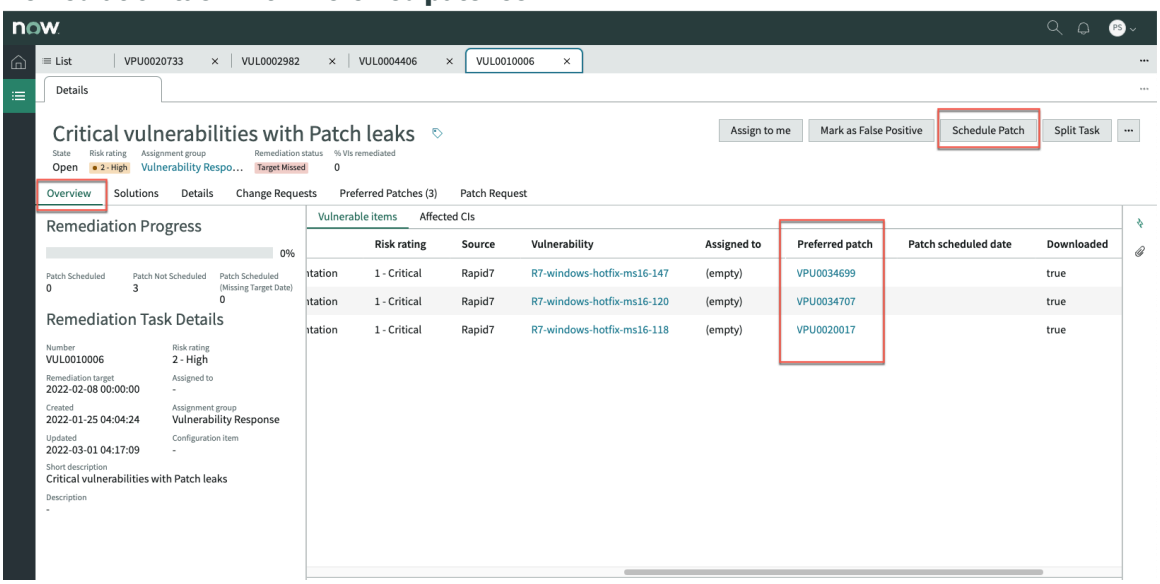
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Allow restart	Default is deactivated. Activate (select) this option to instruct the machines in the group to restart automatically after the patch is suc cessfully completed.
Description	Add more text for about the patch. This infor mation is displayed on the Description field of the Patch Update record.

8. Click **Deploy**.
   The patch request is sent to for review. You can view the status of all your submitted requests from **Exception requests** > **My requests** from the List view.
9. Alternatively, you can schedule patches from remediation tasks (RT)s that are assigned to you or your group.

   Note: The option to schedule a patch from a remediation task record is available only if there are patches mapped to (associated with) the VIs in the task. These patches are displayed in the Preferred patch column if you scroll to the right of a remediation task records with the Overview tab selected.

   Remediation task with Preferred patches



10. Click **Schedule Patch** from the RT record and follow the steps listed above to schedule it in the dialog.
11. **Optional:** You can schedule patches for the steps previously in the classic environment.
    To locate these records, follow these steps.

    a. In the classic environment, navigate to **All** > **Vulnerability Response** > **Patches** > **All**.

    b. From the list that is displayed, locate a Patch Update record.

    c. For remediation tasks, navigate to **Vulnerability Response** > **Remediation Tasks** and locate a record.
    The track the remediation status on the Remediation Status tab. On the bottom of the record, patch data is displayed on the Related Links.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Click **Schedule Patch** and fill in the fields.

Field	Description
Deployment Name	Enter a name for this patch deployment. This name helps you track your updates.
Description	Add more text for about the patch. This information is displayed on the Description field of the Patch Update record.
Deployment type	Choose one option from the list. ▪ Required - this patch is a required update. ▪ Available - this patch is not required, but available for deployment.
Collection	Choose a collection (group of assets) from the list to continue. These groups are the assets collections imported from SCCM.
Deployment time based on	Select a time zone from the list to base your deployment time window on.
Available Time	Set the value for the time the patch first becomes available for deployment.
Deadline	Set the deadline. This value indicates last day the patch can be installed.

e. Click **Deploy**.

REST messages for the Vulnerability Response Patch Orchestration with Microsoft SCCM

The Vulnerability Response Patch Orchestration with Microsoft SCCM uses the SCCM Windows Management Instrumentation (WMI) classes to make calls to the SCCM Server API.

Overview

The SMS Provider provides API an inter-operability access over HTTPS, called the administration service. The administration service is a representational state transfer (REST) API based on the Open Data (OData) v4 protocol.

See What is the administration service in Configuration Manager for more information about the administration service use with this integration.

Since the authentication needed uses the Windows New Technology LAN Manager NTLM protocol, calls to the APIs are made through the MID Server using PowerShell scripts.

Microsoft SCCM integration

You can use the REST message for the Microsoft SCCM integration to retrieve information from Microsoft SCCM. Changes to the record method of the REST message impact the requests made to Microsoft SCCM to retrieve information. REST messages contain the following REST methods.

WMI Class names:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- SMS_Collection
- SMS_DeploymentSummary

Parameter name	Value	Description
url	Dynamic values based on user	Indicates the endpoint of the SCCM Console

Microsoft SCCM deploy patch

You can use the REST message for the Microsoft SCCM integration to schedule patches from your ServiceNow AI Platform® to the Microsoft SCCM. Changes to the record method of the REST message impact the requests made to SCCM to retrieve information. REST messages contain the following REST methods.

REST method	Description
POST Deploy Patch	Schedules the patch to SCCM console on single/multiple computers.

Parameter name	Value	Description
url	Dynamic values based on user	Indicates the endpoint of the SCCM Console.
title	Dynamic values based on user	Title of the deployment.
settings_tag	XML tag-named settings with values	Indicates settings that have different parameters and are sent to SCCM while scheduling the patch.
computer_tag	XML tag-named computers with values	Indicates list of computers on which the patch is going to be scheduled.
site_name	Value from patch update	Name of the site where the Patch is present.
Patch_id	Value from patch update	Id of the Patch.

Data transformation for the Patch Orchestration with Microsoft SCCM Integration

Data is retrieved from the Patch Orchestration with Microsoft SCCM Integration, processed through a set of data sources, and transformed in your ServiceNow AI Platform® instance.

SCCM Collection import

The data from the imported collections are loaded into the SCCM Collection Import [sn_vul_sccm_collection_import] table. The SCCM Collections (transform map) is used to transform the imported information.

Note: Changes to this transform map alter how data from the SCCM Collection import is processed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To access this transform map, navigate to **All** > **System Import Sets** > **Transform Maps** and locate SCCM Collection Transform. The following table lists the transform map fields by integration.

Source field	Target field	Description
u_collectionid	source_id	Unique Id of the collection.
u_name	name	Name of the collection.
u_membercount	device_count	Number of devices in this collection.
[script]	integration_instance	Name of the instance the Patch is imported from.

SCCM Collection Import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script used to initialize the values in the scope variable [sn_vul_sccm] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to update the values in the scope variable [sn_vul_sccm]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

SCCM Patch Update Import

The data from the imported Patches are loaded into SCCM Patch update Import [sn_vul_sccm_patch_update_import] table.

SCCM Patch update transform is used to transform the imported information.

Note: Changes to this transform map alter how data from the SCCM Patch update import is processed.

To access this transform map, navigate to **All** > **System Import Sets** > **Transform Maps** and locate the SCCM Patch update transform.

The following table lists the transform map fields by integration.

SCCM Patch Update Import transform map fields

Source field	Target field	Description
[Script]	urls	URLs for the Patch.
u_nummissing	num_missing	Number of devices missing this patch.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SCCM Patch Update Import transform map fields (continued)

Source field	Target field	Description
[Script]	date_release	Patch release date.
u_bulletinid	bulletin_id	Bulletin ID for the Patch.
u_numtotal	num_total	Total number of devices.
u_localizeddescription	description	Description for the Patch.
[Script]	is_highest_supersedence	Is the Patch with the highest supersedence.
u_numnotapplicable	num_not_applicable	Number of devices not applicable for this Patch.
u_iscontentprovisioned	is_downloaded	If Patch is downloaded to the SCCM Server.
u_numunknown	num_unknown	Total number of unknown devices.
u_articleid	article_id	Article ID of the Patch.
u_localizeddisplayname	title	Title of the Patch.
u_ci_id	source_id	Unique ID for the Patch in SCCM.
u_numpresent	num_present	Number of devices where the Patch is installed.
[Script]	integration_instance	Name of the instance the Patch is imported from.
[Script]	sn_vul_solution	Solution based on the source ID.
[Script]	last_modified	Patch last modified date.
u_severity	source_severity	Severity of the Patch.

SCCM Patch Update Import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_sccm] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to update the values in the scope variable [sn_vul_sccm]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SCCM Device Patch Update Import

The data from the imported relevent Patches on devices are loaded into the SCCM Device Patch Update Import [sn_vul_sccm_device_patch_import] table.

SCCM Device Patch Update Transform is used to transform the imported information.

Note: Changes to this transform map alter how data from the SCCM Device Patch Update Import is processed.

To access this transform map, navigate to **All** > **System Import Sets** > **Transform Maps** and locate the SCCM Device Patch Update Transform.

The following table lists the transform map fields by integration.

SCCM Device Patch Update Transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_sccm] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	Script that is used to Create and Update CIs based on CI Lookup Rules and patches, as well as the relationship between them. Based on the results, this script modifies the values in the scope variable [sn_vul_sccm]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

SCCM Device Collection Import

The data from the imported device collections are loaded into the SCCM Device Collection Import [sn_vul_sccm_device_collection_import] table.

The SCCM Device Collection Import Transform is used to transform the imported information.

Note: Changes to this transform map alter how data from the SCCM Device Collection Import is processed.

To access this transform map, navigate to **All** > **System Import Sets** > **Transform Maps** and locate the SCCM Device Collection Transform.

The following table lists the transform map fields by integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device Collection Import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_sccm] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to create and update CIs based on the CI Lookup Rules and collections, as well as the relationship between them. Based on the results, this script modifies values in the scope variable [sn_vul_sccm]. This script is for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

SCCM Device Collection Import transform map fields

Source field	Target field	Description
u_id	source_id	Unique Id of an action.
U_name	name	Name of the action
[Script]	Sn_vul_sccm_discovered_item	Reference of the discovered item on which the patch is deployed
U_status	status	Status of the action
[Script]	Sn_vul_patch_orch_update	Reference of the patch
U_apply_count	Count_success	Success count of action.
U_retry_count	retry	Retry count of the action.
[Script]	Deployment_time	Start time of the action.
[Script]	deadline	End time of the action.
[Script]	Source_created	Creation time of the action.
[Script]	Integration_instance	Name of the instance from which the action is imported.

SCCM Deployment Import

The data from imported deployments are loaded into the SCCM Deployment Import [sn_vul_sccm_deployment_import] table.

The SCCM Deployment Import Transform is used to transform the imported information.

Note: Changes to this transform map alter how data from the SCCM Deployment Import is processed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To access this transform map, navigate to **All** > **System Import Sets** > **Transform Maps** and locate the SCCM Deployment Transform.

SCCM Deployment Transform map fields

Source field	Target field	Description
u_id	source_id	Unique Id of a Deployment.
u_name	name	Name of the Deployment.
[Script]	deadline	Deadline time for the Deployment.
u_numberinprogress	count_progress	Count of devices in progress for the Deployment.
[Script]	deployment_time	Deployment start time.
[Script]	integration_instance	Name of the instance the Deployment is imported from.
[Script]	source_created	Creation time of the Deployment.
[Script]	sn_vul_patch_orch_update	Reference of the Patch
[Script]	sn_vul_patch_orch_collection	Reference of the discovered item the patch is deployed on.
u_softwarename	name	Name of the Deployment.
u_numberother	count_other	Other count of devices for the Deployment.
u_numberunknown	count_unknown	Unknown state count of devices for the Deployment.
u_deploymentid	source_id	Unique identifier of the Deployment.
u_numbersuccess	count_success	Success count of devices for the Deployment.
u_numbererrors	count_error	Error count of devices for the Deployment.
u_numbertargeted	count_total	Total count of the devices for the Deployment.

SCCM Deployment Import transform map script timing

Script	Description
OnStart (when an import set has created transformation).	Script that is used to initialize the values in the scope variable [sn_vul_sccm] for the integration process. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation).	The script that is used to update the values in the scope variable [sn_vul_sccm]. This script is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SCCM Deployment Import transform map script timing (continued)

Script	Description
	for internal use and should not be modified or deleted.
onComplete (when an import set has completed transformation).	Script that is used to set the number of items created, updated, and ignored. This script is for internal use and should not be modified or deleted.

Example workflow for the Vulnerability Response Patch Orchestration integration with Microsoft SCCM

An example of how patch orchestration works with Microsoft SCCM.

Before you begin

Say, for example, your entire environment is patched once every three weeks. The most recent patching window was completed a week ago, but you want to apply a patch to fix a critical vulnerability that has recently become known. Due to the critical nature of this vulnerability, you cannot wait two more weeks for the next scheduled patch.

Roles required:

- sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin for the Vulnerability Manager Workspace.
- sn_vul.remediation_owner to view the IT Remediaiton Owner workspace.
- sn_vul_patch_orch.configure_patch role to configure and schedule patches.
- sn_vul_patch_orch.read_patch to view (read only) patch information on records. This role is inherited with the sn_vul.remediation_owner and sn_vuln.vulnerability_analyst roles that are required for the IT Remediation and Vulnerability Manager Workspaces.

About this task

As a vulnerability manager or analyst working in the Vulnerability Manager Workspace, you might consider creating watch topics, or editing existing watch topics to help you capture imported VIs with critical vulnerabilities. With the patch orchestration integration, you can also see the patches you want to use to fix and track these vulnerabilities. The following table lists a few samples with the conditions you might set for watch topics for patch orchestration. Use these examples to help you determine settings that work best for your environment. See Create a watch topic in the Vulnerability Manager Workspace for more information about setting up the watch topic.

Sample watch topics for patch orchestration in the Vulnerability Manager Workspace

Watch topic name	Description
Critical Vulnerabilities with Patch Leaks	`Risk rating is 1 - critical` AND `Reason is Patch Not Scheduled`
Critical Vulnerabilities with Patches Scheduled (missing SLA)	`Reason is Patch Scheduled (Missing Target Date)`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample watch topics for patch orchestration in the Vulnerability Manager Workspace (continued)

Watch topic name	Description
Critical Vulnerabilities with Patches Scheduled	`Risk rating is 1 - critical` AND `Patch scheduled date is not empty` AND `Reason is Patch Scheduled`

- As a vulnerability manager or analyst, after you create the watch topics and remediation efforts, you generate remediation tasks. From VI records and remediation tasks, you can drill down into the Detections tab and locate discovered item records that have the vulnerability you are tracking, along with the assets imported by the SCCM product.
- As a vulnerability analyst or admin, you can monitor the patch data associated with the vulnerability. You might also deploy a patch or multiple patches to a specific asset (configuration item) from a discovered item record.

As an IT remediation specialist, you have options for how you address the vulnerability with a patch deployment.

- You can schedule the patch from a Patch Update record (VPU#).
- If vulnerable items (VI)s have preferred solutions mapped to them, and they are assigned to you or your groups, you can schedule the patches from a remediation task that has these vulnerable items.

Procedure

1. As an IT Remediation Specialist, in the IT Remediation Workspace, click the Home view.
2. From the home view, click the **Assigned remediation tasks** scorecard to view the records.

   For the sake of this example, you might check the Short description field on the remediation task (VUL#) for any text that relates to your critical vulnerability. Say, for example, you might know that your vulnerability manager has created a watch topic called, Critical vulnerabilities with Patch leaks to catch VIs (VIT#) with this critical vulnerability.

   With the record open, you can also review the VIs, the Preferred patches, and see if you or any of your group has already submitted any patch requests for approval.

3. If you have enough information, you might prefer to submit a request for a patch now from this remediation task.

   Note: If the VIs associated with the record do not have patches that are mapped to them, the **Schedule Patch** button is not available on the record.

4. Click **Schedule Patch** and fill out the fields in the dialog.
   For more information about how to schedule a patch, see Schedule patches with the Microsoft SCCM integration with Vulnerability Response.
5. Alternatively, from the List view in the IT Remediation Workspace, you can click on the Remediation tasks, Vulnerable items, Solutions, and Patches links to view these records.
   In the case of this example, instead of a watch topic name, you might know the Article ID or the Bulletin ID and title of the patch. If so, you might want to check if any of the VIs with this

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerability are assigned to you or to your groups. From Patch Update records, you can submit patch requests. From VI records, you can check for potential patches and open the associated remediation task if you want to submit a patch request.

6. If you don't have access to the workspaces, or you prefer to view data and schedule patches from the classic environment, follow these steps.

   a. Navigate to **Vulnerability Response** > **Patches** > **All**.

   b. Locate the Patch Update record you want.
   You might prefer to filter the records with `Critical` Risk Scores.

   c. Review the associated VIs and % VIs remediated fields on the Remediation Status tab.
   If the VIs have patches available, the **Schedule Patch** button is displayed in the upper right of the record.

   d. If you decide you want to submit a request, click **Schedule Patch**.
   For more information about how to schedule a patch, see Schedule patches with the Microsoft SCCM integration with Vulnerability Response.

   e. Alternatively, say you don't have the patch ID information, but you might check the Short description field on the remediation tasks that are assigned to your group for any text that relates to your critical vulnerability.

   f. Navigate to **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**.

   g. Locate the record you want and click it to open it.
   On the open record, review the Remediation Status tab for VIs and % VIs remediated. Click the Related Links for VI records, Preferred Solutions, Preferred Patches, and Patch Requests.

      Note: If the VIs associated with the record do not have patches that are mapped to them, the **Schedule Patch** button is not available on the record.

   h. Click **Schedule Patch** from the record if you want to submit a patch request.

Understanding the Qualys Vulnerability Integration

The Qualys product sensors collect the data and automatically send it to the Qualys application, which continuously analyzes and correlates the information. It easily integrates with Vulnerability Response as the Qualys Vulnerability Integration to map vulnerabilities to CIs and business services to determine impact and priority of potentially malicious threats.

Configure your Qualys Vulnerability Integration using **Vulnerability** > **Administration** > **Setup Assistant** to make data retrieval more flexible and scalable.

If you have multiple deployments of the Qualys Cloud Platform application, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from each deployment is identified and available in a single instance of Vulnerability Response. Qualys Vulnerability Integration Knowledge Base records are normalized across deployments, ensuring that instances of the same vulnerability across deployments are treated as the same vulnerability.

Note: You cannot delete the original vulnerability integration but you can disable it. Integrations created from disabled templates are disabled by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Note: While the Qualys Vulnerability Integration creates integrations for Appliance List, Asset Group, Dynamic Search List, and Static Search List, they are not required for normal operation.

Available versions

Release version for Xanadu	Release Notes
Qualys Vulnerability Integration v12.7, v12.8	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Installed components

For a current list of the roles, integration jobs, and tables that are installed with the integration, as well a link to instructions for how to view what is currently installed in your instance, see Components installed with the Qualys Vulnerability Integration.

Primary and Supporting Integrations

Qualys primary and supporting integrations enrich the vulnerability data on your instance by retrieving data from the Qualys Vulnerability Integration. A series of scheduled jobs invoke the integrations automatically. You can also execute them manually. Scheduled jobs simplify the vulnerability remediation lifecycle by keeping the instance synchronized with other vulnerability management systems. Primary and supporting integrations can be modified.

The Qualys integrations are executed as scheduled jobs. There is a configured run-as user for each integration record. The default value for this user is **VR.System**. This value should not be changed.

Note: Failing to set a valid run-as user results in multiple, often duplicate, data retrieval attachments on the data source records, every time the integration runs. Multiple attachments on the data source increase processing time, resulting in inconsistent transform results.

During import, CVE records, not already present, are created as NVD records and referenced in third-party entries for Qualys by default.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Primary integrations

A primary integration is an entry point to the Qualys Cloud Platform interacting with the Qualys API invoked on a schedule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View the primary integrations by navigating to **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.

Supporting integrations

A supporting integration is a process that is not intended to run on a schedule nor without invocation by a primary integration.

View the supporting integrations by navigating to **Qualys Vulnerability Integration** > **Administration** > **Supporting Integrations**.

Service Graph Connector for Qualys

Beginning with version 2.2, the Service Graph Connector for Qualys is available from the ServiceNow® Store. See Service Graph Connector for Qualys for more information.

Data from the Qualys data source fields is imported with the Global Asset API and the Asset Management and Tagging API.

Global Asset API:

- A CSAM license is required.
- Asset information includes details such as Hardware Category and OS Category.

Asset Management and Tagging API:

- A CSAM license is not required
- Asset information does not include details about Hardware Category and OS Category.

For more information, see Service Graph Connector for Qualys APIs

.

Create CIs using the Identification and Reconciliation Engine (IRE)

You can use the Identification and Reconciliation Engine to create new CIs when an existing CI cannot be matched with a host imported from a third-party scanner. Enable the CMDB CI Class Models plugin to create CIs using the new classes, otherwise unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. For more information on how to configure the categorization of unmatched cloud resources into your preferred CI class, see Updating CI class for unmatched cloud assets.

Search lists

Search lists are used in Qualys to create custom groups of vulnerabilities. You can save them and use for ticket creation and to customize vulnerability scans and reports. The Search Lists module allows you to download search list data from Qualys to your instance on a scheduled basis.

Search lists are pulled from Qualys using the Dynamic Search List Import and/or Static Search List Import data transformation maps. In each of these transforms, you can define schedules for performing the import.

Option profiles

Option profiles are available with Qualys scan settings. An option profile is required when you initiate a scan from your ServiceNow AI Platform.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option profiles are imported from the Qualys product by the Option Profile List Integration. You might prefer to run the Option Profile List Integration after an import from the Search Lists Integrations, the Qualys Dynamic Search List and Qualys Static Search List Integrations so that you can see which search lists are associated with option profiles.

Asset groups

Asset groups are setup in the Qualys platform. Asset groups identify which scanner appliances are used for scanning matching IP addresses when a scan is initiated from the ServiceNow AI Platform.

Asset groups that have associated appliances are pulled from Qualys by the Asset Group List Integration.

Initiate the Appliance List Integration after you import asset groups to populate the Appliance name and Appliance status fields on the Qualys Default Applications records in your ServiceNow AI Platform.

Host tags

All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Vulnerability Group Rules. They are displayed in the Discovered Item form.

Note: The Qualys Host List integration should be run prior to creating Assignment or Remediation Task Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case sensitive. If a **San Diego** tag is created, then a **SAN DIEGO** tag cannot be stored in the Host tag table. 'San Diego' and 'SAN DIEGO' are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Remediation Task Rule can have unexpected results. Host tags are intended for use only in the Condition builder.
- Host tags are controlled by the global system property **sn_vul.import_host_tags**. This property is set to true by default. Turning tags off turns them off across all instances.

Host tags (also called asset tags) are used for organizing and tracking the assets in your organization. You can assign tags to your host assets. Then, when launching scans, you can select tags associated with the hosts you want to scan. The Host Tags module allows you to download host tag data from Qualys to your instance on a scheduled basis.

Reopen resolved vulnerable items not closed by scans

Vulnerable items set to 'Resolved' in your ServiceNow AI Platform instance but not transitioned to 'Closed/Fixed' by the third-party integration runs are reopened if they are detected during rescans.

For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- Name: severities
- Value: 3-5 (or whatever appropriate severities are desired)

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Related topics

Qualys REST messages

Preparing for the Qualys Vulnerability Integration

A successful integration requires planning and careful execution of pre-integration tasks. It is essential that you prepare for the integration by performing these procedures. The Qualys Vulnerability Integration assumes that you are familiar with and run Qualys Cloud Platform scans in your environment.

Note: Make any necessary configuration changes based on your requirements before running the integrations.

Important prerequisites

Validate your instance sizing based on the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

Use filtering to limit the number of items for initial import and phase your deployment by adjusting filters in subsequent imports.

The Qualys scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button is not available.

Actions to take

- Determine an initial start date for **Host Detection List Import** integrations.

  Consider setting the **Start time** field to a few hours or days in the past. Ideally, choose the date of the last Qualys scan. The start date can include vulnerabilities discovered prior to using the vulnerability management solution. Set the earliest start time used to the start of your scanning cycle. So, if it takes a week before all hosts are scanned, set this value to a week prior to that time.

- Add users to the roles for admin, sn_vuln.admin, and sn_vul_qualys.admin. For more information see, Assign a role to a user.

- There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If you do not use vulnerability calculators, Disable the default vulnerability calculator if not used, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.
- During the initial import of records, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, disable the business rules.
- If you wish to use a different scanner than the Qualys default, see set up scanner appliances.
- Have your Qualys server URL and authentication credentials ready. The credentials must provide adequate permissions for retrieving knowledge, scan, and detection information for a Qualys subscription.
- If you plan to use host tags in Vulnerability Response Assignment or Vulnerability Group Rules, ensure the Qualys Host List integration was run prior to creating rules.

Install the Qualys Vulnerability Integration

Before you run the Qualys Vulnerability Integration in your instance, you must install and configure the Qualys Vulnerability Integration application. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin to download and install the application

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that it is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.
Get entitlements for the Qualys Vulnerability Integration application and download it to your ServiceNow AI Platform® instance.	If the application is not already downloaded on your instance, see .
Prepare for the integration.	See Preparing for the Qualys Vulnerability Integration.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant**.

   After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the Qualys Vulnerability Integration tile and click **Install**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Follow the prompts in the Setup Assistant.
   For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.
4. Navigate to **Integration Configuration>Scanner Integrations** in Setup Assistant to continue with the configuration.
   For more information on supplement the prompts provided in Setup Assistant, see Configure the Qualys Vulnerability Integration using Setup Assistant.

What to do next

Activate the scanners as the scanners are inactive by default in the Vulnerability Response application. For more information on how to activate the Qualys scanners, see Activate the Qualys scanners.

Activate the Qualys scanners

You must activate the scanners after installing the Qualys Vulnerability Integration because the scanners are deactivated by default in the Vulnerability Response application.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button isn't available.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Locate the scanner product that you want to activate and select the record to open it.
3. Select the **Active** check box.
4. Select **Update**.
5. The product you activated is displayed in the **Source** field on a vulnerable item and remediation task records after the next import, and **Rescan** is available as a UI action.

Components installed with the Qualys Vulnerability Integration

The following roles, integration jobs, and tables are installed with the Qualys Vulnerability Integration.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

View filtered lists for components installed with an application

Filter the Applications Files table so that only the roles, scheduled jobs, and tables that are installed with an application are displayed. The application you want to view these components for should be installed so that its files are loaded onto the instance and into the metadata table. Follow these steps to view filtered lists from the Applications Files table.

1. In the filter navigator, enter **sys_metadata.list** to navigate to the metadata table.
2. Select the condition builder (filter icon), and select, **Application** > **is** followed by the name of your application. For example, **Application** > **is** > **Vulnerability Response**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In the condition builder, to add a second filter, select **AND**, then select, **Class** > **is a** and choose one of the following classes from the list: **Role**, **Scheduled job**, or **Table**.
4. Select **Run**.

The results for the class you selected are displayed in a filtered list.

Roles installed

Role title [name]	Description	Contains roles
sn_vul_qualys.read	Has read access to the Qualys Vulnerability Integration records.	
sn_vul_qualys.user	User for Qualys Vulnerability Integration. Can read and write records	sn_vul_qualys.read
sn_vul_qualys.admin	Administrator forQualys Vulnerability Integration. For example, you can modify integration start dates and perform some advanced configuration settings.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Can configure the Qualys Vulnerability Integration	sn_vul_qualys.admin

Integration jobs installed

Integration job	Description
Qualys Static Search List Integration	Synchronizes Qualys search lists for finding vulnerable entries. Retrieves only static list type records.
Qualys Comprehensive Host Detection Integration	Retrieves host and vulnerability data from Qualys and processes it in your instance. It coordinates the REST message calls to the Host Detection API. The output of this integration is vulnerable items. This integration imports all the states of the vulnerability: New,Fixed, Active, and Reopened. By default, this integration is inactive and runs weekly. **Note:** After this integration is activated, the daily comprehensive job imports only the New, Fixed, and Reopened states.
Qualys Host List Integration	Retrieves authenticated and unauthenticated host scan data and host tags from Qualys once a week and stores it in the Discovered

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration job	Description
	Items module in your instance. Helps identify assets that haven't been scanned recently.
Qualys Host Detection Integration	Retrieves host and vulnerability data from Qualys and processes it in your instance. It coordinates the REST message calls to the Host List Detection API. The outputs of this integration are vulnerable items. Qualys host tags are imported in this integration.
Qualys Ticket Integration	Retrieves Qualys tickets and adds them to your instance. It coordinates the REST message calls to the ticket list API. There are often fewer tickets than Host Detections since Qualys settings can constrain the detections that result in a ticket.
Qualys Option Profile List Integration	Retrieves option profiles from the Qualys product. Option profiles include scan settings which are required when you initiate scans from your ServiceNow AI Platform instance.
Qualys Appliance List Integration	Retrieves scanner appliance information from Qualys.
Qualys Asset Group Integration	Retrieves asset group information from Qualys. Asset groups are used to identify which scanner appliances to use for scanning matching configuration items.
Qualys Knowledge Base (Backfill)	Retrieves Qualys knowledge base entries. Scheduled to run after the Qualys Knowledge Base Integration. Updates your instance with any QIDs that were referenced in the Qualys Knowledge Base or Qualys Host Detection integration but did not exist in the system.
Qualys Knowledge Base	Retrieves Qualys knowledge base entries. The retrieved data is based on the date the vulnerabilities were updated by Qualys and since the last time the integration ran. This data is useful for populating historical data into your instance as well as ensuring the Qualys Identifiers (QIDs) are up to date.
Qualys Dynamic Search List Integration	Synchronizes Qualys search lists for finding vulnerable entries, and retrieves dynamic list type records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration job	Description
Fixing the detections for updated key for Qualys	A hashed combination of fields that provided a way to identify and tie a detection to a Qualys vulnerable item.
Qualys Update existing discovered items with network partition identifier	Updates your existing discovered items. CIs for your existing Qualys Vulnerability Integration data are created or updated to include the network partition identifier granularity.

Tables installed

Table	Description
Search List Vulnerability sn_vul_qualys_m2m_search_list_vul	Stores the mapping between the Qualys search list and a vulnerability.
Qualys Vulnerability Scanner sn_vul_qualys_scanner	Table that extends Vulnerability Scanners to store scanner information for the Qualys rescan feature.
Qualys Search Lists sn_vul_qualys_search_list	Stores search lists retrieved by the Qualys search list integration.
Qualys Appliance Import sn_vul_qualys_appliance_imp	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script.
Qualys CI sn_vul_qualys_ci	Table no longer used.
Host Detection Pagination sn_vul_qualys_host_detection_pagination	Table no longer used.
Qualys Integration Run sn_vul_qualys_integration_run	Table no longer used.
Qualys Integration sn_vul_qualys_integration	Table extending the vulnerability integration and stores all the integrations that correspond to Qualys.
Qualys Static Search List Import sn_vul_qualys_static_search_list_imp	Table extending the import set row. Field maps are used to transform data to the target table, Qualys Search Lists.
Qualys Knowledge Base sn_vul_qualys_knowledge_base	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Qualys Ticket List sn_vul_qualys_ticket_list_imp	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script.
Qualys Option Profile sn_vul_qualys_option_profile	Table storing the option profiles retrived from Qualys. This table used with the rescan.
Qualys Dynamic Search List Import sn_vul_qualys_dynamic_search_list_imp	Table extending the import set row. Field maps are used to transform data to the target table, Qualys Search Lists.
Qualys Import Set Re-Run sn_vul_qualys_import_rerun	Table no longer used.
Qualys Option Profile Import sn_vul_qualys_option_profile_import	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script.

Update configuration items with the network partition identifier for the Qualys Vulnerability Integration

Create unique configuration items (CIs) for assets in your environment that share IP addresses. Identify the distinct assets across your environment and automatically update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.

Before you begin

Role required: admin

About this task

By default, in the Vulnerability Response application, one way to identify your assets is by IP address. In certain cases, assets can share IP addresses, but they are stored as one CI in your CMDB.

For example, as shown in the following tables, multiple assets (CI)s in your environment can share IP addresses but have unique network and repository ids. However, by default, these assets are typically identified and stored as a single CI `(CI 1)` during the IP address lookup.

Default IP lookup and CI creation

Source	IP address	NETWORK_ID	Configuration item
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source	IP address	REPOSITORY_ID	Configuration item
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

You can create individual CIs for assets that have the same IP address so that you can identify them as distinct assets. Starting from a fresh data import, you can update your existing CIs with more granularity that includes the network partition identifier [network_partition_identifier] by running the scheduled job, *Update existing discovered items with network partition identifier*.

This scheduled job is deactivated by default. Activate this feature for the Assets and Fixed and Open Vulnerabilities Integrations for Qualys Vulnerability Integration in the Setup Assistant to view this identifier on your records.

When activated, this scheduled job adds the Network Partition Identifier [network_partition_identifier] to existing CI records from imported data. Existing CIs created by the IRE are also updated. The scheduled job also creates CIs that include the network partition identifier starting with the next import. Alternatively, you can launch the job on-demand to update your existing data.

Starting with v14.0 of Vulnerability Response and v12.1 of the Qualys Vulnerability Integration Vulnerability Integration, the CMDB CI Class Models (1.0.21.) is supported. The class models have the network partition identifier [network_partition_identifier] in the Identification and Reconciliation (IRE) identification rules.

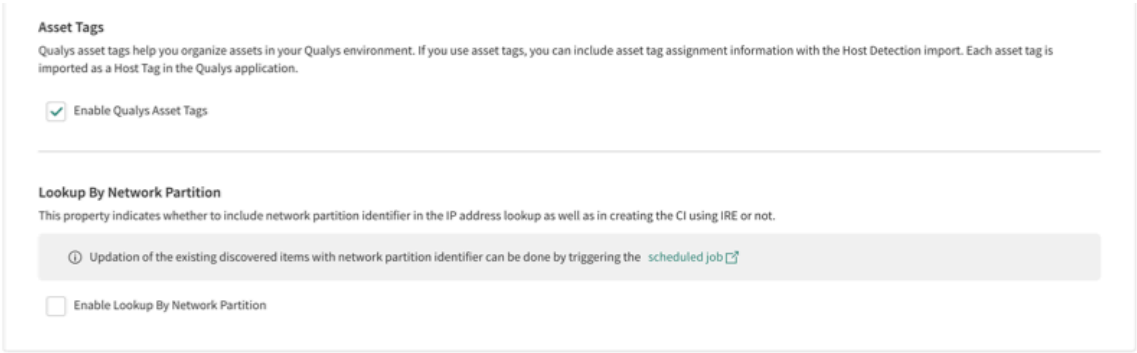
Option	Description
Run the scheduled jobs on-demand.	Update your existing discovered items. CIs for your existing Qualys Vulnerability Integration data are created or updated to include the network partition identifier granularity. Discovered items, vulnerable items, and detection records are all updated with the new CIs.
Wait for imports of fresh data from the integrations with the next scheduled jobs.	Create CIs for each new asset using the network partition identifier starting with the next scheduled job. CI, vulnerable item, and detection records are all updated to include the new granularity. New CIs are created when an exact match is not found.

Procedure

1. Navigate to **Vulnerability Response** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.
2. Choose Qualys Vulnerability Integration.
3. **Edit** the required integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Choose **Host Detection Configuration**.
5. Choose **Enable Lookup By Network Partition** check box from the **Lookup By Network Partition**



section.

6. Click **Finish**.

Network partition identifiers NETWORK_ID and REPOSITORY _ID included in IP lookup and CI creation

Source	IP address	NETWORK_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Qualys: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

The IP Address and Incomplete IP Address CI identification lookup rules include the network partition identifier attribute automatically for a data import from the Assets and Fixed and Open Vulnerabilities Integrations for Qualys Vulnerability Integration.

After you activate the scheduled job and save the records, you alternatively can update your existing discovered items with CIs that include the network partition identifier by launching scheduled jobs on-demand. The CIs on your existing discovered item, vulnerable item, and detection records are automatically updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Optional Qualys modifications

Configure optional modifications and streamline some of the data specifically for the Qualys integration.

You can reset that start date in Setup Assistant or from the primary integration, or modify business rules to disable them during an initial import.

Disable notification-related business rules prior to initial record import

During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

Before you begin
Role required: admin

Procedure

1. Navigate to**All** > **System Definition** > **Business Rules**.
2. Search for **Affected ci notifications**.
3. Open the business rule and insert this condition: `current.sys_class_name != “sn_vul_vulnerable_item"`.
4. Click **Update**.
5. Repeat this procedure for the following business rules:
   - Affected cost center notifications
   - Affected group notifications
   - Affected location notifications

> **Note:** After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

Modify an initial start date

During installation using Setup Assistant, you set an initial start date for the Qualys integrations. You can reset that start date in Setup Assistant or from the primary integration as shown below.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.
2. Click **Qualys Host Detection Integration**.
3. Click **Integration Details**.
4. Set the **Start time** field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.

   If you configured Qualys using Setup Assistant, the **Start time** field is pre-filled, initially to three months prior today's date, and subsequently to today's date.

   Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Qualys API rate limitations, as well as triggering execution timeouts.

5. Click **Submit** or **Update**.
6. **Optional:** Click **Execute Now** to run immediately.

Advanced Qualys configurations and modifications

Configure advanced optional modifications and streamline some of the data specifically for the Qualys integration. Most of these modifications require coding or advanced ServiceNow or Qualys Cloud Platform expertise.

For more tips for Qualys imports, see the Performance tuning tips for Qualys import jobs knowledge article in the HI Knowledge Base.

Modify the Qualys to ServiceNow priority and state mapping values

Modify mapping values for priority and state for your requirements.

Before you begin
Role required: admin

About this task
This is an advanced customization option.

Procedure

1. Navigate to **All** > **System Definition** > **Business Rules**.
2. Search for **Map Qualys Values** and open it.
3. Click the **Advanced** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Modify per your requirements.
   The most common modifications include adding new state values or revising criticality or priority.
5. Click **Update**.

Restrict the ability to write to a record based on an assignment group

You can restrict write/read rights on records based on membership to an assigned group. Modify conditions and script based on specific requirements.

Before you begin

Role required: security_admin (elevated role from admin)

Note: This action is performed in the Vulnerability scope.

Procedure

1. Navigate to **All** > **System Security** > **Access Control (ACL)**.
2. Search for ACLs that start with `sn_vul`.
3. Choose an Access Control record, for example, `sn_vul_vulnerable_item`, **Operation write**.
4. Check the **Advanced** box in the record, if necessary, to display the **Role** entries.
5. Modify the **Role** script for your requirements.
   Script Example of modifying access by group.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Click **Update**.

Set up scanner appliances

If you are initiating scans from your ServiceNow AI Platform® instead of directly from Qualys, you can set up scans for IP address ranges.

Before you begin

The data comes from the Qualys integration based on Qualys asset groups and their related default appliances (scanners).

If no appliances are configured for the targeted IP address ranges, the appliance that is set as the default for the integration instance is used for the scan.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: sn_vul_qualys.admin

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Scanner Appliances**.
2. Fill in the fields on the form, as appropriate.

Field	Description
Appliance name	You are prompted to fill in this field when you create a record manually. Enter the name for the Qualys scanner appliance to be used for invoking scans for matching configuration items. Use the `External` value when you want the scan to be launched with an external scanner.
Appliance ID	Enter the appliance identifier for the Qualys scanner appliance to be used for invoking scans for matching configuration items. You are prompted to fill in this field when you create a record manually. Use the `0` value when you want the scan to be launched with an external scanner.
Appliance status	Displays the last status of the scanner appliance on the data returned by the Qualys integration. For manually created records, the status is updated only if a valid **Appliance ID** is specified.
Asset group ID	Displays the Qualys asset group identifier that created this record. This field displays a value only for records created by the Qualys integration.
Asset group name	Displays the Qualys asset group name that created this record. This field displays a value only for records created by the Qualys integration.
Order	Enter a value to be used for determining scanning priority. For appliance that have conflicting criteria, an appliance with a lower order value is given a higher priority.
Manually created	Indicates whether this record was created manually by the user.
Use filter group	Select this check box to specify a filter group for finding matching configuration items for scanning.
Filter group	Select the filter group you want to use for finding matching configuration items for scanning. This field appears only if you selected **Use filter group**.
IPs	A comma-separated list of IP addresses or ranges of IP addresses to be used by this appliance when invoking scans.
Integration instance	The Qualys integration instance associated with this appliance.
Option profile	Select the option profile you want to use for scans for matching configuration items.

3. Click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure and manage Qualys vulnerability scanners and scans

Qualys vulnerability scans can be performed to find software vulnerabilities that affect your CIs. You can initiate scans from a vulnerable item record or by creating a scan record directly for configuration items (CIs) and IP addresses.

If you scan Qualys vulnerable items directly from the Vulnerable Items screen, you also have the option of scanning multiple vulnerable items at the same time.

If Security Incident Response is activated, you can also initiate a scan from the security incident catalog, a security incident record, or a security scan request.

Scans submitted from Qualys vulnerable items, the Security Incident Catalog, security incidents, or security scan requests are performed by the default Qualys scanner.

You can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your ServiceNow AI Platform®.

Configure the ServiceNow-initiated Qualys IP scan

The Qualys scanner included with the base system provides a baseline integration to initiate scans based on IP addresses.

Before you begin

You can select the option profile you want to use for scans for matching configuration items.

- Option profiles contain Qualys scan settings.
- An option profile is required when you initiate a Qualys scan from your ServiceNow AI Platform®.

Role required: sn_vul_qualys.admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Open the Qualys record.
3. Select the**Active** and **Default** check boxes.

   Selecting **Active** is required to use the Qualys scanner to scan Qualys VIs automatically. You also don't need to select **Default** to have it run automatically.

   Prior to v12.0, **Active** is required to use the scanner. If **Default** is also selected, the scanner is automatically used without having to be selected during scanning.
4. For the Source integration field, click the search icon and select the option for **Qualys**, for example, **Qualys Cloud Platform**.
5. Click **Update**.
6. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Open the **Qualys Asset Group List Integration**.
   a. Select the **Active** check box.
   b. Click **Execute Now**.
8. Follow these steps to populate your scanner appliances.

   Note: You might prefer to run the Option Profile List Integration after an import from the Search Lists Integrations, the Qualys Dynamic Search List, and Qualys Static Search List Integrations, so that you can see which search lists are associated with option profiles.

   a. Open the **Qualys Option Profile List Integration**.
   b. Select the **Active** check box.
   c. Click **Execute Now**.
   d. Follow the steps listed in Set up scanner appliances to configure your scanner appliances. Return here after you complete those steps to continue with the configuration.
   e. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.
   f. Open the **Qualys Appliance List Integration**.
   g. Select the **Active** check box.
   h. Click **Execute Now**.
   Your Qualys scanner appliances are now correctly populated.

Related topics

Understanding the Qualys Vulnerability Integration

Scan multiple Qualys vulnerabilities or vulnerable items

You can simultaneously scan multiple Qualys vulnerabilities or vulnerable items that contain at least one affected configuration item (CI) or an IP address populated on the form.

Before you begin

Role required: sn_vul.vulnerability_write

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Do one of the following:
   - Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
   - Navigate to **All** > **Vulnerability Response** > **All Vulnerable Items**.
2. Select the check boxes for the records you want to scan.
3. Click the **Actions on selected rows** list, and click **Re-scan for Vulnerable items**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A message appears with a link to the scan and the work notes are updated.

4. Click the link to see the progress or results of the scan.

Configure the Qualys auto scan for resolved remediation tasks

You can schedule the scan that runs automatically to update your Qualys vulnerable items.

Before you begin

After a remediation task is transitioned to **Resolved**, a scan is initiated automatically to update the state of the associated vulnerable items.

- The scan is disabled by default.
- Enable the scan with the **scan_on_resolved** integration instance parameter in the **Qualys** record located at **All** > **Qualys Vulnerability Integration** > **Integration Instances** > **Qualys**. See the following steps for more information.
- This scan is instance-specific. If you have multiple instances and you want to enable or disable this scan, you must disable the **scan_on_resolved** parameter in the integration instance parameters in each instance you want changed.
- When the scan is enabled, you can initiate the scan on-demand, or you can schedule the scan to run only within a specified time window. See Configure Qualys rescans to run only within scheduled intervals for how to set the start and end times for the time window.

Role required: sn_vul_qualys.admin

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Integration Instances**.
2. Select **Qualys** to open the record.
   The Integration Instance Parameters for Qualys are displayed on a tab.
3. To enable the auto scan, locate the *scan_on_resolved* parameter.
4. In the Value column for the property, enter `true`.
5. Click **Update**.

Configure Qualys rescans to run only within scheduled intervals

For the Qualys Vulnerability Integration, set the scan start and end time parameters so that rescans run, or are available, only during the hours that you want.

Before you begin

This configuration applies to both scheduled rescans and the rescans you initiate manually in the Qualys product from your ServiceNow AI Platform® instance.

Setting the scan start and end time parameters for integration instances permits you to specify time windows when rescans in the Qualys product are available. For example, you might prefer to specify that rescans are only available during off-hours, for example, midnight to 10 AM.

This setting is instance-specific. If you have multiple instances, you must configure the scan_start_time and scan_end_time values in the integration instance parameters in each instance you want to change.

Role required: sn_vul_qualys.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Integration Instances** > **Qualys**.
2. Click **Qualys** to open the record.
   The integration instance parameters for Qualys are displayed.
3. For the scan_start_time parameter, in the Value column, enter the time in the UTC time zone in 24 hour format (00:00 through 24:00) for the start time of the window that you want rescans available.
4. For the scan_end_time, in the Value column, enter times in the same format (00:00 through 24:00) for the end time of the available window.
   For example, if you enter a start time of 00:00 for the scan_start_time parameter, and an scan_end_time of 10:00 AM that same morning, scans scheduled or manually launched outside of the midnight to 10 AM time window are queued and launched at the start time of the following day's time window, 00:00.

   In the same example, if a remediation owner manually initiates a rescan at 11:00 AM, the rescan is not immediately launched, because it lies outside of the available configured scan times. The scan request remains queued until the start of the following day's time window, in this example, (00:00).
5. Click **Update** to save your settings.

Qualys vulnerability scan rate limits

You can define the rate that different types of scans are performed to limit the number of requests that are sent to an external scanner. After you have defined rate limits, you can apply them to the Qualys scanners.

Define Qualys scan rate limits

You can define the rate that different types of scans are performed to balance the load in your scan queue. Conditions defined in the rate limit determine whether the rate limits are applied to queued entries.

Before you begin

Role required: sn_vul.admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Rate Limit Definitions**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Rate limit definition

Field	Description
Name	Provide a descriptive name that identifies the conditions the queue entry must meet. For example, scans per minute

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Queue conditions	Enter conditions used to determine whether a queued scan entry is subject to this rate limit. The conditions should not be specific to a particular scanner.
Evaluation script	Write a script with the logic to evaluate the queued entry. It is important that the script return true/false to define whether the entry is processed. Also, base the evaluation script on the queued entry being evaluated.

4. Click **Submit**.

Apply scan rate limits to Qualys scanners

After you have defined scan rate limits using **Rate Limit Definitions**, you can apply rate limits to specific Qualys scanners.

Before you begin

Role required: sn.vul_admin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanner Rate Limits**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Scanner rate limit

Field	Description
Scanner	Select the scanner to which you want to apply a rate limit.
Rate limit	Select the rate limit you want to apply to this scanner.
Threshold	Enter the threshold that you want to subject the selected scanner to for the selected rate limit. For example, if the scanner allows 4 scans per minute, and the rate limit is defined as requests per minute, the threshold would be 4.

4. Click **Submit**.

View the Qualys vulnerability scan queue

Vulnerability scan requests submitted to Qualys vulnerability scanning integration are queued so as not to overload system resources. You can view the status of queued requests, as needed.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task
In the list of queued scans, each scan includes an automatically generated scan name that identifies the CI that was scanned.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scan Queue**.
   All Qualys scan requests that have been submitted are shown in a list. The **State** column shows the current state of each queued entry. A state of **Complete** indicates that the scan has left the queue. It does not necessarily indicate that the scan has completed processing. When the scans have been completed or if they failed, the **Processing** column shows the appropriate work notes text.

   Note: If a hash value was submitted for scanning and the scanner fails to find a result, the **State** shows **Complete** and the work note in the **Processing** column indicates **Unknown**.

2. After a scan has finished processing, click a queued record to view details for the scan request.

Enable base system filter for confirmed detection imports

Enable a default filter using integration parameters to import only confirmed detections from Qualys Cloud Platform.

Before you begin
Role required: sn_vul_qualys.admin, sn_vul.vr_import_admin

About this task
A base system integration instance parameter “include_only_confirmed” is available to import a filtered list of detections from Qualys Cloud Platform. By default, this parameter is set to *FALSE*, and all detections whether potential, confirmed, or informational are imported.

Procedure
1. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Integration Instances**.
2. Open the Qualys Cloud platform integration from the Integration instances list.
3. From the Integration Instance Parameters list, open the '*include_only_confirmed*' parameter.
4. Update the default value to *True*.
5. Click **Update**.
   You have enabled the filter to import confirmed detections from the Qualys Cloud Platform integration.

Result
By default, only confirmed detections from the Qualys Cloud Platform integration are imported when the next Qualys Vulnerability Import runs. All other detections such as informational and potential are ignored and not imported. For more information, see View Vulnerability Response vulnerable item detection data.

Initiate rescan for the Qualys Vulnerability Integration

Verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Qualys product from your ServiceNow AI Platform on-demand.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

You can initiate rescans from the Vulnerability Response workspaces. For more information, see Rescan records and remediation tasks in the Vulnerability Manager Workspace and Rescan vulnerable items and remediation tasks in the IT Remediation Workspace.

For rescans in the classic environment, see the following sections for how to initiate rescans.

Required setup for rescans in the Qualys product initiated from your ServiceNow AI Platform:

You can initiate a rescan on-demand for vulnerable items for the Qualys product from your ServiceNow AI Platform® instance.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans in the Qualys product from vulnerable item (VI), remediation tasks (RT), third-party entry (TPE), or discovered item records from your ServiceNow AI Platform instance.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

Use case:

As an example, say your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Qualys vulnerable items.

You can initiate rescans for VIs that have Qualys as the source in states other than closed. See Rescan records and remediation tasks in the Vulnerability Manager Workspace and Rescan vulnerable items and remediation tasks in the IT Remediation Workspace.

Verify you have completed the following setup required for rescans. See the steps starting with Configure and manage Qualys vulnerability scanners and scans listed in the previous sections for more information.

Role required: sn_vul_manually_initiate_rescan

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: You can only initiate rescans for VIs with Qualys as the source. Verify Qualys is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the**Personalize List** icon (Gear icon) and use the Slushbucket to move **Source** from **Available** to **Selected**.

3. Alternatively, navigate to **All** > **Vulnerability Response** > **Remediation Tasks**, **Vulnerability Response** > **Libraries** > **Third-Party**, or to **Discovered items** for the remediation task, third-party entry, or discovered items records, respectively, that you want to use for the rescan.

   Depending on your choice, the **Rescan** button is available on the following records:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- On a single VI record, the VI must be from the Qualys product and in any state other than **Closed**. For multiple VI records, all the VIs must have Qualys as the source and in any state other than **Closed**.
- On an RT record, the remediation task can be in any state other than **Closed**, and all the associated VIs must have Qualys as the source.
- On a third-party entry (TPE) record, the record must have at least one associated VI record in any state other than **Closed** with Qualys as the source.
- On a discovered item record, the configuration item has at least one associated VI with Qualys as the source in any state other than **Closed**.

4. In the upper right of the record you chose, click **Rescan**.
In the dialog that is displayed, choose one to continue.

Option	Description
Select the **Specify option profiles** check box.	From the list, choose the option profile for the Qualys scanner you want to use for the rescan. These are the appliances (scanners) you have configured and listed at **Qualys Vulnerability Integration** > **Scanner Appliances**.
Clear the **Specify option profiles** check box (not selected).	The Qualys option profile for the scanner you have set as your default scanner on the Scanner Appliances list is used for the scan. For more information about setting the default scanners you initiate from your ServiceNow AI Platform, Setup scanner appliances listed in the previous section for more information.

5. Click **Request Scan**.

A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, RT, TPE, and discovered item records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

Your instance tracks the rescan status until it successfully completes, or until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform stopped tracking your rescan status, not when the actual rescan stopped.

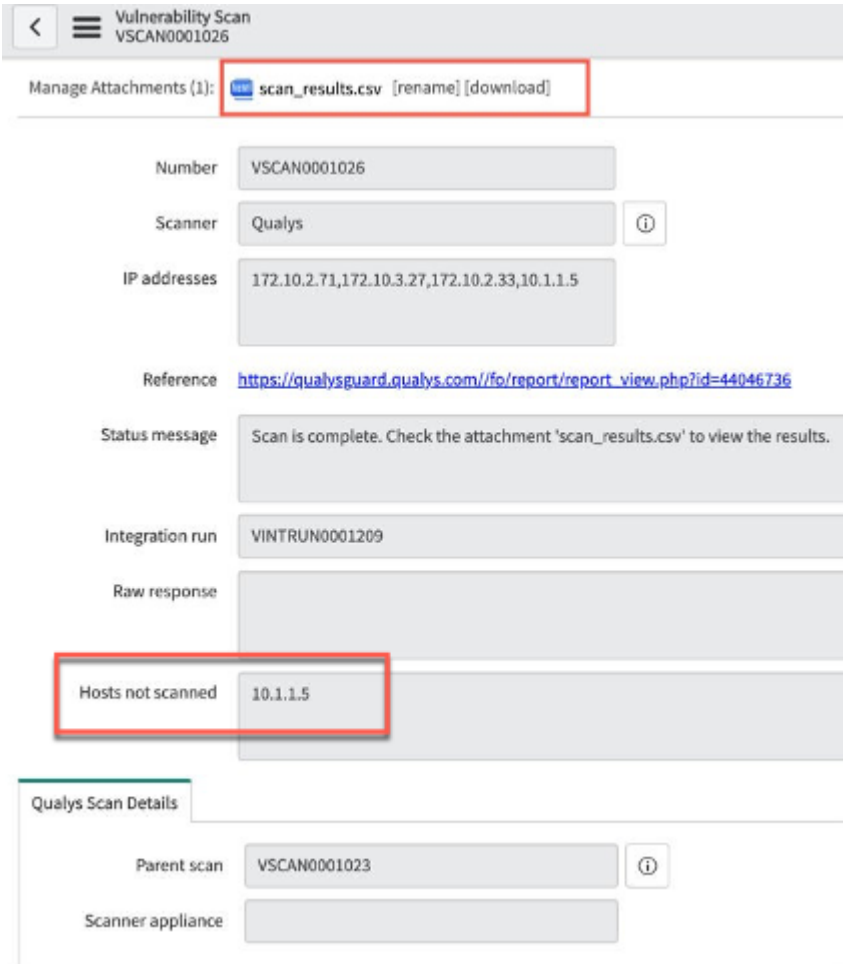
After the rescan is successfully completed, the Qualys Host Detection Integration is automatically initiated to update your vulnerable items. Depending on how many VIs you have, your detections, VIs and RTs are updated after the completion of the Qualys Host Detection Integration scan. Navigate to these records to view the updates after the Host Detection Integration is completed.

This scan is instance-specific and can be disabled. For more information about the Qualys integrations and how to view the integrations, see Understanding the Qualys Vulnerability Integration.

What to do next

You can view a .csv attachment on the scan record to see details about the rescans.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



As shown in the previous image, during the rescan, if hosts (configuration items) in your environment are not accessible, any detections and VIs associated with these assets are not updated when the rescan is completed. To help you understand why they are not included, after the rescan is completed, the asset IP addresses for these CIs are listed on Vulnerability records in the Hosts not scanned field.

Qualys metadata for vulnerabilities

The Qualys Host Detection Integration is enhanced to include more fields from Qualys. These fields help in filtering the non-exploitable Linux vulnerabilities. This enhancement improves the integration at the detection level and at the vulnerable item (VI) level.

Import additional metadata from Qualys

Import additional metadata for vulnerability items (VI) to filter vulnerabilities based on the impact on a kernel or service.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant**.
2. Under Integration Configuration, click **Scanner Integrations**.
3. Under Installed Application, click **Edit** for the Qualys application.
4. Click **Host Detection Configuration**.
5. Navigate to **Import Additional Metadata for Detections**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To import additional metadata from Qualys, manually select any of the following check boxes that you need.
   - **Kernel Metadata**: Identifies vulnerabilities found on running or non-running Linux kernels.

     If the value of the returned metadata is **No**, it means the vulnerability is not exploitable due to a non-running kernel. For information on the retrieved values, see Qualys metadata values for vulnerabilities.
   - **Service Metadata**: Identifies vulnerabilities found on running or non-running ports or services.
   - **Exploitable Configuration Metadata**: Identifies vulnerabilities that may or may not be exploitable due to the current host configuration.

   Note: By default, these check boxes are not selected.

7. Run the Qualys Host Detection Integration with a backdate.
   For more information on how to set the start date, see Optional Qualys modifications.

Result
The metadata has been imported.

What to do next
To view the imported metadata, enter `sn_vul_detection.list` in the Filter Navigation. The Vulnerable Item Detections list is displayed. For more information on the values displayed in the newly added columns, refer to Qualys metadata values for vulnerabilities.

Qualys metadata values for vulnerabilities

When the kernel metadata, service metadata, and configuration metadata are imported, some values are also retrieved. The values **0**, **1** and **Not available** are processed in the back-end and converted to **No**, **Yes** and **Empty** respectively.

These values are populated in the following columns in the Vulnerability Item Detections and Vulnerability Items list:

- Affects running service column
- Affects exploitable config column
- Affects running kernel columns

Note:

- These columns are not visible by default. For more information on how to configure the form layout, see Configure the form layout
- For older detections, the values for these columns may be empty. To update the data, run a back dated Qualys Host Detection Integration. For more information on how to set the start date, see Optional Qualys modifications.

The following table shows the retrieved values and their significance.

Field values retrieved and their significance

Field	Value	Significance
AFFECT_RUNNING_KERNEL	0	Vulnerability is found on a non-running kernel. The vulnerability is not exploitable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field values retrieved and their significance (continued)

Field	Value	Significance
AFFECT_RUNNING_KERNEL	1	Vulnerability is found on a running kernel. The vulnerability is exploitable.
AFFECT_RUNNING_KERNEL	Not Available	Vulnerability is not a kernel-related vulnerability.
AFFECT_RUNNING_SERVICE	0	Vulnerability is found on non-running ports or services. The vulnerability is not exploitable.
AFFECT_RUNNING_SERVICE	1	Vulnerability is found on running ports or services. The vulnerability is exploitable.
AFFECT_RUNNING_SERVICE	Not Available	Vulnerability is not a related vulnerability.
AFFECT_EXPLOITABLE_CONFIG	1	Vulnerability is not-exploitable due to host configuration.
AFFECT_EXPLOITABLE_CONFIG	0	Vulnerability is exploitable due to host configuration.
AFFECT_EXPLOITABLE_CONFIG	Not Available	Vulnerability is not a related vulnerability.

Set additional filter parameters for Qualys imports

Customize the filtering parameters for your scheduled queries with the Qualys Vulnerability Integration to help you further refine the vulnerability data you import with the supported Qualys integrations.

Before you begin

Use cases: As a vulnerability manager or analyst, you might want to filter out data from your queries so that you can review only specific vulnerability details. For example, say you want to view imported vulnerabilities that are filtered by specific IPs or IP ranges. Or, you want to import only machines that are under your scope, for example, only machines within your corporate network that are not external devices.

To help you gather this data, you might add Qualys parameters to help you import the specific vulnerability details you need.

Without adding additional API calls or coding, this feature permits you to customize your HTTP Request information with Qualys parameters in your ServiceNow AI Platform. You modify or add these values on your HTTP Method record under the REST method for the supported Qualys integrations of the Qualys Vulnerability Integration.

Role required: sn_vul.vulnerability_admin

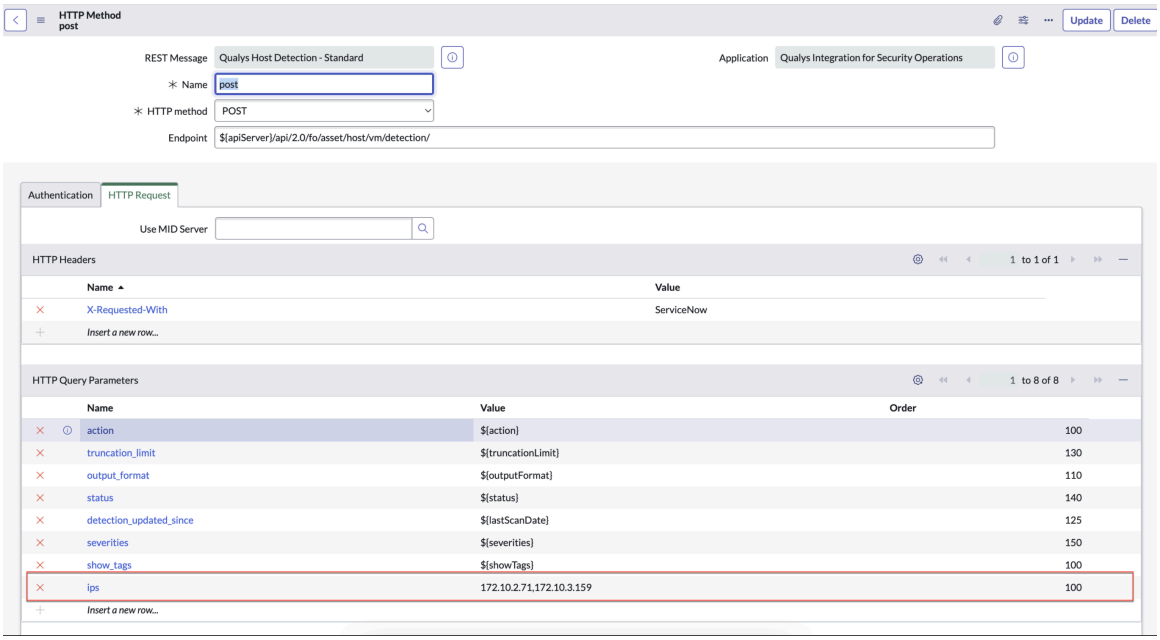
Procedure

1. Locate the parameters supported by the Qualys product on the developer site that you want to use for your filtering.
   Parameters and values you enter from the Qualys product are supported only at the integration instance level in your ServiceNow AI Platform. All Qualys Integrations support filtering using query parameters.
2. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the Qualys Integrations list page, click the record for the integration that you want to open the record.
4. With the Qualys REST Details tab selected, locate and click the information icon (I) for REST method followed by **Open Record** to open the HTTP Method record.
5. Select the **HTTP Request** tab.
6. In the HTTP Query Parameters for the request body, add the values you got from the Qualys developer site.

   In the following image, as an example, the parameter that ingests only certain IP addresses/ranges, *ips={value}* has been added. In this case, **value** is one or more IPs/ranges that you specify. Multiple entries are comma separated, `172.10.2.71, 172.10.3.159`, and a range is specified with a hyphen, `10.10.10.1-10.10.10.100`. Refer to the Qualys developer site for more information.



   If you want to enter more than one parameter, refer to the Qualys documentation for more information about how to separate each value.

   Note: You should be aware of you API requirements. You might have to add these API properties to the Query Parameters, or to the body content.

   Some other parameters you might find useful from the Qualys developer site:

   - *ag_ids* - Asset Group list IDs to retrieve. This parameter ensures only machines under your scope are brought in.
   - *qids* - This parameter limits results to only certain vulnerabilities (QID in Third-Party Entry table). This setting prevents flooding your system with informational records.
   - *arf_filter_keys* - Filters and returns host detections based on the specified values. Acceptable values: non-running-kernel, non-running-service, and config-not-exploitable. You can use any single value or comma-separated values. When you use this parameter in the REST parameters, set the following instance parameters to false because they are mutually exclusive: include_kernel_metadata, include_service_metadata, include_exploitable_config_metadata.
   - *show_arf_data* - Displays ARF-affected data for host detections along with the arf_filter_keys parameter. Acceptable values: 0 or 1. If you set the value to 0, the output does not include the ARF filter output data. When you use this parameter in the REST parameters,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

set the following instance parameters to false because they are mutually exclusive: include_kernel_metadata, include_service_metadata, include_exploitable_config_metadata.

- *code_modified_after* - Returns QIDs modified after the specified date in the Knowledge Base integrations.
- *code_modified_before* - Returns QIDs modified before the specified date in the Knowledge Base integrations.
- *assetDeploymentType* - Returns host IDs of the specified deployment type for PCRS Policy Host integrations. Acceptable values: ON-PREM, CLOUD, or ALL. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *assetState* - Returns host IDs of the specified state for PCRS Policy Host integrations. Acceptable values: TERMINATED, ACTIVE, or ALL. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *cloudMetaDataRequired* - Fetches cloud metadata in the PCRS Test Results Integration response. Acceptable values: 0 or 1. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *status* – Filters results based on result status. Acceptable values: Passed, Failed, and Error. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *previousStatus* – Filters results based on the previous result status. Acceptable values: Passed, Failed, and Error. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *criticalityLabels* – Filters results based on criticality level. Acceptable values: UNDEFINED, MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *criticalityValues* – Filters results based on criticality level. Acceptable values: 0–5. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *extendedEvidenceRequired* – Fetches extended evidence data. Acceptable values: 0 or 1. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.

7. Click **Update**.

Resolving Qualys Vulnerability Integration issues

Some commonly encountered issues, along with workarounds are discussed.

Attachments not appearing after import

If attachments are not appearing as expected for data sources or on a security incident after third-party integration imports, check your IP restrictions.

IP access restrictions can prevent attachments from being seen unless you are logged in from a safe IP. Since a new attachment is added with each import, this can result in duplicates you have to remove.

For example, when you run a third-party host import integration, if you do not see any attachments on your data sources, check your IP restrictions and add users to the safe list prior to import.

Modify transform maps

Transform maps are provided with base configurations and are sufficient usually. You can modify transform mappings depending on the needs of your organization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul_qualys.admin + import_admin

Procedure
1. Navigate to **All** > **System Import Sets** > **Administration** > **Transform Maps** to view the REST messages.
2. Filter the resulting list by application, and limit the list to the **Qualys Vulnerability Integration** application.
3. Modify the transform maps per the customer requirements.

   For details on the data provided by the Qualys API, see the Qualys API documentation.

Check XML attachment property size

Verifies that the XML attachment property is sufficient for large files.

Before you begin
Role required: admin

Procedure
1. Navigate to **All** > **System Properties** > **Import Export**.
2. Scroll down to **Import Properties** > **XML Format** at the bottom of the page.



3. If necessary, change the value to 250 and click **Save**.

Related topics
Available system properties

Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- Name: severities
- Value: 3-5 (or whatever appropriate severities are desired)

Resolving Qualys Knowledge Base Integration failure

Resolve Qualys Knowledge Base Integration failure by reducing the payload attachment size received from Qualys to the specified limit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin

Procedure
1. Ensure that the payload attachment size is within the specified limit.
   a. Navigate to **All** > **Qualys Vulnerability Integration** > **Integration Instances**.
   b. Select the **Integration Instance Parameters** tab.
   c. Select **max_delta_days** and modify the default value to 3.
2. If the integration still fails, perform the following steps:
   a. Navigate to **All** > **Qualys Vulnerability Integration** > **Primary Integrations**.
   b. Select **Qualys Knowledge Base**.
   c. Select the **Integration Details** tab.
   d. In the **Start time** field, select the current date to skip the execution of the run for that day.
   e. Navigate to **All** > **Qualys Vulnerability Integration** > **Integration Instances**.
   f. Select the **Integration Instance Parameters** tab.
   g. Select **kb_backfill_full_import** and modify the default value to true.

Result
Running the Qualys Knowledge Base Backfill integration updates all the third-party entries (TPEs) in the system. While the Qualys Host Detection integration creates a placeholder entry, the Qualys Knowledge Base Backfill integration updates it.

Qualys Vulnerability Integration reporting

The Qualys Cloud Platform overview is an executive view into vulnerability activity. By providing trends, reports, and drill-downs into specific data, an administrator or analyst can quickly pinpoint areas of concern. The charts are populated with data after vulnerable items and the Qualys knowledge base data have been retrieved.

Data visualizations in the Vulnerability Response Workspaces

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Response Workspaces, Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Prior versions of Vulnerability Response

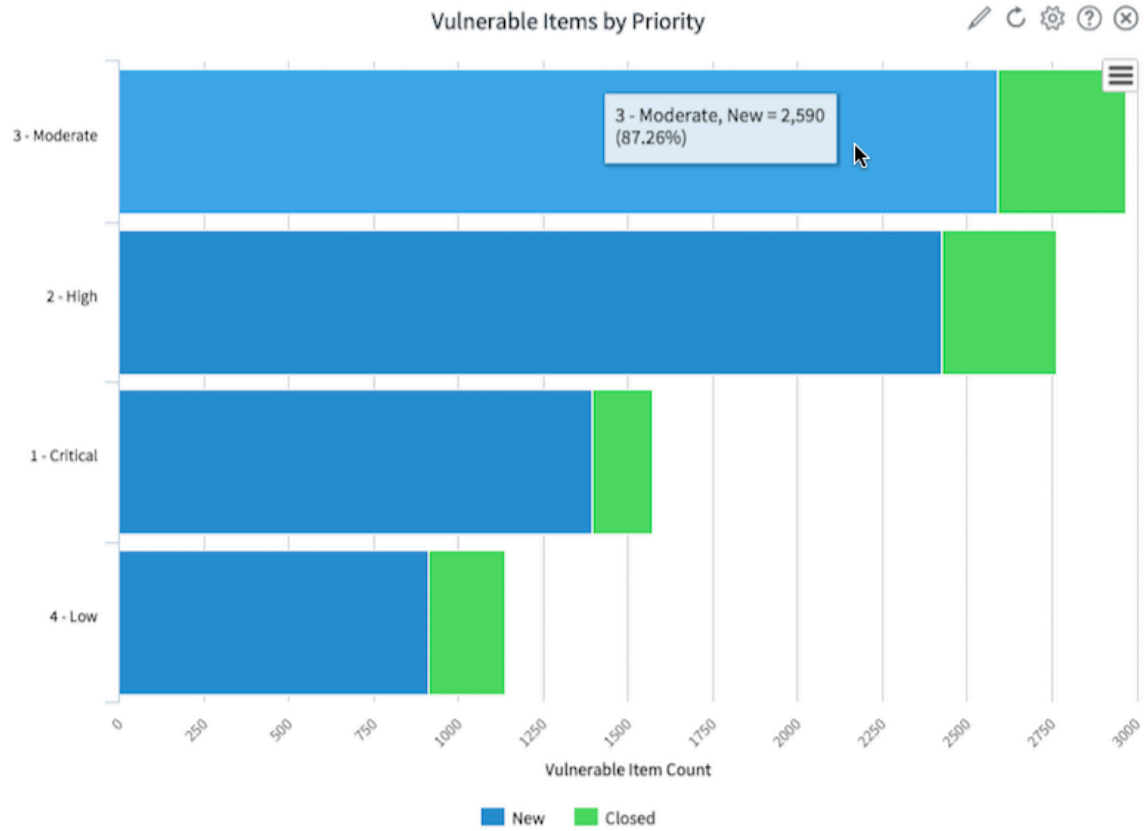
Vulnerability analysts can also use the default dashboards in the classic environment to monitor vulnerability data. See Using the default Vulnerability Response dashboards for more information.

Note: Using the Qualys Cloud Platform Vulnerability integration assumes that tuning, testing and deployment have occurred in your instance. These functions are areas beyond the scope of product documentation. For assistance, contact Customer Service and Support.

In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample Qualys Vulnerability Integration chart



The following reports are available on the Qualys Cloud Platform homepage.

Qualys Vulnerability Integration Overview reports

Name	Visual	Description
CIs Synchronized With Qualys	Bar	Displays the number of open vulnerable items recorded for each CI, from most to least.
Open Qualys Vulnerable Items	Bar	Displays the number of open vulnerable items associated with vulnerabilities (CVE records), from most to least.
Total Qualys Vulnerable Items	Bar	Displays the number of ignored vulnerable items scheduled to be expired within 7 days.
Vulnerable Items by Priority	Trend	Displays the number of vulnerability entries recorded each week.
QID Prevalence	Bar	Displays the number of vulnerable items recorded for each model, from most to least.
Open Qualys Vulnerable Items	List	Displays the number of vulnerable items recorded for each publisher, from most to least.

Qualys integration run status chart

The Qualys Integration Run Status module is a graphical view of the status of Qualys integration runs.

To view the status of integration runs, navigate to **Qualys Vulnerability Integration** > **Integration Run Status**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

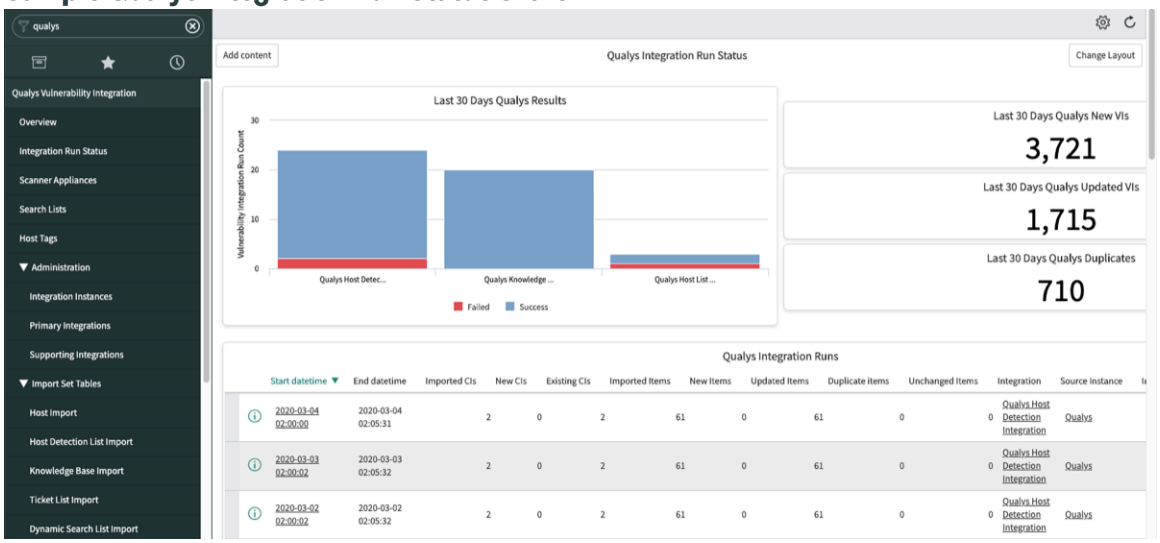
Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

The Qualys Integration Run Status displays the vulnerability integration run status for the last 30 days. The Qualys[qualys] updated VIs count indicates the count for any unique detections in the same asset. The VI then gets updated with the new detection.

Note: The vulnerability integration run count is displayed only for the integrations, which are set to active state. Navigate to **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations** and set the state to active.

Sample Qualys Integration Run Status chart



- The values in the Imported Items column represents the total number of records that are created from an integration run.
- The New items column displays the number of records that are created from an integration run.
- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.
- The Updated items column displays the number of times records are updated during an integration run. This value is not the number of unique records that are updated. If for example, a record is updated two times during the integration run, it is counted two times and displayed as 2 updated items.
- The Unchanged items column displays records found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: **New CIs**, **Existing CIs**, **New Items**, and **Updated Items** are filtered out of the **Qualys Integration Runs** list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys integration run status chart reports

Name	Description
Last 30 Days Qualys Results	The number of integration runs completed for each integration. Shows both successful and failed runs. Run in a bar visual.
Last 30 Days Qualys New VIs	The number of new records imported in the last 30 days. Shown as an integer.
Last 30 Days Qualys Updated VIs	The number of updated records imported in the last 30 days. Shown as an integer.
Last 30 Days Qualys Duplicates	The number of duplicate records imported in the last 30 days. Shown as an integer.
Qualys Integration Runs	The integration run records in a list. **Note: V16.1:** To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.
Last 30 Days Qualys Vulnerable Item Ingestion Performance Metrics	Daily performance metrics for vulnerable items compared for the last 30 days.
Last 30 Days Qualys Vulnerable Item Ingestion Performance Throughput	Daily vulnerable item ingestion throughput measured for the Qualys Host Detection integration for the last 30 days.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Two graphs compare the performance metrics:

- Qualys Vulnerable Item Ingestion Performance Metrics: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance. The performance is calculated based on the time taken for each activity. These parameters are calculated and associated at the integration run level. Each parameter is color coded for easy identification.
- Qualys Vulnerable Item Ingestion Performance Throughput: Compare daily vulnerable item ingestion throughput for the Qualys Host Detection integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Throughput is measured in items per hour. This report shows the overall performance on a particular day and not at the individual parameter level.



Qualys data transformation

The data retrieved from Qualys is processed through a set of data sources and transforms.

Most transforms for the Qualys Vulnerability Integration are performed using transform scripts. These scripts are for internal use deleting is not recommended. Modifications require coding or advanced ServiceNow or Qualys Vulnerability Integration expertise. The remaining maps are listed in this section and use field maps.

Note: During installation, normalized severity maps, that transform imported Qualys Cloud Platform severity levels to standard ServiceNow severity levels, are installed in the Vulnerability Response Normalized Severity Mapping module. See Create a Vulnerability Response severity map for more information.

Dynamic Search List Import

The Qualys dynamic search list transform map is used to transform and import Qualys Dynamic Search Lists. Changes to this transform alter how Dynamic Search Lists are processed and inserted into the system.

To access this transform map, navigate to **Qualys Vulnerability Integration** > **Import Set Tables** > **Dynmaic Search List Import**.

The table shows the fields currently being transformed.

Qualys dynamic search list transform map fields

Source Field	Target field	Description
u_id	id	Used as the identifier for the Qualys Dynamic Search List.
[Script]	list_type	The type of search list. Dynamic is the default for the Dynamic Search List transform.
u_title	title	The name in Qualys for this search list.

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys dynamic search list transform map script timing and purpose

When the script is run	Purpose of the script
onAfter (after an import set has completed transformation).	Creates the relationships between Search Lists and their related vulnerabilities. For internal use. Modifying or deleting is not recommended.

Static Search List Import

The Qualys static search list transform map is used to transform and import Qualys Static Search Lists. Changes to this transform alter how Static Search Lists are processed and inserted into the system.

To access this transform map, navigate to **Qualys Vulnerability Integration** > **Import Set Tables** > **Static Search List Import**.

The table shows the fields currently being transformed.

Qualys static search list transform map fields

Source Field	Target field	Description
u_id	id	Used as the identifier for the Qualys Static Search List.
u_title	title	The name in Qualys for this search list.
[Script]	list_type	The type of search list. Static is the default for the Static Search List transform.

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys static search list transform map script timing and purpose

When the script is run	Purpose of the script
onAfter (after an import set has completed transformation).	Creates the relationships between Search Lists and their related vulnerabilities. For internal use. Modifying or deleting is not recommended.

Asset Group Import

The Qualys Asset Group Appliance Transform map is used to transform Qualys Asset Group data to create scanner appliance records. Changes to this transform alter how scanner appliances are created and modified.

To access this transform map, navigate to **Qualys Vulnerability Integration** > **Import Set Tables** > **Asset Group Import**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The table shows the fields currently being transformed.

Qualys asset group transform map fields

Source Field	Target field	Description
u_id	id	Used as identifier for the Qualys Asset Group.
[Script]	manual	Scripted value to determine how the target record was created. When created through transforms, this field is always false.
[Script]	ips	The IP addresses that are associated with the asset group being transformed.
u_default_appliance_id	appliance_id	The Qualys appliance identifier for the default appliance in this asset group.
u_title	asset_group_name	The name of the Qualys asset group.

In addition to field mappings, there is also a transform script that is executed during the transformation process.

The following table shows when this script runs and what it is used for.

Qualys asset group transform map script timing and purpose

When the script is run	Purpose of the script
onBefore (before an import set has completed transformation).	The script that constrains the asset group imports to only asset groups with a default appliance and a set of mapped IP addresses. For internal use. Modifying or deleting is not recommended.

Appliance Import

The Qualys Appliance Transform map is used to transform Qualys Appliance data into appliance records. This is used to update the appliance records that would initially be created from the Asset Group Import. Changes to this transform alter how appliance records are updated with appliance details.

To access this transform map, navigate to **Qualys Vulnerability Integration** > **Import Set Tables** > **Appliance Import**.

The table shows the fields currently being transformed.

Qualys appliance transform map fields

Source Field	Target field	Description
u_name	appliance_name	The name of the Qualys scanner appliance.
u_status	appliance_status	The last reported status of the Qualys scanner appliance.
u_id	appliance_id	The Qualys appliance identifier.

In addition to field mappings, there is also a transform script that is executed during the transformation process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following table shows when this script runs and what it is used for.

Qualys appliance transform map script timing and purpose

When the script is run	Purpose of the script
onBefore (before an import set has completed transformation).	Used to update appliance names and statuses for the given ID. For internal use. Modifying or deleting is not recommended.

Qualys REST messages

Qualys REST messages are used to make calls to the Qualys API.

Starting with version 12.9.2 of Qualys, you have the option to choose between Basic Authentication or OAuth. The instance parameter Qualys Cloud Authentication method is pre-configured for Basic Auth. If you prefer to use OAuth, you must modify integration instance parameter and then set up the rest message directly for the OAuth.

Qualys Host Detection REST message

The Qualys Host Detection REST message makes the initial call to the Host List Detection API for the Qualys Host Detection Integration.

Qualys host detection REST message parameters

Parameter Name	Value	Description
action	list	Indicates the type of operation requested. Required parameter. Changes aren't required.
output_format	XML	Sets the format of the report returned by Qualys. The various scripts and transforms assume XML, so changes to the value aren't recommended.
detection_processed_after	${lastScanDate}	Shows only detections whose detection status changed after a certain date and time. For detections that have never changed, the date is applied to the last detection date.
truncation_limit	500	The number of hosts to retrieve data from, according to request. This parameter is used for pagination purposes. The default value is 500, but larger or smaller values can be used. Don't set at less than 100 since it significantly increases system load. Smaller values require more calls to the Qualys API and larger values result in larger result sets to process and potential data retrieval/ processing timeouts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys host detection REST message parameters (continued)

Parameter Name	Value	Description
status	New, Fixed, Active, Reopened	Detection statuses to retrieve from Qualys. The default is to retrieve all statuses. For large data pulls (often the initial pull of data), it can be beneficial to exclude Fixed statuses from this list. It's important to include the Fixed status when updating vulnerabilities already in the system.

Qualys Host Detection Integration REST message

The Qualys Host Detection – Standard REST message retrieves host detection data from Qualys.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Host Detection Integration REST message parameters

Parameter Name	Value	Description
vuln_detection_source	1	Returns the vulnerability detection source in the response.
show_tags	${showTag}	Displays asset tags associated with each host in the XML output.
show_cloud_tags	1	Returns cloud provider tags for each scanned host asset in the output.
host_metadata	all	Lists all assets (cloud and non-cloud) and the metadata output applicable for cloud assets.
action	${action}	Action to list host detections.
output_format	${outputFormat}	Specifies the format of the host detection list output.
truncation_limit	${truncationLimit}	Specifies the maximum number of host records processed per request.
status	${status}	Returns only hosts with one or more of these status values.
severities	${severities}	Returns only detection records that have the specified severities.

Qualys Comprehensive Host Detection Integration REST message

The Qualys Host Detection - Standard REST message retrieves host detection data from Qualys.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Host Detection Integration REST message parameters

Parameter Name	Value	Description
vuln_detection_source	1	Returns the vulnerability detection source in the response.
show_tags	${showTag}	Displays asset tags associated with each host in the XML output.
show_cloud_tags	1	Returns cloud provider tags for each scanned host asset in the output.
host_metadata	all	Lists all assets (cloud and non-cloud) and the metadata output applicable for cloud assets.
action	${action}	Action to list host detections.
output_format	${outputFormat}	Specifies the format of the host detection list output.
truncation_limit	${truncationLimit}	Specifies the maximum number of host records processed per request.
status	${status}	Returns only hosts with one or more of these status values.
severities	${severities}	Returns only detection records that have the specified severities.

Qualys Host List Integration REST message

The Qualys Host Detection - Standard REST message retrieves host detection data from Qualys.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Host Detection Integration REST message parameters

Parameter Name	Value	Description
show_tags	${showTag}	Displays asset tags associated with each host in the XML output.
show_cloud_tags	1	Returns cloud provider tags for each scanned host asset in the output.
host_metadata	all	Lists all assets (cloud and non-cloud) and the metadata

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys Host Detection Integration REST message parameters (continued)

Parameter Name	Value	Description
		output applicable for cloud assets.
action	${action}	Action to list host detections.
truncation_limit	${truncationLimit}	Specifies the maximum number of host records processed per request.
details	${status}	Specifies the requested amount of host information for each host to be returned in the response.

Qualys Knowledge Base REST message

The Qualys Knowledge Base (Date Based) REST message retrieves vulnerability data from Qualys.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Host Detection Integration REST message parameters

Parameter Name	Value	Description
action	${action}	Action to list host detections.
details	${status}	Specifies the requested amount of host information for each host to be returned in the response.
last_modified_after	${dateStart}	Filters the XML output to show only vulnerabilities last modified after a certain date and time.
last_modified_before	${dateEnd}	Filters the XML output to show only vulnerabilities last modified before a certain date and time.

Qualys Knowledge Base (Backfill) REST message

The Qualys Knowledge Base (Backfill) REST message retrieves vulnerability backfill data from Qualys.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys Host Detection Integration REST message parameters

Parameter Name	Value	Description
action	${action}	Action to list host detections.
details	${status}	Specifies the requested amount of host information for each host to be returned in the response.
ids	${qids}	Filters the XML output to include only vulnerabilities that have QID numbers matching the QID numbers specified.

Qualys host detection pagination REST message

The Host Detection Pagination REST message handles pagination requests to the Host Detection API.

When the primary host detection runs, if the Qualys API provides a URL to fetch the next page of data, this REST message retrieves that additional data. This data is used by the Host Detection Pagination Handler.

Host detection pagination REST is a specialized REST message and isn't intended to be modified.

Qualys knowledge base (backfill) REST message

The Qualys Knowledge Base (Backfill) REST message retrieves Qualys knowledge base data based on the last modified timestamp of the vulnerability data for the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.

Qualys knowledge base (backfill) REST message parameters

Parameter	Value	Description
action	list	Indicates the type of operation being requested. Required parameter. Changes aren't recommended.
details	All	Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.
ids	${qids}	Specifies which QIDs to retrieve from Qualys. Referenced in code. Modifications aren't recommended.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys knowledge base (date-based) REST message

The Qualys Knowledge Base (Date-Based) REST message is used to retrieve Qualys knowledge base data based on the last modified timestamp of the vulnerability data. This message is used by the Qualys Knowledge Base integration.

Changes to the REST message method record impact the request made to Qualys to retrieve knowledge base information.

The following table shows the request parameters that are sent.

Qualys knowledge base (date-based) REST message parameters

Source Field	Target Field	Description
action	list	Indicates the type of operation requested. Required parameter. Changes aren't recommended.
details	All	Indicates the level of detail shown for vulnerabilities retrieved. Safe to modify as needed.
last_modified_after	${dateStart}	Indicates when to start retrieving historical data. Used by code to determine both the start time and to assist with pagination. Modifications or removal isn't recommended.
last_modifiedbefore	${dateEnd}	Indicates when to end retrieving historical data. Used by code to determine both the end time and to assist with pagination. Modifications or removal isn't recommended.

Qualys tickets REST message

The Qualys tickets REST message retrieves Qualys ticket information for the Qualys Ticket Integration. Changes to the REST message method record impact the requests made to Qualys to retrieve ticket information.

The table shows the request parameters that are sent.

Qualys tickets REST message parameters

Parameter Name	Value	Description
modified_since_datetime	${lastRunDatetime}	Indicates the last run date of the integration and the date after which to pull data. Used by code. Changes aren't recommended.
since_ticket_number	${lastTicketNumber}	Indicates which ticket was last retrieved from Qualys.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys tickets REST message parameters (continued)

Parameter Name	Value	Description
		Used for pagination. Changes aren't recommended.
show_vuln_details	1	Indicates whether the vulnerability details are retrieved.

Understanding the Rapid7 Vulnerability Integration

The ServiceNow® Rapid7 Vulnerability Integration uses data imported from the Rapid7 data warehouse or the Rapid7 InsightVM products to help you determine the impact and priority of potentially malicious threats.

Rapid7 Nexpose sensors collect data and automatically send it to the Rapid7 data warehouse (on-premise) or Rapid7 InsightVM (cloud-based) products, which continuously analyze and correlate the information. It easily integrates with ServiceNow® Vulnerability Response to map vulnerabilities to CIs and services. The Rapid7 Vulnerability Integration enriches the vulnerability data on your instance.

Rapid7 integrations are entry points interacting with the Rapid7 data warehouse or Rapid7 InsightVM products, invoked as scheduled jobs. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems. The scheduled jobs are run automatically and in the order specified. You can also execute individual scheduled jobs manually.

Note:

If you use both Rapid7 data warehouse and Rapid7 InsightVM as sources for your data, you run the risk of duplicate vulnerability records.

Note: When migrating from the **Data Warehouse** integration type to the **InsightVM** type, you can deduplicate your existing data warehouse records. See Deduplicate Rapid7 Vulnerability Integration data warehouse records for more information.

If you have multiple deployments of the Rapid7 InsightVM vulnerability integration, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from each deployment is identified and available in a single instance of Vulnerability Response.

Note: You cannot delete the original vulnerability integration but you can disable it. Integrations created from disabled templates are disabled by default.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Available versions

Release version for Xanadu	Release Notes
Rapid7 Vulnerability Integration v13.6, 13.7	For compatibility information, see KB0856498 Vulnerability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Release version for Xanadu	Release Notes
	Response Compatibility Matrix and Release Schema Changes

Roles

Rapid7 vulnerability integration tasks involve the following roles.

- sn_vul_r7.admin: Can read, write, and delete records.
- sn_vul_r7.user: Can read and write records.
- sn_vul_r7.read: Can read records.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Rapid7 Vulnerability Integration integrations

To view the Rapid7 Vulnerability Integration, navigate to **Rapid7** > **Administration** > **Integrations**.

The following integrations are included in the base system.

Rapid7 data warehouse integrations

Integration	Description
Rapid7 Vulnerability Integration	Retrieves vulnerability data from Rapid7 Nexpose and processes it in your instance.
Rapid7 Asset List Integration	Retrieves scan data once a week from Rapid7 Nexpose data warehouse and stores it in the Discovered Items module in your instance. Helps identify assets that haven't been scanned recently using **Last Scan** date. View the **Last Scan** time in the Discovered Items list in Vulnerability Response.
Rapid7 Category Integration	Retrieves category information from Rapid7 Nexpose. Categories provide high-level classification for vulnerabilities.
Rapid7 Exploit Integration	Retrieves exploit information from Rapid7 Nexpose.
Rapid7 Malware Kit Integration	Retrieves malware kit information from Rapid7 Nexpose.
Rapid7 Reference Integration	Retrieves references to external authority documents such as CVEs or vendor-specific vulnerability references.
Rapid7 Solution Integration	Retrieves solution data from Rapid7 Nexpose, which provides recommended solutions to specific vulnerabilities.
Rapid7 Superceding	Retrieves information about which solutions are superseded by other solutions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rapid7 data warehouse integrations (continued)

Integration	Description
Solution Integration	
Rapid7 Prerequisite Solution Integration	Retrieves information about the solutions that are prerequisites for other solutions. When this integration executes, it fetches the mapping of solutions and prerequisite solutions from the Rapid7 data warehouse. **Note:** This integration works only if the Vulnerability Solution Management plugin is activated.
Rapid7 Vulnerability Solution Map Integration	Retrieves the mapping to associate solutions with vulnerabilities.
Rapid7 Vulnerable Item Integration	Retrieves vulnerable item data from Rapid7 Nexpose and processes it in your instance. The outputs of this integration are vulnerable items.
Rapid7 Vulnerable Item Resolution Integration	Retrieves information about which vulnerable items are marked closed in Rapid7 Nexpose and closes the corresponding vulnerable items in Vulnerability Response.
Rapid7 Site Integration	Retrieves Site data from Rapid7 Nexpose. A site is a collection of assets that are targeted for a scan.
Rapid7 Asset List Integration	Retrieves host tags and scan data once a week from the Rapid7 data warehouse and stores it in the Discovered Items module in your instance. Helps identify assets that haven't been scanned recently using **Last Scan** date. View the **Last Scan** time in the Discovered Items list in Vulnerability Response
Rapid7 Comprehensive Vulnerable Item Integration	Imports all the Rapid7 detections for all configuration items scanned since the last successful integration run. Based on the most current imported data, vulnerable items not recently found during scans are automatically transitioned to 'Closed' when the Auto-Close Stale Vulnerable Items module is enabled.

Rapid7 InsightVM integrations

Integration	Description
Rapid7 Vulnerable Item Integration — API	Retrieves vulnerable item data from Rapid7 InsightVM and processes it in your instance.
Rapid7 Vulnerability Integration — API	Retrieves reference, category, exploit, malware kit, and vulnerability data from Rapid7 InsightVM and processes it in your instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rapid7 InsightVM integrations (continued)

Integration	Description
Rapid7 Asset List Integration - API	Retrieves host tags and scan data once a week from Rapid7 InsightVM and stores it in the Discovered Items module in your instance. Helps identify assets that haven't been scanned recently using **Last Scan** date. View the **Last Scan** time in the Discovered Items list in Vulnerability Response.
Rapid7 Comprehensive Vulnerable Item Integration - API	Imports all the Rapid7 detections for all configuration items scanned since the last successful integration run. Based on the most current imported data, vulnerable items not recently found during scans are automatically transitioned to 'Closed' when the Auto-Close Stale Vulnerable Items module is enabled.
Rapid7 Site Integration	Retrieves Site data from the Rapid7 InsightVM product. This integration is set to run weekly at 00:00:00.

During import, CVE records not already present are created as NVD records and referenced in third-party entries for Rapid7 by default. The template integration for Rapid7 cannot be deleted. Disable it instead.

The Service Graph Connector for Rapid7

Beginning with version 2.0, the Service Graph Connector for Rapid7 is available from the ServiceNow® Store. See Service Graph Connector for Rapid7 for more information.

CI Lookup Rules

CI Lookup Rules determine how to fill in the **Configuration item** field in a vulnerable item record.

For more information on how CI lookup rules work, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

To create or edit lookup rules, see Create a Vulnerability Response CI lookup rule.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Discovered Items

This module lists configuration items detected during import from the Rapid7 Vulnerable Item Integrations (data warehouse or InsightVM API) and the Rapid7 Asset List Integration - API. The Rapid7 Asset List Integration - API imports all Rapid7 assets scanned for vulnerabilities since the last integration run. The Rapid7 data warehouse Asset List Integration is included.

Note: The default filter for this list is set to **Unmatched**. You can view all discovered items from an import by removing the filter.

See Discovered Items in Vulnerability Response for more information on the Discovered Items module.

Host tags

Host tags are imported as part of the Rapid7 Asset List Integration - API integration for Rapid7 InsightVM. They are used primarily for filtering in Vulnerability Response Assignment and Remediation Task Rules in Rapid7 InsightVM. They are displayed in the Discovered Item form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Host tags

Note: The Rapid7 Asset List integration - API integration should be run prior to creating Assignment or Remediation Task Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case-sensitive. If a **San Diego** tag is created, then a **SAN DIEGO** tag cannot be stored in the Host tag table. “San Diego” and “SAN DIEGO” are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Remediation Task Rule can have unexpected results. Host tags are intended for use only in the Condition builder.
- Host tags are controlled by the global system property **sn_vul.import_host_tags**. This property is set to true by default. Turning tags off turns them off across all instances.

Sites

A site is a collection of assets targeted for a scan. A site consists of target assets, a scan template, one or more Scan Engines, and other scan-related settings such as schedules or alerts. Sites are managed by Rapid7 applications.

Rapid7 Vulnerability Integration site filtering during configuration allows you to categorize and request assets by site during import. See Filtering by Rapid7 sites for more information on filtering imports.

The Rapid7 data warehouse and Rapid7 InsightVM Sites integrations import sites as a weekly scheduled job.

To view the imported sites in a list, navigate to **Rapid7** > **Sites**.

Reopen resolved vulnerable items not closed by scans

Vulnerable items set to 'Resolved' in your ServiceNow AI Platform instance but not transitioned to 'Closed/Fixed' by the subsequent integration runs are reopened if they are detected during rescans.

For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days you enter.

Create CIs using the Identification and Reconciliation Engine (IRE)

You can use the Identification and Reconciliation Engine to create new CIs when an existing CI cannot be matched with a host imported from a third-party scanner. Enable the CMDB CI Class Models plugin to create CIs using the new classes, otherwise unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. For more information on how to configure the categorization of unmatched cloud resources into your preferred CI class, see Updating CI class for unmatched cloud assets.

Rescan vulnerable items

Initiate rescans in the Rapid7 platform to verify that your vulnerable items have been remediated between scheduled scanning cycles. See Initiate rescan for the Rapid7 Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Rapid7 solution management

If you have activated the Vulnerability Solution Management plugin, then the Rapid7 solutions for both Rapid7 data warehouse and Rapid7 InsightVM get populated in the Vulnerability Solutions [sn_vul_solution] table. However, if you have not activated the Vulnerability Solution Management plugin, then Rapid7 Vulnerability Integration works as is and imports the solutions in the custom [sn_vul_r7_solution] table. For more information, see Rapid7 solution management.

Preparing for the Rapid7 Vulnerability Integration

A successful integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Rapid7 Vulnerability Integration assumes that you are familiar with and run Rapid7 data warehouse or Rapid7 InsightVM product scans in your environment.

Before you begin

Role required: admin

About this task

The Rapid7 scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button is not available.

Before you download the Rapid7 Vulnerability Integration application from the ServiceNow® Store and install it on your instance, review the following information about the integration types and set up information:

There are two types of integrations included with the Rapid7 Vulnerability Integration that is available in the ServiceNow® Store:

- Rapid7 InsightVM
- Rapid7 data warehouse

The Rapid7 data warehouse type:

- Requires your Rapid7 data warehouse server URL and authentication credentials
- Requires a MID Server
- Uses a PostgresSQL driver to run queries on the data warehouse
- Does not support multiple instances

The Rapid7 InsightVM integration type:

- Is cloud-based and uses a REST API. This integration requires an API key from within your Rapid7 Insight account.
- Supports multiple instances.

See Set up for the Rapid7 data warehouse Integration (data warehouse) and Set up for the Rapid7 InsightVM Integration for more information about setup requirements for these integration types.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up for the Rapid7 data warehouse Integration

The Rapid7 data warehouse Integration is one of the integration types that is included with the Rapid7 Vulnerability Integration Rapid7 Vulnerability Integration.

Before you begin

Before you run the Rapid7 data warehouse integration, complete the following set up tasks:

- Get the Rapid7 data warehouse add-on. See the Rapid7 website and documentation to acquire and install this add-on.
- Get the most current PostgresSQL driver. Go to https://jdbc.postgresql.org/ and download the latest driver.
- A MID Server to run queries to the data warehouse. See MID Server for more information about how to set up a MID Server.

  Note the data warehouse name. The Rapid7 data warehouse integration type only supports standalone MID Servers. Clustered MID Servers are not supported.

- Get your Rapid7 data warehouse server URL and authentication credentials and have them accessible.

Role required: The system administrator [admin] downloads and installs the app. The sn_vul.vulnerability_admin or sn_vul.admin oversees configuration and verifies expected results.

Procedure

1. Log in to the ServiceNow AI Platform instance you want to install the Rapid7 Vulnerability Integration application on.
2. Install the PostgreSQL JAR file you downloaded in the set up tasks listed previously.

   a. In your ServiceNow AI Platform instance, navigate to **All** > **MID Server** > **JAR Files**.

   b. Click **New**.

   c. Enter the name of the PostgresSQL driver that you downloaded earlier.

   Optionally, enter the **Version**, **Source**, and **Description** information. Leave the **Active** check box selected.

   d. Attach the downloaded JAR file using the paper clip icon in the header.

   e. Click **Submit**.

   You have completed the setup for the Rapid7 data warehouse Integration. If you have not reviewed the requirements for the Rapid7 InsightVM Integration, before you install the Rapid7 Vulnerability Integration, see Set up for the Rapid7 InsightVM Integration and Preparing for the Rapid7 Vulnerability Integration.

   For steps to get entitlements, download, and install the Rapid7 Vulnerability Integration, see Install the Rapid7 Vulnerability Integration.

Set up for the Rapid7 InsightVM Integration

The Rapid7 InsightVM Integration is one of the integration types that is included with the Rapid7 Vulnerability Integration Rapid7 Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Before you run the Rapid7 InsightVM integration, complete the following set up tasks.

Role required: The system administrator [admin] downloads and installs the app. The sn_vul.vulnerability_admin or sn_vul.admin oversees configuration and verifies expected results.

Procedure

1. For the Rapid7 InsightVM Integration type, have your region and API key ready.
   Contact Rapid7 to obtain the appropriate region and API key.
   You have completed the setup for the Rapid7 InsightVM Integration. If you have not reviewed the requirements for the Rapid7 data warehouse integration, before you install the Rapid7 Vulnerability Integration, see Set up for the Rapid7 data warehouse Integration and Preparing for the Rapid7 Vulnerability Integration.
2. For steps to get entitlements, download, and install the Rapid7 Vulnerability Integration, see Install the Rapid7 Vulnerability Integration.

Install the Rapid7 Vulnerability Integration

After you complete the set up steps for the integration so that it properly integrates with Vulnerability Response, get entitlements, download, and install the application on your ServiceNow AI Platform® instance.

Before you begin

Roles required: admin for downlaod and installation, sn_vuln.admin oversees configuration and verifies expected results.

1. See Preparing for the Rapid7 Vulnerability Integration, Set up for the Rapid7 data warehouse Integration and Set up for the Rapid7 InsightVM Integration for more information about the integration types and setup requirements for the Rapid7 Vulnerability Integration.
2. Complete the following setup checklist prior to download and installation. These setup tasks are required for a smooth installation and configuration.
3. After the application is activated, follow the steps listed below to configure the Rapid7 Vulnerability Integration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.
Verify that you have the required ServiceNow AI Platform roles for your instance.	The following roles are required for installation, configuration, and verification of expected results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
	Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response. • The system administrator [admin] installs the app. If not already assigned, the admin assigns the Vulnerability Admin [sn_vul.vulnerability_admin or sn_vul.admin] role. • The vulnerability admin oversees configuration and verifies expected results. The Rapid7 admin role is inherited when you are assigned an administrative role in the Vulnerability Response (VR) application.
Validate your instance sizing based on the number of vulnerable items you expect to import.	An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.
Set up filtering	Use filtering to limit the number of items for initial import and phase your deployment by adjusting filters in subsequent imports.
Disable Vulnerability Calculators	If you do not use vulnerability calculators, Disable the default vulnerability calculator if not used, in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is created or updated, and can impact initial import performance.
Keep default value for run-as user	There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.
Using host tags	If you plan to use host tags in Vulnerability Response Assignment or Remediation Task Rules, run the Rapid7 Asset List integration prior to creating rules.
Deduplicate existing data records	When migrating from the **Data Warehouse** integration type to the **InsightVM** type you can deduplicate your existing data warehouse records. See Deduplicate Rapid7 Vulnerability Integration data warehouse records for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Log in to the instance you want to install the Rapid7 Vulnerability Integration application on.
2. Navigate to the ServiceNow Store and log in.
3. In the ServiceNow Store, search for the Rapid7 Vulnerability Integration application.

   Note: In the ServiceNow Store, the application is called, Rapid7 Integration for Security Operations. This application requires a subscription.

4. Click the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
8. Click **Request**.
   You will receive an email with detailed installation instructions.
9. In your ServiceNow AI Platform instance, navigate to **System Applications** > **All Applications** > **All**.
10. Locate the application, select it, and click **Install**.
    In the Install dialog, your dependency status is displayed. If you require a dependency application, the application you need is displayed. Follow the prompts in dialog to install the Rapid7 Vulnerability Integration application on your instance.

    Note: The vulnerability admin can now complete the configuration of the application. See Configure the Rapid7 Vulnerability Integration.

Configure the Rapid7 Vulnerability Integration

Configure the Rapid7 Vulnerability Integration after the application is installed and activated on your ServiceNow AI Platform®.

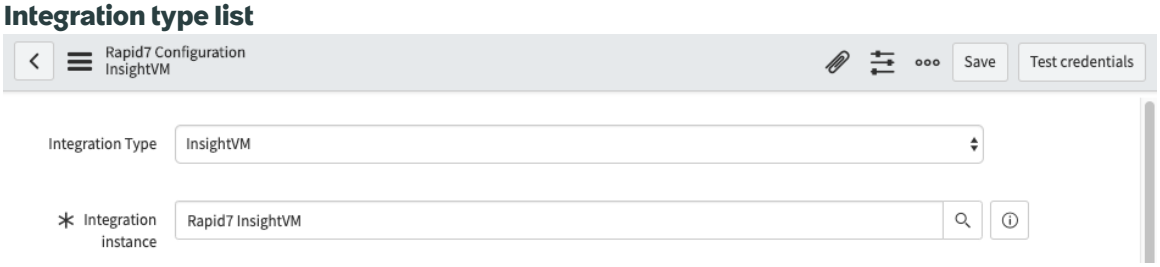
Before you begin

Role required: The administrator [admin] downloads and installs the app. The sn_vul.vulnerability_admin or sn_vul.admin oversees configuration and verifies expected results.

Procedure

1. After the application is activated (installed), navigate to **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
2. Select an integration type from the list.

Integration type list



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select an integration instance.
   The default Rapid7 InsightVM integration instance is selected by default. If that is the integration type you want, follow these steps. If you want to configure the Rapid7 data warehouse integration type, proceed to step 4.

   a. With the **Integration Setup** tab selected on the form that is displayed, fill in the fields:

   Integration Setup tab for InsightVM integration type

Field	Description
InsightVM Region	The server URL you acquired from the Rapid7 site.
API Key	The API key you acquired from your Rapid7 Insight account.
Validation Status	Read only: Status of credential validation process.

   b. Verify successful configuration by clicking **Test credentials**.
   If an error message is displayed during the configuration, reenter your data.

   c. After a successful test, click **Save**.

   d. Click the **Import Configuration** tab.

   On the form that is displayed, fill in the fields.

   Import Configuration tab for InsightVM

Field	Description
Min CVSS score	Minimum vulnerable item CVSS score used to filter vulnerable items during import.
Max CVSS score	Maximum vulnerable item CVSS score used to filter vulnerable items during import.
Site filter	Limits the data to the Rapid7 InsightVM sites chosen from the Sites list. See Filtering by Rapid7 sites. You can choose more than one site. The default (empty) brings in all sites. To pre-populate the Sites list, run the Rapid7 Site Integration — API prior to setting this field. For information on using site filtering, see Filtering by Rapid7 sites.
Auto-create CVE Entry	The system property to create a CVE Entry is active (true) by default. CVE placeholders are created automatically with the Rapid7 knowledge ingestion if the CVE ID does not exist. If you want this feature inactive, deactivate the property [sn_vul_r7.create_cve_for_vulnerabilities] from the System Properties list.
Reopen resolved by age	When selected, vulnerable items are automatically reopened when the number of days they have been resolved but not closed matches the value displayed in the **Reopen resolved after** field.

   e. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For multiple deployments of the Rapid7 InsightVM integration type:

f. On **Integration Instance** field open the Lookup list and select an existing integration instance or click **New** in the pop-up menu.

g. For **New**, enter a **Name** for the integration instance and click **Submit**.
The integration type appears in the Rapid7 configuration form.

Note: You can delete any integration instance except the default. Deleting an instance deletes the following (excluding VIs):

- Integrations
- Instance Parameters
- Integration Runs
- Integration Processes
- Instance column on the VI is marked empty

h. Verify successful configuration by clicking **Test credentials**.

i. After a successful test, click **Save**.

4. In the Integration Type field, expand the list and click **Data Warehouse**.

a. Select the **Integration Setup** tab.

On the form that is displayed, fill in the fields.

Integration Setup tab for Data Warehouse Integration type

Field	Description
JDBC credential name	Name of your data warehouse credentials.
User name	Rapid7 data warehouse user name.
Password	Rapid7 data warehouse password.
Validation Status	Read only: Status of credential validation process.
Validation Detail	Read only: Data warehouse only. Shows additional information about the validation check after you have clicked Test Credentials at least once. This can be useful in debugging your setup, (for example, validating if your MID server is configured incorrectly, or you just have the credentials wrong.
Database server DNS/IP	DNS or IP address for your data warehouse.
Database port	Port to use for your data warehouse integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Database name	Name of your data warehouse.
Data delay offset (Days)	The data delay offset factors in the delay between the real-time data in the Rapid7 Nexpose scanner and the data in the data warehouse.
MID Server	MID Server to use. Only standalone MID servers are supported. Clustered MID servers are not supported.
MID Server timeout (min)	Number of minutes to wait for the MID Server to respond before timing out the integration run.

b. Verify successful configuration by clicking **Test credentials**.

c. After a successful test, click **Save**.

d. Click the **Import Configuration** tab.

On the form that is displayed, fill in the fields.

Import Configuration tab for Data Warehouse

Field	Description
Prior to v12.0: Create CVE entry check box	When checked, placeholders for CVEs, not already present, are created as NVD records and referenced in the third-party entry for Rapid7. When unchecked, these CVEs are ignored.
Min CVSS score	Minimum vulnerable item CVSS score used to filter vulnerable items during import.
Max CVSS score	Maximum vulnerable item CVSS score used to filter vulnerable items during import.
Site filter	Limits the imported Sites Integration data to the sites chosen. You can choose more than one. **Note:** Since the default setting is to import data from all sites, you do not need to use the filter if you want all sites. Doing so slows down the request.
Reopen resolved by age	When selected, vulnerable items are automatically reopened when the number of days they have been resolved but not closed matches the value displayed in the **Reopen resolved after** field.

5. Click **Save**.
6. **Optional:** If you want to set a start date in the Rapid7 Vulnerability Integration - API and the Rapid7 Vulnerable Item Integration - API integration records to retrieve historical data during your initial import from the Rapid7 scan, follow these steps.
   You might use this data to help you with Closing stale detections in Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **Rapid7 Vulnerability Integration** > **Administration** > **Integrations**.
The Rapid7 Integrations list is displayed.

b. Click one of the integration records to open it.

(Optional) Near the top of the form, click the **here** link to edit the record.

The **Import since** date field in the Rapid7 integrations is blank, by default, except for the Rapid7 Vulnerability Integration - API and the Rapid7 Vulnerable Item Integration - API. For these integrations, these fields are set to 1998-12-31 or 1999-01-01.

To retrieve historical data during your initial import from the Rapid7 scan, set a start date in the appropriate integration records. This process works for any Rapid7 integration with the following exceptions:

- The Rapid7 Exploit and Malware Kit integrations do not show the **Import since** field, because they do not do delta updates and therefore do not use that field.
- The Rapid7 Asset List integration ignores the field since its intent is to retrieve all data.
- For the initial run of the Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API when the Auto-Close Stale Vulnerable Items module is enabled and the **Import since** field is left blank.

  When you enable the auto-close feature, a successful run from the Rapid7 Comprehensive Vulnerable Item Integration or the Rapid7 Comprehensive Vulnerable Item Integration - API is required. These integrations are disabled by default.

  When you enable the Rapid7 InsightVM Comprehensive Vulnerable Item Integration – API, if you leave the **Import since** field blank on the integration configuration page, the value in the **days ago** field of the Auto-Close Stale Vulnerable Items form is also used for the **Import since** date on the first integration run. The default value for Auto-Close Stale Vulnerable Items is (90 days).

  For example, if the **days ago** field in the Auto-Close Stale Vulnerable Items form is 90, and the **Import since** field on the Rapid7 Comprehensive Vulnerable Item Integration – API configuration page is blank, the first integration run imports the data for the last 90 days.

  This relationship between the **Import since** and **days ago** fields applies only to the first integration run. After that, changing the **days ago** field on the Auto-Close Stale Vulnerable Items form doesn't affect the **Import since** field on the Rapid7 Comprehensive Vulnerable Item Integration – API configuration page. The field is changed to the first run's start time so that the subsequent integration runs import only the delta information

  The **Import since** field is editable, and you can enter whatever values you want for each of the integrations.

7. Navigate to **All** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

a. The **import_startime_buffer_comprehensive** integration instance parameter sets a buffer time of 24 hours prior to the time specified in the **Import since** field so that the assets that are scanned from this buffer time are fetched during the **Rapid7 Comprehensive Vulnerable Item Integration - API** integration run.
You can modify this buffer time according to your requirement.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. **Optional:** Set the **close_stale_detections** parameter to *true* to close the stale detections that are no longer coming through the Rapid7 API for the assets that are scanned and retrieved through the Rapid7 API via **Rapid7 Comprehensive Vulnerable Item Integration - API**.

You have successfully completed the set up, installation, and configuration steps for the Rapid7 Vulnerability Integration. You are now ready to review and verify imported data.

What to do next

The Rapid7 and Qualys scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button is not available.

To activate these scanners, as a user with the sn_vul.vulnerability_admin role:

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Locate the scanner product you want to activate and click the record to open it.
3. Select the Active check box.
4. Click **Update**.

The product you activated is displayed in the Source field on vulnerable item and remediation task records after the next import, and **Rescan** is available as a UI action.

If your environment requires domain-separated imports, see Create domain-separated imports for an integration.

To create or refine your lookup rules prior to import, see Create a Vulnerability Response CI lookup rule.

Filtering by Rapid7 sites

Filter by site for Rapid7 InsightVM integration types as well as Rapid7 Nexpose data warehouse integration types.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Note: Using site filtering can have a performance impact. For information on performance and other considerations prior to using site filtering, see KB0789221.

About this task

Procedure

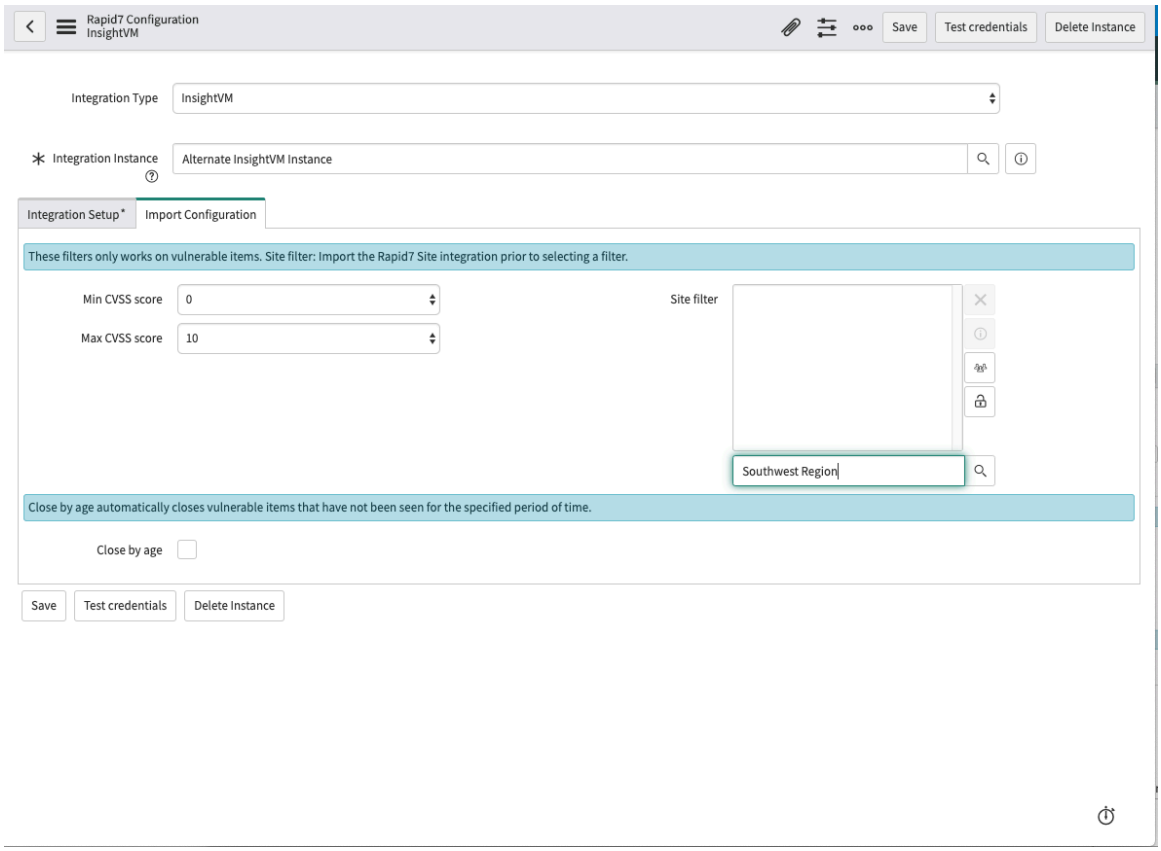
1. Navigate to **All** > **Rapid7 Vulnerability Integration** > **Configuration**.
2. Select an integration instance.
3. Click on the **Import Configuration** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you want all sites, leave the site filter field empty. No site filter is equivalent to adding all sites.

Sites are integration instance specific. The lookup list for site filtering displays both Rapid7 InsightVM and Rapid7 Nexpose data warehouse integration instance sites. Make sure the site you choose matches the integration instance you selected. For example, if you choose a data warehouse site, by mistake, that site will not work for site filtering by Rapid7 InsightVM.

4. Click on the lookup list to view the site records for the current integration instance.
5. Add a site from the list to add to the site filter.



6. Repeat selection to add additional sites.
7. Click **Save**.
   These sites are used to filter by site during the next import. See Prepend SITE to your Rapid7 InsightVM site tags for information on adding the prefix SITE to your site data.

Prepend SITE to your Rapid7 InsightVM site tags

Add the prefix, SITE, to your Rapid7 InsightVM site tags to highlight them among your list of tags.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Note: If necessary, switch your scope, to the Rapid7 Integration for Security Operations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the left navigation box, type: *sys_properties.list*.
2. Under **Name**, search for: *sn_vul_r7.prefix_site_to_rapid7_tags*.
3. Open *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Change **Value** to **true**.
5. Click **Update**.
   New and existing site tags are prefixed during the next import of Rapid7 InsightVM.

Deduplicate Rapid7 Vulnerability Integration data warehouse records

When migrating to the **InsightVM** integration type from the **Data Warehouse** integration type, you can deduplicate existing data warehouse vulnerable items as long as they belong to the same source data as your Rapid7 InsightVM data.

Before you begin

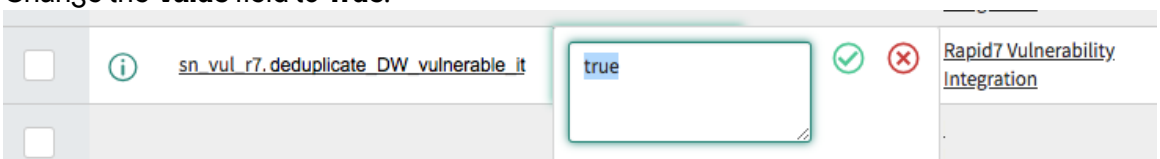
Role required: sn_vul_r7.admin or, sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

This deduplication only works when migrating from the Rapid7 Nexpose data warehouse to the Rapid7 InsightVM Vulnerable Item integration.

Procedure

1. Navigate to **All** > **Rapid 7** > **Integrations**.
2. Set all Rapid7 Nexpose data warehouse integrations **Active** column settings to **False**, disabling the integrations.
3. Enter `sys_properties.list` in the left navigation panel.
4. Search for the **Name**: `sn_vul_r7.deduplicate_DW_vulnerable_item`.
5. Change the **Value** field to **True**.



6. Click the green checkmark icon .
   During the next Rapid7 InsightVM vulnerable item integration import, any match with existing data warehouse records prevents a duplicate vulnerable item from being created.

Rapid7 Vulnerability Integration run status chart

Rapid7 Nexpose sensors collect the data and automatically send it to the Rapid7 Nexpose or Rapid7 InsightVM products, which continuously analyze and correlates the information.

Data visualizations in the Vulnerability Response Workspaces

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

data visualizations that are updated as vulnerability data changes. See Vulnerability Response Workspaces, Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Rapid7 Vulnerability Integration works easily with Vulnerability Response to map vulnerabilities to CIs and business services to determine impact and priority of potentially malicious threats. The Rapid7 Vulnerability Integration Run Status module is a graphical view of the status of Rapid7 Vulnerability Integration runs.

To view this data in the legacy view, navigate to **All** > **All Rapid7 Vulnerability Integration** > **Integration Run Status**.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Previous versions of Vulnerability Response

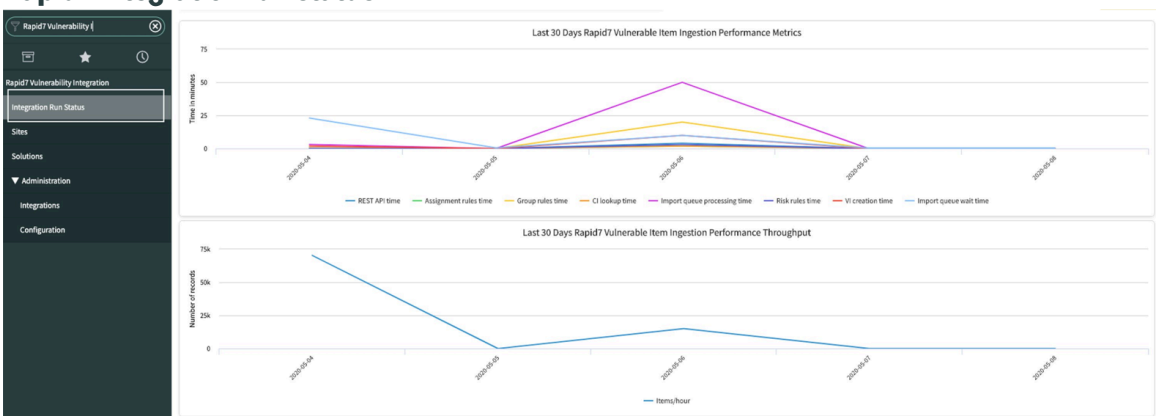
In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Two new graphs have been added to compare the performance metrics:

- Rapid7 Vulnerable Item Ingestion Performance Metrics: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance.
- Rapid7 Vulnerable Item Ingestion Performance Throughput: Compare daily vulnerable item ingestion throughput for the Rapid7 Vulnerable Item Integration - API. Throughput is measured in items per hour.

Note: In Rapid7, these graphs are supported only for the Insight VM integration.

Rapid7 integration run status



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample Rapid7 Vulnerability Integration run status chart



- The value in the Imported Items column represents the total number of vulnerable items that are created from an integration run.
- The New items column displays the number of vulnerable items that are created from an integration run.
- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.
- The Updated items column displays the number of times vulnerable items are updated during an integration run. This value is not the number of unique vulnerable items that are updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.
- The Unchanged items column displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: **New CIs**, **Existing CIs**, **New Items**, and **Updated Items** are filtered out of the **Rapid7 Integration Runs** list.

Rapid7 Vulnerability Integration run status chart reports

Name	Description
Last 30 Days Rapid7 Results	The number of integration runs completed for each integration. Shows both successful and failed runs. Run in a bar visual.
Last 30 Days Rapid7 New VIs	The number of new vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Rapid7 Updated VIs	The number of updated vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Rapid7 Duplicates	The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.
Rapid7 Integration Runs	The integration run records in a list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rapid7 Vulnerability Integration run status chart reports (continued)

Name	Description
	Note: V16.1: To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.
Last 30 Days Rapid7 Vulnerable Item Ingestion Performance Metrics	Daily performance metrics for vulnerable items compared for the last 30 days.
Last 30 Days Rapid7 Vulnerable Item Ingestion Performance Throughput	Daily vulnerable item ingestion throughput for the Rapid7 Vulnerable Item Integration - API measured for the last 30 days.

View the Rapid7 Vulnerability Integration import runs status dashboard

Use the Rapid7 vulnerability import run status dashboard to verify the success of your integration runs, locate any issues and inform your remediation decisions.

Before you begin

Roles required: sn_vuln.admin

About this task

This procedure makes the following assumptions.

- You have Vulnerability Response and the Rapid7 Vulnerability Integration installed and configured.
- Rapid7 Vulnerability Integration imports are scheduled and running.
- Rapid7 integration run status charts are in use.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 19.0 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **Rapid7** > **Integration Run Status**.

   Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

   Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

2. If you are not using the Rapid7 integration run status chart, navigate to **Rapid7** > **Integrations**.
   a. Choose an integration.
   b. Click the **Vulnerability Integration Runs** related list.
3. Verify that all imports have succeeded.

   Trouble?

   The most common causes for a failed run:

   - Network interruption
   - Bit decay in the data transfer resulting in corrupted data during the transform

   For all these conditions, click **Execute now** and rerun the integration.

Initiate rescan for the Rapid7 Vulnerability Integration

Initiate rescans in the Rapid7 platform to verify that your vulnerable items have been remediated between scheduled scanning cycles.

Before you begin

Note: Rescans for Rapid7 data warehouse vulnerable items are not supported.

You can initiate rescans from the Vulnerability Response workspaces. For more information, see Rescan records and remediation tasks in the Vulnerability Manager Workspace and Rescan vulnerable items and remediation tasks in the IT Remediation Workspace.

Roles required: Roles required: sn_vul.write_all or sn_vul.write_assigned

About this task

For rescans in the classic environment, see the following sections.

Rescans are supported. You can initiate a rescan on-demand for vulnerable items imported from Rapid7 InsightVM integrations from your ServiceNow AI Platform® instance.

Note: The Rapid7 scanner is deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have Rapid7 application as a source, the Rescan button is not available.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans from vulnerable item (VI), remediation tasks (RT)s, third-party entry (TPE), or discovered item records from your ServiceNow AI Platform® instance.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

As an example, your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Rapid7 vulnerable items. You can view updated results on your vulnerable items with the next scheduled import of Rapid7 InsightVM Vulnerability and Vulnerable Item Integrations.

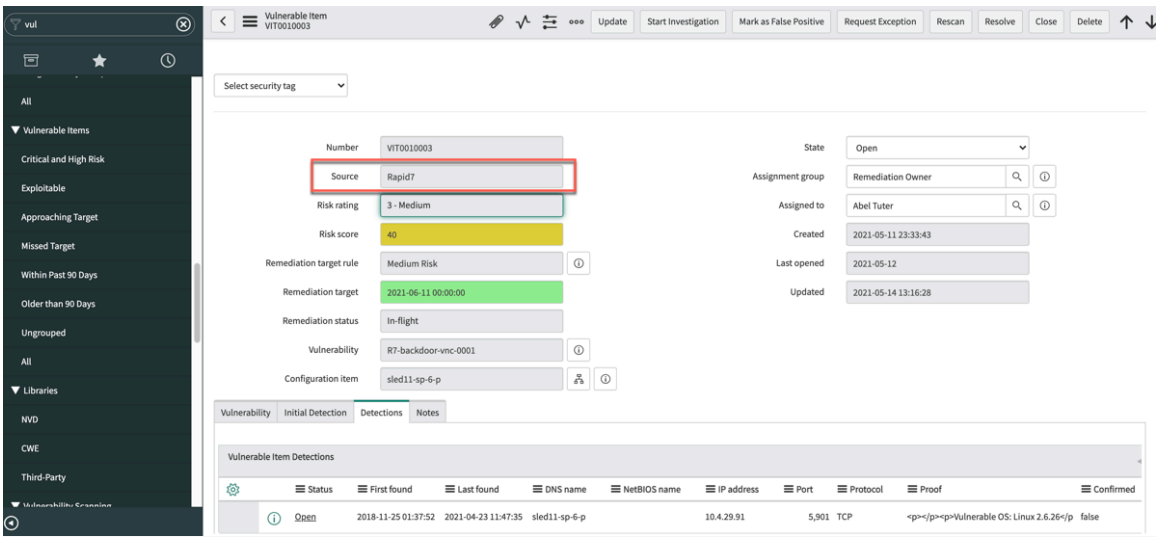
Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: Initiate rescans for VIs with Rapid7 as the source. Verify Rapid7 is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the **Source** column is not displayed on the VI List view, in the upper left of the list, click the gear icon and move **Source** from **Available** to **Selected**.

   When you initiate rescans, avoid simultaneously triggering scans for one source ID from multiple sources. The latest scan request will error out.

   For example, if you initiate a rescan for a VI from a VI record and also request another rescan from a remediation task record that contains that same VI, it is likely that the second request will fail.



3. Alternatively, navigate to **Vulnerability Response** > **Remediation Tasks** or **Vulnerability Response** > **Libraries** > **third party** for the remediation task or third-party entry records, respectively, that you want to use for the rescan.

   Depending on your choice, the **Rescan** button is available on the following records:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

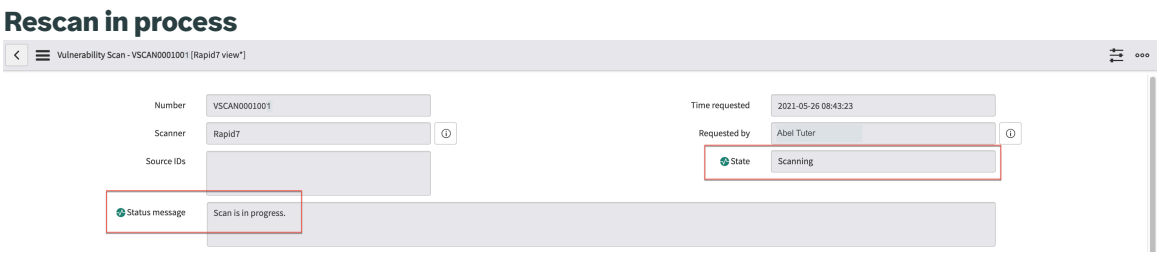
- On a single VI record, the VI must be from the Rapid7 product and in any state other than Closed. For multiple VI records, all the VIs you select from the list view must be from the Rapid7 product and in any state other than Closed.
- On an remediation task record, the remediation task can be in any state other than Closed, and all the associated VIs must be from the Rapid7 product.
- On a third-party entry (TPE) record, the record must have at least one associated VI record from the Rapid7 product in any state other than Closed.
- On a discovered item record, the VI must be from the Rapid7 product and in any state other than **Closed**.

4. In the upper right of the record, click **Rescan**.
   For list views, select the VIs from the list that you want to rescan, and, from the **Action on selected rows** list, select **Rescan**.
5. In the pop-up that is displayed, confirm the rescan.
   A message is displayed that indicates your scan is being processed (**Queued**). In the message, click the **View details** link to check the status of the rescan (child scan) and view any other rescans launched from the record. Status for all rescans can be found at any time under the Scans related list on the bottom of the VI, remediation task, TPE, and discovered item records you use to launch the rescans.

   When the scan is in process, the State field changes to **Scanning**, and the Status message field displays **Scan is in progress**.

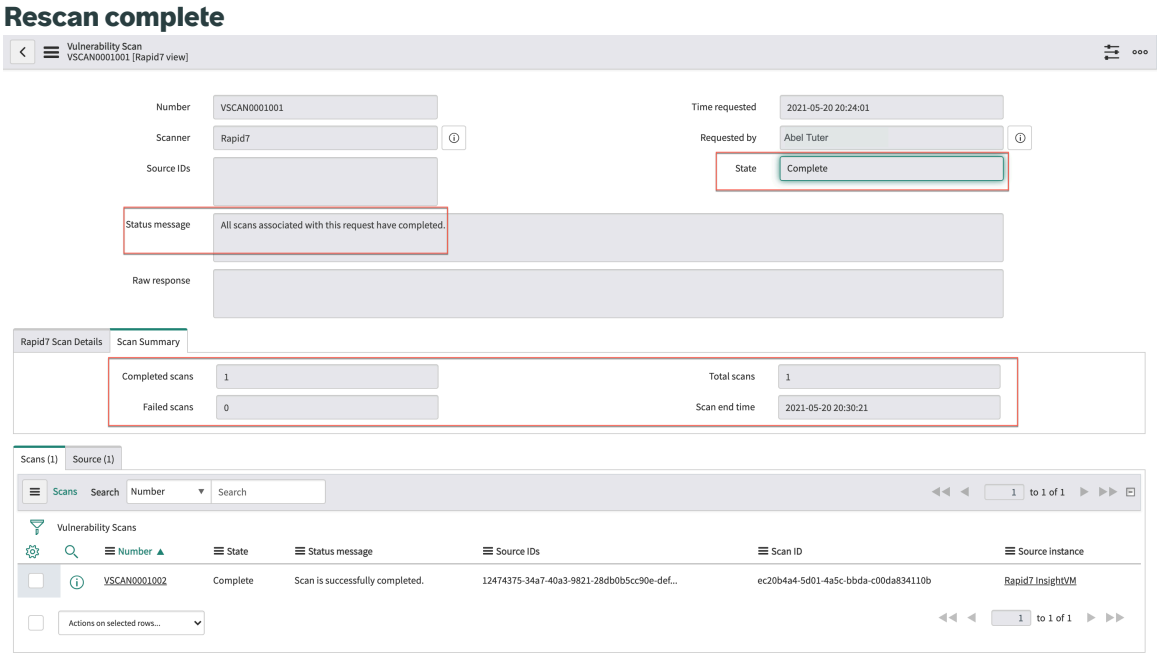
   Note: Each rescan supports 500 assets per scan. If your request has more than 500 assets, more child scans are requested.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first.



   The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to Closed/Fixed are imported with the next scheduled import of the Rapid7 integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Alternatively, you can initiate a rescan on-demand for a specific vulnerability on a specific asset. You can view the results from these scans once the scan has completed on the refreshed VI, remediation task, TPE, and discovered item records you launched the scan from.

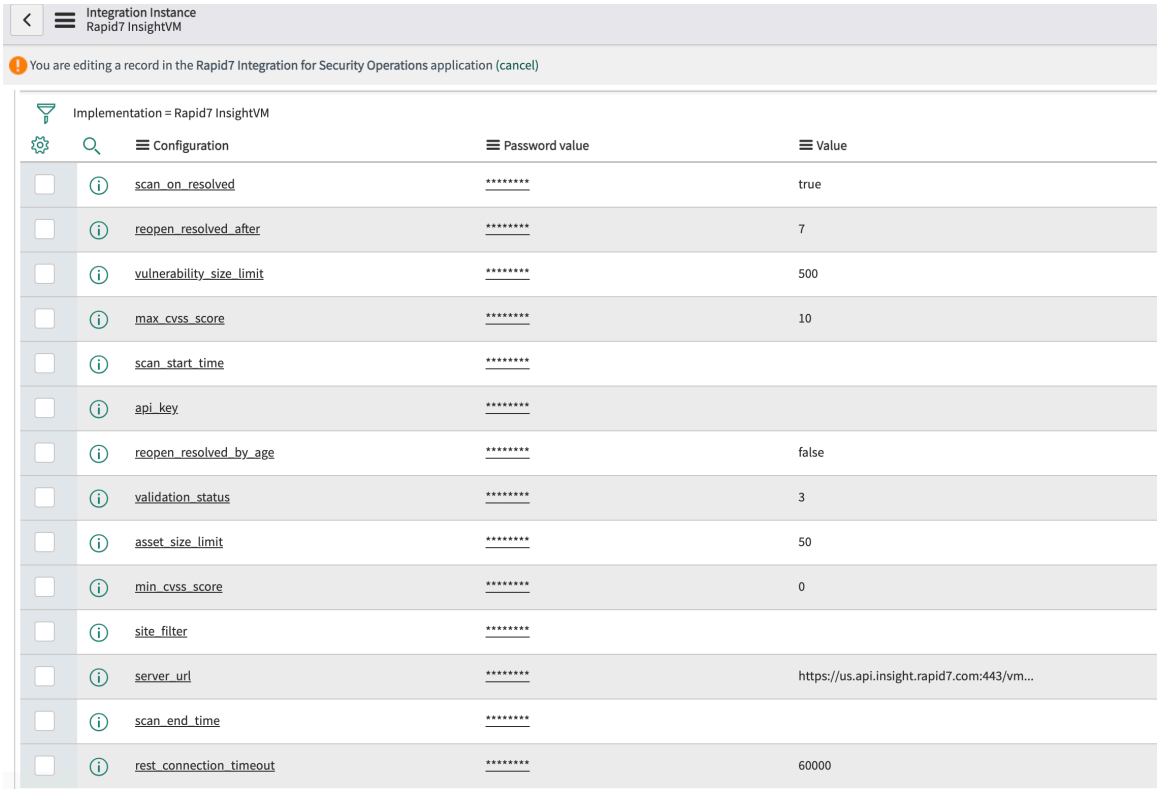
The value of the State field on Vulnerability Scan records is imported from Rapid7. When the scan is successfully finished, the state is set to Complete. If the scan does not successfully complete, an error value is displayed.

Auto Scans and Scheduled Scans

As a vulnerability manager or analyst, you can specify and schedule when rescans are initiated for VIs and RTs. You can also enable auto scans for VIs and remediation tasks that are set to resolve.

6. To modify the integration parameters on the integration instance, navigate to **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
7. On the Rapid7 Configuration record, if not selected, from the **Integration Type** list, select **Rapid7 InsightVM**.
8. To the right of the **Integration instance** field, click the information icon, followed by **Open Record**.
9. On the Integration Instance Rapid7 InsightVM record, locate the parameters for scheduling scans and edit as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



scan_on_resolved indicates if the scan is initiated when a vulnerability is resolved. Default is **false** (disabled).

If this parameter is set to `true`, whenever a VI or RT is set to Resolved, the workflow to rescan the respective VI and remediation task is triggered automatically.

scan_start_time

Set the scan start time in **HH:mm** (24 hours Format) in the UTC Time Zone for the start time of the window that you want rescans available.

The default value is 00 : 00.

scan_end_time

Set the scan end time in **HH:mm** (24 hours Format) in the UTC Time Zone for the end time of the available scan window.

The default value is 23 : 59.

If a scan is initiated within the scheduled time window, it launches instantly. If the scan is initiated outside of the window, it is queued for the next scheduled window.

For example, if you enter a start time of 00 : 00 for the *scan_start_time* parameter, and a *scan_end_time* of 10:00 AM that same morning, scans scheduled or manually launched outside of the midnight to 10 AM time window are queued and launched at the start time of the following day's time window 00 : 00.

In the same example, if you manually initiate a rescan at 11:00 AM, the rescan is not immediately launched, because it lies outside of the available configured scan times. The scan request remains queued until the start of the following day's time window, in this example 00 : 00.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set additional filter parameters for Rapid7 InsightVM imports

Customize the filtering parameters for your scheduled queries with the Rapid7 Integration for Security Operations to help you further refine the vulnerability data you import with the Rapid7 InsightVM product.

Before you begin

Use cases: As a vulnerability manager or analyst, you might want to filter data from your queries so that you can review only specific vulnerability details. For example, you might want to view only imported vulnerabilities that are `Critical` and `Severe`.

To help you gather this data, you add Rapid7 parameters to help you import the specific vulnerability details you need.

Without adding additional API calls or coding, starting with v13.4, feature permits you to customize your HTTP Request information with Rapid7 InsightVM parameters in your ServiceNow AI Platform. The following Rapid7 InsightVM Integrations support filtering by adding JSON content in the request body:

- Rapid7 InsightVM Vulnerable item Integration API
- Rapid7 InsightVM Vulnerability Integration API
- Rapid7 InsightVM

You should know how to use JSON strings for this feature.

Role required: sn_vul.vulnerability_admin

Procedure

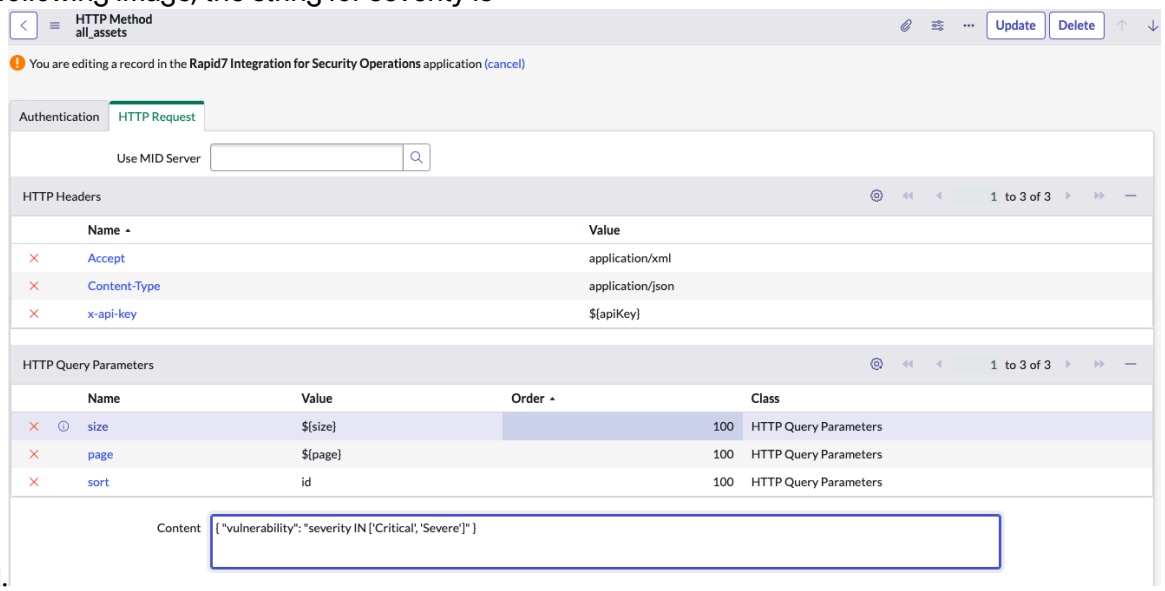
1. Locate the parameters supported by the Rapid7 InsightVM product on the Rapid7 developer site that you want to use for your filtering.

   You can create the parameters for the request body by referring to the Rapid7 documentation. Parameters and values you enter from the Rapid7 InsightVM product are supported only at the integration instance level.

2. Navigate to **All** > **Rapid7 Vulnerability Integration** > **Administration** > **Integrations**.
3. On the Rapid7 Integrations list page, click the record for the Rapid7 InsightVM integration that you want to open it.
4. On the right of the page, click the information icon (I) for REST message followed by **Open Record**.
5. With the HTTP Request tab selected, Under HTTP Methods, in the Name column, click an item to open its HTTP Query parameters.
6. Under HTTP method record, under HTTP Query Parameters, in the Content field, enter the parameter values you found on the Rapid7 developer site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following image, the string for severity is added.



If you want to enter more than one parameter, refer to the Rapid7 documentation for more information about how to separate each value.

7. Click **Update**.

Understanding the Shodan Exploit Integration

The ServiceNow® Shodan Exploit Integration application uses data imported from the Shodan search engine to help you determine the impact and priority of potentially malicious exploits.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Shodan Exploit Integration

The Shodan search engine collects exploit data and the Shodan API makes that database available to the ServiceNow AI Platform®. It easily integrates with the ServiceNow® Vulnerability Response application to map exploits to third-party vulnerabilities enriching the exploit data in your instance.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Every day, scheduled jobs invoke the integrations automatically in the order they are listed. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions

Release version for Xanadu	Release Notes
Shodan Exploit Integration v10.6, 10.7	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Roles

Shodan Exploit Integration tasks involve the following roles.

- sn_vul_shodan.admin: Users with this role can read, write, and delete records.
- sn_vul_shodan.user: Users with this role can read and write records.
- sn_vul_shodan.read: Users with this role can read records.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Shodan exploit integrations

To view the Shodan exploit integrations, navigate to **All** > **Shodan Exploit Integration** > **Integrations**.

The following integrations are included in the base system. These integrations are active by default.

Shodan exploit integrations

Integration	Description
Shodan ExploitDB Integration	Retrieves ExploitDB data from Shodan and enriches your third-party vulnerability data. This integration is set to run daily at 03:15:00.
Shodan Metasploit Integration	Retrieves Metasploit information from Shodan and enriches your third-party vulnerability data. This integration is set to run daily at 01:15:00.

To change the default start time for the scheduled integration imports, see Set Shodan Exploit Integration import time.

To view exploit data in third-party vulnerabilities, see View Vulnerability Response vulnerability libraries.

Changing other Shodan Exploit Integration settings requires advanced ServiceNow and Vulnerability Response expertise and is beyond the scope of the product documentation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Preparing for the Shodan Exploit Integration

A successful Shodan Exploit Integration requires planning and careful execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Shodan Exploit Integration assumes that you are familiar with the Shodan search engine and API.

Before you begin

The Shodan Exploit Integration requires an API key. Register with the Shodan website for a free subscription to acquire this key.

Role required: admin

About this task

Note: Before running the integration, make any necessary configuration changes based on your requirements.

- If you have not imported NIST Vulnerability Database (NVD) data into Vulnerability Response, do so before installing the Shodan Exploit Integration. Importing the NVD data ensures that your Common Vulnerability and Exposure (CVE) data auto-populates the exploit records.

  Without NVD data, a placeholder is created in the exploit record and not entered until the next NVD update. For more information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

- There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Install and configure the Shodan Exploit Integration for Security Operations

Before you can run the Shodan Exploit Integration in your instance, download and install it from the ServiceNow Store. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that you have valid ServiceNow entitlements for the Vulnerability Response application and the Shodan Exploit Integration for Security Operations application.	To verify entitlements, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. For more information about getting entitlements for a Security Operations application from the ServiceNow Store, see Get entitlement for a Security Operations product or application.

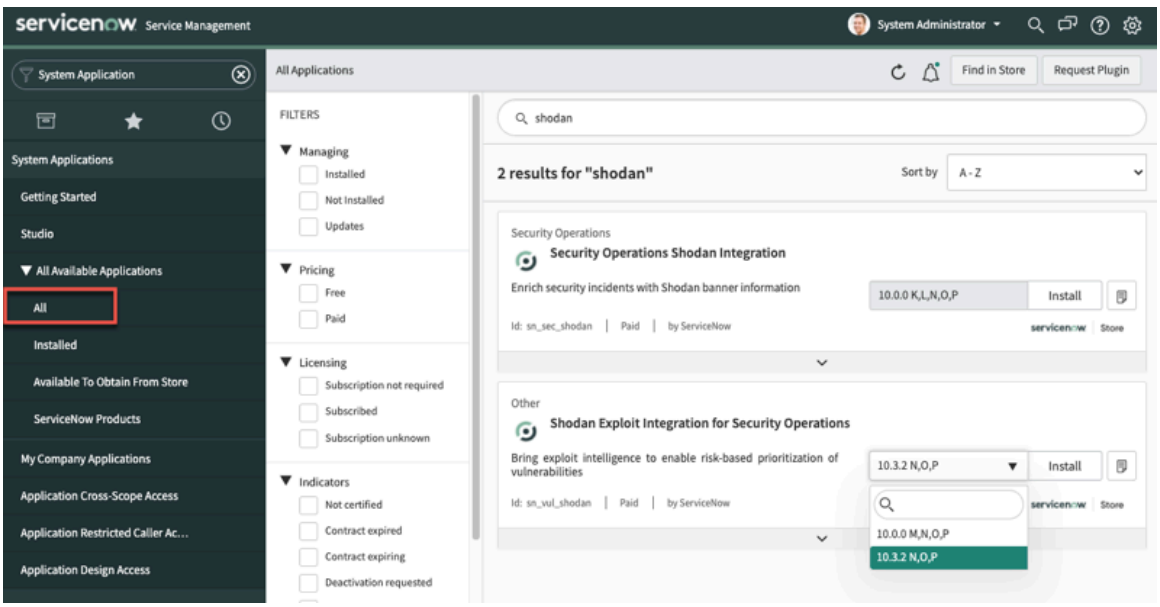
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application.	For more information about installing and activating the Vulnerability Response application, see, Install Vulnerability Response.
Have the Shodan Exploit Integration API key handy.	See Preparing for the Shodan Exploit Integration.

Role required: admin

Procedure

1. Log in to the ServiceNow AI Platform instance you want to install the Shodan Exploit Integration application on.
2. Navigate to **System Applications** > **All Available Applications** > **All**.
3. Locate the Shodan Exploit Integration for Security Operations application, select the version you want, and click **Install**.

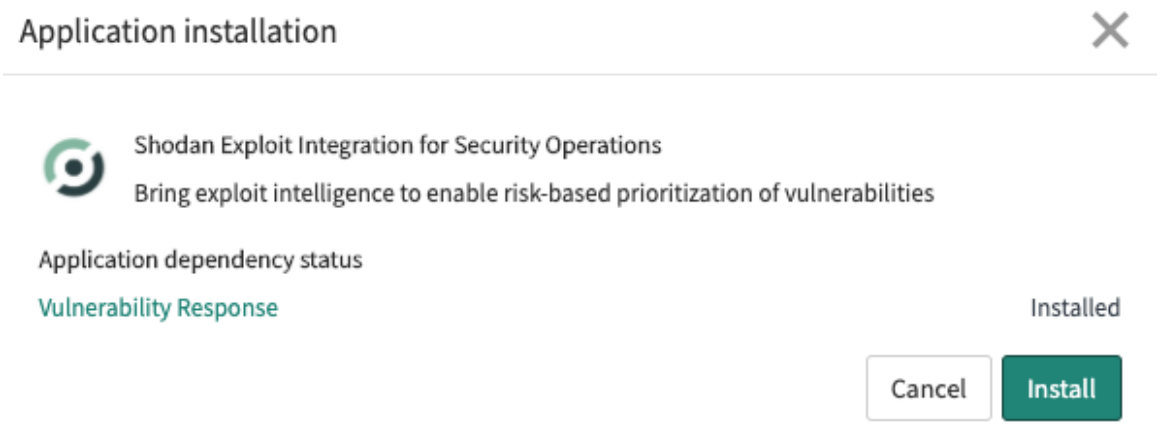


Note: If you are entitled to an update for this application, the **Update** button is displayed.

The Application installation dialog displays the application dependency status. Any required dependencies not already installed are automatically installed along with the application.

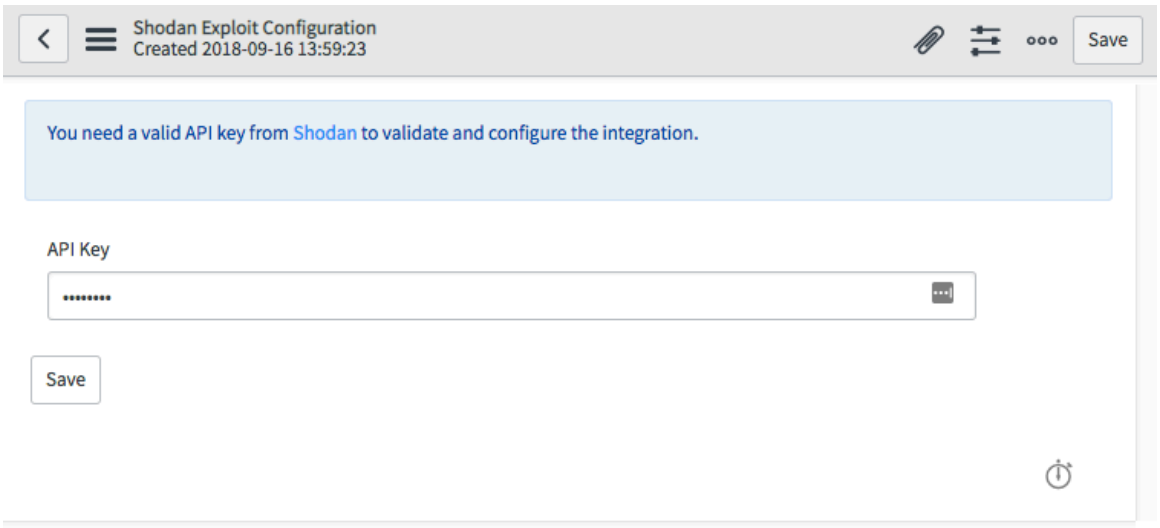
4. In the dialog, click **Install**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Install dialog indicates when the installation is successfully completed.

5. Close the Install dialog.
6. Navigate to **Shodan Exploit Integration** > **Configuration**.
7. Enter your Shodan API key.



8. Click **Save**.
   Your Shodan Exploit Integration configuration is complete.

Set Shodan Exploit Integration import time

For your convenience, you can reset the start time for the Shodan exploit integrations.

Before you begin

Role required: admin

About this task

After the initial import, Shodan exploit integrations bring in delta data unless a full import is requested. See Perform a manual Shodan exploit import for more information on full imports.

Procedure

1. Navigate to **All** > **Shodan Exploit Integration** > **Integrations**.
2. Choose an integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click the link to edit the record.
4. Set the new **Run** and **Time** options.
   Time is calculated as Hours in local time. The default time for the Shodan exploit imports is 03:15:00.
5. Click **Update**.
   The new time is used for the next scheduled import.

Perform a manual Shodan exploit import

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily scheduled job.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Shodan Exploit Integration** > **Integrations**.
2. Choose an integration.
3. Select the **Full data import** check box.
4. Click **Execute Now**.
   Once the import is complete, the check box is unchecked and delta imports resume.

View the Shodan Exploit Integration import run status

Use the Vulnerability Integration Runs related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin

To view the Shodan import run status:

- The Vulnerability Response application and the Shodan Exploit Integration must be installed and configured.
- The Shodan Exploit Integration imports must be scheduled and running.

Role required: sn_vuln.admin

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Shodan Exploit Integration** > **Integrations**.
2. Select an integration.
3. Click the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.

Trouble?

The most common causes for a failed run include:

- Network interruption
- Bit decay in the data transfer resulting in corrupted data during the transform

If you encounter any of these conditions, select the **Full data import** check box, click **Execute Now**, and rerun the integration.

Understanding the Tenable Vulnerability Integration

The Vulnerability Response Integration with Tenable application developed by ServiceNow engineering for the Tenable Vulnerability Integration uses data imported from the Tenable.io, Tenable.sc, and Tenable.cs products to help you prioritize and remediate vulnerabilities for your assets. The application is available with a separate subscription from the ServiceNow® Store.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

The Tenable Vulnerability Integration employs three Tenable integrations, Tenable.io, Tenable.sc and Tenable.cs, to import third-party scanner data about your assets and vulnerabilities. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13 and Tenable.cs product starting with version 5.0.1.

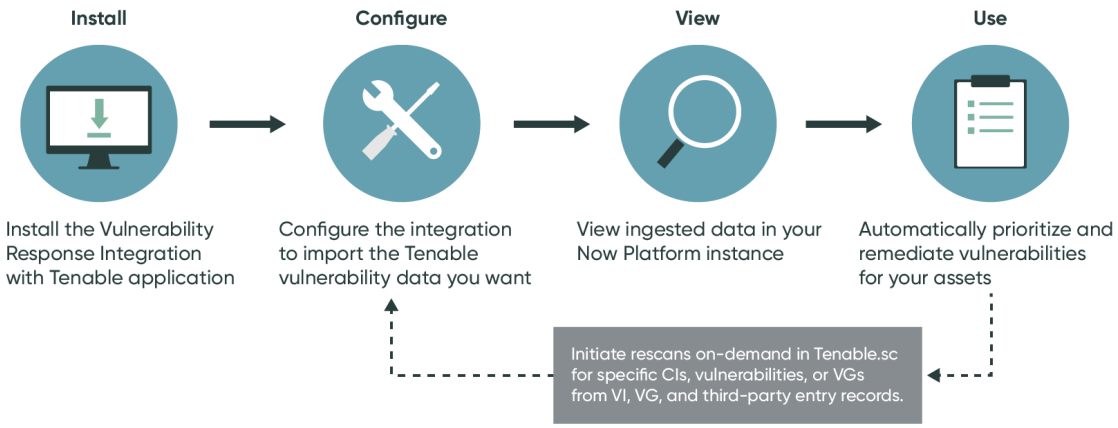
- Tenable.io is a cloud-based enterprise integration.
- Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Tenable.sc product and your ServiceNow AI Platform instance are in the same environment.
- If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server.
- Tenable.cs is a cloud-based enterprise integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Vulnerability Response Integration with Tenable application is available on the ServiceNow Store with a separate subscription.

For lists and descriptions of the integrations in the Tenable Vulnerability Integration, see Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications and Tenable.sc integrations with the Vulnerability Response application.

Tenable Vulnerability Integration



Available versions for Xanadu

Release version	Release notes
Vulnerability Response Integration with Tenable v3.13.1, v4.1, v5.0.1	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Terms and Key features of the integrations

Vulnerable items and vulnerabilities

A vulnerable item is created in your ServiceNow AI Platform instance when:

- An imported vulnerability from a third-party scanner is matched to an existing asset (a configuration item in your CMDB). The Tenable product refers to these matches as **vulnerabilities**.
- An imported vulnerability from a third-party scanner isn't matched to an existing asset in your CMDB. In this case, an unmatched CI is also created along with a vulnerable item.

  For unmatched CIs, you can also use the Identification and Reconciliation Engine (IRE) to create CIs in two new classes when an existing CI can't be matched with a host. Otherwise, unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine.

Third-party vulnerability entries and plugins

Third-party vulnerability entries are imported from third-party scanners and listed in the Third-Party Vulnerability Entries table in your ServiceNow AI Platform instance. Starting with v24.0 of Vulnerability Response, the Softwares column in the Third-Party Vulnerability Entries table populates the Common Platform Enumerations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(CPEs) associated with a third-party entry. Third-party vulnerability entries from Tenable are ingested into Vulnerability Response and matched to existing assets listed in your CMDB. Tenable refers to third-party vulnerability entries as **Plugins**.

Configuration item (CI)

Configuration items are the existing assets listed in your CMDB.

Discovered item

Assets ingested from the Tenable asset import are matched to existing configuration items in your CMDB. Imported assets are updated.

If a match isn't found, a CI is created in the Unmatched CI class of the CMDB. If the CMDB CI Class Models plugin is enabled, the Identification and Reconciliation Engine (IRE) creates CIs using new classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. If the original, unmatched CI is reclassified, discovered item records are updated to reflect the state. Discovered items give you visibility into how assets are identified and mapped to CIs in the CMDB.

CI lookup rules

When data is imported from a third-party integration, Vulnerability Response automatically uses host (asset) data to search for matches in the Configuration Management Database (CMDB). CI lookup rules are used to identify CIs and add them to VI records when VITs are created to aid you with remediation.

Rescan and remediation scan

You can initiate a targeted rescan command on a specific configuration item, remediation task, or third-party entry directly from vulnerable item, remediation task, and third-party vulnerability entry records in your ServiceNow AI Platform instance. Tenable refers to this rescan as a **remediation scan**.

Automatically close older VIs

With the Auto-Close Stale Vulnerable Items module in your ServiceNow AI Platform, you can clean up older, stale vulnerable items (VI)s not recently found by your third-party integrations. Moving these VIs to **Closed** helps you reduce the number of active vulnerable items and remediation tasks and reconcile assets in your CMDB. You can use all the integrations with the Vulnerability Response Integration with Tenable to close stale VIs automatically.

Instance

This term refers to a distinct occurrence of your ServiceNow AI Platform® application.

Integration

An integration is a product-specific reference to an integration, such as the Tenable.io Assets Integration, or the Tenable.sc Plugin Integration. These are the separate integrations that belong to specific Tenable products in the Tenable Vulnerability Integration in your instance.

Integration instance

This term refers to the separate Tenable integrations listed by their Tenable.io and Tenable.sc products.

Deployment

When an integration supports multi-source, a single, distinct integration existence is referred to as a deployment of your integration. The term is used to refer to the integration(s) and products across your environment. For example, you might have multiple deployments of various integrations of the Tenable.io and Tenable.sc products in your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Tenable.io, Tenable.sc, and Tenable.cs integrations also include the following key features:

- Configuration assessment findings, that is, test results along with policies, configuration tests (controls), and citations with authoritative sources can be imported into the Configuration Compliance application with the Tenable.io product. See Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications and Exploring Configuration Compliance for more information about how this integration works with the Configuration Compliance application.
- Starting with v2.1 of the Tenable Vulnerability Integration, create unique configuration items (CIs) that include different network partition identifiers for assets in your environment that share the same IP address. Identify the distinct assets across your environment and update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.
- You can schedule when you want the jobs to run for all the Tenable.io, Tenable.sc and Tenable.cs integrations. You can also execute scheduled jobs manually on-demand.
- For asset imports with Tenable.io, you can enable asset tags to organize and track the assets listed in your CMDB in the Tenable.io environment.
- The Tenable.io, Tenable.sc and Tenable.cs integrations permit you to configure CI Lookup Rules to define how asset data from third-party sources are used to identify Configuration Items (CIs) in your ServiceNow AI Platform CMDB.
- The Tenable.io, Tenable.sc and Tenable.cs integrations permit you to set import filters on the vulnerabilities import so that you import only the vulnerabilities from Tenable that you want. For Tenable.io, you have the option to import **Fixed** vulnerabilities from Tenable with the vulnerabilities import.
- For Tenable.sc, you have the option to initiate rescans on-demand directly from a vulnerable item, remediation task, and third-party entry records in your ServiceNow AI Platform instance. If VIs have been transitioned to **Closed/Fixed** but aren't yet updated in your instance, you can verify vulnerabilities on specific configuration items have been remediated. See Initiate rescan for the Tenable.sc integration.

The following sections list more details about the Tenable integrations.

Required ServiceNow AI Platform roles

The integration tasks require the following roles in your ServiceNow AI Platform instance.

admin

The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant.

sn_vul.vulnerability_admin

Once assigned, the vulnerability admin completes the configuration of the Tenable integrations in Setup Assistant. This role has complete access to the Vulnerability Response (VR) application and its records. The vulnerability admin configures all VR applications and rules for installed third-party integrations.

sn_vul_tenable.configure_integration

This role contains the sn_vul_tenable.read_integration granular role and users with this role can configure the Vulnerability Response Integration with Tenable application.

sn_vul_tenable.read_integration

Users with this roles can view (read) but not edit records of the Vulnerability Response Integration with Tenable application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response group

By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically.

Vulnerable items

Vulnerable items are grouped into remediation tasks according to remediation task rules and assigned for remediation based on your assignment rules. For more information, see Vulnerability Response remediation tasks and remediation task rules overview and Vulnerability Response assignment rules overview.

Configuration item (CI) lookup rules

CI Lookup Rules identify CIs and determine when to add them to a vulnerable item. For more information on how CI lookup rules work, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

Note: Rules, once removed, can't be recovered. Rather than removing existing rules, disable them when creating ones.

The following Tenable.io lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Note: The Tenable.io CI lookup rules prioritize and populate the non-empty network interface values (FDQN, IPV4, and MacAddress) over the regular FDQN, IPV4, and MacAddress values for a discovered item. When these network interface values are empty, the regular FDQN, IPV4, and MacAddress values are populated for a discovered item.

The following Tenable.sc lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Note: Multiple values for ip_address, mac_address, fqdns and network_interfaces are used for an asset. All values are considered in CI lookup rules for matching. All values are used to create multiple network adapters using IRE.

The Tenable.cs lookup rule Cloud Resource Id is shipped with the base system.

For more information on how to configure the categorization of unmatched cloud resources into your preferred CI class, see Updating CI class for unmatched cloud assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

New properties to ignore IP addresses

In Tenable.io, there are two properties available if you want to ignore multiple IP addresses or multiple Mac addresses as part of your CI lookup rules:

ignoreIPAddress

A list of IP addresses to be ignored for CI lookup and CI creation.

ignoreMacAddress

A list of MAC addresses to be ignored for CI lookup or CI creation.

Discovered items

This module lists configuration items detected during import from the Tenable Vulnerable Item integrations and the Tenable Asset integrations.

Note: The default filter for this list is set to `Unmatched`. You can view all discovered items from an import by removing the filter.

For more information on the Discovered Items module, see Discovered Items.

Asset tags

Asset tags (also referred to as host tags) are used for organizing and tracking the assets in your organization. You can assign tags to your assets. Then, when launching the scans, you can select tags associated with the assets you want to scan. The Asset Tags module enables you to download asset tag data from Tenable.io to your instance on a scheduled basis. Asset data that includes asset tags is pulled from Tenable.io and transformed using the Tenable.io Asset Transform integration transformation maps.

All Asset tags are imported as part of the Tenable.io Asset integration. Asset tags are used for filtering in Vulnerability Response assignment rules and Remediation Task Rules. The tags are displayed in the Discovered Item form.

Note: Run the Tenable.io Asset Integration prior to creating Vulnerability Response assignment rules or remediation task rules in the Vulnerability Response application so that all tags are available for these rules before vulnerable items are imported and grouped. Also note the following points about tags:

- Tag storage isn't case-sensitive. For example, if you create a tag to describe assets in your San Diego location, and you create the `San Diego` tag, you can't also create a `SAN DIEGO` tag and store it in the Asset tag table. `San Diego` and `SAN DIEGO` are considered to be the same asset tag by the system. Whichever tag is imported first is the tag that is stored and recognized going forward.
- Using asset tags as a Group Key in a remediation task rule may have unexpected results. Asset tags are intended for use only in the condition builder.
- Asset tags are controlled by the global system property sn_vul.import_asset_tags. This property is set to `true` by default. Disabling tags disables them across all ServiceNow AI Platform® instances.

Data retrieval filters

Data retrieval settings help you determine specifically the type and scope of data you want to import from the Tenable application to your ServiceNow AI Platform® instance. For a list of the most commonly used settings, see Data retrieval settings for the Tenable Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Priority Rating (VPR)

The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with a new default risk calculator in Vulnerability Response. The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response.

This risk rule is inactive by default.

By enabling the Tenable risk calculator rule, the imported VPR values are used to calculate the Risk Score for vulnerable items. The default weight distribution for this risk calculator: VPR = 70%, Asset=15%, and Business Criticality=15%. Enabling this Tenable Risk Calculator rule may impact your data ingestion performance. For more information about Vulnerability Response calculators and the Tenable risk calculator rule, see Vulnerability Response calculators and vulnerability calculator rules.

Installation and configuration

After you download the Vulnerability Response Integration with Tenable from the ServiceNow® Store, installation and configuration is supported by the Setup Assistant in Vulnerability Response. See Configuring Vulnerability Response using the Setup Assistant for more information.

Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications

The Tenable.io integrations in the Vulnerability Response Integration with Tenable with Tenable application are available for use with both the Vulnerability Response and Configuration Compliance applications.

List of Tenable.io integrations

The Tenable.io and Tenable.sc integrations support multi-source deployments. You can add and deploy multiple instances of these integrations across your environment using Setup Assistant in Vulnerability Response. You also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

Tenable.io is a cloud-based enterprise integration. The following sections describe the supported Tenable.io integrations and their behavior.

Starting with v 6.1.3, the Tenable.io Compliance Results Integration is replaced by two separate integrations, the Tenable.io Fixed Compliance Results Integration and the Tenable.io Open Compliance Results Integration. The original Tenable.io Compliance Results Integration is no longer available. Compliance results are now imported separately based on their status, improving ingestion performance for your environment if you have large volumes of compliance data.

Tenable.io integrations

The following table lists the supported integrations for the Tenable.io product.

Integration	Description
Tenable.io Assets Integration	Retrieves all asset data, including asset tags, from the Tenable.io product. Creates unique CIs for unmatched assets.
Tenable.io Compliance Results Integration	Retrieves secure configuration assessment data from Tenable.io and processes it in your ServiceNow AI Platform instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	Imported data includes compliance test results along with associated policies, configuration tests (controls), and citations with authoritative sources. Starting with v 6.1.3, this integration is replaced by the Tenable.io Fixed Compliance Results Integration and Tenable.io Open Compliance Results Integration.
Tenable.io Fixed Compliance Results Integration	Retrieves compliance test results in a fixed state (Passed, Skipped) and processes associated policies, tests, and citations.
Tenable.io Open Compliance Results Integration	Retrieves compliance test results in an open state (Failed, Warning, Error, Unknown) for investigation and remediation. Triggered after the Tenable.io Fixed Compliance Results integration.
Tenable.io Compliance Results Backfill Integration	Matches compliance results with assets that were previously missing. Runs automatically after the Assets Integration and removes resolved entries from the missing asset table.
Tenable.io Scan Credential Integration	Retrieves scan credentials configured in Tenable.io for use in rescan requests. Runs weekly.
Tenable.io Template Integration	Retrieves available Tenable.io credentials for rescans. Stores a single template record temporarily.
Tenable.io Plugin Integration	Retrieves plugin data from Tenable.io to keep Tenable Identifiers (Ten IDs) current.
Tenable.io Fixed Vulnerabilities Integration	Retrieves vulnerability data based on severity filters. Outputs Closed/Fixed vulnerable items. Scheduled; chains to Open.
Tenable.io Open Vulnerabilities Integration	Retrieves open vulnerability data. Triggered after the Fixed Vulnerabilities integration. Outputs New/Reopened VIs.
Tenable.io Scan Metadata Integration	Retrieves scan metadata from the `/scans` endpoint using the `last_schedule_id` from existing asset data and associates scan records with discovered items and vulnerabilities.

Tenable.io Assets Integration

Retrieves all asset data, including asset tags, from the Tenable.io product and processes it in your instance.

- Starting with v3.0, if the Tenable.io Compliance Results Integration is activated, you can import secure configuration assessment data along with imported asset data. This data can help you identify and respond to configuration-related vulnerabilities on your assets.
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Asset API.
- The output of this integration is discovered items.
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.
- Starting with v2.2, Last Scan Time is imported and updated only for assets that have vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results Integration

Note: Deprecated starting with v 6.1.3. This integration is replaced by the Tenable.io Fixed Compliance Results Integration and the Tenable.io Open Compliance Results Integration.

This integration retrieves all secure configuration assessment data and processes it in your ServiceNow instance. Imported data includes test results along with policies, configuration tests (controls), and citations with authoritative sources.

- Assessment data for missing assets or assets without asset IDs aren't imported.
- If a test result is imported and its corresponding asset couldn't be matched in your instance, the test result is ignored and the ID for the missing asset is stored in a temporary record in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets are listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Tenable.io Fixed Compliance Results Integration

Retrieves secure configuration assessment data for compliance test results with a status of Passed or Skipped and processes it in your ServiceNow instance.

- Imported data includes test results along with associated policies, configuration tests (controls), and citations with authoritative sources.
- This integration is scheduled and executes first in the compliance chain. Upon successful completion, it automatically triggers the Tenable.io Open Compliance Results Integration, provided the Open integration is active and configured in the **Next Integration** field.
- Assessment data for missing assets or assets without asset IDs isn't imported.
- If a test result is imported and its corresponding asset can't be matched in your instance, the test result is ignored and the missing asset ID is stored in a temporary record in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets is listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Tenable.io Open Compliance Results Integration

Retrieves secure configuration assessment data for compliance test results with a status of Failed, Warning, Error, or Unknown and processes it in your ServiceNow instance.

- This integration is triggered upon successful completion of the Tenable.io Fixed Compliance Results Integration.
- By default, this integration is configured to run on demand. You can modify the scheduling configuration from the integration record in **Tenable Vulnerability Integration** > **Integrations**.
- Assessment data for missing assets or assets without asset IDs isn't imported.
- If a test result is imported and its corresponding asset can't be matched in your instance, the test result is ignored and the missing asset ID is stored in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets is listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Execution behavior for the split compliance results integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Fixed Compliance Results Integration is designed to execute first. When active, it automatically triggers the Open Compliance Results Integration upon successful completion, provided the Open integration is active and configured in the **Next Integration** field of the Fixed integration record.
- If the Fixed Compliance Results Integration is inactive or encounters an error during execution, the Open Compliance Results Integration isn't triggered. You must execute it manually or configure its own schedule.
- Execution details and error information are captured in the integration run record.

Upgrade considerations

- If you are upgrading from an earlier release, your existing compliance data remains unchanged. The Fixed and Open Compliance Results integrations preserve their configured Start time and continue fetching data incrementally from where the previous integration left off.
- To continue ingesting compliance results, ensure that both integrations are active.
- You can modify scheduling behaviour or disable automatic chaining as needed.

Both the Fixed and Open Compliance Results integrations use the same Tenable.io Compliance Results Transform map and import data into the Tenable.io Test Results Import [sn_vul_tenable_io_tr_import] table. The data mapping behaviour remains unchanged.

Tenable.io Compliance Results Backfill Integration

When activated, this integration runs automatically after the Assets integration completes as part of a chained integration run. It matches configuration assessment data with missing assets listed in the `sn_vul_tenable_missing_asset` table.

- Imports up to 200 asset IDs for any missing assets discovered or present in your instance after the Assets integration import completes successfully.
- Removes the temporary records from the `sn_vul_tenable_missing_asset` table when assets can be matched with corresponding configuration assessment data.
- Coordinates the REST message calls to the Compliance Export API.

Tenable.io Scan Credential Integration

Retrieves the scan credentials configured in Tenable.io for use in rescan requests initiated from the ServiceNow AI Platform.

- Coordinates the REST message calls to the Credentials API.
- The output of this integration is scan credentials populated in the `sn_vul_tenable_scan_credential` table.
- The imported credentials are used to access the scanner when you initiate scan requests from the ServiceNow AI Platform.
- This integration is scheduled to run weekly.

Tenable.io Template Integration

A template record is sent to Tenable.io during rescan. This integration retrieves available Tenable.io credentials to use for rescans. Credentials are instance-specific, and a single template record is imported and securely stored temporarily on the `sn_vul_tenable_io_template` table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Plugin Integration

Retrieves the plugin data from the Tenable.io product to keep Tenable Identifiers (Ten IDs) current.

- Retrieved data is based on the date that the plugins were last updated by a Tenable.io integration run.
- Coordinates the REST message calls to the Plugin API.
- The output of this integration is third-party vulnerabilities.

Tenable.io Fixed Vulnerabilities Integration

Retrieves vulnerability data based on severity filters from the Tenable.io product and processes it in your instance.

- Vulnerable items are created for detection records in the Open and Reopened states because these records require remediation. Existing vulnerable items are updated if detections are Fixed, but vulnerable items aren't created for Fixed detections by default because Tenable considers Fixed vulnerabilities Mitigated.
- When you activate the flag **Create vulnerable items for Fixed Vulnerability detections** in Setup Assistant, new VIs are created in the Fixed state so you have visibility into the detections that created them. Since VIs are created for Fixed detections that don't exist in your instance, this might negatively impact your import performance. You may prefer to leave this feature deactivated so that Fixed detections only update the states of existing vulnerable items.
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Vulnerabilities API.
- The output of this integration is Closed/Fixed vulnerable items (VIs). It also creates assets and third-party entries if they don't exist.
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.

This integration run is scheduled. It's a chained integration, which means after a run is successfully completed, the Open Vulnerabilities integration is triggered.

Starting from Tenable v3.3, you can view the following information for vulnerability integration runs:

- **Total chunks**: The total number of chunks being generated by Tenable.
- **Available chunks**: Number of chunks available for download for ServiceNow.

Tenable.io Open Vulnerabilities Integration

This integration is triggered upon successful completion of the Tenable.io Fixed Vulnerabilities Integration.

- Retrieves vulnerability data based on the severity filters from the Tenable.io product and processes it in your instance.
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Vulnerabilities API.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The output of this integration is New/Reopened vulnerable items (VIs). It also creates configuration items and third-party entries if they don't exist. Tenable considers active vulnerabilities Cumulative (current).
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.

Starting from Tenable v3.3, you can view the following information for vulnerability integration runs:

- **Total chunks**: The total number of chunks being generated by Tenable.
- **Available chunks**: Number of chunks available for download for ServiceNow.

Tenable.io Scan Metadata Integration

Retrieves metadata from the /scans endpoint. It pulls scan information based on the last_schedule_id from the existing asset data in Tenable.io.

- Table Creation: A new custom table, `sn_vul_tenable_scan`, stores scan metadata retrieved from the Tenable.io /scans endpoint, including scan ID, name, status, start time, end time, and scan type.
- Data Association: A reference field is established between discovered items (configuration items or vulnerabilities) and the corresponding latest scan record in the `sn_vul_tenable_scan` table. This linkage enables you to:
  - View the most recent scan information associated with each discovered item.
  - Improve the context for vulnerability triage and remediation decisions.
  - Enhance auditability and reporting capabilities by maintaining a historical record of scan activities.

Activate Tenable.io integrations

The Tenable.io Compliance Results Integration and the Tenable.io Compliance Results Backfill Integration are inactive by default. Follow these steps to activate an integration:

1. Navigate to **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
2. From the **Tenable Integrations** list, open the integration record.
3. Select the **Active** check box.
4. Select **Update**.

You can keep the default schedule settings when activating these integrations initially.

Note: Starting with v 6.1.3, the original Tenable.io Compliance Results Integration is no longer available. You must activate both the Fixed and Open Compliance Results integrations to continue ingesting compliance data.

Tenable.sc integrations with the Vulnerability Response application

The Tenable.sc integrations in the Vulnerability Response Integration with Tenable application.

Starting with Vulnerability Response v20.0, if an asset is scanned by an agent, the "Agent exists" column in the Discovered Items list displays the value as "true." This indicates that the scan is authentic.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

List of Tenable.sc integrations

Multi-source is supported for all the Tenable.io and Tenable.sc integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You can also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

- Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Tenable.sc product and your ServiceNow AI Platform instance are in the same environment.
- If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server.

Tenable.sc integrations

Integration	Description
Tenable.sc Assets Integration	To avoid creating duplicate discovered items with imported asset data, the Asset Integration of the Tenable.sc product is comprised of two integrations. **The Tenable.sc Open Assets Integration** This integration imports vulnerability data about your assets that Tenable considers **Cumulative** (current), or **Open**. The vulnerable items (VIs) that are created in your instance with this imported asset data are considered open, that is, in the **Open** state. These vulnerable items require investigation and might need remediation. **The Tenable.sc Fixed Assets Integration** This integration imports vulnerability data about your assets that Tenable considers **Mitigated** (no longer vulnerable) or **Fixed**. The vulnerable items for these assets transition from the **Open** state to the **Closed/Fixed** state in your instance, because the results of scans show they're no longer vulnerable. • Retrieves all asset data from the Tenable.sc product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Assets API. • The output of this integration is discovered items. • The Tenable query filter that you select in the Setup Assistant also applies to the Tenable.sc Assets Integration. Only the assets with the vulnerabilities that match the conditions of the query filter are imported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
Tenable.sc Plugin Integration	• Retrieves the plugin data from the Tenable.sc product. Retrieved data are based on the date that the plugins were last updated by a Tenable.sc integration run. • This import ensures that the Tenable.sc Identifiers (Ten IDs) are current and only active vulnerabilities are imported. • Coordinates the REST message calls to the Plugins API. • The output of this integration is third-party vulnerabilities.
Tenable.sc Fixed Vulnerabilities Integration	• Retrieves vulnerability data based on severity filters from the Tenable.sc product and processes it in your instance. Vulnerable items are created for detection records which are in the **Open** and **Reopened** states, because these records require remediation. Existing vulnerable items are updated by Vulnerability Response if detections are **Fixed**, but vulnerable items aren't created for **Fixed** detections by default, because Tenable considers **Fixed** vulnerabilities **Mitigated**. • When the flag **Create vulnerable times for Fixed Vulnerability detections** is activated in Setup Assistant, it creates VIs in the **Fixed** state so you have visibility into the detections that created them. As VIs are created for **Fixed** detections that don't exist in your instance, this might negatively impact your import performance. You may prefer to leave this feature deactivated so that **Fixed** detections only update the states of existing vulnerable items. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is **Closed/Fixed** vulnerable items (VIs). It also creates assets and third-party entries if they don't exist. This integration run is a scheduled run. It's a chained integration which means after a run is successfully completed, the Tenable.sc Open Vulnerabilities Integration described next is triggered. **Note:** By default, the family IDs 0 and 39 are excluded from this integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
Tenable.sc Open Vulnerabilities Integration	• This integration is triggered on successful completion of the Tenable.sc Fixed Vulnerabilities Integration. • Retrieves vulnerability data based on the query filters selected from the Tenable.sc product and processes it in your instance. • Creates corresponding vulnerable items for active vulnerabilities. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Vulnerabilities API. • The output of this integration is **Update/Create new** vulnerable items (VIs) if they don't exist. It also creates configuration items and third-party entries if they don't exist. **Note:** By default, the family IDs 0 and 39 are excluded from this integration.
Tenable.sc Scan Credential Integration	• This integration retrieves the scan credentials configured in Tenable.sc. • Coordinates the REST message calls to the Credentials API. • The output of this integration is scan credentials populated in table, [sn_vul_tenable_scan_credential]. • The imported credentials are used to access the scanner when scan requests are initiated from the ServiceNow AI Platform. • This integration is scheduled to run weekly.
Tenable.sc Backfill Vulnerabilities Integration	• This backfill integration imports any open and fixed vulnerabilities that might have been missed during an import. • This integration imports both open and fixed vulnerabilities from the last seven days to update your detections and vulnerable items. • This integration might impact your performance. • This integration is inactive by default. • To update your vulnerability data and avoid potential performance problems, you might prefer to schedule the Tenable.sc Fixed Vulnerabilities and Open Vulnerabilities Integrations to run when no other scans are running. • The output of this integration is:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
	○ **Closed/Fixed** vulnerable items (VIs). It also creates assets and third-party entries if they don't exist. ○ to **Update/Create new** vulnerable items (VIs) if they don't exist. It also creates configuration items and third-party entries if they don't exist.

User authentication and Tenable.sc

User authentication is supported by your ServiceNow AI Platform® instance and version 5.13 of the Tenable.sc product. User authentication is required if you're using version 5.12 and earlier of the Tenable.sc product.

When you select user authentication for the Tenable.sc integrations, tokens might expire and be replaced during integration runs. In the Notes column on the Vulnerability Integration Run record (VIN), the following message is displayed for a process when a token expires, `Error: Token validation is failed`. No action is required if this message is displayed. Expired tokens are automatically refreshed in the background and the message doesn't indicate a pause or error with the integration process.

Tenable.cs integrations with the Vulnerability Response and Container Vulnerability Response application

The Tenable.cs integrations in the Vulnerability Response Integration with Tenable application are available in the Vulnerability Response and Container Vulnerability Response applications.

Starting with v20.0 Vulnerability Response, if an asset is scanned by an agent, the "Agent exists" column in the Discovered Items list displays "true," indicating that the scan is authentic.

List of Tenable.cs integrations

Multi-source is supported for all the Tenable.io, Tenable.sc, and Tenable.cs integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You can also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

Tenable.cs is a cloud-based enterprise integration. See the following table for the names and descriptions of the supported integrations for the Tenable.cs product.

Tenable.cs integrations

Integration	Description
Tenable.cs Cloud Container Assets Integration	• Retrieves all container asset data from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. Coordinates the REST message calls to the Asset API. The output of this integration is Discovered Container Images, Docker Images, and Container Repositories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs integrations (continued)

Integration	Description
Tenable.cs Open Cloud Container Vulnerabilities Integration	When activated, this integration runs automatically after the container assets integration is successfully completed as part of a chained integration run. • Retrieves container vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopenedcontainer vulnerable items (CVIs). If they don't exist, it also creates discovered container images, docker images, container repositories, image findings, third-party entries, and Common Vulnerabilities and Exposures (CVE).
Tenable.cs Fixed Cloud Container Vulnerabilities Integration	This integration is triggered on successful completion of the Tenable.cs Open Cloud Container Vulnerabilities Integration. • Retrieves container vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopened container vulnerable items (CVIs). If they don't exist, it also creates discover container images, docker images, container repositories, image findings, third-party entries, and CVEs. Image findings are created in closed state.
Tenable.cs Open Cloud Host Vulnerabilities Integration	• Retrieves vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopened vulnerable items (VIs). If they don't exist, it also creates configuration items, third-party entries, and CVEs. Vulnerability Detections are created in open state.
Tenable.cs Fixed Cloud Host Vulnerabilities Integration	This integration is triggered on successful completion of the Tenable.cs Open Cloud Host Vulnerabilities Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs integrations (continued)

Integration	Description
	• Retrieves vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is close vulnerable items (VIs). If they don't exist, it also creates configuration items, third-party entries, and CVEs. Vulnerability Detections are created in closed state.

User authentication and Tenable.sc

User authentication is supported by your ServiceNow AI Platform® instance and version 5.13 of the Tenable.sc product. User authentication is required if you're using version 5.12 and earlier of the Tenable.sc product.

When you select user authentication for the Tenable.sc integrations, tokens might expire and be replaced during integration runs. In the Notes column on the Vulnerability Integration Run record (VIN), the following message is displayed for a process when a token expires, `Error: Token validation is failed`. If this message is displayed, no action is required. Expired tokens are automatically refreshed in the background and the message doesn't indicate a pause or error with the integration process.

Preparing for the Tenable Vulnerability Integration

Prepare for the ServiceNow® Tenable Vulnerability integration by performing the following setup tasks.

Before you begin

A successful integration requires planning and careful execution of pre-integration tasks. For a smooth installation and configuration of the Vulnerability Response Integration with Tenable application, you may prefer to print the following checklist and verify the items listed are completed before you install the application and import vulnerability data into your ServiceNow AI Platform® instance.

Note: If you have been importing data with the Tenable-built integration, and you want to start using the ServiceNow® Vulnerability Response Integration with Tenable, see the

For current data cleanup and migration information from the Tenable-built integration to the integration built by ServiceNow, see the Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] article.

Role required: Admin to download and install the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
☐	(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application. For more information about installing and activating the Vulnerability Response application, see, Install Vulnerability Response. This integration requires version 12.1 of Vulnerability Response or later.
☐	If you don't already have it on your instance, get entitlements and download the Vulnerability Response Integration with Tenable application to your ServiceNow AI Platform® instance. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13 and Tenable.cs product starting with version 5.0.1. .
☐	Estimate the number of vulnerable items that you expect to import. Verify that your instance can accept the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you don’t know the size of your instance, or, if you need assistance, contact ServiceNow® Technical Support.
☐	Verify that you have groups or users to manage the integrations and remediate vulnerable items. **admin** The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant. **sn_vul.vulnerability_admin** Once assigned, the vulnerability admin completes the configuration of the Tenable integrations. This role has complete access to the Vulnerability Response (VR) application and its records. Configures all VR applications and rules and configures third-party integrations. **sn_vul_tenable.configure_integration** Can configure the Tenable Vulnerability Integration. This role contains the sn_vul_tenable.read_integration granular role. **sn_vul_tenable.read_integration** Can view (read) records of the Tenable Vulnerability Integration. **Vulnerability Response group** By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically. The system admin performs the initial assignment of roles to users and groups in Setup Assistant for the integration. By default, the Vulnerability Response group is available. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance prior to using Setup Assistant. See Create a user group. Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.
☐	To promote improved performance for your first import, you may prefer to disable certain features, rules, or jobs in your instance. • Disable vulnerability calculators if you don't use them. These calculators, plus any you have defined, run every time a vulnerable item record is created or updated. See Disable vulnerability calculators. • During the initial import of records, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, you may prefer to Disable notification-related business rules as described in Import modifications for the Tenable Vulnerability Integration.
☐	Verify you have enabled any features, rules, dependency plugins, or jobs in your instance required for the integration. • Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Vulnerability Response Integration with Tenable product and your ServiceNow AI Platform instance are in the same environment. If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server. For more information about MID Servers in your instance, see MID Server. • Verify the IntegrationHub plugin is installed and activated. This plugin enables base system components to call external systems using integration APIs and activates protocol steps like REST. Navigate to **System Applications** > **All Available Applications** > **All** and locate the plugin. If not installed in your instance, install and activate it.
☐	Obtain Tenable credentials. Verify you have any account names, passwords, and other service information required by your Tenable products so that you have access to them.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	Tenable.io requires Administrator access with a permission attribute greater than or equal to 64. Tenable.sc requires Security Analyst or Manager access. **Note:** Starting with v3.8 of Vulnerability Response Integration with Tenable, accessing Tenable.io no longer needs administrator privileges. A basic user with a permission attribute equal to 16 can also access the product.

You're ready to Install the Vulnerability Response Integration with Tenable application using Setup Assistant.

Install the Vulnerability Response Integration with Tenable application using Setup Assistant

Before you run the ServiceNow® Tenable Vulnerability Integration, you need to download the Vulnerability Response Integration with Tenable application from the ServiceNow Store and install and configure it using the Setup Assistant in the Vulnerability Response application.

Before you begin

Before you install the Tenable application, verify you have completed all the items in the checklist in Preparing for the Tenable Vulnerability Integration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Roles required: admin for initial assignment of the sn_vul.vulnerability_admin role and installing the Tenable application in Setup Assistant. Vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin (deprecated) to configure the application in Setup Assistant after it is installed.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration application Installation**.

   After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the **Tenable (Tenable Platform)** tile and click **Install**.

   This action installs the Vulnerability Response Integration with Tenable application you downloaded from the ServiceNow Store.

3. Follow the prompts provided in the Setup Assistant to continue with the installation.
4. For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation in Setup Assistant, navigate to **Integration Configuration>Scanner Integrations** in Setup Assistant to continue with the configuration. If you want more information to supplement the prompts provided in Setup Assistant, see Configure the Tenable Vulnerability Integration using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data retrieval settings for the Tenable Vulnerability Integration

The following data retrieval settings help you determine specifically the type and scope of data you want to import from the ServiceNow® Tenable Vulnerability Integration to your ServiceNow AI Platform® instance.

The settings described in the following sections help you control the data you want to import. Additionally, you can set the values of these filters in Integration Instances. To view integration instances, navigate to **Tenable Vulnerability Integration** > **Integration Instances** and select your integration, Tenable.io, Tenable.sc, or Tenable.cs.

On the Integration Instance page that is displayed, select the Integration Instance Parameters to display a list of parameters, or the Vulnerability Integrations tabs for a schedule, REST Details, Integration details, Data Sources, and integration run information.

Common severity and retrieval settings and filters for Tenable.io, Tenable.sc and Tenable.cs in your ServiceNow AI Platform instance

The following settings are available for the Tenable.io, Tenable.sc, and Tenable.cs integrations in your ServiceNow AI Platform instance. These and other configuration settings are displayed on the Integration Instance page of your ServiceNow AI Platform instance. You may prefer to leave these settings in their defaults for the first few integration runs.

Tenable.io

insert_fixed

If you enable the **insert_fixed** flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created for detections in the **Fixed** state that don't exist in your instance.

severity_critical

This filter is enabled by default (true) to receive critical severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_high

This filter is enabled by default (true) to receive high-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_info

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_low

This filter is inactive by default (false). Enable this filter to receive low-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

size

This setting defines the number of plugin records to include in the result set from the Tenable.io Plugins Integration. Must be in the int32 format. The default value is 1,000. The maximum size is 10,000.

num_assets

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The maximum number of vulnerabilities per exported chunk from the Tenable.io Fixed Vulnerabilities and Tenable.io Open Vulnerabilities Integrations. The default value is 50.

chunk_size

Specifies the number of assets per exported chunk by the Tenable.io Assets Integration. The default is 1,000.

Tenable.sc

async_request

This parameter is inactive by default (false). Enable or disable this parameter to make asynchronous or synchronous API calls with Tenable.sc respectively. For synchronous calls, if there's a timeout at 30 seconds, contact support for the Tenable product to tune the box. This parameter once enabled is applicable for all the integrations of Tenable.sc. For existing customers using asynchronous calls, a fix script is available, which adds a new async_request parameter to the existing Tenable.sc integration instances. To view the fix scripts, navigate to **System Definition** > **Fix Scripts**.

insert_fixed

If you enable the **insert_fixed** flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created fordetections in the **Fixed** state that don't exist in your instance.

offset

Specifies the number of assets, plugins, and vulnerabilities imported in one integration run.

Query filters

Query filters are configured from within the Tenable console. These query filters have IDs that can be selected from Setup Assistant or from the Integration Instances page in your ServiceNow AI Platform instance. These filters are applied while retrieving the data from the Tenable.sc integrations.

Tenable.cs

compute_severity_critical

This filter is enabled by default (true) to receive critical severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_high

This filter is enabled by default (true) to receive high-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_info

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_low

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This filter is inactive by default (false). Enable this filter to receive low-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

container_severity_critical

This filter is enabled by default (true) to receive critical severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_high

This filter is enabled by default (true) to receive high-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_info

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_low

This filter is inactive by default (false). Enable this filter to receive low-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

asset_page_limit

This setting defines the number of container asset records to include in the result set from the Tenable.cs Cloud Container Assets Integration. The default value is 1,000. The maximum size is 1,000.

vuln_page_limit

This setting defines the number of vulnerabilities records to include in the result set from the Tenable.cs Open Cloud Host Vulnerabilities Integration, Tenable.cs Fixed Cloud Host Vulnerabilities Integration, Tenable.cs Open Cloud Container Vulnerabilities Integration, and Tenable.cs Fixed Cloud Container Vulnerabilities Integration. The default value is 1,000. The maximum size is 10,000.

REST messages for the Tenable Vulnerability Integration

The ServiceNow® Tenable Vulnerability Integration REST messages are used to make calls to the Tenable API.

Tenable.io Assets REST message

The Tenable.io Assets REST message retrieves Assets information for the Tenable.io Asset Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve assets information. The export job for assets is submitted with the following filters:

- "is_deleted": false
- "is_licensed": true

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Plugins REST message

The Tenable.io Plugins REST message retrieves Plugin information for the Tenable.io Plugin Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve plugins information.

Tenable.io Vulnerabilities REST message

The Tenable.io Vulnerabilities REST message retrieves vulnerability information for both Open and Closed vulnerabilities from the Tenable.io Vulnerability Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve vulnerabilities information.

Tenable.sc Queries REST message

The Tenable.sc Queries rest message retrieves the query filter information for the Tenable.sc Asset integration and Tenable.sc vulnerabilities integration where the query filter is configured.

Tenable.sc Plugins REST message

The Tenable.sc Plugin REST message retrieves plugin information for the Tenable.sc Plugins Integration. Changes to the REST message Get Plugins method record impact the requests made to Tenable.sc to retrieve plugins information.

Parameter name	Value	Description
type	active	Indicates the source Tenable pulls data from. Used by code. Changes aren't recommended.
fields	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Indicates the list of fields imported from Tenable.

Tenable.sc Vulnerabilities REST message

The Tenable.sc vulnerabilities REST message retrieves vulnerability information from the Tenable.sc Integration. Changes to the REST message Fetch Vulnerabilities or Fetch Patched

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerabilities method or, starting with v14.0 Vulnerability Response and v2.2 of the Tenable Vulnerability Integration, Fetch Backfill Vulnerabilities record impact the requests made to Tenable.sc to retrieve vulnerabilities information.

Tenable.sc Scan Credentials REST message

Tenable.sc Policy REST message

The Tenable.sc policy POST REST message adds a policy for requested plugins. Generated policy is used in Tenable.sc scan requests.

Tenable.sc Scan REST message

The Tenable.sc scan POST REST message adds a scan that is dependent on the access and permission defined in the request body of the rest message. It uses policy, plugin id, and IP(s) in the request body for the scan request.

Tenable.sc Scan Result REST message

The Tenable.sc Scan Result GET REST message provides scan details of the scan generated using the Scan REST message. It uses the scanResultId in the response of the scan REST messages and retrieves scan details for the triggered scan.

Tenable.sc Scan Credentials

The Tenable.sc scan credentials REST message retrieves the credentials information from Tenable.sc. Changes to the REST message 'Import' method record impact the requests made to Tenable.sc to retrieve the credentials information.

Parameter name	Value	Description
fields	id,name,description,type	Indicates the list of fields imported from Tenable.sc
filter	usable	Indicates that the integration pulls only usable credentials from Tenable.sc Changes to either of the parameters isn't recommended.

Tenable.cs GraphQl REST message: The Tenable.cs GraphQl REST message retrieves container asset information, host, and container vulnerability information for Tenable.cs Integration. Changes to the REST message Fetch Container Assets, Fetch Container Vulnerabilities, Fetch Compute Vulnerabilities method record impact the requests made to Tenable.cs to retrieve asset and vulnerabilities information.

Data transformation for the Tenable Vulnerability Integration

After you identify the data to import, it's retrieved from the Tenable product and processed through a set of data sources and transforms in your instance.

During installation, normalized severity maps are installed in the Normalized Severity Mapping module. These maps transform imported Tenable severity levels to standard severity levels for processing in your instance. For information about creating severity maps, see Create a Vulnerability Response severity map in the Vulnerability Response documentation.

Tenable.io Asset Import

Imported asset data is first loaded into the Tenable.io Asset Import [sn_vul_tenable_io_asset_import] Table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Tenable.io Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for `Tenable.io Asset Transform`.

The following table lists the transform map fields by integration.

Tenable.io Asset transform map fields

Source field	Target field	Description
u_id	source_id	Tenable provides a unique id for assets and maps to the discovered item record and is used for CI lookup.
u_ipv4s	ip_address	Maps the first ip value to the ip_address field on the discovered item record.
u_mac_addresses	mac_address	Maps the first mac_address value to the mac address field on the discovered item record.
u_fqdns	fqdn	Maps the first fqdn value to the fqdn field on the discovered item record.
u_netbios_names	netbios	Maps the first netbios value to the netbios field on the discovered item record.
u_plugin.cvss4_base_score	v4_base_score	CVSS v4 base score is mapped to the v4 base score in third party entry record.
u_plugin.cvss4_threat_score	v4_threat_score	CVSS v4 threat score is mapped to the v4 threat score in third party entry record.
u_operating_systems	os	Maps the first OS value to the os field on the discovered item record.
(Prior to v14.0 Vulnerability Response and v2.2 of the Tenable Vulnerability Integration)u_last_scan_time	last_scan_date	Maps to the last_scan_date field on the discovered item record.
u_last_authenticated_scan_dat	last_auth_scan_date	Maps to the last_auth_scan_date field on the discovered item record.
[script]	name	Maps the host name using the script's logic.
u_tags		The Tags are saved in sn_sec_cmn_host_tag. The mapping from tags to assets is saved in sn_sec_cmn_m2m_src_ci_tag.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.io Asset transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored.This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.io Plugins Integration

The Tenable.io plugins transform map is used to transform plugins imported from Tenable.io.

Note: Changes to this transform map alters how data received from the Tenable plugins is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the Tenable.io Plugin Transform.

The tenable.io plugins payload contains all the fields in the u_attributes column of the sn_vul_tenable_io_plugin_import table. The attributes field is parsed and mapped to the third-party entry table records as listed in the following table.

Source field	Target field	Description
id	id	Maps id from source and adds the TEN-prefix to it. For example, if the id received is 12345, the id in the target table is TEN-12345.
Description	summary	Maps the description of the plugin to the summary column.
[script]	source	The source for imported third-party entry (TPE) is Tenable.io.
[script]	source_instance	Reference to the Tenable deployment that imports this record.
family	category	Maps the family of plugin to the category column

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
plugin_modification_date	last_modified	Maps the plugin_modification_date to the last modified field.
plugin_publication_date	date_published	Maps the plugin_publication_date to the published date.
has_patch	remediation_type	Maps the remediation type from has_patch value.
synopsis	threat	Maps the threat information about this vulnerability.
cvss_base__score	score	Maps the Common Vulnerability Scoring System (CVSS) base score to the score column in third-party entry table.
solution	solution	Maps the solution provided by scanner to the solution column in the third-party entry table.
exploit_available	exploit	Maps the exploit_available provided by scanner to the exploit column in the third-party entry table.
vpr.score	source_risk_score	Maps the vpr score provided by scanner to the source_risk_score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
vpr.drivers.age_of_vuln	age_of_vuln	Maps the age of the vulnerability from the scanner to the age_of_vuln column in the third-party entry table.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
vpr.drivers.product_coverage	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
vpr.drivers.threat_sources_last28	threat_sources	Maps threat sources in the last 28 days from the scanner to the threat_sources in the third-party table.
vpr.drivers.threat_intensity_last28	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
vpr.drivers.threat_recency	threat_recency	Maps the threat recency information from scanner to threat_recency in the third-party entry table.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Maps cvss3 impact score to v3_impact_subscore column in the third-party entry table.
cvss_temporal_score	cvss_temporal_score	Maps the temporal score for CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Maps the temporal score for CVSS v3.
risk_factor	source_severity	Maps to the source severity in the third-party entry table.
name	name	Maps the name of the plugin to name in third-party entry table.
stig_severity	stig_severity	Maps the vpr score provided by the scanner to the source_risk_score in the third-party entry table.
plugin_type	check_type	Maps the plugin type to check_type in third-party entry table.
unsupported_by_vendor	unsupported_by_vendor	Maps the unsupported_by_vendor field to the unsupported_by_vendor column.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same Common

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Description
	Vulnerabilities and Exposures (CVE) in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.
bid	The list of bug traqs is added as a reference.
see_also	The list of URLs is added as a reference.
xrefs	The list of X-REF is added as a reference.
[script]	The list of exploits for that plugin and inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates the values in the third-party entry, and verify if the third-party entry exists. Based on the results, modifies the values in a third-party entry. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

The TenableIOPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from Tenable.io plugins integration and transforms it into ServiceNow AI Platform third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.io plugins data in the third-party entry table.

Tenable.io Vulnerabilities Import

The Tenable.io Vulnerable Item transform map is used to transform open and fixed vulnerabilities information imported from Tenable.io.

Note: Changes to this transform map alter how data from the Tenable Vulnerabilities Import is processed.

The same transform map is used for both the Tenable.io Fixed Vulnerabilities Integration and the Tenable.io Open Vulnerabilities Integration. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the `Tenable.io Vulnerable Item transform map`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_asset.uuid	id	Uuid is mapped to the id field of the cmdb_ci record.
u_asset.ipv4	ip_address	The ipv4 field is mapped to the ip address field of the cmdb_ci record.
u_asset.last_authenticated_results	last_auth_scan_date	The last authenticated scan date is mapped to the last auth scan date of the cmdb_ci record.
u_asset.mac_addess	mac_address	Mac address is mapped to the host mac address field of the cmdb_ci record.
u_asset.netbios_name	netbios	Netbios is mapped to the netbios field of cmdb_ci record.
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 base score is mapped to the v3 base score of the third-party entry record. These changes will be implemented as part of Tenable 5.2.1 Version.
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 temporal score is mapped to the v3 temporal score in the third-party entry record. These changes will be implemented as part of Tenable 5.2.1 Version.
u._plugin.cvss_base_score	score	CVSS base score is mapped to the score field of the third party entry record.
u._plugin.cvss_temporal_score	temporal_score	Temporal Score is mapped to the temporal score in the third-party entry record.
u_plugin.description	summary	Description is mapped to the summary field in the third-party entry record.
u_plugin.family	category	Maps the family of plugin to the category column of the third-party entry record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.modification_date	last_modified	Last modified date is mapped to the plugin last modified date in the third-party entry record.
u_plugin.publication_date	date_published	Publication date is mapped to the date published field of the third-party entry record.
u_plugin.risk_factor	source_severity	Risk factor is mapped to the source_severity field of the third-party entry record.
u_plugin.solution	solution	Solution is mapped to the solution field of the third-party entry record.
u_plugin.synopsis	threat	Synopsis is mapped to the threat field of the third-party entry record.
u_severity_id	priority	Priority is mapped to the severity id from the payload. The default value is 5.
u_plugin.exploit_available	exploit	Maps the exploit_available provided by the scanner to the exploit column in the third-party entry table.
vpr.score	source_risk_score	Maps the vpr score provided by the scanner to the source_risk_score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Maps the age of vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		in the third-party entry table.
u_plugin.vpr.drivers.product_coverage	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party entry table.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_plugin.vpr.drivers.threat_recency	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-party entry table.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Maps CVSS3 v3 impact score to v3_impact_subscore column in the third-party entry table.
u_plugin.type	check_type	Maps the plugin type to check_type in third-party entry table.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Maps the unsupported_by_vendor field in plugin to the unsupported_by_vendor column.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.
U_plugin.on_cisa_kev	cisa_exists	Maps on_cisa_kev field with cisa_exists in third-party entry table.
u_plugin.family_id	Family_id	Maps the plugin Family id to family_id column in third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
port	port	Port is mapped to the port field of the vulnerable item record.
protocol	protocol	Protocol is mapped to the protocol field of the vulnerable item record.
u_first_found	first_found	First found is mapped to the first found field of the vulnerable item record.
u_last_found	last_found	Last found is mapped to the last found field of the vulnerable item record.
u_state	state	State is mapped to the State field in the vulnerable item record
[script]	source	The source of the integration is populated. The vulnerable items created from this integration have Tenable.io as the source.
[script]	integration_instance	The integration_instance is the name of the instance from which the vulnerable item is imported.
u_plugin.name	name	Maps the name of the plugin to name in third party entry table.
u_plugin.stig_severity	stig_severity	Maps the stig severity of the plugin to stig severity column in third-party entry table
u_plugin.vpr_v2.malware_observations_intensity_last30	vprv2_malware_observations_intensity	Maps the VPRv2 malware_observations_intensity_last30 value to the vprv2_malware_observations_intensity field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.targeted_industries	vprv2_targeted_industries	Maps the VPRv2 targeted_industries value to the vprv2_targeted_industries field in the Tenable TPE Additional Attributes table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.vpr_v2.targeted_regions	vprv2_targeted_regions	Maps the VPRv2 targeted_regions value to the vprv2_targeted_regions field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.threat_summary	vprv2_threat_summary	Maps the VPRv2 threat_summary value to the vprv2_threat_summary field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.remediation	vprv2_remediation	Maps the VPRv2 remediation value to the vprv2_remediation field in the Tenable TPE Additional Attributes table.
u_plugin.d2_elliot_name	d2_elliot_name	Maps the d2_elliot_name value to the d2_elliot_name field in the Tenable TPE Additional Attributes table.
u_plugin.canvas_package	canvas_package	Maps the canvas_package value to the canvas_package field in the Tenable TPE Additional Attributes table.
u_plugin. checks_for_default_account	checks_for_default_account	Maps the checks_for_default_account value to the checks_for_default_account field in the Tenable TPE Additional Attributes table.
u_plugin.checks_for_malware	checks_for_malware	Maps the checks_for_malware value to the checks_for_malware field in the Tenable TPE Additional Attributes table.
u_plugin.exploitability_ease	exploitability_ease	Maps the exploitability_ease value to the exploitability_ease field in the Tenable TPE

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		Additional Attributes table.
u_plugin.exploithub_sku	exploithub_sku	Maps the exploithub_sku value to the exploithub_sku field in the Tenable TPE Additional Attributes table.
u_plugin.in_the_news	in_the_news	Maps the in_the_news value to the in_the_news field in the Tenable TPE Additional Attributes table.
u_plugin.metasploit_name	metasploit_name	Maps the metasploit_name value to the metasploit_name field in the Tenable TPE Additional Attributes table.
u_plugin.ms_bulletin	ms_bulletin	Maps the ms_bulletin value to the ms_bulletin field in the Tenable TPE Additional Attributes table.
u_plugin.usn	usn	Maps the usn value to the usn field in the Tenable TPE Additional Attributes table.
u_plugin.version	version	Maps the version value to the version field in the Tenable TPE Additional Attributes table.
u_plugin.vuln_publication_date	vuln_publication_date	Maps the vuln_publication_date value to the vuln_publication_date field in the Tenable TPE Additional Attributes table.
u_plugin.workaround	workaround	Maps the workaround value to the workaround field in the Tenable TPE Additional Attributes table.
u_plugin.workaround_type	workaround_type	Maps the workaround_type value to the workaround_type field in the Tenable TPE Additional Attributes table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.workaround_published	workaround_published	Maps the workaround_published value to the workaround_published field in the Tenable TPE Additional Attributes table.
u_plugin.vendor_unpatched	vendor_unpatched	Maps the vendor_unpatched value to the vendor_unpatched field in the Tenable TPE Additional Attributes table.
u_plugin.has_workaround	has_workaround	Maps the has_workaround value to the has_workaround field in the Tenable TPE Additional Attributes table.
u_plugin.vendor_severity	vendor_severity	Maps the vendor_severity value to the vendor_severity field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.cve_id	vprv2_cve_id	Maps the VPRv2 cve_id value to the vprv2_cve_id field in the Tenable TPE Additional Attributes table.
u_plugin.epss_score	epss_score	Maps the epss_score value to the epss_score field in the Tenable TPE Additional Attributes table.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.
bid	The list of bug traqs is added as a reference.
see_also	The list of URLs is added as a reference.
xrefs	The list of X-REF is added as a reference.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Description
[script]	The list of exploits for that plugin and Inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	TTriggers Tenable IO Vulnerabilities Processor which imports data from Tenable.io using the import set and loads each record into the CMDB CI table, the Vulnerable Items table, and the Third-party vulnerability table. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Checks if the Third-Party Entry and Detections exist. If not, these records are created in their respective tables. isn'tThis script is for internal use, and modifying or deleting them is not recommended.
onComplete (when an import set has completed transformation).	Updates the count of CIs, VITs, and Detections as imported from Tenable.io. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.io Compliance Results Integration

Tenable.io Compliance Results transform map enables you to import secure configuration assessment findings from Tenable.io into ServiceNow. This integration leverages Tenable's compliance export APIs to retrieve test results on assets, supporting regular differential imports to keep data up to date.

Imported data is first loaded into the Tenable.io Test Results Import [sn_vul_tenable_io_tr_import] table.

To access the transform map, navigate to **System Import Sets** > **Transform Maps**. Search for *`Tenable.io Compliance Results Transform`*.

The following table lists the transform map fields by integration.

Tenable.io Compliance Results fields

Source field	Table	Target field	Description
asset_uuid	sn_vulc_result	sn_sec_cmn_src_ci -> source_id	Unique identifier for the asset in Tenable.io, mapped to the corresponding CMDB CI in ServiceNow after transformation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results fields (continued)

Source field	Table	Target field	Description
first_seen	sn_vulc_result	first_seen	Date and time when the compliance check was first observed on the asset.
last_seen	sn_vulc_result	last_seen	Date and time when the compliance check was last observed on the asset.
audit_file	sn_vulc_policy	short_description	Name or identifier of the audit file used for the compliance check.
check_id	sn_vulc_test	source_id	Unique identifier for the compliance check within Tenable.io.
check_name	sn_vulc_test	short_description	Human-readable name of the compliance check.
check_info	sn_vulc_test	description	Detailed information about the compliance check, including its purpose and context.
expected_value	sn_vulc_result	expected_values	The value expected for the configuration setting according to the compliance policy.
actual_value	sn_vulc_result	actual_values	The actual value found on the asset during the compliance check.
status	sn_vulc_result	result	Result of the compliance evaluation. Possible values (from Tenable): PASSED, FAILED.
see_also	sn_vulc_result	remediation	Additional references or links for remediation guidance.
reference.framework	sn_vulc_auth_src	short_description	Compliance framework associated with the check (e.g., CIS, NIST).
reference.control	sn_vulc_citation	section	Specific control or section within the compliance framework.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results fields (continued)

Source field	Table	Target field	Description
solution	sn_vulc_test	remediation	Recommended steps to remediate the compliance failure.
profile_name	sn_vulc_citation	section_name	Name of the compliance profile or benchmark applied.
db_type	sn_vulc_technology	name	Database type or technology associated with the compliance check.

Note: Tenable does not provide a risk score for compliance test results. ServiceNow calculates risk scores using Configuration Compliance calculators and applies the default Medium risk value of 20 when no risk score is available. To ensure accurate prioritization, review and customize the risk calculator rules to reflect your organization's priorities.

For more information, see Configuration Compliance calculators and calculator rules.

Tenable.sc Asset Import

Asset data imported from Tenable.sc is first loaded into the Tenable.sc Asset Import table (sn_vul_tenable_sc_asset_import). The Tenable.sc Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is Processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the `Tenable.sc Asset Transform`.

Source field	Target field	Description
u_uuid	id	The uuid isn't populated from the Tenable API, so the 'u_uniqueness' attribute is used to create a unique uuid field for assets and map it to the cmdb_ci record.
u_ip	ip_address	Maps ip field from API to the ip_address field on a cmdb_ci record.
u_macaddress	mac_address	Maps the mac address field from the API to the address field on the cmdb_ci record.
u_dnsname	fqdn	Maps the dnsname field from the API to the fqdn field on the cmdb_ci record.
u_netbiosname	netbios	Maps the netbios field from the API to the netbios field on the cmdb_ci record.
u_oscpe	os	The OS information is extracted from the oscpe

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		attribute in the payload and maps it to the os field on the cmdb_ci record.
u_lastauthrun	last_auth_scan_date	Maps the lastauthrun field from the API to the last_auth_scan_date field on the discovered item record.
u_lastauthrun and u_lastunauthrun	last_scan_date	The lastauthrun is extracted from the Tenable API or lastunauthrun. The last_scan_date field on the discovered item record is populated based on the value that appears in the payload.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates the values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.sc Plugins import

Plugins data imported from Tenable.sc is first loaded into the Tenable.sc Plugins Import table (sn_vul_tenable_sc_plugin_import). The Tenable.sc Plugin Transform Map is used to transform the plugins information that has been imported. Changes to this transform alter how data from the Tenable Plugin import is Processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for `Tenable.sc Plugin Transform Map`.

Source field	Target field	Description
u_id	id	Maps id from source and adds the TEN-prefix. For example, if the id received is 12345, the id in the target table is TEN-12345.
u_description	summary	Maps the description of the plugin to the summary column.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
[script]	source	Imported TPE from this integration has Tenable.sc as the source.
[script]	source_instance	Reference to the Tenable deployment that imports this record.
u_family	category	Maps the name field in family object of plugin to the category column.
u_plugin_modification_date	last_modified	Maps the plugin_modification_date to the last modified field.
u_plugin_publication_date	date_published	Maps the plugin_publication_date to published date.
u_has_patch	Remediation_type	Maps the remediation type from has_patch value.
u_synopsis	threat	Maps the threat information about this vulnerability.
u_cvss_base_score	score	Maps the CVSS base score to the score column in third-party entry table.
u_solution	solution	Maps the solution provided by the scanner to the solution column in the third-party entry table.
u_cvss_temporal_score	cvss_temporal_score	Maps the temporal score for CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Maps the temporal score for CVSS v3.
u_risk_factor	source severity	Maps to the source severity in the third-party entry table.
u_cvss_v3_base_score	v3_base_score	Maps the CVSS base score in the third-party entry table.
u_exploit_available	exploit	Maps the exploitAvailable provided by the scanner to the exploit column in the third-party entry table.
u_vpr_score	source_risk_score	Maps VPR score from the scanner to the Source risk score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		• 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
u_vpr_context[id=age_of_vuln]	age_of_vuln	Maps the age of the vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
u_vpr_context[id=product_coverage]	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Maps threat sources in the last 28 days from scanner to threat_sources in the third-party table.
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_vpr_context[id="threat_recency"]	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-part entry table.
u_vpr_context[id=cvssV3_impact_score]	v3_impact_subscore	Maps CVSS v3 impact score from the scanner to v3_impact_subscore in the third-party entry table.
u_name	name	Maps the name of the plugin to the name column in the third-party entry table.
u_stig_severity	stig_severity	Maps the stig_severity field in the plugin to stig_severity in the third-party entry table.
u_check_type	check_type	Maps the check type to check_type in the third-party entry table.
u_family.id	family_id	Maps the plugin family_id to family_id in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
u_cpe	The list of CPEs is added as a reference.
u_see_also	The list of URLs is added as a reference.
u_exploit_frameworks	The list of exploits for that plugin and inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Function used to update the values in the third-party entry and verify if the third-party entry exists. Based on the results, modifies the values in a third-party entry. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of Plugins created and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

The TenableSCPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from the Tenable.sc plugins integration and transforms it into ServiceNow third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.sc plugins data in the third-party entry table.

Tenable.sc Vulnerabilities import

The Tenable.sc Open Vulnerabilities transform map is used to transform imported data from the Tenable.sc Open Vulnerabilities integration, and the Tenable.sc and Fixed Vulnerabilities transform map is used to transform imported data from the Tenable.sc Fixed Vulnerabilities Integration.

Note: Changes to these transform maps alter how data from the Fixed/Open Tenable Vulnerabilities Import is processed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To access the Tenable.sc Open and Fixed Vulnerabilities transform maps, navigate to **Tenable Vulnerability Integration** > **Administration** > **Integration Instances** > **Tenable.sc Fixed/ Open Vulnerabilities Integration** > **Data Sources** > **Tenable.sc Open/Fixed Vulnerabilities** > **Tranforms**.

Source field	Target field	Description
u_pluginID	Id	Used as the identifier for the plugin. This field is mapped to the plugin Id in the third-party entry record.
u_riskfactor	source_severity	This field is mapped to source_severity in the third-party entry record.
u_severity	priority	The priority field is mapped with the severity. The default value is 5.
u_hasbeenmitigated	state	Has been mitigated is mapped to the state field of vulnerability record. For the Fixed vulnerabilities integration, all the VIs are in the 'Closed' state.
u_ip	ip_address	Ip address is mapped to the host ip field of cmdb_ci table.
u_port	port	Port is mapped to the port field of the vulnerable item record.
u_protocol	protocol	Protocol is mapped to the port field of the vulnerfable item record.
u_firstSeen	first_found	The first seen value is mapped to the first found field of the VI record.
u_lastSeen	last_found	The last seen value is mapped to the last found field of the VI record.
u_exploitAvailable	exploit	ExploitAvailable is mapped to the exploit field in the third-party entry record.
u_synopsis	threat	Synopsis is mapped to the threat field in the third-party entry record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_description	summary	Description is mapped to the summary field in the third-party entry record.
u_solution	solution	Solution is mapped to the solution field in the third-party entry record.
u_basescore	score	BaseScore is mapped to the score field in the third-party entry record.
u_temporalScore	temporal_score	Temporal Score is mapped to the temporal score in the third-party entry record.
u_cvssv3basescore	v3_base_score	Cvssv3basescore is mapped to the v3 base score in the third-party entry record.
u_cvsstemporalscore	v3_temporal_score	Cvssv3temporal score is mapped to the v3 temporal score in the third-party entry record.
u_pluginpubdate	date_published	Plugin published date is mapped to the plugin published date in the third-party entry record.
u_pluginmoddate	last_modified	Last modified date is mapped to the plugin last modified date in the third-party entry record.
u_dnsname	fqdn	DnsName is mapped to the FQDN field of the cmdb_ci record.
u_macaddress	mac_address	MacAddress is mapped to the mac_address field of the cmdb_ci record.
u_netbiosName	netbios	NetbiosName is mapped to the NETBIOS field of the cmdb_ci record.
u_ip	ip	IP is mapped to the IP field of cmdb_ci record.
hostUniqueness	uuid	Host uniqueness is not mapped to any field but is used to determine uuid for the host.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_family	category	Maps the name field in the family object of the plugin to the category column of third-party entry record.
u_plugintext	proof	Plugin text is mapped to proof in tpe record.
[script]	source	The source of the integration is populated. The vulnerable items created from this integration have Tenable.sc as the source.
[script}	integration_instance	The integration_instance is the name of the instance from which the vulnerable item is imported.
u_vpr_score	source_risk_score	Maps VPR score from the scanner to the Source risk score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9 - 10 – Critical • 7 – 9 – High • 4–7 – Medium • 0–4 - Low
u_vpr_context[id=age_of_vuln]	age_of_vuln	Maps the age of the vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
u_vpr_context[id=product_coverage]	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_vpr_context[id="threat_sources_last_28]	threat_sources	Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party table.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_vpr_context[id="threat_recency"]	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-part entry table.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Maps CVSS v3 impact score from the scanner to v3_impact_subscore in the third-party entry table.
u_pluginname	name	Maps the name of the plugin to name column in third-party entry table.
u_stigseverity	stig_severity	Maps the stig_severity field in the plugin to stig_severity in third-party entry table.
u_checktype	check_type	Maps the check type to check_type in third-party entry table.
u_family.id	family_id	Maps the plugin family.id to family_id in the third-party entry table.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third_party_entry table is populated based on exploit_available and v3_attack_vector of columns.

Source field	Description
u_cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Description
	to the NVD entry. The mapping is found in sn_vul_m2m_entry_cve.
u_bid	The list of bug traqs is added as a reference.
u_cpe	The list of CPEs is added as a reference.
u_seealso	The list of URLs is added as a reference.
u_xrefs	The list of X-REFs is added as a reference.
u_exploitframeworks	The list of exploits for that plugin and Inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Function used to update the values in the vulnerability and verify if the vulnerability exists. Based on the results, modifies the values in a vulnerable items table. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of new VIs created, and VIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Asset Import

Imported asset data is first loaded into the Tenable.cs Container Asset Import [sn_vul_tenable_cs_container_asset_import] Table.

The Tenable.cs Container Asset transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable.cs Container Asset import is processed. To access this transform map, navigate to System Import Sets > Transform Maps. Search for Tenable.cs Container Asset Transform.

The following tables lists the transform map fields by integration.

Tenable.cs Container Asset transform map fields

Source field	Target field	Description
u_digest	Image_id	Tenable provides a unique digest for the container assets and maps to the discovered container image and docker

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Asset transform map fields (continued)

Source field	Target field	Description
		image record and is used for CI lookup.
u_digest	Image_digest	Tenable provides a unique digest for the container assets and maps to the discovered container image and docker image record and is used for CI lookup.
u_name	name	Maps to the name field of the docker image record.
u_repositoryuri	name	Maps to the container repository record
u_repositoryuri	repo	Maps to the discovered container image record.
u_virtualmachines	host_list	Maps to the discovered container image record
u_labels	Image_labels	Maps the first OS value to the os field o discovered item record.
u_clusters	image_cluster	Maps to the discovered container image record
u_imagetags	tags	Maps to the discovered container image record
u_cloudprovider	cloud_providers	Maps to the discovered container image record
u_accountid	cloud_account_ids	Maps to the discovered container image record
u_region	cloud_regions	Maps to the discovered container image record
u_operatingsystem	os	Maps to the discovered container image record
u_scantime	last_scan_date	Maps to the discovered container image record

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Container Asset transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Asset transform map script timing and purpose (continued)

When the script is run	Purpose
onBefore (before an import set has completed transformation).	A function used to update values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of new CIs created, and CIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Vulnerability Import

Imported container vulnerability data is first loaded into the Tenable.cs Container Vulnerability Import [sn_vul_tenable_cs_container_vuln_import] Table.

The Tenable.cs Container Vuln transform map is used to transform the imported container vulnerability information. Changes to this transform alter how data from the Tenable.cs Container Vulnerability Import is processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for Tenable.cs Container Vuln Transform.

The following tables list the transform map fields by integration.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
[script]	Image_id	Digest is extracted from the Resource.Id field from the API and mapped to image_id field of discovered container image and docker image record.
[script]	Image_digest	Digest is extracted from the Resource.Id field from the API and mapped to image_digest field of discovered container image and docker image record.
[script]	name	Repository information is extracted from name field and mapped to docker image and container repository record.
[script]	repo	Repository information is extracted from name field and mapped to discover container image record.
u_resource.Labels	Image_labels	Maps to the discovered container image record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
u_resource.CloudProvider	cloud_providers	Maps to the discovered container image record
u_resource. AccountId	cloud_account_ids	Maps to the discovered container image record
u_resource.Region	cloud_regions	Maps to the discovered container image record
u_vulnerability. Id	id	Maps id from source and adds the TEN- prefix. For example, if the id received is 12345, the id in the third party entry table is TEN-12345.
u_vulnerability. Description Id	summaryid	Maps to the third party entry record. or CVE record.
u_vulnerability.Severity	v4_base_severity	Maps to the third party entry record.
u_vulnerability.VprScore	source_risk_score	Maps to the third party entry record.
u_vulnerability.VprSeverity	source_severity	Maps to the third party entry record.
u_vulnerability.AttackVector	v4_attack_vector	Maps to the third party entry record.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Maps to the third party entry record.
[script]	source	he source for imported TPE is Tenable.cs.
u_vulnerability.Id	name	Maps to the vulnerability references record
u_vulnerability. Links	url	Maps to the vulnerability references record
	vulnerability	Reference of TPE or CVE in vulnerability references record
u_software.Name	name	Maps to the container image package record
u_software.Version	version	Maps to the container image package record
u_software.Type	package_type	Maps to the container image package record
u_softwarepaths	path	Maps to the container image package record
u_resolved	status	Maps to the container image finding record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
u_firstscantime	first_found	Maps to the container image finding record
u_resource.ScanTime	last_found	Maps to the container image finding record
u_vulnerability.Description	proof	Maps to the container image finding record
u_resolved	state	Maps to the container vulnerable item record
u_firstscantime	first_found	Maps to the container vulnerable item record
u_resource.ScanTime	last_found	Maps to the container vulnerable item record
[script]	source	The source for container vulnerable item record is Tenable.cs.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Container Vuln transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Triggers TenableCS Container Vulnerabilities Processor which imports data from Tenable.cs using the import set and loads each record into the CMDB CI table, the Vulnerable Item table, Third-party Vulnerability Entry table, Vulnerability Reference table, Container Image Package, Container Image Finding, and Container Vulnerable Item. Modifying or deleting isn't recommended.
onBefore (before an import set has completed transformation)	Checks if the third party Entry and Image Findings exist. If not, these records are created in their respective tables. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation)	Updates the count of CIs, VITs, and Findings as imported from Tenable.cs. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Compute Vulnerability Import

Imported host vulnerability data is first loaded into the Tenable.cs Compute Vulnerability Import [sn_vul_tenable_cs_compute_vuln_import] Table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Tenable.cs Compute Vuln transform map is used to transform the imported host vulnerability information. Changes to this transform alter how data from the Tenable.cs Compute Vulnerability Import is processed. To access this transform map, navigate to **System Import Sets** > **System Import Sets**. Search for Tenable.cs Compute Vuln Transform.

The following table lists the transform map fields by integration.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
u_resource.Id	object_id	Maps to the CMDB Ci record.
u_resource.Name	name	Maps to the CMDB Ci record.
	asset_category	Cloud is mapped as Asset Category in discovered item record.
U_resource.CloudProvider	cloud_service_provider	Maps to the discovered item record
u_resource.Region	cloud_region	Maps to the discovered item record
u_resource.AccountId	cloud_account	Maps to the discovered item record
u_resource. CloudProvider	cloud_resource_type	Maps to the discovered item record
u_resource.Id	resource_id	Maps to the discovered item record
u_resource.Name	resource_name	Maps to the discovered item record
u_vulnerability.Id	id	Maps id from source and adds the TEN- prefix. For example, if the id received is 12345, the id in the third party entry table is TEN-12345. Maps id to CVEs as well.
u_vulnerability. Description	summary	Maps to the third party entry record.
u_vulnerability.Severity	v4_base_severity	Maps to the third party entry record.
u_vulnerability.VprScore	source_risk_score	Maps to the third party entry record.
u_vulnerability.VprSeverity	source_severity	Maps to the third party entry record.
u_vulnerability.AttackVector	v4_attack_vector	Maps to the third party entry record.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Maps to the third party entry record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
[script]	source	The source for imported TPE is Tenable.cs.
u_vulnerability.Id	name	Maps to the vulnerability references record
u_vulnerability.Links	url	Maps to the vulnerability references record
	vulnerability	Reference of TPE or CVE in vulnerability references record
u_resolved	status	Maps to the vulnerable item detection record
u_firstscantime	first_found	Maps to the vulnerable item detection record
u_resource.ScanTime	last_found	Maps to the vulnerable item detection record
u_softwarepaths	proof	Maps to the vulnerable item detection record
u_softwareresolutionversions	solution_summary	Maps to the vulnerable item detection record
u_resolved	state	Maps to the vulnerable item record
u_firstscantime	first_found	Maps to the vulnerable item record
u_resource.ScanTime	last_found	Maps to the vulnerable item record
[script]	source	The source for vulnerable item record is Tenable.cs.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Compute Vuln transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Triggers Tenable CS Compute Vulnerabilities Processor which imports data from Tenable.cs using the import set and loads each record into the CMDB CI table, the Vulnerable Items table, and the Third-party vulnerability table. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Checks if the third-party entry and detections exist. If not, these records are created in their respective tables. This script is for internal

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Compute Vuln transform map script timing and purpose (continued)

When the script is run	Purpose
	use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Updates the count of CIs, VITs, and detections as imported from Tenable.cs. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
u_digest	Image_id	A unique digest provided by Tenable for the container assets. It maps to the discovered container image and docker image record and is used for CI lookup.
u_name	name	Maps to the name field of the docker image record.

Standardized logic for calculating source_risk_score and source_risk_rating

As part of the standardized data-transformation, the Tenable integration uses a centralized business rule to populate both **source_risk_score** and **source_risk_rating**.

During the integration run, if either **vprv1_risk_score** or **vprv2_risk_score** is updated, the system automatically recalculates and populates **source_risk_score** and **source_risk_rating** using the values from the **vprv2_risk_score** and **vprv1_risk_score** fields in the Third-Party Entry table.

- If **vprv2_risk_score** is present, it takes precedence over**vprv1_risk_score**.
- If the **vprv1_risk_score** and **vprv2_risk_score** are empty, then source_risk_score will not be changed.
- **source_risk_rating** is derived from the finalized **source_risk_score** using the standardized thresholds:
  - 9-10 → **Critical**
  - 7-9 → **High**
  - 4-7 → **Medium**
  - 0-4 → **Low**
  - NaN → **None**

Note: The above changes will be implemented as part of Tenable 5.2.1 Version.

Set additional filter parameters for Tenable.io imports

Customize the filtering parameters for your scheduled queries with the Tenable Vulnerability Integration to help you further refine the vulnerability data you import with the Tenable.io product.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Use cases: As a vulnerability manager or analyst, you might want to filter out data from your queries so that you can review only specific vulnerability details. For example, say you want to view imported vulnerabilities that are filtered by *cidr_range*, *num_assets*, *indexed_at*, and *plugin_family*. Or, say you want to run a Tenable.io integration such that one run imports only critical vulnerabilities every four hours, and another runs every 24 hours to fetch all the other non-critical vulnerabilities.

To help you gather this data, you might add tenable-supported parameters to help you import the specific vulnerability details you need.

Without adding additional API calls or coding, this feature permits you to customize your HTTP Request information with Tenable parameters in your ServiceNow AI Platform. The following Tenable.io Integrations support filtering by providing JSON content in the request body:

- Assets Integration
- Fixed Vulnerability Integration
- Open Vulnerabilities Integration

You should know how to use JSON strings for this feature.

Role required: sn_vul.vulnerability_admin

Procedure

1. Locate the parameters supported by the Tenable.io product on the developer site that you want to use for your filtering.

   Parameters and values you enter from the Tenable.io product are supported only at the integration instance level.

2. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
3. On the Tenable Integrations list page, click the record for the Tenable.io integration that you want to open.
4. With the Tenable REST methods tab selected, click the information icon (I) for REST method followed by **Open Record**.
5. Select the **HTTP Request** tab.
6. To edit the record, at the top of the page, click the link in, To edit the record click **here**.
7. In the REST Method record in the Content field, enter the JSON content that you want as part of the request body.

   As an example, you might set the severity parameter for imported vulnerabilities as, *{"filters": {"severity": ["critical"]}}* for the Tenable.io Assets Integration so it imports only critical vulnerabilities (CVSS score of 10.0).

   If you want to enter more than one parameter, refer to the Tenable.io documentation for more information about how to separate each value.

8. Click **Update**.

Tenable Vulnerability Integration reporting

View reports about vulnerabilities and vulnerable items on the Vulnerability Response dashboards.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data visualizations in the Vulnerability Response Workspaces

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Response Workspaces, Exploring the Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Previous versions of Vulnerability Response

The Vulnerability Response overview dashboard (Vulnerability Management) provides an executive view into vulnerabilities and vulnerable items, helping the Vulnerability Admin pinpoint areas of concern quickly. The Vulnerability Response remediation dashboard (Vulnerability Remediation) allows a remediation specialist to focus on the remediation tasks and vulnerable items they own.

See Using the default Vulnerability Response dashboards for more information.

Role required: Remediation owner.

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

to view the dashboard, navigate to **Vulnerability Response** > **Remediation Overview**.

Integration run status chart for the Tenable Vulnerability Integration

The Tenable Integration Run Status module provides you with a graphical view of the status of Tenable integration runs.

In the chart, point to any part of the graph to display a summary of data specific to that part. If you click any part on the bar graph, a list opens to provide more detailed information.

Role required: Vulnerability admin.

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

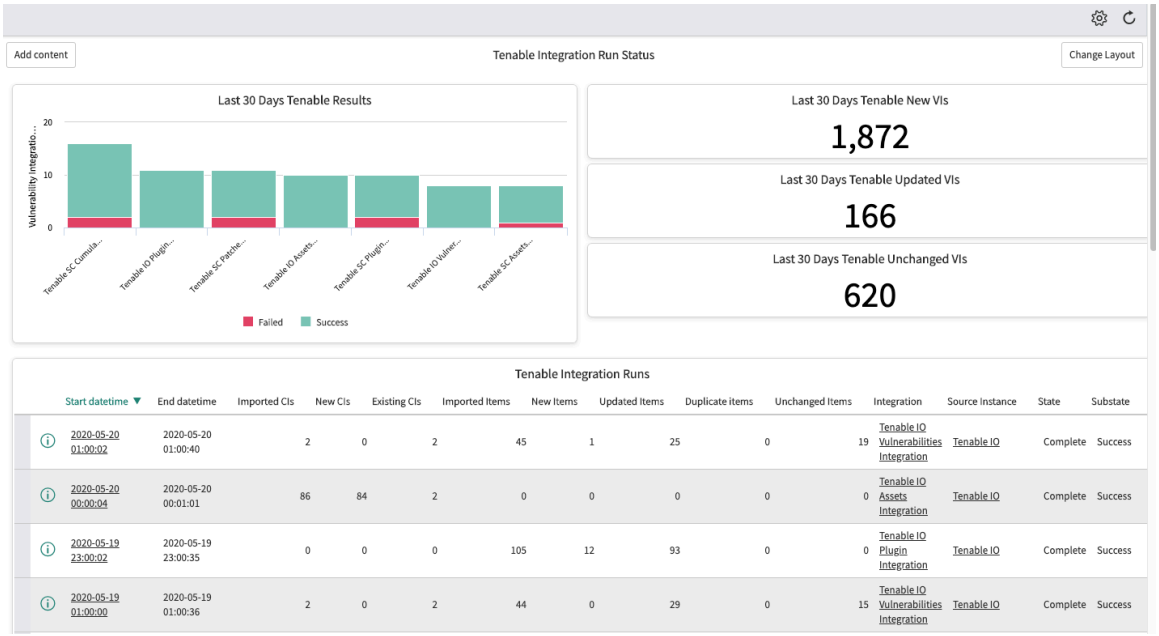
To view the data, navigate to **All** > **Tenable Vulnerability Integration** > **Integration Run Status**.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run status



Tenable integration run status chart reports

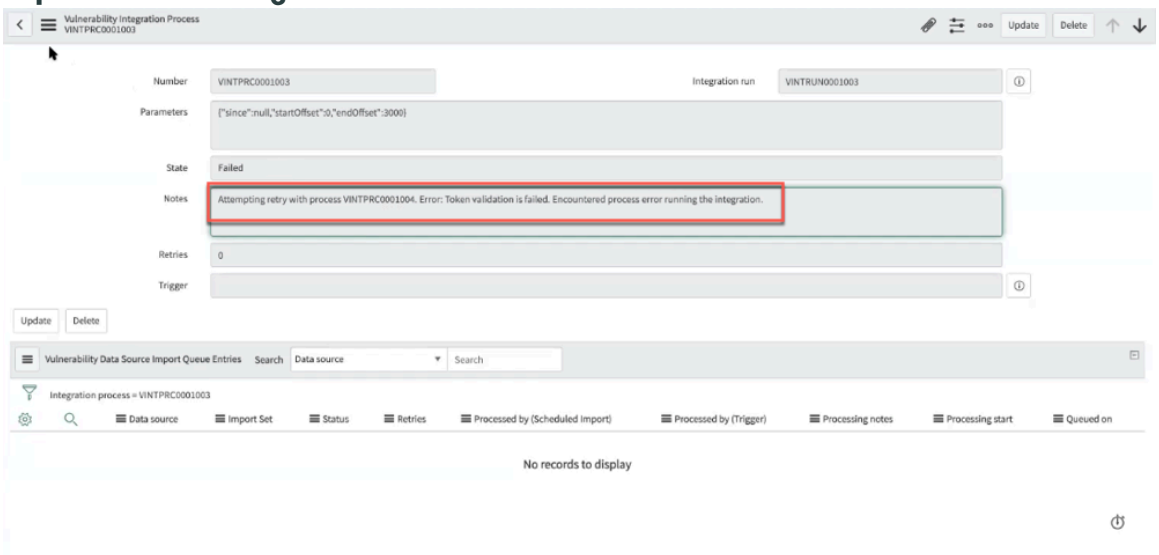
Name	Description
Last 30 days Tenable Results	The number of integration runs completed for each integration. Shows both successful and failed runs. Each run displayed as a bar in the graph.
Last 30 Days Tenable New VIs	The number of new vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Tenable Updated VIs	The number of updated vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Tenable Unchanged VIs	The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.
Tenable Integration Runs	The integration run records in a list. **Note: V16.1:** To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.

Token validation expiration

If a Tenable.sc integration run fails for any reason, the authentication token for Tenable.sc automatically expires and a message is displayed on the Vulnerability Integration Process record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Expired token message



A new token is automatically generated for the next integration process. All the integration processes, failed and successful, are displayed on the Vulnerability Integration Process tab on the Vulnerability Integration Process record.

Initiate rescan for the Tenable.sc integration

Verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Tenable platform. You can initiate a rescan on-demand for vulnerable items for the Tenable.sc product from your ServiceNow AI Platform® instance.

Before you begin

Roles required: sn_vul.write_all or sn_vul.write_assigned

Note: Tenable.sc does not support launching rescan on agent based machines.

Verify your scanner is activated before you begin. Navigate to **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.

About this task

To initiate rescan from the workspaces, see Rescan Tenable.io and Tenable.sc vulnerable items from the Vulnerability Response workspaces.

Follow the steps listed below to initiate a rescan in the classic environment.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans from vulnerable item (VI), remediation tasks (RT)s, third-party entry (TPE), or discovered item records from your ServiceNow AI Platform instance.

Rescans permit your remediation owners and vulnerability analysts to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

As an example, your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Tenable.sc vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When requesting rescan from your ServiceNow AI Platform® instance, selecting the Vulnerability Response Integration with Tenable credentials is optional. The ServiceNow® Tenable.sc Scan Credential Integration imports and updates scanner credentials from the Tenable.sc product in your instance. This integration runs weekly to import and securely store your Tenable credentials data.

Note that this imported data does not include Tenable passwords or other sensitive Tenable account information. The ServiceNow® Tenable.sc Scan Credential Integration is enabled (`Active`) automatically from within the Setup Assistant in your instance when you configure the Tenable.sc Vulnerabilities integrations (Tenable.sc Open and Fixed Vulnerabilities Integrations).

Note the following information about the credentials you import so that your users can see them as needed from your ServiceNow AI Platform instance:

- Credentials created with the Tenable.sc administrator user role are available to users across all your organizations.
- Credentials created with the Tenable.sc organizational users role are only available to users within that organization. These credentials are not imported into the ServiceNow AI Platform for users outside of the creator's organization unless they are shared with the user's account being used to connect to the instance.

See the Tenable.sc documentation website for more information.

See Configure the Tenable Vulnerability Integration using Setup Assistant for more information about configuring the Tenable.sc application. To view more information about the Scan Credential Integration, navigate to **All** > **Tenable Vulnerability Integration** > **Integrations** > **Tenable.sc Scan Credential Integration**.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *`sn_sec_cmn.record_threshold_heartbeat`*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *`sn_sec_cmn.maximum_heartbeat_delay`*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can only initiate rescans for VIs with Tenable.sc as the source. Verify Tenable.sc is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the **Personalize List** icon (Gear icon) and use the Slushbucket to move **Source** from **Available** to **Selected**.

3. Alternatively, navigate to **All** > **Vulnerability Response** > **Remediation Tasks** or **Vulnerability Response** > **Libraries** > **Third-Party** for the remediation task or third-party entry records, respectively, that you want to use for the rescan.

   Depending on your choice, the **Rescan** button is available on the following records:

   - On a single VI record, the VI must be from the Tenable.sc product and in any state other than **Closed**. For multiple VI records, all the VIs must be from the Tenable.sc product and in any state other than **Closed**.
   - On an RT record, the remediation task can be in any state other than **Closed**, and all the associated VIs must be from the Tenable.sc product.
   - On a third-party entry (TPE) record, the record must have at least one associated VI record from the Tenable.sc product in any state other than **Closed**.

4. In the upper right of the record, click **Rescan**.
   You are prompted to choose the scanner credentials to access the scanner. These are the credentials imported by the Tenable.sc Scan Credential Integration.
5. In the dialog, select the filters and credential types you want.
6. Click **Request Scan**.

   A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, RT, TPE records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

   The State field on the parent scan record is marked as complete after all the child scans are successfully completed. The child scans import data. The parent scan record is a container for the child scans.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to **Closed/Fixed** are imported with the next scheduled import of the Tenable.sc Fixed Vulnerabilities Integration.

Initiate rescan for the Tenable.io integration

Verify that your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Tenable platform. You can initiate a rescan on-demand for vulnerable items for the Tenable.io product from your ServiceNow AI Platform® instance.

Before you begin

Roles required: sn_vul.write_all or sn_vul.write_assigned

Verify your scanner is activated before you begin. Navigate to **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

- See and Rescan records and remediation tasks in the Vulnerability Manager Workspace and Rescan vulnerable items and remediation tasks in the IT Remediation Workspace to initiate a rescan in the Vulnerability Response workspaces.
- Follow the steps listed below to initiate a rescan in the classic environment.

Note: Tenable.io does not support launching rescan on agent based machines.

To help reduce the overhead and volume involved with scheduled, full scans, as a remediation owner, IT specialist, vulnerability analyst, or vulnerability manager, you can initiate targeted rescans on-demand. you can scan for specific vulnerabilities on assets (configuration items) in your environments. You can initiate rescans from vulnerable item (VI), remediation tasks (VUL), third-party entry (TPE), or discovered item (SDI) records from your ServiceNow AI Platform instance. Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

Note: When requesting rescan from your ServiceNow AI Platform® instance, selecting the Vulnerability Response Integration with Tenable credentials is optional. The ServiceNow® Tenable.io Scan Credential Integration imports and updates scanner credentials from the Tenable.io product in your instance. This integration runs weekly to import and securely store your Tenable credentials data.

Note that this imported data does not include Tenable passwords or other sensitive Tenable account information.

The following information describes the credentials you import so that your users can see them as needed from your ServiceNow AI Platform instance:

- Credentials created with the Tenable.io administrator user role are available to users across all your organizations.
- Credentials created with the Tenable.io organizational users role are only available to users within that organization. These credentials are not imported into the ServiceNow AI Platform for users outside of the creator's organization unless they are shared with the user's account being used to connect to the instance.

  See the Tenable.io documentation website for more information.

- The Tenable.io Template Integration and the Tenable.io Scan Credential Integration are required to be activated prior to initiating rescans. To view more information about the Scan Credential Integration, navigate to **Tenable Vulnerability Integration** > **Integrations** > **Tenable.io Scan Credential Integration**.

  By default, the Template and scan Credential Integrations are deactivated. When you enter your credentials for Tenable.io, all Tenable.io integrations are automatically activated. To manually activate or deactivate these integrations:

  1. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
  2. On the list that is displayed, locate the Tenable.io integration records you want.
  3. Open each record and select the **Active** check box to activate the integration.
  4. Click **Update** to save your changes.
  5. Return to the Setup Assistant to continue with your configuration for the Tenable Vulnerability Integration with Vulnerability Response.

See Configure the Tenable Vulnerability Integration using Setup Assistant for more information about configuring the Tenable.io and Tenable.sc products.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Say your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Tenable.io vulnerable items.

You can view updated results on the records you initiated the scans from after the next scheduled import of the Fixed Vulnerabilities Integration.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: If you are using the Tenable.io Scanner, you can only initiate rescans for VIs with Tenable.io as the source. Verify Tenable.io is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the **Personalize List** icon (Gear icon) and use the Slushbucket to move **Source** from **Available** to **Selected**.

3. Alternatively, navigate to **All** > **Vulnerability Response** > **Remediation Tasks** or **Vulnerability Response** > **Libraries** > **Third-Party** for the records that you want to use for the rescan.

   Depending on your choice, the **Rescan** button is available on the following records:

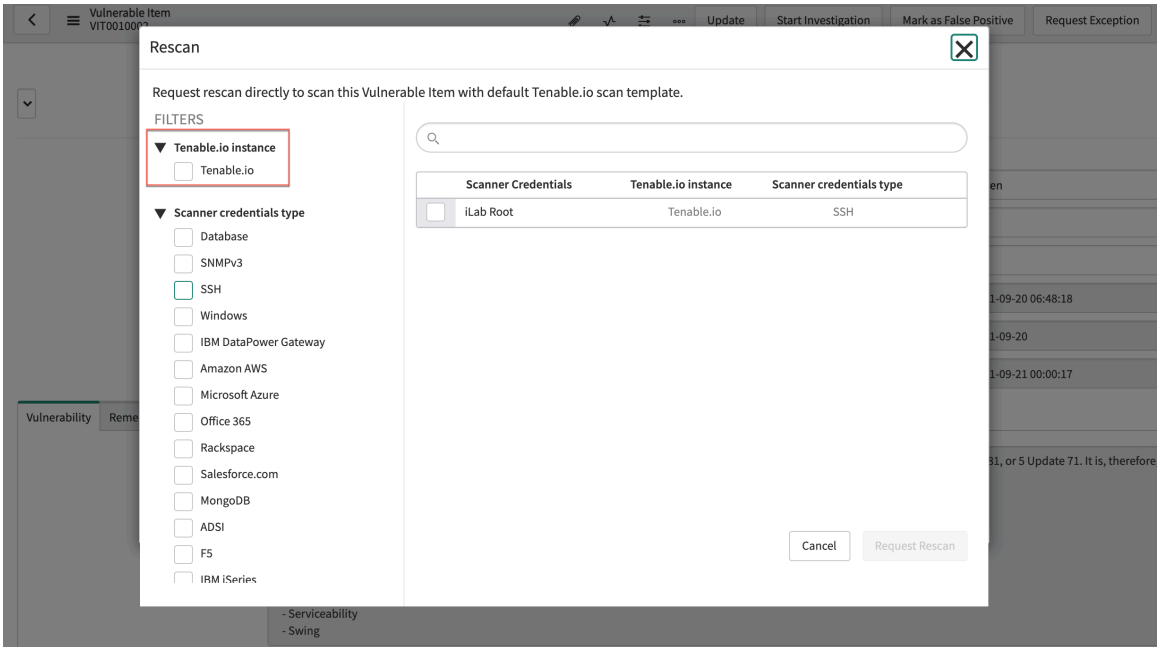
   - On a single VI record, the VI must be in any state other than **Closed**. For multiple VI records, all the VIs must be from the Tenable.io product and in any state other than **Closed**.
   - For remediation task records, only remediation tasks in any state other than **Closed** are supported. All the associated VIs must be in any state other than **Closed** and use Tenable.io as the source.
   - On a third-party entry (TPE) record, the record must have at least one associated VI record from the Tenable.io product in any state other than **Closed**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- On Discovered Items records, the record must have at least one associated VI record from the Tenable.io product in any state other than **Closed**.
- From the Vulnerable items list, you can select individual vulnerable items that you want to rescan. Use the Actions on selected rows menu in the lower left of the screen to launch the rescan. You are prompted to enter your credentials.

4. In the upper right of a record, click **Rescan**.
   You are prompted to choose the instance or instances for the rescan and the scanner credentials you want to use to access the scanner. The displayed credentials are those imported by the Tenable.io Scan Credential Integration.
5. In the dialog, select the instance and or instances and the credential types that you want to use.

   In the following image, one integration instance, `Tenable.io` is displayed. If you have more than one Tenable.io instance, they are all displayed under the `Tenable.io` section on the form.



Field	Description
Tenable.io instance	Choose a Tenable.io integration instance that you want to initiate the rescan from. All your integration instances for Tenable.io are displayed. If a VI exists in more than one integration instance, you can use this filter to limit or expand the instances you want to scan. **Note:** If you choose to rescan VIs from a remediation task record for a single in tegration instance, only the active VIs that are associated with that remedia tion task, for that instance, using the cre dential(s) that you select are scanned.
Scanner credentials type filter	Use this filter to display credentials by type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Pane with Scanner Credentials, Tenable.io instance, Scanner credentials type	These are the available scanner credentials imported from the Tenable.io products. Choose one or more credentials to use for the scan.

6. Click **Request Rescan**.

   A message is displayed that indicates your scan is being processed and a parent scan record is created. Status for all the child scans can be found at any time under the Scan related lists on the VI, remediation task, TPE, and SDI records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

   The State field on the parent scan record is marked as complete after all the child scans are successfully completed. The child scans import data. Each scan supports a unique combination of integration instance, TPE, IP, and Network ID. You might see multiple child scans on a parent scan record. For example, the maximum number of IP Addresses a child scan can support is 1000. If there are 1002 IPs for a vulnerable item, two child scans are created and listed on the Scans related list to support the request. The parent scan record is a container for the child scans and its state of reflects the status of the child scans.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to **Closed/Fixed** are imported with the next scheduled import of the Tenable.io Fixed Vulnerabilities Integration.

   For scans that error out, you can check the child scans on the parent scan record. View the error in the response payload of the child scan.

   You can view updated results on the records you initiated the scans from after the next scheduled import of the Fixed Vulnerabilities Integration.

Update configuration items with the network partition identifier for the Tenable Vulnerability Integration

Create unique configuration items (CIs) for assets in your environment that share IP addresses. Identify the distinct assets across your environment and automatically update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.

Before you begin

Role required: admin

About this task

By default in the Vulnerability Response application, one way to identify your assets is by IP address. In certain cases, assets can share IP addresses, but they are stored as one CI in your CMDB.

For example, as shown in the following tables, multiple assets (CI)s in your environment can share IP addresses but have unique network and repository ids. However, by default, these assets are typically identified and stored as a single CI (`CI 1`) during the IP address lookup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Default IP lookup and CI creation

Source	IP address	Network_id	Configuration item
Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	IP address	Repository_id	Configuration item
Tenable.sc: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

You can create individual CIs for assets that have the same IP address so that you can identify them as distinct assets. Starting from a fresh data import, you can update your existing CIs with more granularity that includes the network partition identifier [network_partition_identifier] by running the scheduled job, *`Update existing discovered items with network partition identifier`*.

This scheduled job is deactivated by default. Activate this feature for the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products in the Setup Assistant to view this identifier on your records.

When activated, this scheduled job adds the Network Partition Identifier [network_partition_identifier] to existing CI records from imported data. Existing CIs created by the IRE are also updated. The scheduled job also creates CIs that include the network partition identifier starting with the next import. Alternatively, you can launch the job on-demand to update your existing data.

When you upgrade starting with v14.0 of Vulnerability Response and v2.2 of the Tenable Vulnerability Integration, the CMDB CI Class Models (1.0.21.) is supported. The class models have the network partition identifier [network_partition_identifier] in the Identification and Reconciliation (IRE) identification rules.

Option	Description
Run the scheduled jobs on-demand.	Update your existing discovered items. CIs for your existing Tenable data are created or updated to include the network partition identifier granularity. Discovered items, vulnerable items, and detection records are all updated with the new CIs.
Wait for imports of fresh data from the integrations with the next scheduled jobs.	Create CIs for each new asset using the network partition identifier starting with the next scheduled job. CI, vulnerable item, and detection records are all updated to include

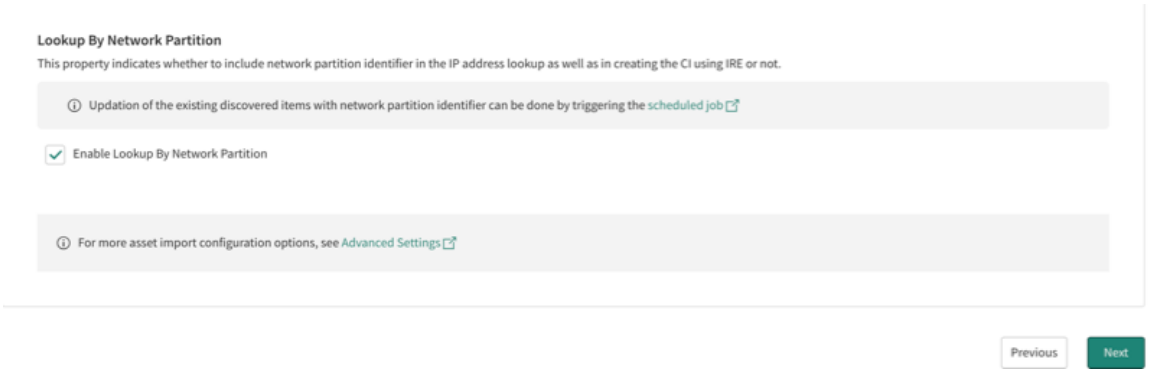
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Option	Description
	the new granularity. New CIs are created when an exact match is not found.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.
2. Select Tenable.io integrations or Tenable.sc integrations.
3. **Edit** the required integration.
4. Select **Asset Import Configuration**.
5. Select **Enable Lookup By Network Partition** check box from the **Enable Lookup By Network Partition** section.



6. Click **Next**.

   Network partition identifiers NETWORK_ID and REPOSITORY _ID are included and update existing CIs or create CIs with the next scheduled job.

Network partition identifier attribute included in IP lookup and CI creation

Source	IP address	NETWORK_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Tenable.sc: Assets and Fixed and Open	123.12.12.141	12	CI 1	CI 1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Vulnerabilities Integrations				
	123.12.12.141	13	CI 1	CI 2

With the next scheduled job, the IP Address and Incomplete IP Address CI identification lookup rules include the network partition identifier attribute automatically for a data import from the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products.

After you enable the system property and save the records, you alternatively can update your existing discovered items with CIs that include the network partition identifier by launching the scheduled jobs on-demand.

Import modifications for the Tenable Vulnerability Integration

Configure optional modifications and streamline some of the data specifically for the Tenable Vulnerabilities import integration in the ServiceNow® Tenable Vulnerability Integration.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

This set of tasks requires coding and advanced knowledge about the ServiceNow AI Platform.

Follow these steps to create domain-separated imports for the Tenable Vulnerabilities Integrations. The following example is for the Tenable.io Open Vulnerabilities integration, but this content is applicable to the other Tenable integrations.

Procedure

1. Create a domain.
2. For every domain you create, create a user and assign the user to that domain.

   Think of this user as a run_as placeholder for the domain in Tenable.io.

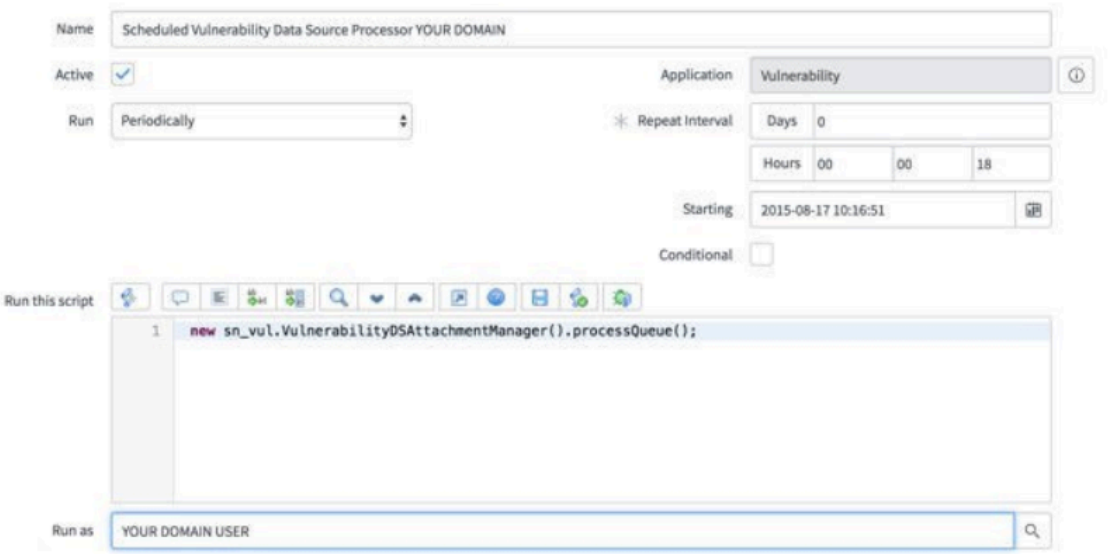
3. Open Vulnerabilities Integration.
   The user is the equivalent to the VR.System user in the global domain and must have the following roles: sn_vul.tenable_configure_integration, import_admin, and sn_vul.vulnerability_write. This user requires access to data sources, transform maps, and vulnerability data.

   Note: Consider this user as specific to this role. The user should not have any other purpose

4. In each domain, create a scheduled job by copying Scheduled Vulnerablity Data Source Processor found under **System Definition** > **Scheduled Jobs**.
5. Append the domain to the name to identify the scheduled job.
6. Change the run_as user to the user you created in the previous step.

   Note: Edit the following UI action so that the integration runs in the run_as user domain.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Edit the Execute Now UI action in the Tenable.io Open Vulnerabilities Integration to add this code block to the top of the file.
   //sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }

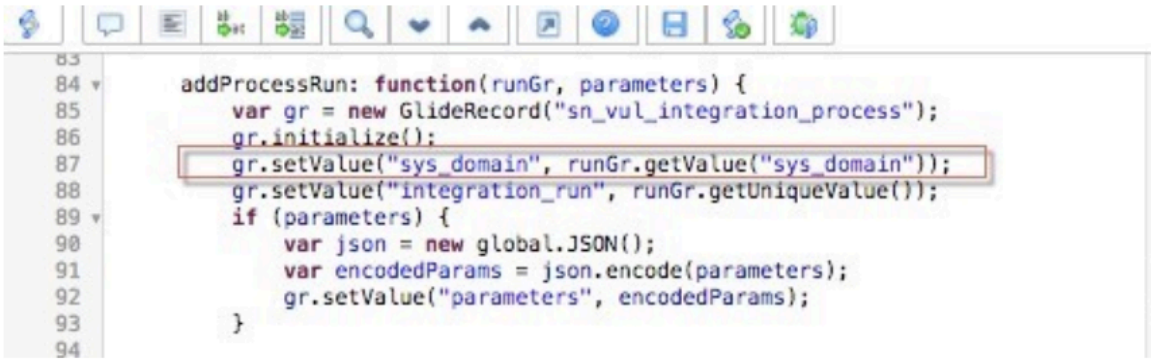
   Note: Edit the following script includes so that integration runs in the run_as user domain.

8. Edit the VulnerabilityIntegrationUtils script include method addIntegrationRun to add the highlighted code.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edit the VulnerabilityIntegrationUtils script include method addProcessRun to add the highlighted code.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edit the DataSourceVulnReportRefreshProcessor script include method _processFromDataSourceGroups to change this original code: Original _processFromDataSourcesGroups code to Edited _processFromDataSourcesGroups code.
11. Edit the VulnerabilityDSAttachmentManager script include method, queueItem to add the following highlighted code blocks queueItem, _getNext, _processQueueEntry function.

    You are ready for domain-separated host detection imports.

    Disable calculators prior to import

    Follow these steps to disable the default calculator if not used. If you do not use vulnerability calculators, it is best to disable the default calculators in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is accessed and can impact instance performance.

    Role required: sn_vul.vulnerability_admin.

12. Navigate to **All** > **Vulnerability** > **Administration** > **Vulnerability Calculators**.
13. Open the Vulnerability Impact group.
14. Open the Score and Service Based Impact calculator.
15. Deselect the Active field to deactivate the calculator.
16. Click Update.

    You have disabled the default calculator.

    Disable notification-based business rules prior to initial import

    Follow these steps to disable Disable notification-related business rules prior to initial record import. During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

    Role required is sn_vul.vulnerability_admin.

17. Navigate to **All** > **System Definition** > **Business Rules**.
18. Search for Affected ci notifications.
19. Open the business rule and insert the following condition: *`current.sys_class_name != "sn_vul_vulnerable_item"`*.
20. Click **Update**.
21. Repeat this procedure for the following business rules:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Affected cost center notifications
- Affected group notifications
- Affected location notifications

Note: After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

Modify an initial start date

Follow these steps to Modify an initial start date. During installation using Setup Assistant, you set an initial start date for the Tenable integrations. You can reset that start date in Setup Assistant or from the primary integration as shown in the following steps.

22. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
23. Click any integration.
24. Click Integration Details.
25. Set the Start time field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.

    If you configured Tenable using Setup Assistant, the Start time field is pre-populated, initially to three months prior today's date, and subsequently to today's date. Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Tenable API rate limitations, as well as triggering execution timeouts.
26. Click **Submit** or **Update**.
27. **Optional:** Click **Execute Now** to run immediately.

Split Tenable detections based on the vulnerability instance to split vulnerable items

ServiceNow® Vulnerability Response enables the splitting of detections from Tenable scanners, enabling for the creation of a unique vulnerable item (VIT) for each detected vulnerability instance. This split enables the assignment of VITs to various remediation teams, enhancing the management and tracking of vulnerabilities.

Before you begin

Role required: admin

About this task

The Tenable scanner's payload contains detection data, with each path within the proof used to split the detections. The output tag in the payload identifies the vulnerability's location, facilitating accurate identification and management of vulnerabilities according to their specific paths.

After a plugin is added to the [sn_vul_proof_key_vulnerability] table, run the integration to split existing VITs. To verify, inspect the VITs for distinct detection paths.

Scenario 1: Detection exists before plugin is added

- Before Adding Plugin: Detection A with 4 file paths → VIT1
- After Adding Plugin & Ingestion Run: The existing VIT is updated with new proof, and three additional VITs are created.
- Closure Behavior: If a path is no longer seen in Tenable data, ServiceNow closes the corresponding detection and its VIT using a hash-based comparison of the file path.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scenario 2: Detection ingested after plugin is added

Detections are split during ingestion.

Note: Splitting occurs automatically during the ingestion run after plugin configuration.

Procedure

1. In the Third-party Integrations table [sn_sec_int_integration], set the **Include proof in VI key** column value to true for Tenable.io, Tenable.sc, and Tenable.cs.
2. Navigate to **All** > **Vulnerability Response** > **Administration** > **Configure VI granularity**.
3. For Tenable.cs product, navigate to **Detection Key Configuration** [sn_vul_detection_key_config] table, select Tenable.cs record and update,
4. **Optional:** On the Include port form, select the **Include port** check box and select the **click here** link (applies only to Tenable.io and Tenable.sc).
5. On the Add proof to VI keys list, select **New**.
6. On the Add proof to the VI key- New record form, in the **Vulnerability** field, add the Tenable ID for which you want to include the proof.

   Note: You can split the detections based solely on path information or by combining path and version details. For additional details, refer to the section 'Splitting detections from Tenable scanners' on this page.

7. In the **Regular Expression to Split Tenable VITs** field:
   - Split the detection based on only the path by entering Path\s+:\s+([A\n]+).
   - Split the detection based on path and installed and fixed versions by entering Path\s+:\s +([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+).
8. Select **Submit**.

Example: Splitting detections from Tenable scanners

The following detection from a Tenable scanner shows proof in the output tag that includes both path and version information.


```
{
  "results": {
    "asset": {
      "agent_uuid": "92124caabdb9459baa9d053186df48b9",
      "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df",
      "device_type": "aws-ec2-instance",
      "fqdn": "ip-ac0a0004.secops.com",
      "hostname": "ip-ac0a0004",
      "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
      "ipv4": "18.220.145.158",
      "last_authenticated_results": "2024-05-17T03:34:04.424Z",
      "mac_address": "0a:3e:8b:ed:63:e6",
      "netbios_name": "IP-AC0A0094",
      "operating_system": [
        "Microsoft Windows Server 2019 Datacenter Build 17763"
      ],
      "network_id": "00000000-0000-0000-0000-000000000008",
      "tracked": true
    },
```


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
    "output": "\n  Path: C:\\Program Files (x86)\\Common
 Files\\Oracle\\Java\\javapath_target_1190440625\\\n
 Installed version : 1.8.0_361.9\n Fixed version : Upgrade
 to version 8.0.401 or greater\n  Path : C:\\Program
 Files\\Java\\jre1.8.0_361\\\n  Installed version :
 1.8.0_361.9\n  Fixed version : Upgrade to version 8.0.401 or
 greater\n  Path : C:\\Program Files\\Java\\jdk1.8.0_351\\\n
 Installed version : 1.8.0_351.10\n  Fixed version : Upgrade to
 version 8.0.401 or greater\n"
    "plugin": {
      "bid": 123456,
      "checks_for_default_account": false,
      "checks_for_malware": false,
      "coe": "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b",
      "cvSs3_base_score": 7.8,
      "cvss3_temporal_score": 7.0,
      "cvss3_temporal_vector": {
        "exploitability": "Proof-of-Concept",
        "remediation_level": "Official Fix",
        "report_confidence": "Confirmed",
        "raw": "E:P/RL:O/RC:C"
      }
    }
  }
}
```


Configure Tenable test result granularity

Configure the Tenable test result granularity to ensure the system imports results at a more detailed level based on your selected configuration keys. In addition to the default keys, you can configure additional keys based on your requirements to increase granularity. Granular imports allow teams to manage their respective assets independently and prevent data from being overwritten when multiple records share common identifiers.

Before you begin

Role required:

- sn_vulc.admin

Procedure

1. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Configure Tenable Test Result Granularity**.
2. In the Key Configuration form, confirm that:
   - **Source integration** is `Tenable.io`.
   - **Table** is set to `Test Result`.
3. In the **Configuration Key** section, choose the field for which you want to create unique test results.
   For example, selecting *`instance`* creates unique test results for each instance within a database.

   Note: Use this feature with caution. Each additional configuration key increases integration time. To maintain optimal performance, limit your use to no more than three extra keys.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Enter *true* next to *instance* to enable granularity, or *false* to disable it.
5. Select **Update** to save your changes.

Understanding the Atlassian Jira integration with Vulnerability Response

The Atlassian Jira integration with Vulnerability Response enables you to leverage different issue-tracking and agile management tools for tracking efforts of vulnerability remediation.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview

ServiceNow® Vulnerability Response is integrated with Atlassian Jira to create issues corresponding to vulnerabilities and synchronized the issue entity in Jira and the vulnerability item entity in Vulnerability Response bi-directionally to reflect the latest updates. Vulnerability Managers require vulnerability items present in ServiceNow Vulnerability Response to be created and assigned to remediation users (developers in case of Application Vulnerability Response) in their preferred system of record and issue management tool such as Atlassian Jira. Any progress performed on the vulnerabilities in the issue management tool should be updated in ServiceNow Vulnerability Response for visibility to Vulnerability Managers. Further, any updates made by Vulnerability Managers in Vulnerability Response for vulnerability items must also be passed on to the issue management tool for visibility to remediation users.

Available versions

Release version	Release Notes
Vulnerability Response	Vulnerability Response Integration release notes
Vulnerability Response and Configuration Compliance for Container	Container Vulnerability Response release notes
Jira Spoke	Jira spoke release notes

Jira Vulnerability integrations

To view the Jira Vulnerability integration, navigate to **All** > **Agile Management for VR** > **Configure Agile Tools** .

The following integrations are included in the base system. These integrations are not all active by default.

After the initial run, every day, scheduled jobs are chained to run the integrations automatically in order. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Preparing for the Jira Vulnerability Response integration

A successful Jira Vulnerability integration requires planning and the execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Jira Vulnerability Response integration assumes that you are familiar with the Jira product and API.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Components installed with the Agile Integration for Vulnerability Response and Jira Integration for Vulnerability Response

Several types of components are installed with activation of the Agile Integration for Vulnerability Response and Jira Integration for Vulnerability Response plugin, including tables and user roles.

Roles installed

Role Title [name]	Description
Agile Tool Admin [sn_vul_agile.agile_tool_admin]	Allows you to create configuration rule for Agile Management to create or update issues. Create rule configurations for Agile Management.
JIRA Admin [sn_vul_jira.admin]	Allows you to select Agile tool to create issues for selected entity table.

Tables installed

Table	Description
Agile Tool Configuration [sn_vul_agile_tool_rule_config]	Contains configuration rules to create issues on the Agile platform.
Agile Tool Field Mapping [sn_vul_agile_tool_field_mapping]	Contains the field mapping of the Configuration Rule.
Agile Tool State Mapping [sn_vul_agile_tool_state_mapping]	Contains the state mapping of the Jira issue status with the Application Vulnerable Item, Container Vulnerable Item, Application Remediation Task and Container Remediation Task state.
Agile Tool Manifest [sn_vul_agile_tool_manifest]	Contains payload for Issue creation.
Agile Tool Data Resource [sn_vul_agile_tool_data_resource]	Contains the information about the created Jira Issue.
JIRA Admin [sn_vul_jira.admin]	Allows you to select Agile tool to create issues for selected entity table.

Install the Vulnerability Response Integration with Jira

Before you run the integration on your instance, the installation and configuration steps must be completed so the Jira product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: admin.

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	• Jira Integration for Vulnerability Response requires the Vulnerability Response application. • For the most current version of Jira Integration for Vulnerability Response, verify you have the most current version of Vulnerability Response installed. See KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes. • If the application is not installed and activated see, Install Vulnerability Response.
Verify that the Integration Hub plugin is installed.	• Jira Spoke requires the Integration Hub. • See KB1112383 for Integration hub installation. • For more information, see Legal schedules-IntegrationHub overview.
Verify that the latest version of Jira Spoke is installed.	See KB0792632 for Jira Spoke installation.
Verify that the Vulnerability Response Integration with Agile Management is installed.	Vulnerability Response Integration with Atlassian Jira requires this integration.

Procedure

1. Log in to the instance you want to install the Jira Vulnerability Response integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Vulnerability Response integration with Jira application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
8. Click **Request**.
   You will receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.
    Your application is automatically installed on your instance.

Configure rules in the agile tool configuration

Jira issues are created on the Jira platform if the records created in the Application Vulnerable Item, Container Vulnerable Item, Application Remediation Task and Container Remediation Task match the rules created in the agile tool configuration.

Before you begin

Roles required: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin or sn_vul_jira.admin.

Procedure

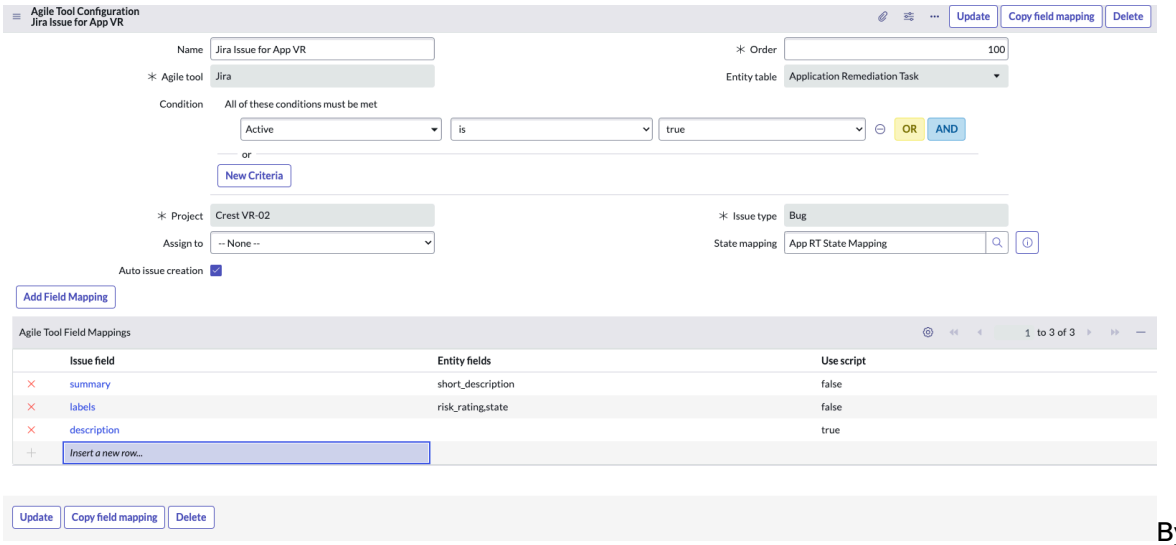
1. Navigate to **All** > **Agile Management for VR** > **Configure Agile Tools**.
2. To create a new configuration rule in the Agile Tool Configuration, select **New**.
3. On the form, fill in the fields.

Agile Tool configuration form

Field	Description
Name	Name of the Agile Tool Configuration.
Order	Order of the Agile Tool Configuration.
Agile Tool	The agile tool to create issues on the specific agile platform.
Entity Table	Table on which the Configuration rule is to be applied.
Condition	Filter condition on the selected entity table to create Issues on the Agile platform.
Auto Issue Creation	The configuration rule will be queried when any new record is created in the selected entity table, only if the check box is selected. **Note:** The user must use list action to create issues for existing entity records.
Project	The project in which the Jira Issue will be created.
Issue Type	The type of issue to be created in a particular project.
Assign To	The assignee to whom the issue should be assigned upon creation of the issue. To keep the created issues as unassigned, select “None”.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
State Mapping	The existing state mappings from the Agile Tool State Mapping table or create a new state mapping between the issue status in the agile platform and the ServiceNow entity table states.



By default, when the application is installed Application Remediation Task and Container Remediation Task are displayed in the Entity Table field on the Agile Tool Configuration form.

4. To add the Application Vulnerable Item and Container Vulnerable Item in the Entity Table choice list navigate to **System Properties** > **sn_vul_agile.tablesToShow** and add all in the Value field.

System property form

Field	Description
Choices	Comma-separated values for a choice list.
Value	Set the desired value for property. All property values are stored as strings. When retrieving properties via the gs.getProperty() method, treat the results as strings. For example, a true|false property returns 'true' or 'false' (strings), not the boolean equivalent.

5. Select the existing state mapping record or create a new state mapping in the Agile Tool State Mapping.

Agile Tool State Mapping form

Field	Description
Name	Insert the unique name of the State Mapping.
Agile Tool	Select the agile tool.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Entity Table	Select the source table on which state mapping will be created.
Project	Select the project in which the state will be mapped.
ServiceNow Entity State	Select the state that you want to map with agile tool status.
Agile Tool Status	Select the state that you want to map from vulnerability item states.

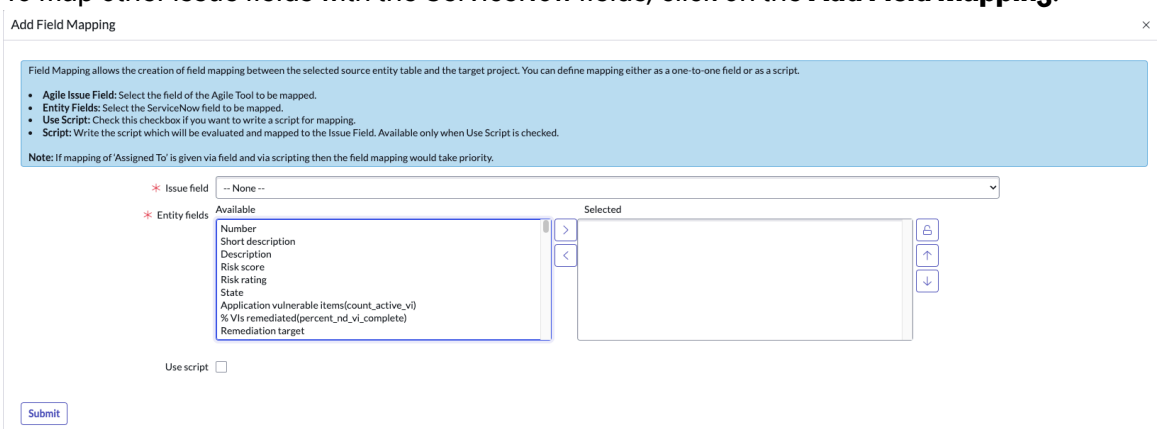
6. Click on **Save and Fetch Projects** to fetch the projects in the Project field Configuration rule and validate the credentials of the Agile tool.

   Tip: You can set the System Property **projectsPageSize** to fetch a particular number of projects per page.

7. Navigate to **System Properties** > **sn_vul_jira.projectsPageSize** and add the number of projects to be fetched per page in the Value field for Jira Cloud.
8. Select the Project, Issue Type and Assign to in the Configuration rule after the projects are fetched.

   Default field mapping will get populated in the embedded list of Agile Tool Field Mappings. By default, Summary and Description fields of Issues are mapped.

9. To map other issue fields with the ServiceNow fields, click on the **Add Field Mapping**.



Note:

- You must map String and Choice type fields only.
- Make sure all the mandatory issue fields from the Agile tool are mapped properly with the entity field.

Agile Tool State Mapping form

Field	Description
Issue Field	Contains the issue fields of the currently selected project and issue type in the Configuration Rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Entity Fields	Contains the fields of the entity table selected in the Configuration Rule.
Use the Script	Select to use the script for mapping the issue fields with entity fields.
Script	Script to map the Issue Field with Entity Fields.

10. Click **Submit** in the glide modal to submit the field mapping record in the Agile Tool Field Mappings table.

    Note: If you do not map the mandatory fields, issues will not be created for that configuration rule.

    Mandatory fields are displayed on the top in the Agile Tool Configuration form.
    All the field mapping for a particular Configuration rule are displayed in the embedded list of the Agile Tool Field Mapping table in the Agile Tool Configuration table.
11. Right-click in the header to save your changes.
    The saved record is visible in the Agile Tool Configuration table. If any record is created in the Application Vulnerable Item, Container Vulnerable Item, Application Remediation Task and Container Remediation Task matches any Configuration rule the issue will be created for the record according to the mapping in the Configuration rule.
12. Navigate to **System Properties** > **sn_vul_jira.cloudBulkSize** and set the number of issues to be created per batch in the Value field.

    Note: Maximum number of issues that can be created per batch in Jira cloud is 50).

    You can set the batch size for creating issues on Jira Server.
13. Navigate to **System Properties** > **sn_vul_jira.onPremBulkIssue** and set the number of issues to be created per batch in the **Value** field.
    You can also set the error count in the Value field in the system property to process the records in the manifest table to create Jira issues up to a specific error count.
14. Navigate to **System Properties** > **sn_vul_agile.ManifestErrorCount** and set the maximum number of times till which the manifest with error should be processed.

Create agile issue manually using list action

When a list action: Create Jira Issue is triggered, records that match the rule configuration criteria should be considered for “Create Jira Issue” and those records should be ingested into the sn_vul_agile_tool_manifest table with the mapping selected in the configuration rule.

Before you begin

Role required: sn_vul_agile.agile_tool_admin or sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedure

1. Navigate to **All** > **Workspaces** > **Vulnerability Manager Workspace** > **List** > **Remediation Tasks/ Application Vulnerable items / Container Vulnerable items**.
2. Select multiple records to create Jira issues, and click **Create Jira Issue**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected records should consider the field mapping and state mapping of the associated Agile tool.
The selected records that satisfy the configuration rule condition should be eligible for Jira issue creation and those records should be added to the *sn_vul_agile_tool_manifest* table.

Create agile issue manually using form action

Create an agile issue manually using form action. If the record is matched with any configuration rule condition, then a pop-up box will be populated with values that are selected in the configuration rule and if it does not match any criteria then the user will be allowed to select values for pre-defined fields.

Before you begin

Ensure that all the mandatory issue fields from the Agile tool are mapped properly with the entity field.

Roles required: sn_vul_agile.agile_tool_admin or sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedure

1. Navigate to **All** > **Workspaces** > **Vulnerability Manager Workspace** > **List** > **Remediation Tasks/ Application Vulnerable items / Container Vulnerable items**.
2. Select any record to create an agile issue manually.
3. Select **Create Agile Issue**.
4. Insert valid details for the mentioned fields.

   If the record satisfies the condition of any configuration rule, then below fields should be populated with configured value and the user can modify the field values.

Field	Description
Project	Select the project in which the Jira Issue will be created.
Issue Type	Select the type of issue to be created in a particular project.
Assign To	Select the assignee to whom the issue should be assigned upon creation of the issue.
Field Mapping	Select the issue type fields of the agile tool and insert the direct values for the selected field.

5. Select **Create Agile Issue** to submit the record.
   After submitting the record, the record entry will be created in sn_vul_agile_tool_manifest table.

Manually synchronize the status of the Jira issue

Update the state of the single record by clicking on the **Sync Agile Status** button of the form context menu and update the states of multiple records by clicking the list action **Sync Agile Status** of the Application Vulnerable Item, Container Vulnerable Item, and Remediation Task table in the Vulnerability Manager Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Roles required: sn_vul_agile.agile_tool_admin or sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

About this task
The state is synchronized from ServiceNow to the agile tool if the entity state is closed in ServiceNow or if any entity is reopened (i.e., State is Open). All other states will be reflected from Agile tool to ServiceNow. The user will not be allowed to synchronize state for the records whose associated configured rule does not have state mapping or the issues that are directly created from the form action.

Procedure
1. Navigate to **All** > **Workspaces** > **Vulnerability Manager Workspace** > **List** > **Remediation Tasks/ Application Vulnerable items / Container Vulnerable items**.
2. Select multiple records to create Jira issues, and click on **Sync Agile Status**.
   States of the records for which issues are already created get updated if the record is not in the closed state and the state mapping exists for the selected records in the configuration rule.
3. Open a record and the **Sync Agile Status** is visible in the form context menu if the following conditions are met.
   - Issue is created for the record and the record is not in Closed state
   - State mapping exists for the record
4. Click **Sync Agile Status** to synchronize the agile status with the mapped state.
   You can set the system property to set the batch size for fetching the issue status from Jira.
5. Navigate to **System Property** > **sn_vul_jira.bulkIssueStatusSize**.
   - For Jira Server, the maximum number of issues to return (defaults to 50). The maximum allowable value is dictated by the Jira property 'jira.search.views.default.max'. If you specify a value that is higher than this number, your search results will be truncated).
   - If the issue is created from form action or the configured rule does not have any state mapping, then those records will not be considered for state sync.

Configure scheduler to create issues automatically

Configure the scheduler to run and automatically create the Jira issues for the records that have been created in the sn_vul_agile_tool_manifest table.

Before you begin
Role required: admin or schedule_admin.

About this task
All the records of the Application Vulnerable Item, Container Vulnerable Item, Application Remediation Task, and Container Remediation created in the sn_vul_agile_manifest table will be considered for Jira issue creation.

Procedure
1. Navigate to **All** > **System Definition** > **Scheduled Jobs** > **Create Jira Issues**.
2. You can modify the Run, Time zone and Time fields in the Scheduled script.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled Script Execution form

Field	Description
Run	Time interval to use for running the scheduled job: ○ Daily–Runs daily, at a designated time. ○ Weekly–Runs weekly, at a designated time and day. ○ Monthly–Runs monthly, at a designated time and day of the month. ○ Periodically–Runs on a designated repeating interval. ○ Once–Runs for a single occurrence only. ○ On Demand–Runs immediately on demand. ○ Business Calendar: Entry Start–Runs on the starting entry dates for the business calendar you select in the field. A scheduled job runs for the starting date of each business entry you defined for the business calendar. For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month. ○ Business Calendar: Entry End– Runs for the ending date for the business calendar you select in the field. This selection runs in the same manner as Business Calendar: Entry Start, but for the end dates of the associated business calendar entries. **Note:** When you select Business Calendar: Entry Start or Business Calendar: Entry End, you can apply an offset factor to schedule the job to run before or after the time span of the selected business calendar. To learn more, see the Offset Type and Offset fields. To learn more about creating and using business calendars and defining business calendar entries, see Create a business calendar and Define business calendar entries.
Day	Day on which the scheduled job should run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ If Run is set to Weekly, select the day of the week. For example, select Wednesday. ○ If Run is set to Monthly, select the day of the month. For example, select 25 for the 25th day of the month. This field appears only if you select Monthly or Weekly in the Run field.
Repeat Interval	Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example: ○ To run the scheduled job every four days, enter 04 in the Days field. ○ To run it every 26 hours, enter 26 in the Hours field. ○ If it should repeat at an interval of 13:30:25, enter 13 in the Hours field, and then enter 30 and 25 in the two unlabeled fields after it.
Time	Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection that you make in the Time zone field determines the time zone for this entry.
Time zone	Time zone to use with the Time field entry when you specify the time at which the scheduled job should run. Select a time zone entry: ○ **None**: Use the default time zone for the logged-in user who is creating the scheduled job. For example, the scheduled job runs at 04:45 p.m. US/Pacific time if it is the user's assigned time zone, and you enter 16:45 into the Time field. ○ **Use System Time Zone**: Use the default system time zone that is specified for the instance in which it runs. For example, the scheduled job runs at 10:15 p.m. London time if Europe/London is the default system time zone for the instance, and you enter 22:15 in the Time field. ○ Actual time zone.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ For example, the scheduled job runs at 1:30 p.m. in the US Eastern time zone if you select US/Eastern and enter 13:30 in the Time field.
run_as	By default, run_ as field value should be empty. The user can set the value as domain user value to create issue for specific domain.

Configure scheduler to update issues automatically

Configure the scheduler to update the Jira issues automatically for the records that have been added in the sn_vul_agile_tool_manifest table.

Before you begin

Role required: admin or schedule_admin.

About this task

All the records of the Application Vulnerable Item, Container Vulnerable Item, Application Remediation task and Container Remediation created in the sn_vul_agile_manifest table is considered for Jira issue update. If the record gets closed, and comments are added then those values also should get updated to the associated Jira issue.

Note:

- The "update issues" scheduled job won't update the Jira state if the workflow for the chosen agile issue project restricts any user from directly changing the state from another state.
- If you close any entity record with additional comments, then only the last comment is considered at the time of update, and for the next update, all the comments are added to the associated Jira.

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs** > **Update Jira Issues**.
2. You can modify the **Run**, **Time zone**, and **Time** fields in the Scheduled script.

Scheduled Script Execution form

Field	Description
Run	Time interval to use for running the scheduled job: ○ Daily: Runs daily, at a designated time. ○ Weekly: Runs weekly, at a designated time and day. ○ Monthly: Runs monthly, at a designated time and day of the month. ○ Periodically: Runs on a designated repeating interval. ○ Once: Runs for a single occurrence only.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ On Demand: Runs immediately on demand. ○ Business Calendar: Entry Start: Runs on the starting entry dates for the business calendar that you select in the field. A scheduled job runs for the starting date of each business entry you defined for the business calendar. For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month. ○ Business Calendar: Entry End: Runs for the ending date for the business calendar you select in the field. This selection runs in the same manner as Business Calendar: Entry Start, but for the end dates of the associated business calendar entries. **Note:** When you select Business Calendar: Entry Start or Business Calendar: Entry End, you can apply an offset factor to schedule the job to run before or after the time span of the selected business calendar. To learn more, see the Offset Type and Offset fields. To learn more about creating and using business calendars and defining business calendar entries, see and Create a business calendar Define business calendar entries.
Day	Day on which the scheduled job should run. ○ If Run is set to Weekly, select the day of the week. For example, select Wednesday. ○ If Run is set to Monthly, select the day of the month. For example, select 25 for the 25th day of the month. This field appears only if you select Monthly or Weekly in the Run field.
Repeat Interval	Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ To run the scheduled job every four days, enter 04 in the Days field. ○ To run it every 26 hours, enter 26 in the Hours field. ○ If it should repeat at an interval of 13:30:25, enter 13 in the Hours field, and then enter 30 and 25 in the two unlabeled fields after it.
Time	Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection that you make in the Time zone field determines the time zone for this entry.
Time zone	Time zone to use with the Time field entry when you specify the time at which the scheduled job should run. Select a time zone entry: ○ None: Use the default time zone for the logged-in user who is creating the scheduled job. For example, the scheduled job runs at 04:45 PM. US/Pacific time if it's the user's assigned time zone, and you enter 16:45 into the Time field. ○ Use System Time Zone: Use the default system time zone that is specified for the instance in which it runs. For example, the scheduled job runs at 10:15 PM London time if Europe/London is the default system time zone for the instance, and you enter 22:15 in the Time field. ○ Actual time zone. ○ For example, the scheduled job runs at 1:30 PM in the US Eastern time zone if you select US/Eastern and enter 13:30 in the Time field.
run_as	By default, the **run_ as** field value is empty. You can set the value to a domain user to create an issue for a specific domain.

Configure scheduler to synchronize the Jira status to ServiceNow® automatically

Configure the scheduler to synchronize the state of Jira issues with application vulnerability item, container vulnerability items and tasks in the sn_vul_agile_manifest table.

Before you begin

Role required: schedule_admin or admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The scheduler runs automatically according to the configured schedule. The state of the records created in the Application Vulnerable item, Container Vulnerable item, Application Remediation task, and Container Remediation task table that have issues created in Jira gets updated according to the current status of the issue in the Jira platform based on the state mapping in the Configuration Rule.

All the records of Application Vulnerable item, Container Vulnerable item, Application Remediation task, and Container remediation created in the sn_vul_agile_manifest table will be considered for Jira issue creation.

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs** > **Sync Status**.
2. You can modify the Run, Time zone and Time fields in the Scheduled script.

Scheduled Script Execution form

Field	Description
Run	Time interval to use for running the scheduled job: ○ Daily: Runs daily, at a designated time. ○ Weekly: Runs weekly, at a designated time and day. ○ Monthly: Runs monthly, at a designated time and day of the month. ○ Periodically: Runs on a designated repeating interval. ○ Once: Runs for a single occurrence only. ○ On Demand: Runs immediately on demand. ○ Business Calendar: Entry Start: Runs on the starting entry dates for the business calendar you select in the field. A scheduled job runs for the starting date of each business entry you defined for the business calendar. For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month. ○ Business Calendar: Entry End: Runs for the ending date for the business calendar you select in the field. This selection runs in the same manner as Business Calendar: Entry Start, but for the end dates of the associated business calendar entries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: When you select Business Calendar: Entry Start or Business Calendar: Entry End, you can apply an offset factor to schedule the job to run before or after the time span of the selected business calendar. To learn more, see the Offset Type and Offset fields. To learn more about creating and using business calendars and defining business calendar entries, see Create a business calendar and Define business calendar entries.
Day	Day on which the scheduled job should run. ○ If Run is set to Weekly, select the day of the week. For example, select Wednesday. ○ If Run is set to Monthly, select the day of the month. For example, select 25 for the 25th day of the month. This field appears only if you select Monthly or Weekly in the Run field.
Repeat Interval	Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example: ○ To run the scheduled job every four days, enter 04 in the Days field. ○ To run it every 26 hours, enter 26 in the Hours field. ○ If it should repeat at an interval of 13:30:25, enter 13 in the Hours field, and then enter 30 and 25 in the two unlabeled fields after it.
Time	Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection that you make in the Time zone field determines the time zone for this entry.
Time zone	Time zone to use with the Time field entry when you specify the time at which the scheduled job should run. Select a time zone entry:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ -None-: Use the default time zone for the logged-in user who is creating the scheduled job. For example, the scheduled job runs at 04:45 p.m. US/Pacific time if it is the user's assigned time zone, and you enter 16:45 into the Time field. ○ Use System Time Zone: Use the default system time zone that is specified for the instance in which it runs. For example, the scheduled job runs at 10:15 PM London time if Europe/London is the default system time zone for the instance, and you enter 22:15 in the Time field. ○ Actual time zone. ○ For example, the scheduled job runs at 1:30 PM in the US Eastern time zone if you select US/Eastern and enter 13:30 in the Time field.
run_as	By default, the run_ as field value is empty. You can set the value as the required domain user's value to create issue for specific domain.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integration

The Prisma Cloud Compute integration enables you to scan hosts to detect vulnerabilities.

Starting with version 24.02.0 of the Vulnerability Response, you can use the Prisma Cloud Compute Integration to import vulnerabilities on the running hosts. The Prisma Host APIs enable retrieval of comprehensive vulnerability information for a specific host and also provides a snapshot of the host vulnerabilities at a specific time. This API enables regular synchronization between Prisma and ServiceNow instance. As Prisma is offered both as software as a service (SaaS) and on-prem solution, using a MID Server is necessary to invoke Prisma APIs from the ServiceNow instance. In addition, you're required to use a MID Server if the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute product and your ServiceNow AI Platform instance aren't in the same environment. For more information, see MID Server system requirements.

You can also view reports on vulnerabilities and vulnerable items on the Vulnerability Response dashboards. These vulnerabilities can then be prioritized and remediated.

Viewing the integrations

You can view the integrations that are part of the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. To view the integrations, navigate to **All** > **Prisma Cloud Compute Integration** > **Integrations**.

The following integrations are available.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run Sequence	Schedule	Integration	Description
1	Daily	Prisma Cloud Compute Hosts Integration	Retrieves hosts vulnerabilities and creates VITs, detections, and discovered items for hosts.

Note: If Container Vulnerability Response plugin is installed, you can also view Container Vulnerability Response related integrations.

Configure CVR based VI granularity

To configure the granularity of VITs, navigate to **All** > **Prisma Cloud Compute Integration** > **Configure VI Granularity** and specify the key combinations. By default, a CVIT is created for a combination of image repository, image tag, and vulnerability. You can add additional components to the key for further granularity. For example, you can create a CVIT for a combination of image repository, image tag, vulnerability, and cluster.

Prisma integration process

When the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute is run, it checks if a Common Vulnerability and Exposure (CVE) exists in the National Vulnerability Database (NVD) table. If it's already present, the existing information is used. However, if the CVE isn't found, placeholder records are generated in the NVD table. When creating these placeholder NVD records, initially only the CVE and its name is populated. Other details aren't populated with the assumption that the NVD integration fills in these details later. If the integration instance parameter *update_nvd* is set to true, it updates the placeholder NVD records. By default, the instance parameter is set to false. However, at least until the NVD integration runs and populates these details, some understanding of the CVE, such as its severity or some basic information about the issue is needed. To meet this requirement, the fields **Exploit exists** and **Remediation notes** are populated with the details obtained from Prisma. Additionally, this configuration is made customizable, enabling you to specify any other fields you want to populate in the NVD entry based on the information provided by Prisma.

Preparing for the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

You can prepare for the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute by performing setup tasks.

Before you begin

To install and configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application, you may print the following checklist. Verify the items listed are completed before you install the application and import the vulnerability data into your ServiceNow AI Platform® instance.

Integration preparation checklist

Task	Description
☐	Verify that you have the following sets of information: • API base URL • Username and Password.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist (continued)

Task	Description
	These credentials are used to pull the vulnerabilities from the Prisma Cloud Compute integration. For more information, see https://pan.dev/compute/api/ **Note:** MID Server is optional. The user credential used for Prisma Cloud Compute integration needs permission to monitor the images. See the following code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	If not already installed and activated, install the Vulnerability Response application before you install the third-party application. For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 16.1 of Vulnerability Response or later.
☐	Get entitlements and download the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application on your ServiceNow AI Platform® instance.
☐	Estimate the number of vulnerable items that you expect to import. Verify that your instance can accept the number of vulnerable items that you expect to import. An undersized instance can lead to long load times. If you don't know the size of your instance, or if you need assistance, contact ServiceNow Technical Support.
☐	Verify that you have the following groups or users to manage the integrations and to remediate the vulnerable items: **admin** Install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application. If not assigned, the admin assigns the container vulnerability admin (sn_vul_container.vulnerability_admin) and other roles. **sn_vul_container.vulnerability_admin** Completes the configuration of the Prisma Cloud Compute integration. This role has complete access to the Container Vulnerability Response (CVR) application and its records. This admin configures integrations and rules in Container Vulnerability Response. **Vulnerability Response Group** By default, the Vulnerability Response group is available. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all, sn_vul_container.read_all. **Container Remediation Owner Group** By default, the Container Remediation Owner group is available. Users assigned to this group inherit the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist (continued)

Task	Description
	sn_vul_container.remediation_owner. The Container Remediation Owner remediates container vulnerabilities assigned to them or to a group they belong to. **Vulnerability Analyst** Users assigned to Container Vulnerability Analyst group inherit sn_vul.vulnerability_analyst. The Vulnerability Analyst monitors remediation of all vulnerable items. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance. For more information, see Create a user group.
☐	Install the Vulnerability Response integration with NVD and run the NIST National Vulnerability Database Integration - API (CVE only).

You are ready to Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.

Install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Before you run the integration on your instance, complete the installation and configuration steps so that the Prisma Cloud Compute product properly integrates with Vulnerability Response and Container Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin

Procedure

1. Log in to the instance you want to install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Read the **Other Requirements** and **Dependencies** sections, if needed.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Update the **Instance Name** and **Reason for the Instance** fields, and click **Validate Instance**.
8. Click **Request**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You receive an email with detailed installation instructions.

9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.

Result
Your application is automatically installed on your instance.

What to do next
Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute for your environment. See Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.

Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application

Install and configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application to import data from Prisma Cloud Compute. You can use the imported data to prioritize and remediate vulnerabilities for your hosts.

Before you begin
Role required: admin

Procedure
1. Open the email from ServiceNow that you received about the integration.
2. Log in to your instance as an admin.
3. Follow the instructions in the email to get the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navigate to **All** > **Prisma Cloud Compute Integration** > **Administration** > **Configuration**.
   On the Prisma Cloud Compute Configuration form, fill in the fields. For more information, see Prisma Cloud Compute Configuration form.
5. From the Projects list, select either **All Projects** or **Specific Projects** to configure either all projects or selected projects respectively.
   If you select **Specific Projects**, you can select the projects from the Available list.
6. Complete the configuration by selecting either **Finish** or **Save and Test Credentials**.
   - If you configured a project, select **Finish**.
   - If you didn't configure a project, select **Save and Test Credentials**
7. View the newly created instance by navigating to **Prisma Cloud Compute Integration** > **Administration** > **Integration Instances**.
8. View the projects that you configured earlier by selecting **Integration Instance Parameters**.
9. Run the newly created integration instance to import the vulnerable items.
   The VITs are further created based on the granularity.
10. Configure the granularity of a vulnerable item.
    a. Navigate to **Prisma Cloud Compute Integration** > **Configure Image Vulnerability Keys**
    b. Configure the granularity of the VITs by selecting the required check boxes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The vulnerable items are created based on the selected keys during the next import.

Note: By default, a VIT is created for a combination of Image Repository,] Vulnerability, and Image tag. You can add components to the key for further granularity. For example, you can create a CVIT for a combination of Image Repository, Vulnerability, Image tag, and Cluster. Once the vulnerable items or vulnerable item findings are created, the check boxes are no longer editable.

Integration run status chart for Prisma Cloud Compute Integration

The Prisma Cloud Compute Integration Run Status module provides you with a graphical view of the status of Prisma Cloud Compute Integration runs.

In the chart, point to any part of the graph to display a summary of data specific to that part. If you click any part on the bar graph, a list opens to provide more detailed information.

Role required: Vulnerability admin

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

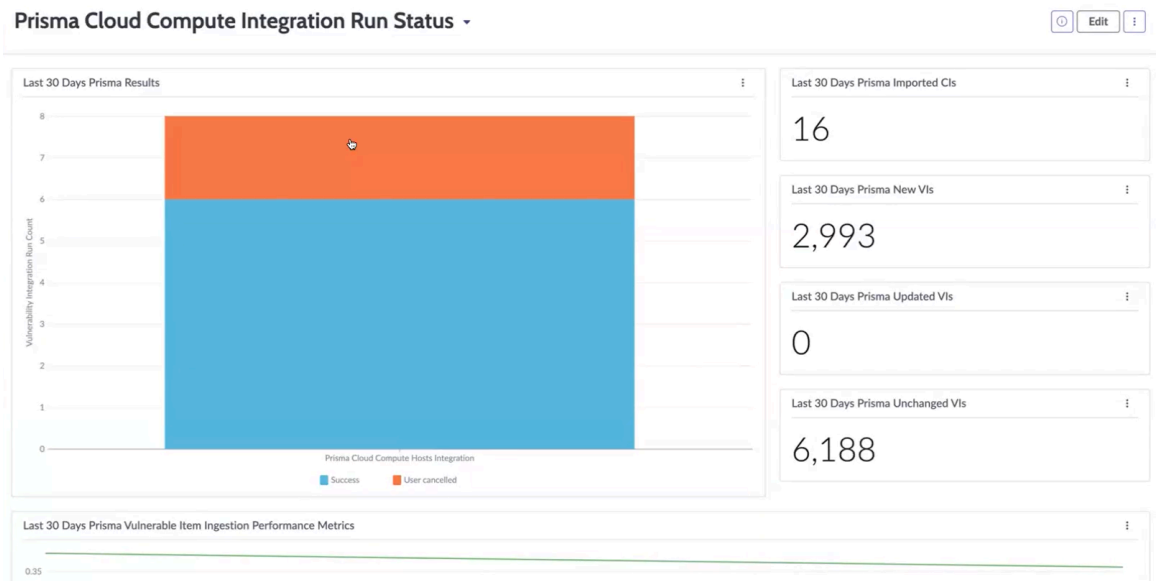
For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

To view the data, navigate to **All** > **Prisma Cloud Compute Integration** > **Integration Run Status**.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Run status



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prisma Cloud Compute integration run status chart reports

Name	Description
Last 30 days Prisma Results	The number of integration runs completed for the integration. Shows both successful and failed runs. Each run displayed as a bar in the graph.
Last 30 days Prisma imported CIs	The number of configuration items (CIs) imported by Prisma in the last 30 days. Shown as an integer.
Last 30 Days Prisma New VIs	The number of new vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Prisma Updated VIs	The number of updated vulnerable items (VIs) imported in the last 30 days. Shown as an integer.
Last 30 Days Prisma Unchanged VIs	The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Prisma Vulnerable Item Ingestion Performance Metrics	Daily performance metrics for vulnerable items compared for the last 30 days.

Understanding the Wiz Vulnerability Response Integration

Import vulnerability and compliance data from Wiz scanners into your ServiceNow® AI Platform instance to help you get deeper insights into your cloud infrastructure risks. These integrations provide you with a comprehensive assessment of your overall cloud security posture and help you drive remediation actions directly from your instance.

Integrations included with the Vulnerability Response Integration with Wiz

The Vulnerability Response Integration with Wiz includes the following integrations that import your asset, vulnerability, and compliance data:

- Wiz Asset Integration
- Wiz Container Vulnerability Response Integration
- Wiz Host Test Results Integration
- Wiz Host Vulnerability Integration
- Wiz Configuration Compliance (test results) Integration and Issues integration

Please review more information about the Wiz integration at SecOps articles on the Security Operations Community.

Starting with v1.1, the Missing Assets [sn_vul_wiz_missing_asset] table for storing assets from the backfill integrations is deprecated. After upgrading to version 1.1, you must backdate your primary Wiz integrations by three days and run them.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

After you upgrade to v1.1, the following backfill integrations are no longer required:

- Host Vulnerability Backfill Integration
- Test Results Backfill Integration
- Host Test Results Backfill Integration
- Issues Backfill Integration

Note: The Wiz Asset and Container Vulnerability Integrations don't have backfill integrations. See Wiz Backfill Integrations for more information.

You identify the specific Resource Types (assets) that you want to import on the Wiz Vulnerability Integration Configuration module in your ServiceNow AI Platform instance.

Benefits and users for the integrations

Benefit	Wiz Integration	Users
Import data about your cloud assets reported by the Wiz scanner. Create and update discovered item records for cloud assets in your ServiceNow AI Platform instance. **Note:** Activating the **Wiz Asset Integration** is optional. You are no longer required to schedule or run it so it runs before the other integrations.	Wiz Asset Integration	Vulnerability managers, analysts, and Cloud security teams
Import and evaluate early detections vulnerabilities on running hosts. The host vulnerability integration imports findings related to virtual machines and serverless assets in your cloud environment. These findings are mapped to Host Vulnerable Items (VITs) within the Vulnerability Response application to support remediation workflows.	Wiz Host Vulnerability Integration.	Vulnerability managers, analysts, and Cloud security teams
Import test results associated with the resource type, VIRTUAL MACHINE.	Wiz Host Test Result Integration	Vulnerability managers, analysts, and Cloud security teams
Import and evaluate container image vulnerability data for vulnerable and non-compliant assets in your cloud infrastructure. Findings are mapped to container vulnerable items (CVITs) to support triage, risk prioritization, and targeted remediation workflows for container-based workloads.	Wiz Container Vulnerability Integration.	Vulnerability managers, analysts, and Cloud security teams

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Benefit	Wiz Integration	Users
Import and evaluate configuration test results from Wiz to detect non-compliant cloud configurations. Findings are mapped to cloud test results (CTRs) in the Configuration Compliance application to help you enforce security policies and standards across your cloud environment.	Wiz Configuration Compliance Integration (Wiz Test Results).	Vulnerability managers, analysts, and Cloud security teams
Import Wiz Issues that identify assets involved in toxic combinations of vulnerabilities and misconfigurations. These findings are mapped to CTRs and labeled with `Wiz Issues` as the source to help you track and remediate assets that might pose complex, multi-vector risks.	Wiz Issues Integration.	Vulnerability managers, analysts, and Cloud security teams
Note: Starting with v1.1, the Missing Assets [sn_vul_wiz_missing_asset] table for storing assets is deprecated. After upgrading to version 1.1, you must backdate and run your primary integrations by three days. See Backfill integrations and upgrading to version 1.1 for more information. The Wiz Backfill integrations retrieve and process data for missing assets that were not processed by the primary vulnerability and compliance integrations.	Wiz Backfill integrations: • Host Vulnerability Backfill Integration • Test Results Backfill Integration • Host Test Results Backfill Integration • Issues Backfill Integration	Vulnerability admins
Apply remediation steps across host vulnerable items (VITs), container vulnerable items (CVTs), cloud test results (CTRs) and CTRs labeled `Wiz Issues`.	Vulnerability Response, Container Vulnerability Response, and the Configuration Compliance applications.	Remediation owners

What to explore next

For more information about installing, configuring, and viewing imported data with the Wiz Vulnerability Response Integration, see:

- Activate the Wiz Vulnerability Response Integration application
- Configure the Wiz Vulnerability Response Integration
- Identify Wiz Resource types for the Wiz Vulnerability Integrations
- Set filtering for the Wiz Host Vulnerabilities Integration
- Set filtering for the Wiz Container Vulnerabilities Integration
- Set filtering for the Wiz Test Results Integration
- Set filtering for the Wiz Issues Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Set filtering for the Wiz Host Test Results Integration
- Wiz Backfill Integrations
- Field mapping for the Wiz Vulnerability Response Integrations

Activate the Wiz Vulnerability Response Integration application

Activate the required application.

Before you begin

Verify you have reviewed the checklists and installed the following ServiceNow® applications:

- Installation of Vulnerability Response and supported applications that include the NVD integration, Vulnerability Response Integration with CISA, and the CWE scheduled job.
- Vulnerability Response and Configuration Compliance for Containers.
- Configuration Compliance.

  These applications are available as separate subscriptions. See Install a ServiceNow Store application for more information about installing Store applications.

Role required: admin

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications**.
2. Locate the Wiz Vulnerability Response Integration application.
3. Select the card to open it and select **Install**.
   See Install a ServiceNow Store application for more information about installing Store applications.
   The Dependency Checklist dialog is displayed. Select any **(Needs to be installed)** links to install any required dependencies you have not already installed.
4. Select **Install** in the Application Installation dialog.
   A message is displayed after the application is successfully installed.
5. See configure the Wiz Vulnerability Response Integration for the steps required to set configure the integrations.

Configure the Wiz Vulnerability Response Integration

Configure the integration in your Wiz service account and assign roles in your ServiceNow AI Platform instance.

Before you begin

You must configure the integration tile in your Wiz account that was created for this integration with the permissions pre-selected. See the Wiz product documentation for more information.

The following Wiz API permissions are required:

- [read:resources]
- [read:host_configuration]
- [read:issues read:threat_issues]
- [read:cloud_configuration]
- [read:vulnerabilities]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required:

- admin to assign roles in your ServiceNow AI Platform instance.

Procedure

1. Assign roles to users for the Wiz integration and for the applications that support the in integration in your ServiceNow AI Platform instance.

   a. Navigate to **User administration** > **Users**

   b. Assign the following roles.

   - sn_vul.vulnerability_admin to configure the Vulnerability Response and Container Vulnerability Response applications.
   - sn_vulc.admin
   - sn_vul_wiz.configure_integration to set up the integration.
   - sn_vul_wiz.read_integration for the users in your organization who you want to view data and records for this integration.

   c. See User administration for more information about creating users and managing roles.

2. As a user with the sn_vul_wiz.configure_integration role, navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration** in your instance.
3. Fill in the fields.

Field	Description
Integration instance	Vulnerability Response Integration with Wiz.
Auth URL	Authentication URL you entered in your Wiz environment.
Api URL	API URL you entered in your Wiz environment.
Client ID	Client ID you want to use for this integration you entered in your Wiz environment.
Client Secret	Client Secret you want to use for this integration you entered in your Wiz environment.

4. **Select Save and test**.
   A message is displayed if the credentials have been saved and validated successfully.
5. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Integrations**.
6. Verify the integrations you want to import data with are activated (Active column set to `true`).
7. Select a record to open it and activate or deactivate the integrations.
8. **Optional:** Select the Schedule tab to modify the run schedule.

   (Optional) By default, all the integrations except the Host Test Results Integration are set to run daily. The Host Test Results Integration is set to run on-demand.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Select **Update** to save your changes.
10. See Identify Wiz Resource types for the Wiz Vulnerability Integrations to identify the asset types that you want to import.

Identify Wiz Resource types for the Wiz Vulnerability Integrations

Set filtering on the Wiz integration configuration page so that you import only the Resource Types (assets) reported by Wiz that you want.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. Select the **Resource Type Configuration** tab and select the **Unlock Resource types** icon ( ).
3. With the Resource types field displayed, select the **Add/Remove multiple** icon ( ) the third icon from the top to the right of the Resources types field.
   The Edit Members modal is displayed.
4. Select one or more resources from the **Available Wiz Resource Types** field and select the right arrow ( ) to move them to the **Selected Wiz Resource Types** field.

   Note: The resource types you configure on the configuration tab apply to all the Wiz integrations except the Wiz Container Vulnerability Integration. The Wiz Container Vulnerability Integration works with discovered container image records, not discovered item records.

   At a minimum, you must add either the `VIRTUAL_MACHINE` or `SERVERLESS` resource type for the Host Vulnerability Integration. You can add both. For the Host Test Results Integration, you must, at a minimum, add the `VIRTUAL_MACHINE` resource type.

5. Select **Save**.
   The **Resource Type Configuration** tab is displayed. Your saved resources are displayed on the tab.
6. Select the lock **Resource types** icon ( ).
7. Select **Save** to save your edits.
8. Select **Save and test** if you're ready to validate your credentials.

   If your credentials are successfully saved and validated, a message is displayed.

   After you validate and test, you have the option to set more filtering parameters on the integration instance records. With this filtering, you can further limit imports to only the specific resource types that you want to import for the Host Vulnerability and Test Results integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If you configure resource types on the Resource Type Configuration tab, and you choose to configure parameters on the integration instance records, your configurations on integration instance take precedence over your settings on the Resource Type Configuration tab.

For example, if you add **VIRTUAL_MACHINE** on the **Resource Type Configuration Tab**, and you also configure **SERVERLESS** for the Host Vulnerability integration instance, the Host Vulnerability integration will import only the SERVERLESS Resource Type.

If you add **VIRTUAL_MACHINE** and **SERVERLESS** resource types on the **Resource Type Configuration Tab**, and you also configure **SERVERLESS** for the Host Vulnerability integration instance, the Host Vulnerability integration will import only the SERVERLESS Resource Type.

9. **Optional:** To add more filter parameters, follow these steps on the integration instance records.

   a. To navigate to the Integration Instance [sn_sec_int_impl] table, enter `sn_sec_int_impl.LIST` in the navigation panel.

   b. Select the **Vulnerability Response Integration with Wiz** record to open it.

   c. On the **Integration Instance Parameters** tab, enter one of the following parameters into the **Search** field under the Configuration column.
      - `host_asset_type`
      - `cc_resource_type`

   d. Select the information icon (ⓘ) next to the record link to open the record.

      Note: You might have to select the link to change the scope for the record.

      The Integration Parameter record is displayed.

   e. Enter the resources that you want to import in the **Default value** field for the respective integration.

      (Optional) You can enter values only for the Host Vulnerability and Test Results Integrations. These values must also be on the **Resource Type Configuration** tab that you entered in the previous steps.

      For example, for the Host Integration, enter any values in the **host_asset_type** field that you entered on the **Resource Type Configuration** tab for this integration.

      For the Test Results Integration, enter any values in the **cc_resource_type** field that you entered on the **Resource Type Configuration** tab for this integration.

   f. Select **Update** to save your changes.
      The Integration Instance record is displayed.

      (Optional) You have the option to limit the number of assets you import with each integration run for the Wiz Asset Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. **Optional:** To modify the number of records processed per Integration Process for the Asset Integration, follow these steps.

    a. Navigate to **All** > **Wiz Vulnerability Integration** > **Admin** > **Integrations**.

    b. Select the **Wiz Asset Integration** record to open it.
    This integration is activated by default. The default setting for imported records is 500.

    c. Select the information icon next to the **Source Instance** field to open the integration instance record.

    d. In the **Search** field with the **Integration Instance Parameters** tab selected, enter the `asset_record_count` parameter.

    e. Select the record in the Configuration column to open it.

    f. Verify that you are in the proper scope to edit the record.

    g. Double-click the **Value** field to modify it.

    h. Select **Update** to save your changes.

What to do next

After you configure all of the integrations, schedule the **Wiz Asset Integration** or initiate it on-demand so it runs before the other integrations. This is the only integration that can discover, import, and create discovered item records for Wiz data. The other integrations depend on imported data from the Wiz Asset Integration. The Wiz Container Vulnerability Integration imports and processes discovered container image records.

See schedule Wiz integrations for more information about scheduling and activating the Wiz integrations and backfill integrations on-demand.

To set filtering for the integrations, for more information see:

- Set filtering for the Wiz Host Vulnerabilities Integration
- Set filtering for the Wiz Container Vulnerabilities Integration
- Set filtering for the Wiz Test Results Integration
- Set filtering for the Wiz Test Results Integration
- Set filtering for the Wiz Issues Integration
- Set filtering for the Wiz Host Test Results Integration

Set filtering for the Wiz Host Vulnerabilities Integration

Set the filtering values to import the host vulnerability data that you want.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. If not already selected, select the **Host Vulnerabilities Configuration** tab.
3. Fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These fields that are displayed provide you with filters to import basic host vulnerability data. Refer to the following tables for more information.

Field	Description
First	Pagination. Enter a value. You might prefer to start with 1000.
Severity	Finding severity. None is the default. If selected, this indicates you don't want to import any data for this field. You can specify multiple values: ○ NONE - Return assets with no available severity values. ○ LOW ○ MEDIUM ○ HIGH ○ CRITICAL
Resource Status	Return only vulnerability findings for assets with these statuses. You can specify multiple values: ○ None (default) - If selected, this indicates you do not want to import any data for this field. ○ Active ○ Error ○ Inactive

To view more filtering options, select the **Advanced** check box.

4. Select the Advanced check box to view more filtering options.

   For most fields, you can specify multiple values. - -None- - is the (default). If - -None- - remains selected for a field, no data is imported for this field.

   If displayed select the lock icons () and () to edit and lock your edits.

Field	Description
Detection Method	Filter on vulnerability findings found by these detection methods: ○ --None-- ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ LIBRARY

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ OS ○ PACKAGE
Vulnerability	Filter on vulnerability findings with matching external ID(s) that you enter, for example, CVE-1234-5678,CVE-9110-26117.
Status	Filter by finding status: ○ --None-- ○ OPEN ○ REJECTED ○ RESOLVED
Related Issue Severity	○ --None-- ○ CRITICAL ○ HIGH ○ INFORMATIONAL ○ LOW ○ MEDIUM
Has Public Exploit	Filter on vulnerability findings for vulnerabilities with an available exploit: (true/false).
Project ID	Filter for vulnerability findings with strings that you enter for the given projects.
Has Fix	Filter on vulnerability findings for vulnerabilities with an available fix (true/false).
Resource	Filter on a resource you enter.
Resource Has Admin Privileges	Filter for vulnerability findings for assets that have admin privileges (true/false).
Subscription	Import findings from the following strings for external subscriptions: (AWS Account, Azure Subscription, GCP Project, and OCI Compartment). You can specify multiple values in an array. If you do not provide a value, all subscriptions are returned.
Has CISA KEV Exploit	Filter for vulnerability findings for vulnerabilities with an available CISA KEV exploit (true/false).
Resource Has High Privileges	Filter for vulnerability findings for assets that have high privileges (true/false).
Validated In Runtime	○ --None-- ○ Yes- Select **Yes** to pull in data for resources that have this flag set to Yes in the Runtime field. In Wiz console, the 'Validated in Runtime' status for a finding typically persists for a 48-hour period from the last time the vulnerable package was detected in memory. ○ No. Do not pull data for these resources.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Resource Has Wide Internet Exposure	Filter for vulnerability findings for assets that have high internet exposure (true/false).
Resource Has Limited Internet Exposure	Filter for vulnerability findings for assets that have low internet exposure (true/false).
First Seen At (After)	Filter by assets seen starting with a date you select.
Resolved At (After)	Filter by assets with vulnerabilities that have been resolved starting with a date you select.
Updated At (After)	Filter by assets that have been updated starting with a date you select.

5. **Select Save and test**.
   If the credentials have been saved and validated successfully a message is displayed. You can select filtering for another integration import.

Set filtering for the Wiz Container Vulnerabilities Integration

Set the filtering values to import the container vulnerability data that you want.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. Select the **Container Vulnerabilities Configuration** tab.
3. Fill in the fields.

   For some fields, you can specify multiple values. - -None- - is the (default). If - -None- - remains selected for a field, no data is imported for this field.

   If displayed select the lock icons () and () to edit and lock your edits.

Field	Description
First	Pagination. Enter a value. You might prefer to start with 1000.
Has Public Exploit	Filter on vulnerability findings for vulnerabilities with an available exploit: (true/false).
Subscription	Import findings from the following strings for external subscription IDs: (AWS Account, Azure Subscription, GCP Project, and OCI Compartment). If you do not provide a value, all subscriptions are returned.
Has Fix	Import vulnerability findings for vulnerabilities with an available fix (true/false).
Vulnerability	Import vulnerability findings with matching external ID(s), for example, CVE-1234-5678,CVE-9110-26117.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Has CISA KEV Exploit	Import only vulnerability findings for vulnerabilities with an available CISA KEV exploit (true/false).
Project ID	Import only vulnerability findings for the given projects (strings).
Resource Has High Privileges	Return only vulnerability findings that have high privileges (true/false).
Resource Status	Return only findings with these statuses. You can specify multiple values: ○ --None-- ○ Active ○ Error ○ Inactive
Resource Has Admin Privileges	Return only vulnerability findings that have admin privileges. (true/false)
Detection Method	Filter on vulnerability findings found by these detection methods: ○ --None-- ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ LIBRARY ○ OS ○ PACKAGE
Resource Has Limited Internet Exposure	Filter for vulnerability findings that have low internet exposure ○ --None-- ○ TRUE ○ FALSE
Status	Filter findings by status: ○ --None-- ○ OPEN ○ RESOLVED
Vulnerability Severity	Filter findings by vulnerability severity: ○ --None-- ○ CRITICAL ○ HIGH

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ LOW ○ MEDIUM
Validated In Runtime	○ --None-- ○ Yes- Select **Yes** to pull in data for resources that have this flag set to Yes in the Runtime field. In Wiz console, the 'Validated in Runtime' status for a finding typically persists for a 48-hour period from the last time the vulnerable package was detected in memory. ○ No. Do not pull data for these resources.

4. **Select Save and test**.
   If the credentials have been saved and validated successfully a message is displayed. You can select filtering for another integration import.
5. **Optional:** Configure the granularity of the container vulnerable items (CVITs) by specifying the key combination.

   (Optional) A CVIT is created by default by combining the image repository, vulnerability, and image. You can add components to the key for further granularity. For example, create a CVIT is for a combination of image repository, vulnerability, image, and cluster.

   To configure the granularity, navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configure CVR based VI Granularity**.

   Select the keys you want to add. If data is imported, keys are considered and CVITs are created.

Configure Container image vulnerability keys for the Vulnerability Response Integration with Wiz

You can configure the granularity of container vulnerable items (CVITs) by specifying the key combination.

Before you begin

You have the option to configure the granularity of container vulnerable items (CVITs) for the Vulnerability Response Integration with Wiz by specifying the key combination. A CVIT is created by default by combining the image repository, vulnerability, and image. You can add components to the key for further granularity. For example, you might create a CVIT that has a combination of image repository, vulnerability, image, and cluster.

Adding this level of granularity can help you locate processes in specific containers.

Role required: sn_vul_wiz.configure_integration

Procedure

1. **Optional:** Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configure CVR based VI Granularity**.
2. Select the check boxes for any additional components (keys) that you want included when your CVITs are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Registry	Centralized location where your container images are stored and managed.
Namespace	Logical grouping of related resources that belongs to a specific application, a team, and so on within a single cluster.
Cluster	Collection of machines that provides resources for containers.
Service	Cloud computing service that manages the applications of deployed containers.

3. Select **Save**.
   CVITs will be created that include the one or more keys you selected in addition to the image repository, vulnerability, and image starting with the next Wiz Container Vulnerabilities Integration import.

Set filtering for the Wiz Test Results Integration

Set the filtering values to import the cloud test results data that you want.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. Select the **Test Results Configuration** tab.
3. Fill in the fields.

   For some fields, you can specify multiple values. - - None - - is the (default). If - - None - - remains selected for a field, no data is imported for this field.

   Note: Host configurations from Wiz are not imported.

   If displayed select the lock icons ( ) and ( ) to edit and lock your edits.

   Select the **Add/Remove multiple** icon ( ) to open the Edit members modal.

Field	Description
Severity	Choose one for Severity filtering: ○ --None-- ○ LOW ○ MEDIUM ○ HIGH ○ CRITICAL ○ NONE - Return findings with no available severity values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	You might prefer to start with HIGH or CRITICAL to limit your import to findings of critical importance.
Project ID	Specify only Cloud Configuration findings for Projects, for example, `Named "Project ID"`.
Cloud platform	Configuration findings by Cloud platform. You can specify multiple values, for example, AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS.
Subscription ID	Specify by entering subscription ID. You can specify multiple values in an array.
Resource Status	Specify by status: ○ --None-- ○ Active ○ Error ○ Inactive
Framework Category	Enter security frameworks, security subcategories, or security categories. You can specify multiple values.
Resource type	Select **Add/Remove multiple** icon to display the modal. Move your choices to the right column and select **Save**. Or, search for an asset target record type, for example, FIREWALL. You also have the open to add a new resource type record.
Native type	Specify findings based on the native type of the cloud resource, for example, `bucket`.
Has remediation	Specify findings with (TRUE), without (FALSE) remediation instructions, or --None--.
Status	Filter by status: ○ --None-- ○ OPEN ○ RESOLVED
First	Pagination. Enter a value. You might prefer to start with 500.
Fetch rejected findings	Select this check box if you want to import Cloud test results in a failed state (rejected) from Wiz. If not selected, failed Cloud test results reported by Wiz are not imported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If imported, these test results remain in a failed state but are not rolled up to Configuration Compliance findings.
Close rejected findings	Select this check box if you want to import failed Cloud test results reported by Wiz and automatically close them after import. If not selected, these test results remain in a failed state but are neither closed nor rolled up to Configuration Compliance findings.

4. **Select Save and test**.
   If the credentials have been saved and validated successfully a message is displayed. You can select filtering for another integration import.

Set filtering for the Wiz Issues Integration

Set the filtering values to import Wiz Issues that identify assets involved in toxic combinations of vulnerabilities and misconfigurations.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. Select the **Issues Configuration** tab.
3. Fill in the fields.

   For some fields, you can specify multiple values. - -None- - is the (default). If - -None- - remains selected for a field, no data is imported for this field.

   If displayed select the lock icons ( ) and ( ) to edit and lock your edits.

Field	Description
Severity	Filter by finding severity. ○ --None-- ○ LOW ○ MEDIUM ○ HIGH ○ CRITICAL ○ INFORMATIONAL
Project ID	Import only findings for the given projects (strings).
Issue type	Issues by the rule type they are generated by.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ CLOUD_CONFIGURATION ○ THREAT_DETECTION ○ TOXIC_COMBINATION
Subscription ID	Specify findings by entering a subscription ID. You can specify multiple values in an array.
Cloud platform	Configuration findings by Cloud platform. You can specify multiple values, for example, AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS.
Framework Category	Enter security frameworks, security subcategories, or security categories. You can specify multiple values.
Native type	Issues based on the native type of the cloud resource, for example, `bucket`.
First	Pagination. Enter a value. You might prefer to start with 1000.
Status	Filter by status: ○ --None-- ○ OPEN ○ IN PROGRESS ○ RESOLVED
Fetch rejected findings	Select this check box if you want to import Cloud test results in a failed state (rejected) from Wiz. **Note:** These findings are mapped to CTRs and labeled with `Wiz Issues` as the source to help you track them. If not selected, failed test results reported by Wiz are not imported. If imported, these test results remain in a failed state but are not rolled up to Configuration Compliance findings.
Close rejected findings	Select this check box if you want to import failed Cloud test results reported by Wiz and automatically close them after import. If not selected, these test results remain in a failed state but are neither closed nor rolled up to Configuration Compliance findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. **Select Save and test**.
   If the credentials have been saved and validated successfully a message is displayed. You can select filtering for another integration import.

Set filtering for the Wiz Host Test Results Integration

Set the filtering values to import Wiz host test results.

Before you begin

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Configuration**.
2. Select the **Host Test Results Configuration** tab.
3. Fill in the fields.

   For some fields, you can specify multiple values. - -None- - is the (default). If - -None- - remains selected for a field, no data is imported for this field.

   If displayed select the lock icons () and () to edit and lock your edits.

   Select the **Add/Remove multiple** icon () to open the Edit members modal.

Field	Description
Status	Filter by status: ○ --None-- ○ OPEN ○ RESOLVED
Cloud platform	Configuration findings by Cloud platform. You can specify multiple values, for example, AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS.
Severity	Choose one for Severity filtering: ○ --None-- ○ LOW ○ MEDIUM ○ HIGH ○ CRITICAL ○ NONE - Return findings with no available severity values. You might prefer to start with HIGH or CRITICAL to limit your import to findings of critical importance.
Resource Status	Specify by status:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ --None-- ○ Active ○ Error ○ Inactive
Framework Category	Enter security frameworks, security subcategories, or security categories. You can specify multiple values.
Resource type	Select **Add/Remove multiple** icon to display the modal. Move your choices to the right column and select **Save**. Or, search for an asset target record type, for example, FIREWALL. You also have the open to add a new resource type record.
Native type	Specify findings based on the native type of the cloud resource, for example, `bucket`.
Subscription ID	Specify by entering subscription ID. You can specify multiple values in an array.
First	Pagination. Enter a value. You might prefer to start with 500.

4. **Select Save and test**.
   If the credentials have been saved and validated successfully a message is displayed. You can select filtering for another integration import.

Wiz Backfill Integrations

Prior to v1.1, the Wiz Backfill integrations import and process details for your Assets IDs that are flagged as missing by the primary vulnerability integrations. Starting with v1.1, the backfill integrations are deprecated.

Upgrading to version 1.1

Starting with v1.1, the Missing Assets [sn_vul_wiz_missing_asset] table for storing assets from the backfill integrations is deprecated. After upgrading to version 1.1, you must backdate your primary Wiz integrations by three days and run them.

The Wiz Backfill Integrations are activated by default.

After you upgrade, the following backfill integrations are no longer required. The primary integrations can create discovered item records if they are not found.

- Host Vulnerability Backfill Integration
- Test Results Backfill Integration
- Host Test Results Backfill Integration
- Issues Backfill Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Backfill Integrations overview (for versions prior to v1.1)

A backfill integration is a specialized Wiz integration that processes asset IDs that are reported as missing by the primary Wiz integration imports. Asset IDs flagged as missing, that is, their discovered item records are not found, are stored on the Wiz Missing Assets [sn_vul_wiz_missing_asset] table.

The following Wiz Backfill integrations are activated automatically after their corresponding primary Wiz vulnerability integrations are successfully completed. These integrations process the missing Asset IDs based on their integration type that are stored on the Missing Assets table.

Primary integration	Backfill integration	Integration type
Host Vulnerability Integration	Host Vulnerability Backfill Integration	host_vr
Test Results Integration	Test Results Backfill Integration	test_results
Host Test Results Integration	Host Test Results Backfill Integration	host_test_results
Issues Integration	Issues Backfill Integration	issues

Note: The Wiz Asset Integration does not have a backfill integration, because it can discover assets and create and update discovered item records on the Discovered item [sn_sec_cmn_src_ci] table. The Wiz Container Vulnerability Integration imports and processes discovered container image records.

For example, the Wiz Host Vulnerability Backfill Integration is activated automatically after the Wiz Host Vulnerability Integration is successfully completed. The backfill integration imports and processes any Asset IDs (type host_vr) that are not found by the Host Vulnerability Integration.

If discovered items are found for these Asset IDs by the backfill integration, they are reconciled with their corresponding records and processed. If a corresponding discovered item record is not found, the backfill integration skips these assets, and they remain stored on the Missing Assets table. After records on the Wiz Missing Assets table are successfully reconciled with discovered item records, they are removed from the Missing Assets table.

The backfill integrations by default import and process 100 records on the Wiz Missing Assets table for their corresponding primary Wiz vulnerability integrations. If more than 100 records are found by a backfill integration, an additional integration run for the backfill integration is automatically initiated to process the remaining records.

For example, if the Test Results Integration runs and reports 120 missing Asset IDs, these are stored on the Wiz Missing Asset table. The Test Results Backfill integration is automatically activated to process 100 records for type, test_results. After this Test Results Backfill Integration run is completed, an additional run for the Test Results Backfill Integration is automatically activated to process the remaining 20 records.

Schedule and activate the integrations on-demand

See Schedule the Wiz Vulnerability Integrations for more information about activating the integrations on-demand and scheduling integration runs.

Schedule the Wiz Vulnerability Integrations

You can schedule the integration import times on the their records on the Vulnerability Integrations [sn_vul_int_fw_integration] table and launch them on-demand.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Starting with v1.1, the Missing Assets [sn_vul_wiz_missing_asset] table for storing assets from the backfill integrations is deprecated. After upgrading to version 1.1, you must backdate your primary Wiz integrations by three days and run them.

Note: Activating the **Wiz Asset Integration** is optional. You are no longer required to schedule or run it so it runs before the other integrations.

Role required: sn_vul_wiz.configure_integration

Procedure

1. Navigate to **All** > **Wiz Vulnerability Integration** > **Administration** > **Integrations**.
2. Select an integration record in the **Name** column to open it.
3. Set how often, when you want to run the integration, and any conditions you want on **Schedule** tab.
4. Select **Update** to save your changes.
5. **Optional:** Select **Execute Now** to run the integration on-demand.

   (Optional) Asset data is imported and discovered item records are created or updated in your ServiceNow AI Platform instance based on the Resource types that you selected on the Configuration tab.

   - The Asset Integration imports data about your cloud assets reported by the Wiz scanner.
   - Host vulnerability findings are mapped to host vulnerable items (VITs).
   - Host test results that are associated with the resource type, VIRTUAL MACHINE are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
   - Container vulnerability findings are mapped to container vulnerable items (CVITs).
   - Configuration test results findings are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
   - Issues findings are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
   - The Backfill Integrations import and process any Asset IDs that are reported as missing by the primary vulnerability and compliance integrations.

   The backfill integrations are activated automatically after their primary integrations are successfully completed. See Wiz Backfill Integrations for more information.

Field mapping for the Wiz Vulnerability Response Integrations

Review source and target fields and view imported data on tables and records in your ServiceNow Now Platform AI instance.

Asset Integration field mapping

Wiz field	ServiceNow table	ServiceNow field
id	sn_sec_cmn_src_ci	source_id
nativeType	sn_sec_cmn_src_ci	cloud_resource_type Also, stored in source_data as wiz_native_type

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Wiz field	ServiceNow table	ServiceNow field
type	sn_sec_cmn_src_ci	source_data stored in source_data as ciType
name	sn_sec_cmn_src_ci	name
name	sn_sec_cmn_src_ci	resource_name
graphEntity.providerUniqueId	sn_sec_cmn_src_ci	source_data If exist, stored in source_data as provider_unique_id
graphEntity.properties.externalId	sn_sec_cmn_src_ci	source_data If exist and graphEntity.providerUniqueId does not exist, then it gets stored in source_data as provider_unique_id
lastSeen	sn_sec_cmn_src_ci	non_infra_last_scan_date Also stored as last_scan_time in source_data field in Discovered item table
firstSeen	sn_sec_cmn_src_ci	source_data Stored in source_data as first_seen
isOpenToAllInternet	sn_sec_cmn_src_ci	source_data Stored in source_data as is_open_to_all_internet
isAccessibleFromInternet	sn_sec_cmn_src_ci	cmdb_ci_internet_facing Stored in source_data as is_accessible_from_internet
hasAccessToSensitiveData	sn_sec_cmn_src_ci	source_data Stored in source_data as has_access_to_sensitive_data
hasAdminPrivileges	sn_sec_cmn_src_ci	source_data Stored in source_data as has_admin_privileges
hasHighPrivileges	sn_sec_cmn_src_ci	source_data Stored in source_data as has_high_privileges

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Wiz field	ServiceNow table	ServiceNow field
hasSensitiveData	sn_sec_cmn_src_ci	source_data Stored in source_data as has_sensitive_data
typeFields.operatingSystem	sn_sec_cmn_src_ci	os
typeFields.instanceType	sn_sec_cmn_src_ci	source_data Stored in source_data as instance_type
resourceGroup.id	sn_sec_cmn_src_ci	source_data Stored in source_data as resource_group_id
resourceGroup.name	sn_sec_cmn_src_ci	source_data Stored in source_data as resource_group_name
tags	sn_sec_cmn_src_ci	host_tag
cloudPlatform	sn_sec_cmn_src_ci	cloud_service_provider
region	sn_sec_cmn_src_ci	cloud_region
cloudAccount.externalId	sn_sec_cmn_src_ci	cloud_account
projects	sn_sec_cmn_src_ci	projects
cloudProviderURL	sn_sec_cmn_src_ci	resource_id This is used to retrieve project id in case of GCP cloud platform Serverless resource type.
externalId	sn_sec_cmn_src_ci	resource_id This is used as resource_id in case of Azure cloud platform Virtual machine resource type.

Host vulnerability Integration field mapping

Wiz field	ServiceNow table	ServiceNow field
description	sn_vul_detection	proof
status	sn_vul_detection	source_status
lastDetectedAt	sn_vul_detection	last_found
firstDetectedAt	sn_vul_detection	first_found
vulnerableAsset.name	sn_vul_detection	dns

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Wiz field	ServiceNow table	ServiceNow field
remediation	sn_vul_detection	solution_summary
vulnerableAsset.ipAddresses[0]	sn_vul_detection	ip_address
vendorSeverity	sn_vul_detection	source_severity
fixedVersion	sn_vul_detection	fixed_version
status	sn_vul_detection	is_ignored
status	sn_vul_detection	status
name	sn_vul_entry	id
score	sn_vul_third_party_entry	v3_base_score
CVEDescription	sn_vul_third_party_entry	summary
vendorSeverity	sn_vul_third_party_entry	source_severity
cvssv3.attackVector	sn_vul_third_party_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_third_party_entry	v3_attack_complexity
cvssv3.confidentialityImpact	sn_vul_third_party_entry	v3_confidentiality_impact
cvssv3.privilegesRequired	sn_vul_third_party_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_third_party_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_third_party_entry	v3_user_interaction
hasExploit	sn_vul_third_party_entry	exploit
hasCisaKevExploit	sn_vul_third_party_entry	cisa_exists
vulnerableAsset.tags	sn_sec_cmn_src_ci	host_tag
vulnerableAsset.id	sn_sec_cmn_src_ci	source_id
vulnerableAsset.name	sn_sec_cmn_src_ci	name
vulnerableAsset.region	sn_sec_cmn_src_ci	cloud_region
vulnerableAsset.providerUniqueId	sn_sec_cmn_src_ci	resource_id
vulnerableAsset.cloudPlatform	sn_sec_cmn_src_ci	cloud_service_provider
vulnerableAsset.type	sn_sec_cmn_src_ci	assetType
relatedIssueAnalytics	sn_sec_cmn_src_ci	source_data
vulnerableAsset.nativeType	sn_sec_cmn_src_ci	cloud_resource_type
vulnerableAsset.subscriptionExternalId	sn_sec_cmn_src_ci	cloud_account
vulnerableAsset.name	sn_sec_cmn_src_ci	resource_name
vulnerableAsset.imageName	sn_sec_cmn_src_ci	image_id
vulnerableAsset.*	sn_sec_cmn_src_ci	source_data All the details inside vulnerableAsset are added in source_data field.
lastDetectedAt	sn_sec_cmn_src_ci	source_data

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Container vulnerability Integration field mapping

Wiz field	ServiceNow table	ServiceNow field
imageId	sn_vul_container_image	image_id
vulnerableAsset.name	sn_vul_container_image	image_name
vulnerableAsset.repository.externalId after ##	sn_vul_container_image	registry
vulnerableAsset.repository.externalId before ##	sn_vul_container_image	repo
vulnerableAsset.tags	sn_vul_container_image	image_labels
projects	sn_vul_container_image	image_projects
vulnerableAsset.region	sn_vul_container_image	cloud_regions
vulnerableAsset.cloudPlatform	sn_vul_container_image	cloud_providers
vulnerableAsset.subscriptionExternalId	sn_vul_container_image	cloud_account_ids
vulnerableAsset.executionControllers.name	sn_vul_container_image	image_namespace
vulnerableAsset.executionControllers.name	sn_vul_container_image	image_clusters
vulnerableAsset.executionControllers.name	sn_vul_container_image_vulnerable_item	image_clusters
vulnerableAsset.executionControllers.name	sn_vul_container_image_vulnerable_item	image_namespace
vulnerableAsset.repository.externalId before ##	sn_vul_container_image_vulnerable_item	image_repository
layerMetadata.isBaseLayer	sn_vul_container_image_findings	is_base_image
firstDetectedAt	sn_vul_container_image_findings	first_found
lastDetectedAt	sn_vul_container_image_findings	last_found
detailedName	sn_vul_container_image_package	name
version	sn_vul_container_image_package	version
locationPath	sn_vul_container_image_package	path
name	sn_vul_entry	id
score	sn_vul_third_party_entry	v3_base_score
CVEDescription	sn_vul_third_party_entry	summary
vendorseverity	sn_vul_third_party_entry	source_severity
cvssv3.attackVector	sn_vul_third_party_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_third_party_entry	v3_attack_complexity
cvssv3.confidentialityImpact	sn_vul_third_party_entry	v3_confidentiality_impact
cvssv3.privilegesRequired	sn_vul_third_party_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_third_party_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_third_party_entry	v3_user_interaction
hasExploit	sn_vul_third_party_entry	hasExploit

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Wiz field	ServiceNow table	ServiceNow field
layerMetadata.isBaseLayer	sn_vul_container_image_layer	Base layer
layerMetadata.details	sn_vul_container_image_layer	instruction
layerMetadata.id	sn_vul_container_image_layer	id
status	sn_vul_container_image_findings	is_ignored
validate_at_runtime	sn_vul_container_image_findings	validate_at_runtime
id	sn_vul_container_image_findings	unique_key
fixed_version	sn_vul_container_image_findings	fix_status

Configuration Compliance Test Results Integration field mapping

Wiz field	ServiceNow table	ServiceNow field
rule.id	sn_vulc_test	source_id
rule.name	sn_vulc_test	short_description
rule.remediationInstructions	sn_vulc_test	remediation
rule.description	sn_vulc_test	description
severity	sn_vulc_test	source_criticality
status	sn_vulc_result	result
id	sn_vulc_result	source_id
analyzedAt	sn_vulc_result	last_seen
firstSeenAt	sn_vulc_result	first_seen
rule.remediationInstructions	sn_vulc_result	remediation
resource.nativeType	sn_sec_cmn_src_ci	source_data
resource.type	sn_sec_cmn_src_ci	source_data
id	sn_vulc_result	description
id	sn_vulc_result	source_id
securitySubCategories.category.framework.id	sn_vulc_citation_src	source_id
securitySubCategories.category.framework.name	sn_vulc_citation_src	short_description
securitySubCategories.category.framework.description	sn_vulc_citation_src	description
securitySubCategories.id	sn_vulc_citation	section
securitySubCategories.title	sn_vulc_citation	section_name
resource.projects	sn_sec_cmn_src_ci	projects
status	sn_vulc_result	is_ignored if status is Rejected, is_ignored is set to true, else false.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issues Integration field mapping

Note: Data mapped for the Issues Integration to cloud test results (CTRs) are labeled with `Wiz Issues` as the source to help you differentiate these CTRs from the test results integration CTRs.

Wiz field	ServiceNow table	ServiceNow field
sourceRule.id	sn_vulc_test	source_id
sourceRule.name	sn_vulc_test	short_description
sourceRule.resolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_test	remediation
sourceRule.description	sn_vulc_test	description
severity	sn_vulc_test	source_criticality
createdAt	sn_vulc_result	first_seen
updatedAt	sn_vulc_result	last_seen
status	sn_vulc_result	result
id	sn_vulc_result	source_id
sourceRule.resolutionRecommendation/ sourceRule.remediationInstructions	sn_vulc_result	remediation
sourceRule.controlDescription	sn_vulc_result	description
entitySnapshot.nativeType	sn_sec_cmn_src_ci	source_data
entitySnapshot.type	sn_sec_cmn_src_ci	source_data
Wiz issue	sn_vulc_result	result_type
id	sn_vulc_result	description
severity	sn_vulc_test	source_criticality
id	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.id	sn_vulc_framework	source_id
sourcerule.securitySubCategories.category.framework.name	sn_vulc_framework	short_description
sourcerule.securitySubCategories.category.framework.description	sn_vulc_framework	description
sourcerule.securitySubCategories.id	sn_vulc_citation	section
sourcerule.securitySubCategories.title	sn_vulc_citation	section_name
projects	sn_sec_cmn_src_ci	projects
status	sn_vulc_result	is_ignored if status is Rejected, is_ignored is set to true, else false.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mapping to vulnerable item and test result records

- The Asset Integration imports data about your cloud assets reported by the Wiz scanner.
- Host vulnerability findings are mapped to host vulnerable items (VITs).
- Host test results that are associated with the resource type, VIRTUAL MACHINE are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
- Container vulnerability findings are mapped to container vulnerable items (CVITs).
- Configuration test results findings are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
- Issues findings are mapped to cloud test results records (CTRs) in the Configuration Compliance application.
- The Backfill Integrations import and process any Asset IDs that are reported as missing by the primary vulnerability and compliance integrations.

Manually create a vulnerability integration

Vulnerability integrations provide the ability for customers and vendors to enrich the vulnerability data on their instance by retrieving data from external systems and vendors. This ability can simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

For detailed instructions on creating integrations, see Define a new vulnerability integration.

Define a new vulnerability integration

A vulnerability integration pulls report data from a third-party system, generally to retrieve vulnerability data, and process that reporting data using data sources or a custom processor.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Integrations**.
2. Click **New**.
3. Fill in the fields, as needed.

Vulnerability integration

Field	Description
Name	A descriptive name for the integration.
Active	Whether the integration is active. If you do not want it to run for a specific time period, you can set up the parameters you want to use and deactivate the job.
Run	The frequency you want the integration to run, Daily, Weekly, Periodically, and so on. As

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	noted, subsequent fields are displayed or not based on your setting in this field.
Day	The day you want the integration to run. ○ If you selected **Weekly** in the **Run** field, this field displays the days of the week. ○ If you selected **Monthly** in the **Run** field, this field displays the days of the month.
Time	The time you want the integration to start. This field appears only if you selected **Daily**, **Weekly**, or **Monthly** in the **Run** field.
Application	[Read only] The name of the application for which this integration was created.
Repeat Interval	If you selected **Periodically** in the **Run** field, this field displays the number of days and hours before the integration runs again.
Starting	If you selected **Periodically** in the **Run** field, this field displays the dates and time to be used as the starting point for periodic updates.
Conditional	Select this field if you want to add conditional parameters.
Condition	If you selected the **Conditional** check box, enter the conditions here.
Integration Details	
Integration script	Select the script include that extends the VulnerabilityIntegrationBase to be executed when the integration runs. This script defines how to retrieve data from a third-party system.
Integration factory script	Enter a script that defines how to construct the script include selected for the **Integration script**. For more information, see Integration factory script fields. **Note:** Scripts require both ServiceNow and Vulnerability Response expertise.
Report processor strategy	Select the strategy you want to use to handle the data returned by the integration script when the integration runs. ○ Select **Data Source Attachment** if you want to process data using a data source. ○ Select **Custom Report Processor** to select a custom processor.
Report processor	If you selected **Custom Report Processor** in the **Report processor strategy** field, select the script include that extends the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	VulnerabilityReportProcessorBase script include to be executed when the integration runs. This script defines how to process the data returned by the integration script.
Processor factory script	Enter a script that defines how to construct the script include selected for the **Report processor**.

4. Click **Submit**.

Related topics

Vulnerability integration script

Report processor strategies

Integration factory script fields

Manually run a vulnerability integration

Vulnerability integration script

On the Vulnerability Integration form, the integration script is a reference to a script include that extends the VulnerabilityIntegrationBase script include.

The functionality contained in this script is called by the VulnerabilityIntegrationController to manage the means by which data is retrieved from an external data source. Each subclass of VulnerabilityIntegrationBase has access to contextual information about the calling process. That information is available through the following member variables:

- integrationGr — a GlideRecord of the vulnerability integration record that requested the integration to run.
- integrationProcessGr — a GlideRecord that provides contextual information for the current process of an integration.

The vulnerability process contains special parameters to be used within an integration, generally for pagination purposes. Each run of a vulnerability integration (called a Vulnerability Integration Run) has at least one associated vulnerability integration process. For multi-call integrations, there are one or more vulnerability integration process records for each Vulnerability Integration Run.

The script include must provide an implementation for the `retrieveData()` method and return an object that is processed by the report processor script. The object returned by retrieveData is a simple object with properties for content, contentType, and extension.

Here is a screen shot of VulnerabilityIntegrationBase.retrieveData():

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

The logic in the `retrieveData()` depends on the interface required for retrieving the data. For example, if the source of the data being pulled has a REST API, the body of this method could be calling the REST endpoint, likely via RESTMessageV2. The response of the call can then be parsed or put into an attachment, and the details could be used to construct the return object.

Single call integrations

Single call (single page) integration scripts are the simplest types of integrations. They require one call, often to an external source of data, to retrieve data. Only retrieveData() is required to be implemented for single page/single call integrations.

A sample that demonstrates a simple single call integration script follows. It creates a RESTMessageV2 and executes it. It then returns an object using the response body as the contents, along with an assumed contentType and extension.

Single call integration script

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Multiple call integrations

Multiple call (or multiple page) integration scripts are a bit more complicated. They require multiple calls to a data source to retrieve data.

Like a single call integration, a multiple call integration must also have retrieveData() implemented. In the body of retrieveData(), the integration uses the hasMoreData() and setNextRunParameters() methods provided by VulnerabilityIntegrationBase.

The hasMoreData() method accepts a single Boolean that instructs the VulnerabilityIntegrationController to insert more processes to pull more data. When passing true to hasMoreData(), a call to setNextRunParameters() is made to provide context to the next process.

The setNextRunParameters() method accepts a single object that provides context information to be used by the next call to retrieveData(). This object is used to pass state to subsequent calls to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

retrieveData(). An example use case is to pass an object that indicates the current page number and page size to a web service.

For multiple call integrations, each retrieveData() call first checks the current process parameters. The _getProcessParameters() method is provided to all VulnerabilityIntegrationBase as a convenience to get the parameters set by the previous process. If there are no parameters, it would indicate that it is the first process.

A screen shot of a sample multiple call integration script follows. Extending on the single call integration example, this script demonstrates making calls to a REST endpoint that has basic pagination support. It shows how you can get a single page of data, recognize that there is more data to retrieve, and then tell the next process which page to retrieve.

Multiple call integration script

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Attachments as retrieveData() return values

Sometimes, it is preferable be return an attachment from retrieveData(). The logic to create and/or retrieve an attachment is implementation-specific, but after the attachment is known, its information can be returned.

To provide an attachment, retrieveData() returns an object like:

```
{
       contents: "attachment-sys-id",
       contentType: "sys_attachment"
}
```

An example that extends on the previous example, but saves the response body of the REST Message to the integration process record follows. It then returns that attachment identifier as the contents of the return object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Return attachment from retrieveData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Report processor strategies

The **Report processor strategy** field on the Vulnerability Integration form is used to select the method to process the data returned by the vulnerability integration script when the vulnerability integration process is executed.

The default value is **Data Source Attachment**. This method is the baseline implementation that takes the retrieved data and pass it to a data source to be imported into the system. Selecting **Custom Report Processor** allows you to select a custom processor script for processing the data.

Use the data source attachment report processor strategy

The Data Source Attachment report processor strategy is used to pass data retrieved by the integration script to configured data sources.

Before you begin

Role required: sn_vul.vulnerability_write

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Integrations** and create a new integration.
2. In the **Report processor strategy** field, select **Data Source Attachment**.
3. Right-click in the form header, and click **Save**.
4. In the **Vulnerability Integration Data Sources** related list, click **New**.
5. Define the data source to be used.
6. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Repeat steps 4 through 6 if you require additional data sources.
   Be sure to specify the order that the multiple data sources send information in the **Order** field.
8. Click **Update**.

About custom report processor scripts

On the Vulnerability Integration form, the Report processor is a reference to a script include that extends the VulnerabilityReportProcessorBase script include. The functionality contained in this script is called by the VulnerabilityIntegrationController and defines the means by which the data returned by the integration script are processed.

Each subclass of VulnerabilityReportProcessorBase has access to contextual information about the calling process. That information is available through the following member variables:

- integrationGr — a GlideRecord of the Vulnerability Integration record that requested the integration to run.
- integrationProcessGr — GlideRecord of the Vulnerability Process that provides contextual information for the current process of an integration.

The script include must provide an implementation for the `processReport()` method. The object passed to processReport() is the object returned by retrieveData, and as such, is a simple object with properties for content, contentType, and extension. The actual logic in processReport() is implementation-specific and dependent of the report data provided.

Here is a screen shot of the VulnerabilityReportProcessorBase.processReport():

Custom report processor script

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Integration factory script fields

The Vulnerability Integration form contains the integration factory script and, when the **Custom Report Processor** report processor strategy is selected, the Processor factory script. These fields are used to provide the logic to actually instantiate the object defined by the script include reference fields, Integration script, and Report processor, respectively.

When the script include is selected, both fields are pre-populated with a no-argument constructor call. Often, this is sufficient, but there can be occasions where more logic is required to instantiate the script object.

The integrationProcessGr record is exposed to the factory script fields so process-specific information can be used, as needed.

Manually run a vulnerability integration

A vulnerability integration is configured to run on a scheduled basis. However, you can run them manually when needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_write

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure
1. Navigate to **All** > **Vulnerability** > **Administration** > **Integrations**.
2. Open the integration you want to run.
3. Click **Execute Now**.

Manual ingestion of vulnerabilities
Manually ingest vulnerabilities into the Vulnerability Response application so that you can remediate them quickly without having to wait for scanner results.

Third-party scanners such as Rapid7 help import vulnerability data into Vulnerability Response and process the data to report the findings. With Manual Ingestion integration, you can proactively ingest the vulnerabilities and remediate them instead of waiting for scanners to report the assets that are at risk. Manual ingestion of vulnerabilities effectively protects the assets against unknown threats such as zero-day exploits.

Manual ingestion of vulnerabilities

You can import the vulnerability data by uploading a template in the following file formats:

- Excel
- Comma-separated value (CSV)

To access and download the template, navigate to **All** > **Vulnerability Response** > **Manual Vulnerability Item Ingestion** > **Upload File UI**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ensure that you follow these key points while populating the records in the template:

- Do not make any typing errors in the Severity/ State column records. If there is a typing error, the record is skipped.
- Do not change the column names.
- Do not put column names in any row except the first row.
- Do not change the order of the sheets in the Microsoft Excel template. The vulnerabilities data must always be present in the second sheet.
- Do not put vulnerabilities details in any sheet except the Input Manual Detections sheet.
- Do not use any character except alphanumeric and special characters such as dash (-), period (.), plus (+), underscore (_), space, brackets '(' ')', and at symbol (@) for the filename.

For instructions on how to populate the data in the template, see Template for manual ingestion of vulnerabilities.

Starting with v24.0.6 of Vulnerability Response, you can also create additional columns in the Microsoft Excel template. For more information, see KB1646630.

Manual Ingestion integrations

The integration is triggered when a file is uploaded. Based on the type of file uploaded, the related integration is triggered.

To view the integrations, navigate to **All** > **Vulnerability Response** > **Manual Vulnerability Item Ingestion** > **Integrations**.

The following base system Manual Ingestion integrations are available by default.

Integrations

Integration type	Description
Manual Ingestion Excel Integration	Retrieves data by fetching the latest Microsoft Excel file uploaded from the Vulnerability Ingestion Push Queue table and copies the attachment to the respective Integration run.
Manual Ingestion CSV Integration	Retrieves data by fetching the latest CSV file uploaded from the Vulnerability Ingestion Push Queue table and copies the attachment to the respective Integration run.

The Manual Ingestion third-party integration creates an integration instance, by default, with the following two integration instance parameters:

- max_input_records: Defines the number of records that can be created in the template. If you add more records than what is specified in this parameter, the additional records are skipped. The number of records can be updated in the Value column. The recommended number of record creations in the template is 1000. Anything above this value can pose performance challenges.
- insert_fixed: Imports fixed vulnerability detections.

To view the integration instance parameters, navigate to **All** > **Vulnerability Response** > **Manual Vulnerability Item Ingestion** > **Integrations** and click the source instance of any integration. Alternatively, you can navigate to **All** > **Vulnerability Response** > **Integration Instances** and click **Manual Ingestion**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ingest vulnerabilities manually

Manually ingest vulnerabilities by uploading a template with vulnerabilities data.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Upload File UI**.
2. Click the Excel or CSV links and download the template in the respective format.
3. In the template, enter the vulnerability data in the records.
   For instructions on how to populate the data in the template, see Template for manual ingestion of vulnerabilities.
4. Click **Import File** and upload the updated template.
5. Click **Submit**.
   The Vulnerability Integration Push Queues page is displayed. You can view the list of integration instances, status of the integration runs, and log notes after the integration run is completed.

What to do next

After you upload the file, navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Integrations**. Verify that the integration run is successful.

Verify manual integration run

Verify that the integration run is successful. View the number of individual detections and the vulnerable items (VIs) created or updated due to the integration run.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Integrations**.
2. Click the name of the integration based on the file type uploaded.
3. Click the **Vulnerability Integration Runs** tab.
4. Click the integration run number.
5. Click the **Items** tab.
6. Review the information in the **Items** tab.

Items tab

Tab/ Field	Description
Items tab	Displays the total number of VIs that are imported. You can see the total detections imported by adding the numbers listed on the Detections tab.
New items	Displays the number of vulnerable items that are created from this integration run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tab/ Field	Description
Imported items	Displays the sum of the all the fields in this section.
Duplicate items	Displays duplicate items. This field is not populated anymore.
Updated items	Displays the number of times vulnerable items are updated during this integration run. This value is not the number of unique vulnerable items that are updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.
Unchanged items	Displays vulnerable items found during the integration run that exist in the database but were not updated, because none of the relevant field values had changed.

What to do next

After you verify that the integration run is successful, navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Upload File History**. Verify if there are any failed records from the Notes.

Configure auto-close manual detections

Enable the auto-close manual detections to close stale manual detections automatically.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Upload File UI**.
2. Click **Change Auto-Close Configuration**.
3. Click the **Manual Detections** tab.
4. Make sure the **Auto-close manual detections** check box is selected.
5. In the **Manual detections last found (days ago)** field, enter the number of days after which the manual detections should be closed.
   The default is 90 days. You can enter any positive value for the number of days.

Verify upload status

Verify whether the vulnerability integration run was successful, partially successful, or a failure.

Before you begin

Role required: sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Manual Vulnerable Item Ingestion** > **Upload File History**.
2. In the Vulnerability Integration Push Queues table, check the time of the upload and status of the upload in the Created and State columns respectively.
3. **Optional:** In the **Notes** field, view the reason for the failure.

Template for manual ingestion of vulnerabilities

The template provides columns that must be filled with vulnerability and configuration item (CI) data. After the template is populated and uploaded, the data is processed.

Instructions for populating the template

To enter the details in the template, follow the instructions provided in the following table.

Template instructions

Column	Required/ Optional?	String length (max)/ Valid values	Description
Asset ID	Optional	255	Universally unique identifier (UUID) or Asset ID. It can be the value generated by a scanner.
Enter information in at least one of the following five columns:			
MAC Address	Required	24	Host or asset information. The combination of all values provided must be unique for an asset.
FQDN	Required	255	
NETBIOS	Required	255	
IP Address	Required	255	
Hostname	Required	255	
The remaining columns don't depend on each other.			
Vulnerability ID	Required	255	Represents a vulnerability in the National Vulnerability Database (NVD) or an ID returned from a third-party scanner.
Vulnerability Summary	Optional	512	Brief description of the vulnerability. It is added to the database only when the Vulnerability ID is unavailable.
Severity	Optional	critical, high, medium, low, none	Severity of the vulnerability. It is added to the database only when the Vulnerability ID is unavailable. If the record is empty, then by default it is considered as critical.
Port	Optional	Not applicable	Port from which the vulnerability is detected. The value must be a valid integer. If there is an invalid input, the record is skipped.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Template instructions (continued)

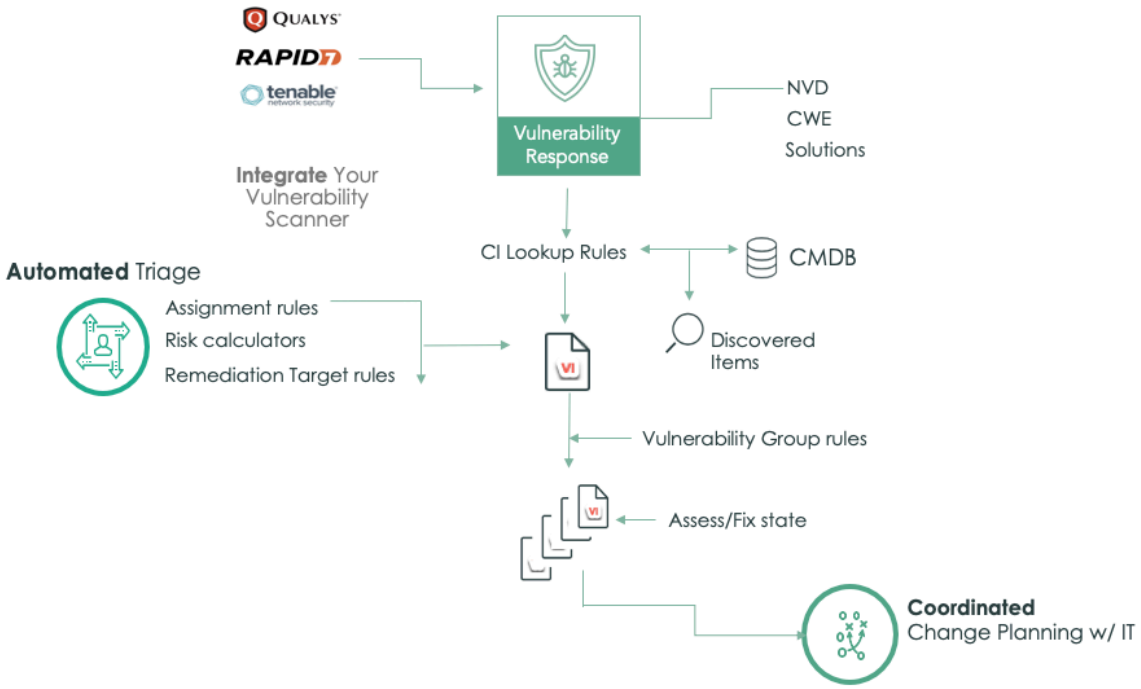
Column	Required/ Optional?	String length (max)/ Valid values	Description
Protocol	Optional	40	Type of network protocol used.
Proof	Optional	4000	Represents the location or system path of the vulnerability.
State	Optional	open, fixed	Status of the detection. If the record is empty, then by default it is considered open.

Vulnerability Response remediation overview

Vulnerability Response remediation is a phased process consisting of verifying import completion, triaging new vulnerabilities, and monitoring progress to completion. Approached in this way, remediation becomes manageable, timely, and in many ways, automated.

Understanding your security posture across company assets helps you identify the most critical vulnerabilities for remediation. This remediation process requires that Vulnerability Response and a third-party integration such as the Qualys Vulnerability Integration are installed and configured.

Vulnerability Response integration process flow



Verify the successful completion of third-party integration imports

The first phase in this process is to ensure that everything is working correctly. Vulnerability Response is preset to download National Vulnerability Database (NVD) and Common Enumeration Weakness (CWE) vulnerabilities. Third-party imports provide you with the data you need to create vulnerable items and remediation tasks. Successful remediation depends on the consistent and successful import of vulnerabilities and vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

During import CI Lookup Rules match third-party assets to assets in the Configuration Management Database (CMDB). All assets are stored in the Discovered Items module. CI information is critical to solution implementation.

Note: Once a third-party integration has been installed and configured, there are few instances where an import can fail, for example, if the third-party vendor throttles their API calls. When imports do fail, they require prompt attention.

Integration status run reports for the supported third-party integrations are shipped with the applications to give you a graphical overview of your imports. Use this report, or create your own, to easily determine whether your latest import has succeeded. For more information about supported integrations, see Vulnerability Response integrations.

Review and triage vulnerabilities and vulnerable items

The next phase of remediation calls for the review of new vulnerabilities and vulnerable items. A vulnerable item (VI) is a detected combination of vulnerability and configuration item (CI). As vulnerable items are formed, various rules are run that assign VIs, determine the risk they pose and set remediation targets. Adjust any rules, as necessary, to ensure that the vulnerable items have been triaged successfully.

Monitor the progress of existing vulnerability remediation

The final phase of remediation consists of monitoring your progress.

- Review the status of imports for patch implementations that have not shown up and follow up with IT Operations.
- Track the progress of regulatory compliance obligations and ensure their completion.
- Review deferred item status and revise or implement fixes.
- Monitor Vulnerability Management dashboards. To review trends, view reports in real-time, and use metrics that track your remediation target attainment rates, you may prefer to monitor your processes with the Performance Analytics for Vulnerability Response application.
- Closing stale detections in Vulnerability Response.

Verify successful completion of Vulnerability Response integration imports

The easiest way to determine whether your imports have succeeded is to use an Integration Run Status dashboard. The Integration Run Status dashboard provides an example of a graphical view of the status of third-party integration runs.

The Qualys and Rapid7 vulnerability integrations have an integration run status dashboard. See Qualys integration run status chart or Rapid7 Vulnerability Integration run status chart for detailed information on the chart contents.

Note: Charts, for integrations not provided by ServiceNow®, can be created from reports in a dashboard but may require ServiceNow expertise. For more information on creating reports and dashboards, see Getting started with reports and Dashboards.

View Vulnerability Response vulnerable item detection data

The complete data gathered by your third-party scanner integrations with Vulnerability Response are displayed on the Detections and Initial Detections tabs on the vulnerable item records (VIT). It is also displayed on Detection records on the Vulnerable Item Detection list in your ServiceNow AI Platform® instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Third-party Integrations retrieve vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners. Detection data are paired with vulnerable items and VI state is updated based on the state of the detections. If a VI is not found, a new one is created. Detections are only opened or closed by data found directly by a scanner.

Role required:

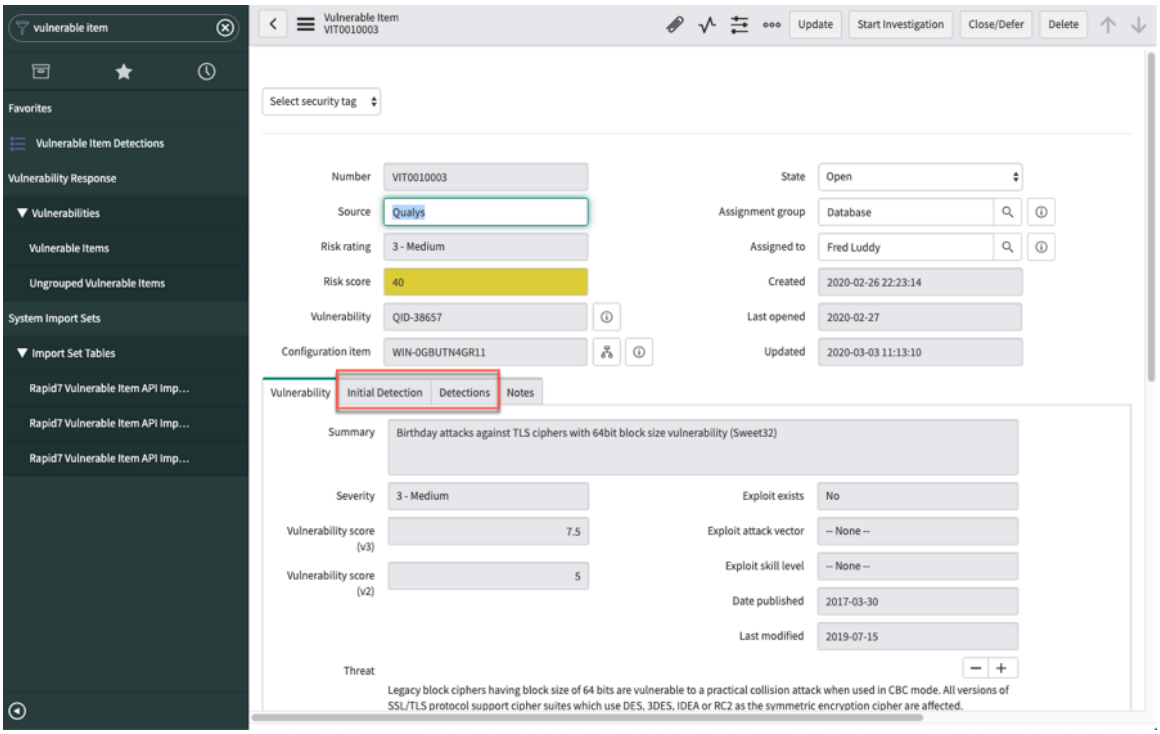
- sn_vuln.admin initiates integration runs and views vulnerable item detection data.
- sn_vul.remediation_owner is assigned vulnerable items created from vulnerable item detections and views data on VI records.

Procedure

1. To view the vulnerable item detection data, navigate to a vulnerable item record and open it.

   The record is displayed with the Initial Detections and Detections tabs.

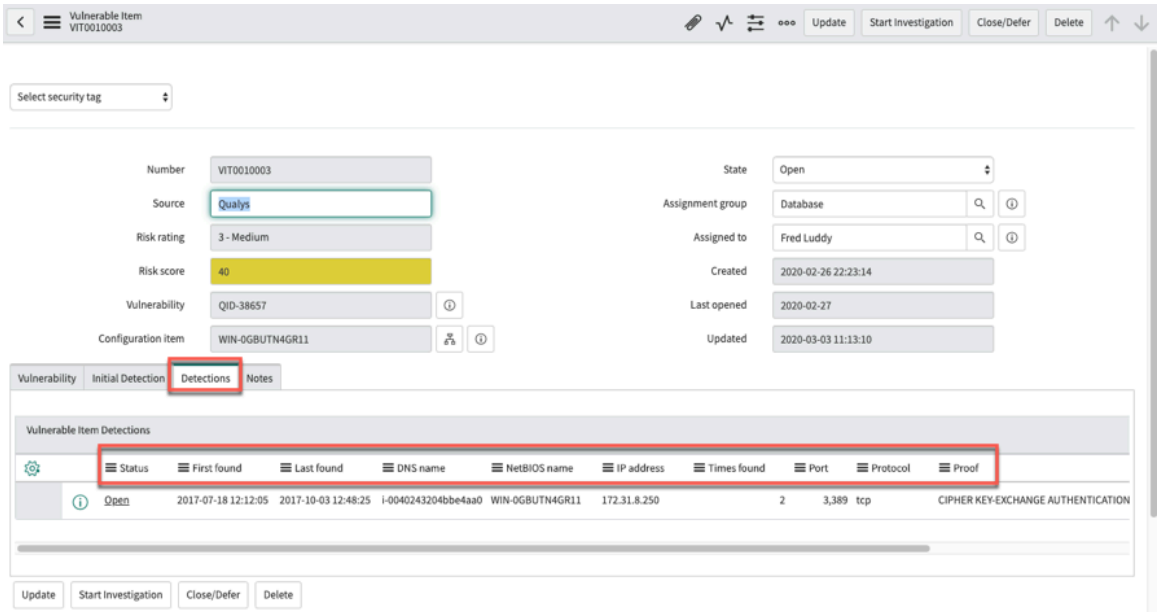
   Note: Data previously displayed on the Configuration Details tab is displayed along with other detection data on the Initial Detection and Detections tabs.



2. Click the **Detections** tab.

   When a vulnerable item is created from the results of a third-party scan, the data from the scan are displayed on the detection record, as shown in the following figure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Each row in the Vulnerable Item Detections section represents data from a distinct detection. In the First found column, the date the vulnerable item is first detected by the scanner is displayed. In the Last found column, the date of the most current detection is displayed. The Source field displays the scanner that retrieved the data.

Note: For Qualys, with vulnerable item detections, the following fields are deprecated on the VI record and are no longer populated:

- Qualys severity
- Last updated by source

Also for Qualys, as shown in the preceding figure, when a VI is created from a scan, the value from the scan for Results is displayed in the Proof column on the detection record. However, this value is not displayed on the upper portion of the VI record.

For Rapid7, when a VI is created from a scan, the value for Proof from the scan can be displayed in both the Proof column on the detection record and on the upper portion of the VI record, but not by default. To display this value on the upper portion of the VI record, select the Proof field from the form layout.

3. **Optional:** To configure the layout of the Detections tab on the record, follow these steps.

a. The following columns are displayed on the Detections tab by default.

- Status
- First found (data)
- Last found (date)
- DNS name
- Net BIOSname
- IP address
- Times found
- Port
- Protocol

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Proof
- SSL

Note:

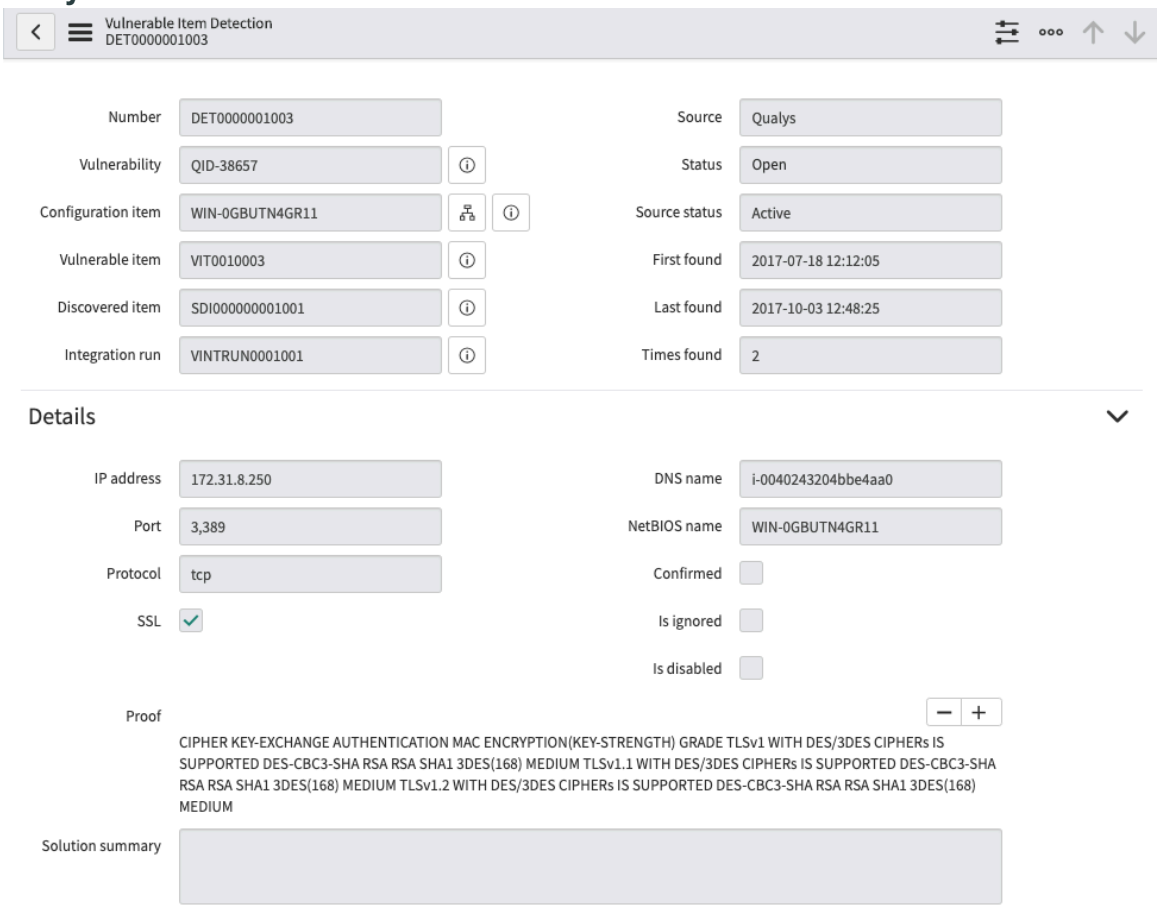
Note: if there is no value in a column, data for that field was not detected by the scanner.

b. Click the gear icon ( ) to personalize your view.

c. Select the columns from the slushbucket to display specific data and click **OK**.

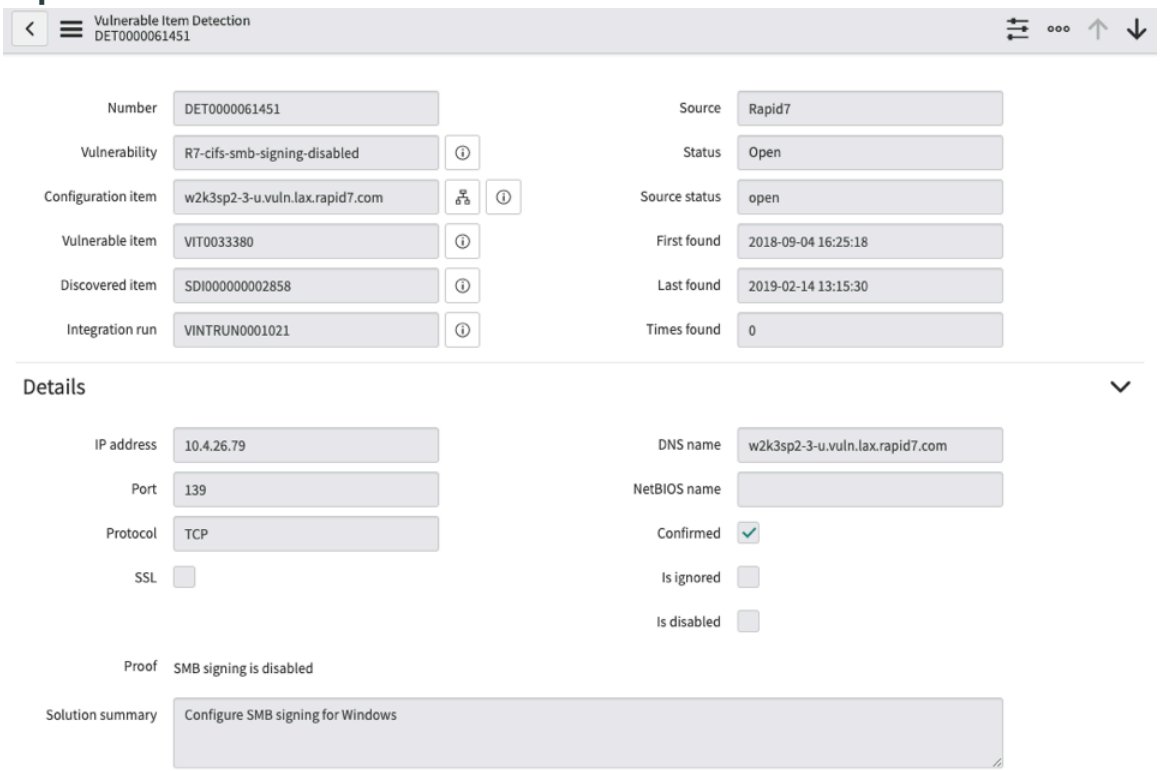
4. With the Detections tab selected, in the Status column, click an item to open the detection record and view the details associated with that vulnerable item, including a Solution summary (Rapid7 InsightVM integration only).

Qualys detection record



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

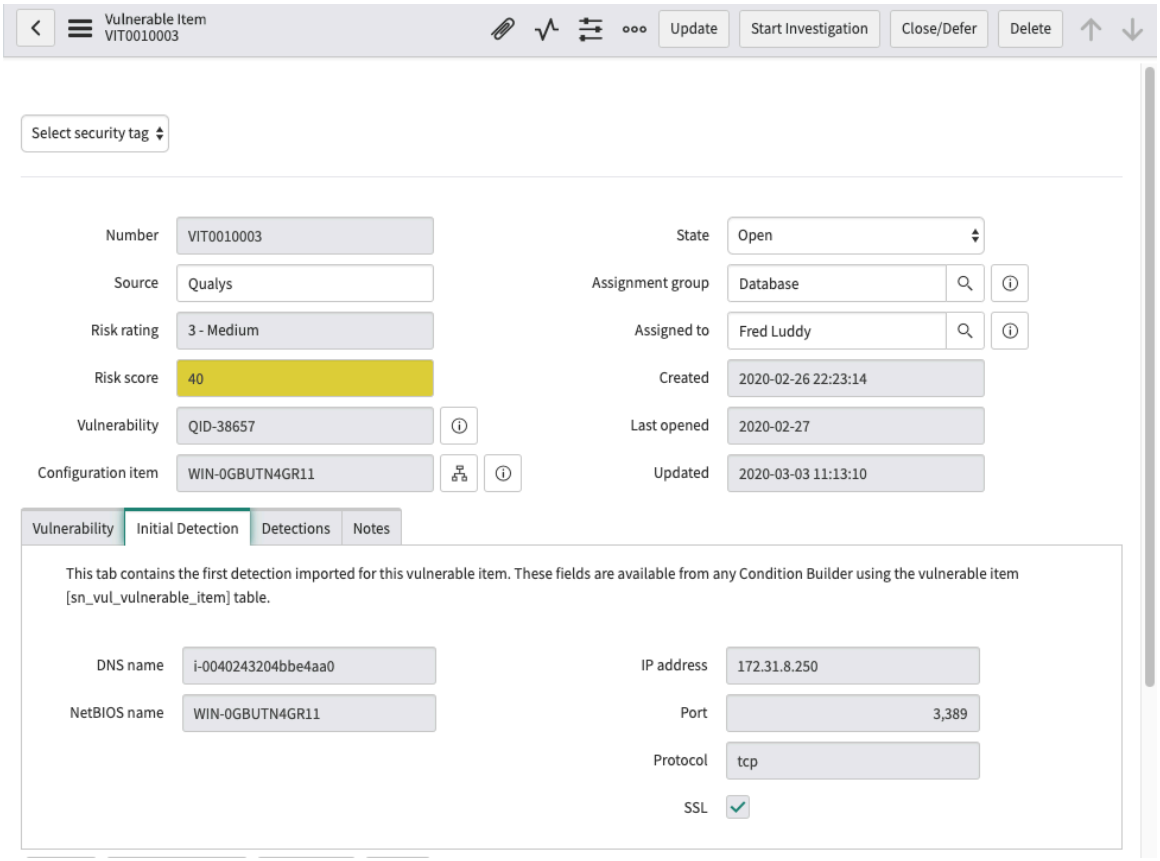
Rapid7 detection record



5. Return to the record and select the Initial Detection tab.

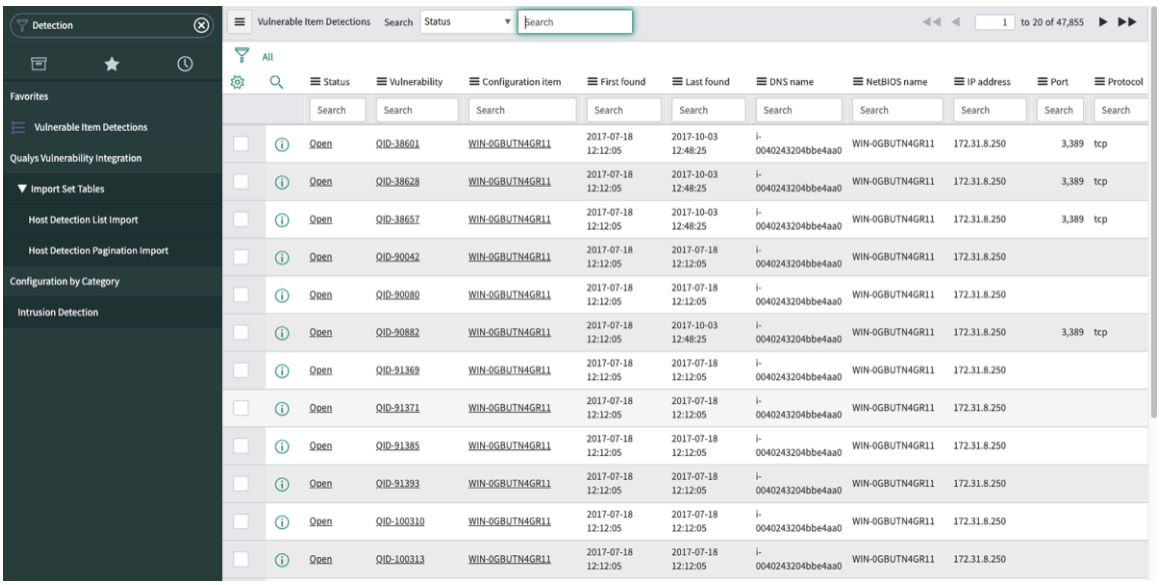
   The Initial Detections tab displays the data imported from the third-party scanner on the first occurrence of the detection. This information on the initial detection tab does not change as detection data are updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. **Optional:** Navigate to Vulnerable Item Detections to view the Vulnerable Item Detection List.

(Optional) The Vulnerable Item Detection list is displayed. Each row on the Vulnerable Items Detections list represents a distinct detection. The columns display the same data as the VI record.



Detections are only opened or closed by data that is found by a scanner, they do not roll down from VIs. As Detections are imported, they are used to create VIs and update the states of VIs. If all detections are closed for a vulnerable item, that vulnerable item will be closed. On the VI record, the state is `closed`, and the substate is `fixed`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Errors are logged while:

- Processing attachments retrieved from the scanner.
- Creating or updating detections or vulnerable items.

For information on handling detection errors, see Error handling for detections.

When all VIs are closed for a remediation task, the remediation task is closed.

Closed VIs with a substate of **fixed** or **stale** are reopened if a new detection is created and the VIs can be matched with the new vulnerability.

Vulnerable items set to **Resolved** in your instance but not transitioned to **Closed/Fixed** by the subsequent integration runs are reopened if they are detected during rescans.

When all VIs are closed for a remediation task, the record is closed.

Vulnerable items set to 'Resolved' in your instance but not transitioned to 'Closed/Fixed' by the subsequent integration runs are reopened if they are detected during rescans.

For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to **Resolved** but then not transitioned to **Closed/Fixed** by subsequent scans transition back to **Open** after the number of days you enter.

For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to **Closed/Fixed** by subsequent scans, these VIs move back to **Open** when the last found date is later than the Resolved date.

What to do next

To view more data, including item and detection counts, you can Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records.

Verify Vulnerability Response vulnerable item detection data on integration run (VINTRUN) records

From integration run records in your ServiceNow AI Platform® instance, you can locate third-party integration vulnerable item detection data based on the date and time of scans. Verify the scan successfully completed, view the number (counts) of individual detections, as well as any vulnerable items (VIs) that are created or updated directly as a result of the scans.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vuln.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

You may prefer to have the integration run information, either date and time of the scan, or the integration run record number (VINTRUN#) from the vulnerable item or detection records to help you locate specific records from the following lists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Choose one to continue.

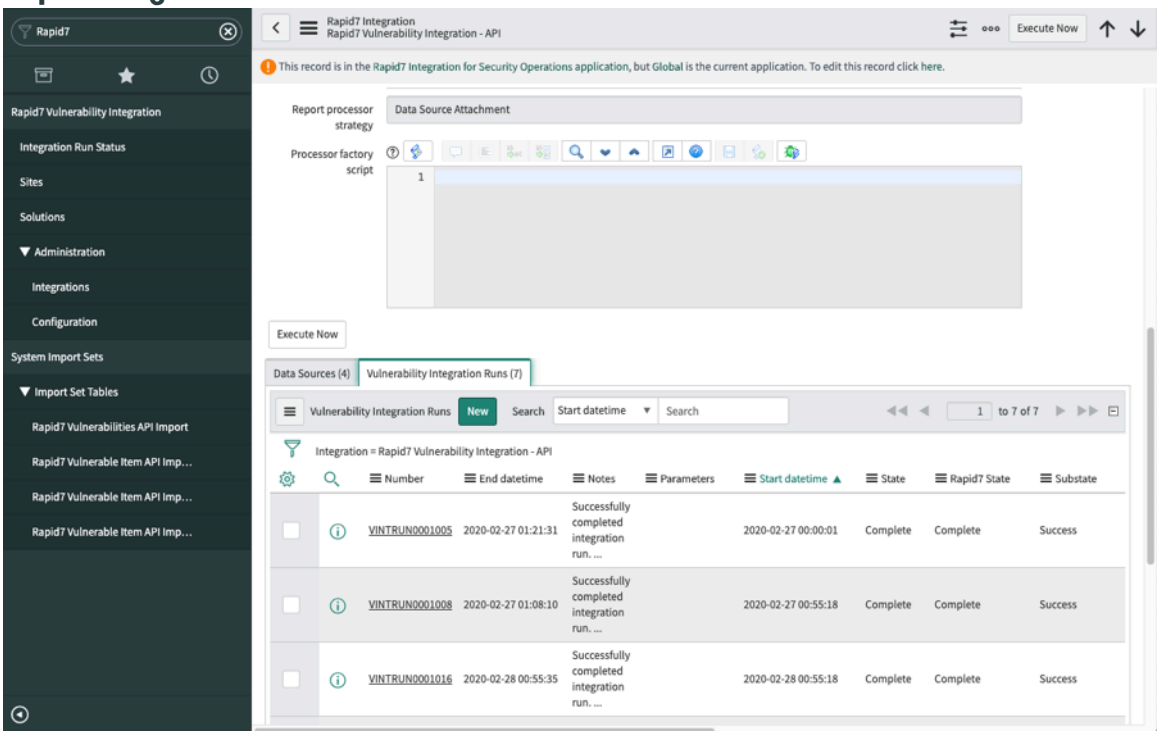
Integration	Description
Navigate to Rapid7 Vulnerability Integration > Administration > Integrations	From the Rapid7 Integrations list, choose the integration you want to view the detection scan results for. **a.** Rapid7 Data Warehouse: ▪ Rapid7 Vulnerable Item Integration ▪ Rapid7 Vulnerable Item Resolution Integration ▪ Rapid7 Comprehensive Vulnerable Item Integration **b.** Rapid7#Vulnerable Item Resolution Integration (InsightVM) ▪ Rapid7 Vulnerable Item Integration - API ▪ Rapid7 Comprehensive Vulnerable Item Integration - API
Navigate to Qualys > Qualys Vulnerability integration > Primary Integrations	From the Qualys Integrations list, choose from: ○ Qualys Host Detection Integration ○ Qualys Comprehensive Host Detection Integration
Navigate to Tenable Vulnerability Integration > Administration > Integrations	From the Tenable Integrations list, choose the integration you want to view the detection scan results for.
Navigate to Microsoft TVM Vulnerability Integration > Administration > Integrations	From the Microsoft TVM Integrations list, choose the integration you want to view the detection scan results for.

2. On the bottom of the page that is displayed, click the **Vulnerability Integration Runs** tab.
3. Click an item in either the Number or Import Source columns to open a record.

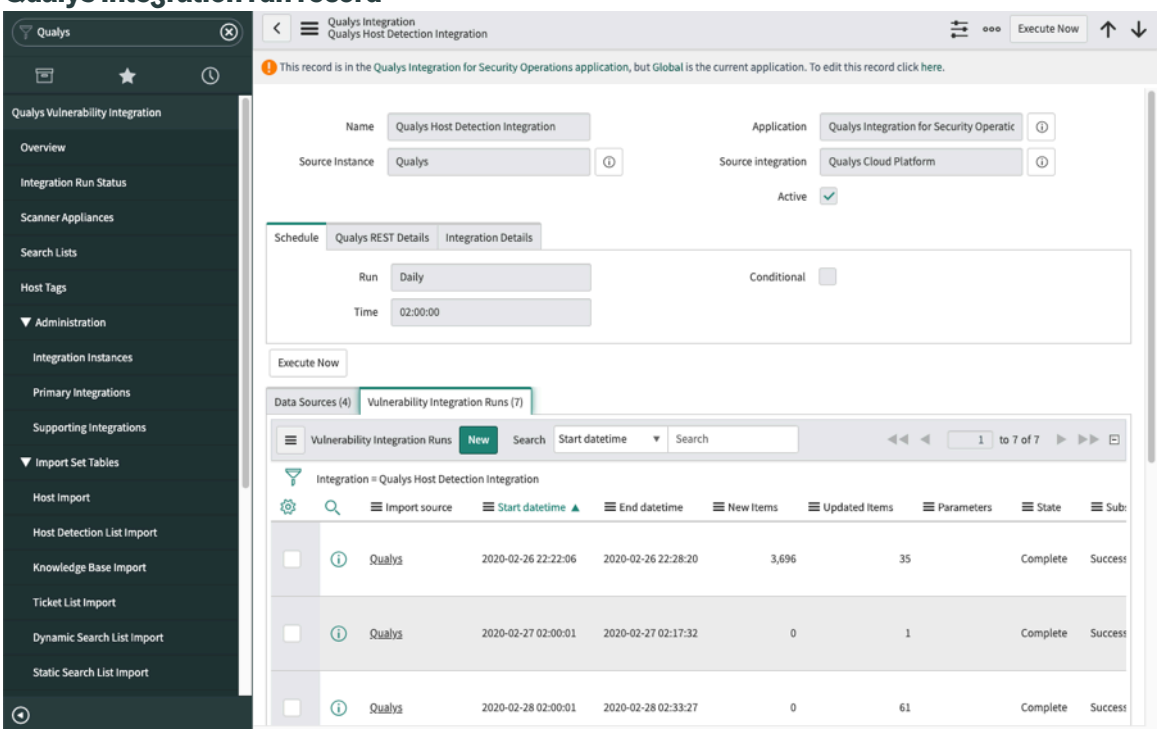
   The integration run record is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rapid7 Integration run record

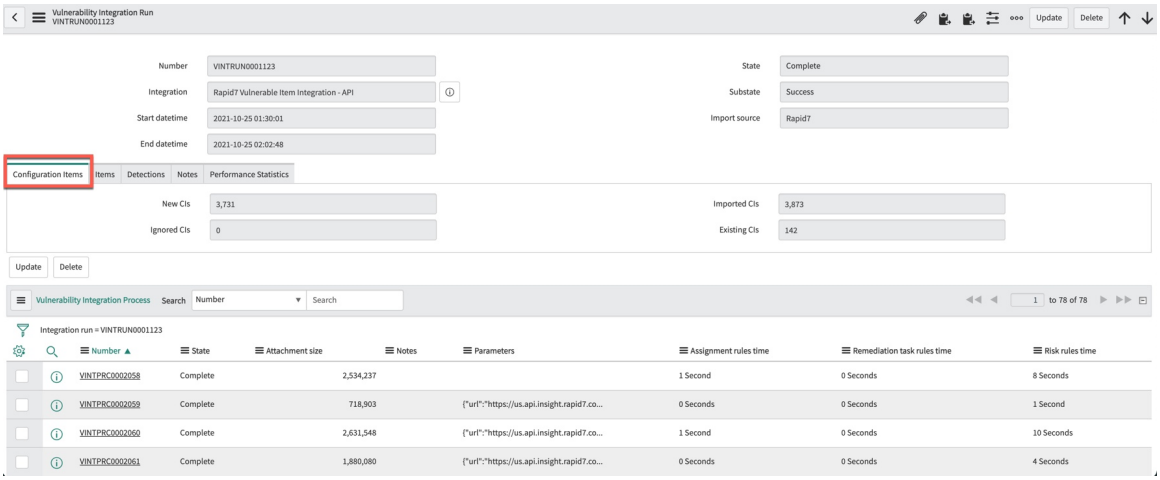


Qualys Integration run record



The integration run record is displayed. You can verify in the State field that the integration ran successfully. Select the **Configuration Items** tab.

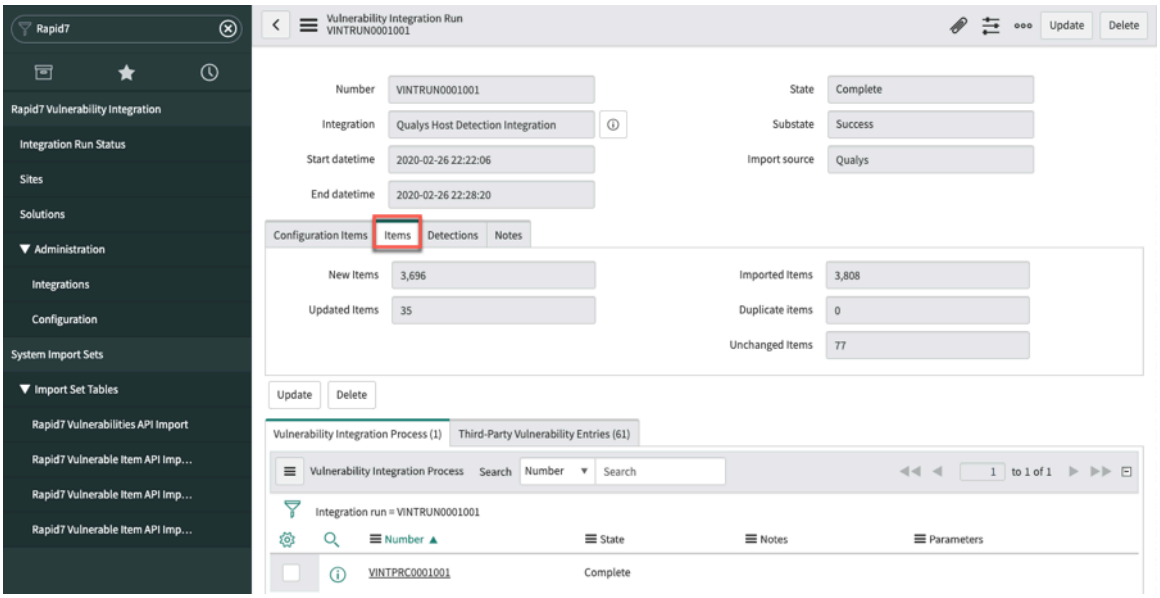
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Configuration Items tab displays the following information:

- The Configuration Items tab displays the total number of configuration items that are imported.
- The New CIs field displays the number of CIs created as a part of this integration run.
- The Imported CIs field displays the sum of all the CIs in this section.
- The value of the Ignored CIs field is always 0 for the Vulnerability Response integrations.
- The Existing CIs field displays the total number of CIs that are already in existence.

Click the **Items** tab.



The Items tab displays the following information:

- The Items tab displays the total number of VIs that are imported. You can see the total detections imported by adding the numbers listed on the Detections tab.
- The New items field displays the number of vulnerable items that are created from this integration run.
- The Imported items field displays the sum of the all the fields in this section.
- The Duplicate items field is no longer populated.
- The Updated items field displays the number of times vulnerable items are updated during this integration run. This value is not the number of unique vulnerable items that are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

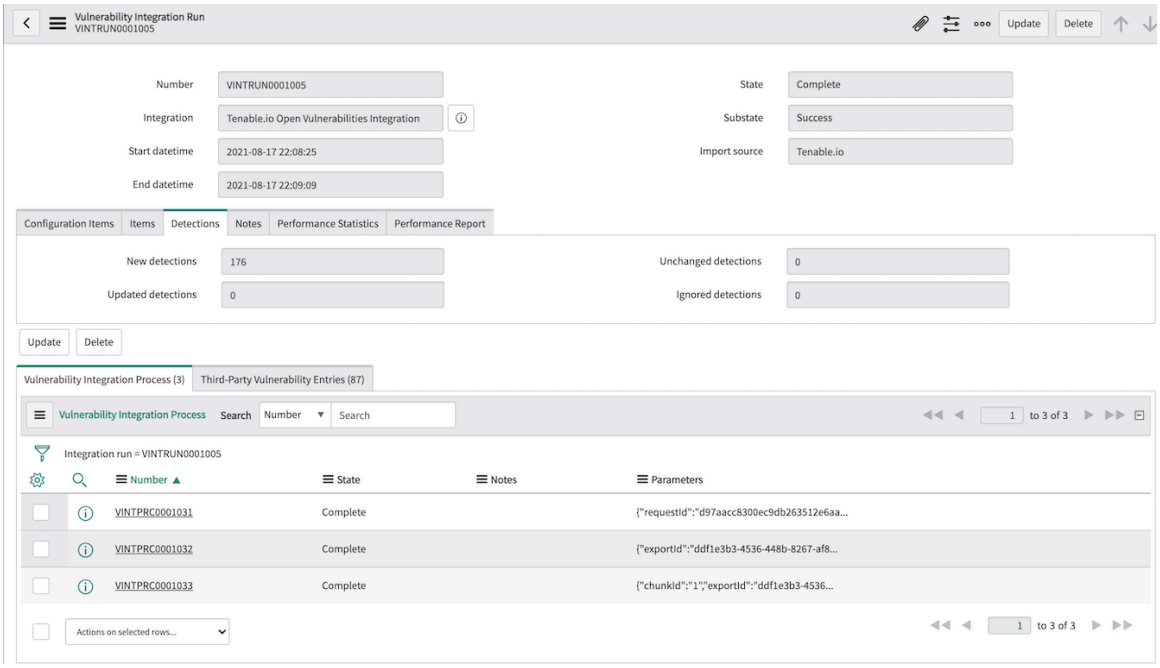
updated. If for example, a vulnerable item is updated two times during the integration run, it is counted two times and displayed as 2 updated items.

- The Unchanged items field displays vulnerable items found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

4. Click the **Detections** tab.

This tab is only displayed if the integration run has any detections. You can verify the total detections imported by adding the numbers listed.

Detections tab from VR v15.0



Note: Prior to v15.0, there was no field for Ignored detections.

The Detections tab displays the following information:

- Starting with v15, a new field Ignored detections has been added to track the detections, which were previously ignored. With this implementation, the count of detections imported, and the count tracked on integration run records becomes consistent. This functionality has been implemented for all the scanners i.e., Qualys Vulnerability Integration, Rapid7 Vulnerability Integration, Tenable Vulnerability Integration and Microsoft TVM.
- The New detections field displays new detections that are created during this integration run.
- The Unchanged detections field displays detections found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.
- The Updated detections field displays the number of times detections are updated during this integration run. This value is not the number of unique detections updated. If for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

example, a detection is updated twice as part of the integration run, it is counted two times and displayed as 2 updated detections.

> **Note:** Detections that are not displayed in these counts are detections that are in a closed state (Fixed), because fixed records are used to update existing VIs. If you want more visibility to these detection records, you can display the closed VIs that are created when there is not an existing, matching VI in an open state. For more information about Vulnerabilities in the fixed state that you can enable in Setup Assistant for the Qualys integration, see Configuring Vulnerability Response using the Setup Assistant.

5. Click an item in either the Number or Import Source columns to open a record.

Viewing patch data and scheduling patches in Vulnerability Response

Starting with v16.1 of Vulnerability Response, you can schedule patches and view patch data along with solution and other vulnerability information on records in both the classic environment and the Vulnerability Response Workspaces in your ServiceNow AI Platform instance.

Roles required

Users need roles that are specific to the patch orchestration integration you are using to import your patches to view data and schedule patches. See the supported integrations for more information.

- Understanding the HCL BigFix patch orchestration integration with Vulnerability Response and Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM.
- Viewing patch orchestration data on the Vulnerability Response dashboards in the classic environment.
- View data on scorecards in the Vulnerability Response Workspaces.

Scheduling patches

You can schedule patches from the following records:

- Patch Update (VPU)
- Remediation task (RT)
- Discovered Item (SDI)

Patch Data in the classic environment

From the classic environment in the Vulnerability Response application:

- To view Patch Update records, navigate to **All** > **Vulnerability Response** > **Patches**.
- To view Solutions, navigate to **All** > **Vulnerability Response** > **Solutions**.
- To view VIs that are assigned to you that have patches, navigate to **All** > **Vulnerability Response** > **Vulnerable Items** > **Assigned to Me with patches**.
- To view remediation tasks, navigate to **All** > **Vulnerability Response** > **Vulnerable Items** > **Assigned to Me with patches**
- To view Discovered item records, navigate to **All** > **Security Operations** > **Discovered items**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Patch data and state rollup for patch orchestration in Vulnerability Response

Starting with v16.1 of Vulnerability Response patch data and states are rolled up to Patch Update and other records in the Vulnerability Response application.

Patch Update records in the workspaces in the classic environment in Vulnerability Response

Information about patches, vulnerability solutions, and vulnerabilities is all connected in the Vulnerability Response application.

Patch data and patch rollup data and status are displayed on records in your instance. Patch records are included as part of the patch orchestration feature of this integration with Vulnerability Response. View Patch (VPU) records in Vulnerability Response Workspaces from the List view in the IT Remediation Workspace. Patch Update records in both the classic view and Vulnerability Response Workspaces include the following data:

- Vulnerability solution data and information from patch vendors imported by the Vulnerability Solution Management application.
- Source Remediation Status that includes the total number of devices that have a vulnerability that can be fixed by a patch, and any devices that are missing updates.
- Remediation Status that includes % of VIs remediated, and the total VIs that have a patch as a preferred patch.
- Associated Devices, Vulnerable Items, Patch Deployments and Patch Requests on the Related Links on records in the class view. This data is displayed on tabs on records in the Vulnerability Response Workspaces.
- Patch Requests that remediation owners have submitted for approval.

Roles required

Users need roles that are specific to the patch orchestration integration you are using to view data and schedule patches. See the supported integrations for more information.

- Understanding the HCL BigFix patch orchestration integration with Vulnerability Response and Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM.
- Viewing patch orchestration data on the Vulnerability Response dashboards in the classic environment.
- View data on scorecards in the Vulnerability Response Workspaces.

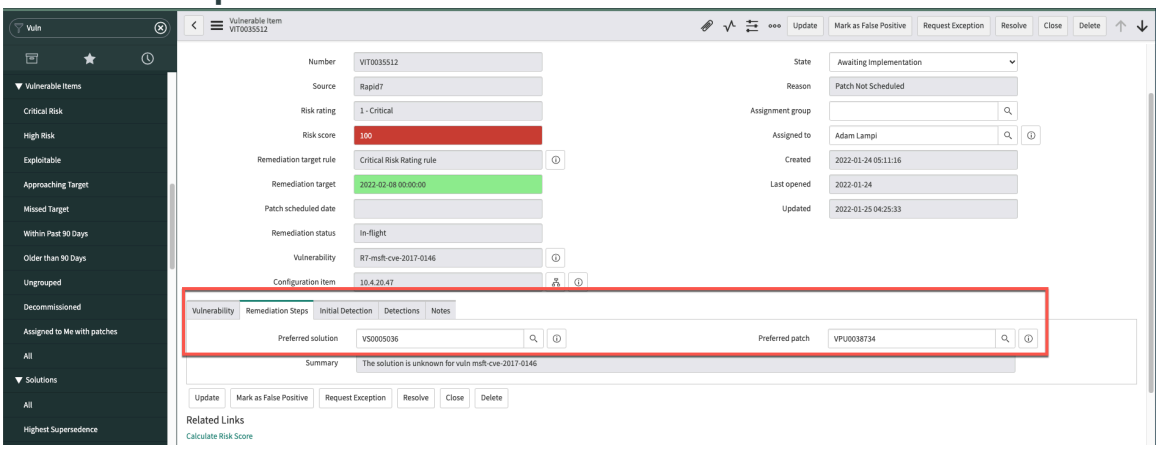
Patch data and state rollup

To view the vulnerable items that have patches and that are assigned to you in the classic environment, navigate to **All** > **Vulnerability Response** > **Vulnerable items** > **Assigned to me with patches**.

If a vulnerable item record is populated with a preferred patch, it transitions automatically to **Awaiting Implementation** only if the state of the VI is not **Closed**, **Resolved**, **Deferred** or **In Review**. To drill down into the data to view the preferred solution and other data, click the **Remediation** tab on the VI record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Steps tab



A VI with a preferred patch transitions to **Awaiting Implementation** in the following cases:

- If a patch is scheduled for deployment on a CI that is part of a collection import, and the CI has an associated VI, the reason the VI is **Awaiting Implementation** is **Patch Scheduled**.
- If a patch is scheduled for deployment on a CI that is part of a collection import, and the CI has an associated VI, and the Remediation target date (deadline) that is later than the Time to Remediation (TTR) date, the state of the VI is **Awaiting Implementation** with the reason as **Patch Scheduled (Missing Target Date)**.
- If a patch is not scheduled for deployment on a CI that is part of a collection import, the state of the VI is **Awaiting Implementation**, with the reason as **Patch Not Scheduled**.

Click the **Preferred Patch** information icon to open the Patch updates and view the following information on the Related Links:

Vulnerable items

Vulnerable items that are associated with this patch.

Associated Devices

Devices that have updates and those that are missing updates.

Patch deployments

Deployments scheduled for this patch on individual machines (assets) or on groups of assets.

Patch Requests

A list of patch requests that have been sent for approval before they are scheduled for deployment.

Potential Patches

Patches that might address a vulnerability.

Click the **Preferred patch information** icon to open the record to view the information listed previously, in addition to the following Patch Update data:

Source Remediation Status

The total devices that require this patch and any devices that are missing the patch.

Remediation Status

The status (total VIs, % remediated, VIs deferred) for the VIs that have this preferred patch.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Preferred patches and solutions

When an imported vulnerability matches an asset in your Configuration Management Database (CMDB), a vulnerable item (VI) is created in Vulnerability Response. If the configuration item (CI) that is associated with this VI is also imported from a third-party patch vendor and is shown as missing a patch for the same vulnerability, a preferred patch is listed and rolled up to your solutions. This information lets you know that an asset (CI) has a fix from an available patch that is the best match for its vulnerability.

Viewing patches without solutions

After an import, if no vulnerability solution data is available, the **Vulnerability solution** field on the Patch Update record is left blank. For more information about how to view information for these types of patches, see View patches without solutions in Vulnerability Response.

View patches without solutions in Vulnerability Response

Starting with v16.0 of Vulnerability Response, for patches that have no solutions after an import, the system then searches for patch IDs in the vulnerability reference data so that you can view these patches on vulnerability records.

Patches without solutions

Role required: sn_vul.vulnerability_admin.

The data imported from the patch orchestration and vulnerability solution applications, as well as patch scanner integrations, are processed, connected, and displayed in the Vulnerability Response application on Patch Update records.

When a solution exists for a vulnerability, related information is correlated in your instance and is rolled up from the patches, to vulnerability solutions, and to the vulnerabilities. To view this information, navigate to **All** > **Vulnerability Response** > **Patches** > **All**.

After an import, if no vulnerability solution data is available, the **Vulnerability solution** field on the Patch Update record is left blank. So that you can see the related solution information for these patches, a system property, [**sn_vul_patch_orch.no_solution_patch_rollup**], is activated by default in your instance. This property searches for Bulletin IDs and Article IDs in the vulnerability reference data from scanner imports. If a match is found, the associated data is populated on the potential patches table, and this information is displayed on the related lists of vulnerability records.

If you have a large number of vulnerabilities, or the rollup scheduled job is taking a long time to complete, you might prefer to deactivate this system property to avoid possible performance issues. However, note that if you deactivate this system property, imported solution data is neither searched for nor rolled up to your vulnerabilities with no solutions.

As a user with the sn_vul.vulnerability_admin role, to deactivate the system property, follow these steps:

1. Navigate to **sys.properties.list**.
2. Locate **sn_vul_patch_orch.no_solution_patch_rollup** and click it to open the record.
3. In the Value field, type `false`.
4. Click **Update**.

Viewing patch orchestration data on the Vulnerability Response dashboards

Starting with v16.1, you can view patch update data in the classic environment on the dashboards that are included with the Vulnerability Response application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information.

You can also view this data on the CISO and Vulnerability Management (PA) dashboards if you have a subscription to Performance Analytics.

You can also view patch data in the classic environment. For more information about the required roles and how to view data on the Vulnerability Response dashboards in the classic environment that are included with the Vulnerability Response application and those that require a separate subscription, see Using the default Vulnerability Response dashboards.

View a solution

View all solutions, solutions with highest-supersedence and solutions associated with vulnerable items to inform your remediation activities.

Before you begin

Role required: sn_vul.read, sn_vul.vulnerability_admin, or sn_vul.remediation_owner
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

As a Vulnerability Analyst or Remediation Owner, you can view different solution sets related to vulnerable items.

Note: Solution records are read-only except under **Notes** in the **Internal notes** section or user-created solutions.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Solutions**.
2. Choose a solution list.

   Note: You can filter a solution list using wildcards for the Product name.

3. To review, click each item.
4. **Optional:** Enter notes under the **Notes** tab and right-click **Save** to remain on the page or click **Update** to save and return to the **Vulnerability Solutions** list.

   Note: If you only have the sn_vul.read role, you would not be able to perform this step.

Create a vulnerability solution

Create a vulnerability solution so that you can track vulnerability solutions that are not covered by third-party solution content.

Before you begin

Role required: admin, sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or vulnerability.write
Vulnerability Solution Management is a feature available within the Vulnerability Response application. Vulnerability Solution Management requires a separate subscription.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

You can create a solution from any of the solution lists. You must install the Vulnerability Solution Management application before you can create a solution.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Solutions**.
2. Choose a solution list: **All**, **Highest Supersedence** or **With Vulnerable Items**.
3. Click **New**.
4. Fill in the editable fields on the form, as appropriate.
   You can leave any unused fields blank. For more information about individual fields, see Solution form fields.
5. Right-click **Save** in the header.
   The solution record is added and appears in the **All** and **Highest Supersedence** lists, by default.
6. The Related Lists appear.

   You can associate this solution to the following related lists: **Vulnerable Items**,**Third-Party Vulnerabilities**, **CVEs**, **Superseding Solutions** and **Preceding Solutions**. Choose a vulnerability or solution and click **Submit**.

Note:

Vulnerability Solution Management automatically associates vulnerable items and remediation tasks with solutions when vulnerability records are associated manually with solutions.

Vulnerable items manually re-assigned to another solution are not automatically updated with solution changes at the vulnerability level.

If you want to exclude the relationship between a third-party vulnerability and a solution because it is not relevant to the CI you are remediating, or it is not a concern in your environment, see Manually exclude solutions from third-party records or vice versa.

Manually exclude solutions from third-party records or vice versa

Exclude the relationship between a third-party vulnerability and a solution because it is not relevant to the CI you are remediating, or it is not a concern in your environment. Manually exclude solutions using either a third-party vulnerability or solution record.

Before you begin

Role required:

- sn_vul.write
- sn_vul.remediation_owner

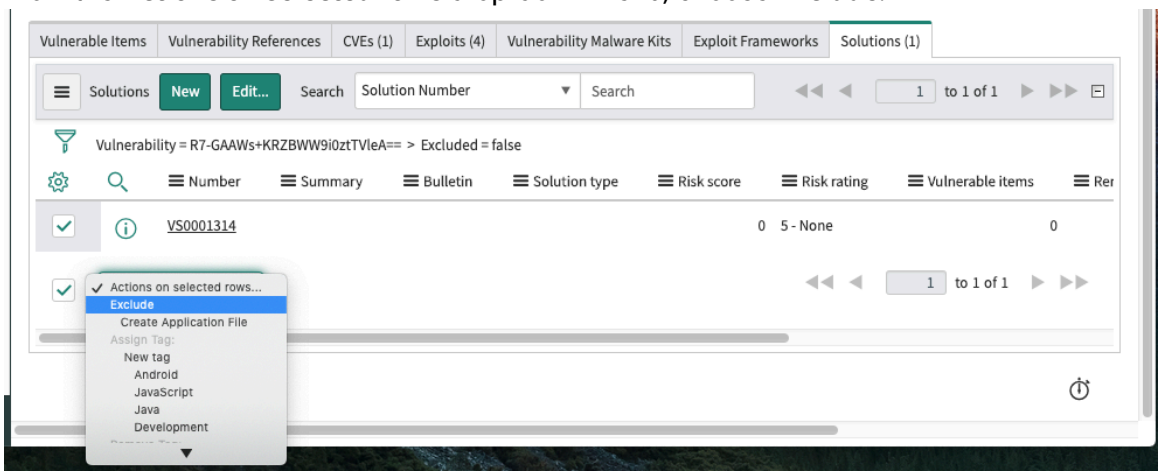
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Libraries** > **Third-Party** or **Vulnerability Response** > **All Solutions**
2. Open a third-party vulnerability or solution record.
   a. For a third-party record: Select the **Solutions** related tab.
   b. For a solution record: Select the **Third-Party Vulnerabilities** related tab.
3. Check the box next to each vulnerability or solution record you want to exclude.
4. From the **Actions on selected rows** drop-down menu, choose **Exclude**.



The third-party or solution record no longer appears in the related tab.

Third-party vulnerability relationships to solutions are also excluded when solutions are updated or if the nightly job is enabled.

Third-party vulnerability relationships to solutions are excluded during the nightly scheduled job.

Excluding third-party vulnerabilities means that the solution is no longer a factor for any preferred solution evaluation. Exclusion impacts:

- All counts for solutions since the third-party vulnerability, vulnerable items (VIs), and, configuration items (CIs) attached to the third-party vulnerability do not count toward the solution anymore.
- Determining the preferred solution for the third-party vulnerability and by extension the preferred solution of any attached VIs and remediation tasks containing the VI.

Triage vulnerabilities automatically

Reviewing and triaging new vulnerabilities is necessary to ensure successful remediation. Transform vulnerability imports into remediation tasks with automated vulnerable item (VI) assignment, risk calculation, remediation targets, and VI grouping.

Starting with imported vulnerabilities, reconcile the assets not found in the CMDB, prioritize the results, translate that to remediation activities that are automatically assigned, orchestrate the remediation process, and confirm completion with a validation scan.

New vulnerable items are usually sorted into remediation tasks upon import, based on remediation tasks rules. Sometimes, vulnerable items cannot be grouped or do not contain a recognized configuration item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

An overview of the vulnerability triage process:

- Log in to your Vulnerability Response instance.
- Validate that your rules (CI Lookup, Assignment) for vulnerable item are working as expected. For information on revising CI Lookup Rules, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations. For information on Assignment rules, see Vulnerability Response assignment rules overview.

  Note: Due to the large volume in data imports, care should be taken with automated vulnerable item assignment.

- Validate that your remediation targets are correct. See Vulnerability Response remediation target rules for information on how remediation target rules work and how to revise them.
- View ungrouped vulnerable items.
  - Looking at the ungrouped vulnerable items, consider revising your group rules and performing a rescan. See Create or edit Vulnerability Response remediation task rules for more information.
  - Manually group the vulnerable items. Manually create a remediation task in Vulnerability Response for more information.
  - Revise risk scores for the vulnerable items in your remediation tasks. See Vulnerability Response calculators and vulnerability calculator rules for more information.
  - Close older vulnerable items not recently detected by your third-party integrations. See Automatic closing of vulnerable items and detections for more information.
- View and reclassify unmatched configuration items.
- Research what needs to be done for remediation.

  This step can include:

  - Determine what to deal with now and what you can defer. This determination is often based on risk score, affected systems, and patches with change windows.

    Note: Remediation target rules belong to vulnerable items. These rules are run when the vulnerable item is imported. These rules were created previously in the Setup Assistant.

  - Refresh vulnerable items, if necessary, and View the remediation target status of a Vulnerability Response vulnerable item.
  - Create a **Change Request** and assign the remediation task to an assignment group (IT Operations) for remediation.

    Note: If the vulnerability constitutes a security incident and the Security Incident Response plugin (com.snc.security_incident) is activated, you can create security incident records from the remediation tasks instead.

  - After submitting one or more change requests, move the group state to Under Investigation.

Edit vulnerable items in bulk in Vulnerability Response

Edit vulnerable items in bulk to save time by selecting fields and running an asynchronous bulk edit job in the background.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Important: The Bulk Edit feature is available for host vulnerable items in the Vulnerability Manager Workspace. For more information, see Using bulk edit in the Vulnerability Manager Workspace.

Procedure

1. Navigate to **All** > **Vulnerability** > **Vulnerabilities** > **Vulnerable Items**.
2. Select the vulnerable items by performing one of the following actions:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the #unique_364_Connect_42_entry-be-record-selection field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the #unique_364_Connect_42_entry-be-record-selection field.
3. Select the **Bulk Edit** button.
4. On the Bulk Edit modal, fill in the fields.

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Vulnerable Items ○ All Vulnerable Items that match filter ○ Remediation task ○ Vulnerability entry
State	Change for the **State** in the vulnerable item. Choices are: ○ Do Not Update ○ Open ○ Under Investigation ○ Awaiting Implementation ○ Deferred **Note:** ▪ When you select this option, the Reason, Short description, Until,and Additional information fields appear. ▪ When you defer VITs, a remediation task is created and this task is sent for approval. ○ Closed

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: ▪ When you select this option to mark the records as false-positive, the Reason, Short description, Until,and Additional information fields appear. ▪ When you mark the records as false-positive, a remediation task is created and this task is sent for approval. ○ Resolved
Preferred Solution	Solution that is targeted for remediating all the vulnerable items that are selected for bulk edit. Select the change for the **Preferred Solution** field in the vulnerable item (VITs). Choices are from a lookup list of available preferred solutions for the VITs selected. **Note:** ○ The set of available preferred solutions is an intersection of all potential solutions of the vulnerabilities across all selected VITs. ○ When selecting **Record selection** > **Vulnerability Entry** for a bulk edit, all VITs for the vulnerability will be set to the selected preferred solution. **Note:** This operation doesn't set the **Preferred solution** at the vulnerability entry level. Setting the **Preferred solution** at the vulnerability entry level would set the **Preferred solution** for all new VITs going forward. The bulk edit only modifies the current set of VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message displays asking you to select VITs with different criteria for setting the **Preferred solution**. ○ The total number of solutions that can be shown in the lookup list is limited to 170. If there are more than 170 solutions, a warning message is displayed. The updated value is shown in the Vulnerable item list view.
Preferred patch	Patch that is targeted for remediating all the vulnerability items selected for bulk edit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: ○ You must install Patch Orchestration to view the list preferred patches. ○ The set of available preferred patches is an intersection of all potential patches across all selected VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message displays asking you to select VITs with different criteria for setting the **Preferred patch**. ○ The total number of patches that can be shown in the lookup list is limited to 170. If there are more than 170 patches, a warning message is displayed.
Reason	Reason for deferring records: ○ Awaiting Maintenance Window ○ Fix Unavailable ○ Risk Accepted ○ Mitigating Control in Place ○ Other Reason for closing records: ○ False Positive **Note:** ▪ When you select the this option, the Short description, Until,and Additional information fields appear. ▪ A remediation task is created when you mark the records as False-positive and this task is sent for approval. ○ Cancelled ○ Fixed **Note:** This field appears when you select the State as Deferred or Closed.
Short description	Brief note describing the reason for deferral and Closed-False positive requests. This information reflects in the Description field of the Remediation task that is created for deferral and Closed-False positive requests. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Until	Date till which the record remains deferred.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This field appears when you select the State as Deferred.
Additional information	Any other necessary information. This information reflects in the Additional Information field in the Overview tab. If your deferral request is approved, this additional information appears as deferral notes in both VIT and remediation task. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Unassign	All the selected items are unassigned for the assignment group and remediation owner. For more information on how a remediation owner can remove the assignments from vulnerable items, see Remove assignments from vulnerable items for you or your groups. **Note:** ○ This field appears when you select the State as Do Not Update. ○ When you unassign records, a remediation task is created and this task is sent for approval.
Assignment group	Assignment group for the VIT. Select manually or use Assignment Recommendations if it's enabled. **Note:** This field is disabled when you select the **Unassign** check box.
Work notes	Text that you enter to describe the changes.

5. Select **OK**.
   A bulk edit asynchronous job updates the selected records. The job number with a link is displayed on the Vulnerable Items page where you can view its status. A remediation task is created with the selected vulnerable items when you defer, unassign, or close (false-positive) vulnerable items in bulk. And this remediation task is sent for approval.

Ungrouped Vulnerability Response vulnerable items

Vulnerable items are automatically assigned to a remediation task when they are imported. However, sometimes, if a vulnerable item (VI) is created manually, for example, the VI can become an orphan. The **Ungrouped** vulnerable item module lists those vulnerable items without a group.

Note: Integration automated processes do not create orphans, so this use case is expected to be small.

Being ungrouped occurs if a vulnerable item was created without a vulnerability, or there is no remediation task rule that assigns the VI to a group.

In that case, review the list of ungrouped vulnerable items by navigating to **All** > **Vulnerability Response** > **Vulnerable items** > **Ungrouped**.

After review, your choices are as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can Create or edit Vulnerability Response remediation task rules to catch any items that appear on this list.
- You can Manually create a remediation task in Vulnerability Response and manually add items from this list to the group or define a condition that matches these items.
- You can open an existing remediation task and add any relevant vulnerable items to the group as long as it is in the Open or Under Investigation state.

Note: Manually added vulnerable items are not automatically removed from remediation tasks by remediation task rules or group conditions.

For more information on how remediation tasks and task rules behave, see Vulnerability Response remediation tasks and remediation task rules overview.

View ungrouped Vulnerability Response vulnerable items

Vulnerable items that are not assigned to a group are placed in a viewable list.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability** > **Vulnerabilities** > **Ungrouped Vulnerable Items**.
2. Review the vulnerable items in the list.
3. Click each vulnerable item to view and determine how to include in a group.

Manually add a vulnerable item to a remediation task

If a vulnerable item is left ungrouped, you can add it to a remediation task.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Record the vulnerable number.
2. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
3. Choose a remediation task (VUL) for your vulnerable item.
4. Select **Edit** in the lower right.
5. Enter the **vulnerable item** number in the search field for Collection.
6. Select the vulnerable item from the collection and add to the list.
7. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remove assignments from vulnerable items and remediation tasks

Clear the **Assigned to** and **Assignment group** fields on vulnerable item records in the Vulnerability Response, Application Vulnerability Response, and Container Vulnerability Response applications.

Before you begin

Roles required:

- sn_vul.remediation_owner or sn_vul.vulnerability_analyst for vulnerable items (VITs) and remediation tasks (VULs).
- sn_vul.app_sec_manager for Application Vulnerability Response vulnerable items (AVITs) and remediation tasks (AVULs).
- sn_vul_container.remediation_owner or sn_vul_container.vulnerability_analyst for container vulnerable items (CVITs) and remediation tasks (CVULs).

About this task

The **Unassign** UI action is supported in both the classic environment and the workspaces for the following records in any state other than Closed or Resolved:

- Remediation tasks (VULs, AVULs, and CVULs). If a remediation task is updated with this feature, the **Assigned to** and **Assignment group** fields on all of its associated VITs that have the same assignment group are also cleared.
- Vulnerable items (VITs).
- Application vulnerable items (AVITs).
- Container vulnerable items (CVITs).

Important: You can unassign host vulnerable items in bulk in the Vulnerability Manager Workspace. For more information, see Using bulk edit in the Vulnerability Manager Workspace.

Procedure

1. In either the classic environment, or in the IT Remediation Owner Workspace, navigate to a vulnerable item (VIT) record that is assigned to you that is in any state other than Closed or Resolved.
2. To clear the **Assigned to** and **Assignment group** fields in the classic view, at the top of the record, select **Unassign**.
3. Alternatively, navigate to a vulnerable item (VIT, AVIT, or CVIT) record in the IT Remediation workspace that is assigned to you or your groups and click **Unassign** in the More options menu () to clear the assignment fields.
4. For remediation task records in the workspace that are assigned to you or your groups, open a record select **Unassign** in the More options menu () to clear the assignment fields.
5. In the Unassign dialog for both vulnerable items and remediation tasks, provide work notes and select **Submit**.
   The state change approval request is submitted for approval.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For remediation tasks, you are notified that the **Assigned to** and **Assignment group** fields on all of a remediation task's associated VITs are also cleared.

After the request to clear the fields is approved for a remediation task, all the **Assigned to** and **Assignment group** fields on its vulnerable items that have the same assignment group are also unassigned. If any vulnerable item has a different assignment group than its associated remediation task, it is not unassigned. In most cases these vulnerable items have been manually assigned.

6. View the following information:
   - The work notes that you provided is displayed in the Notes section.
   - On the **State Change Approval** tab, the state change approval record displays with the In Review state, which helps to track the approval workflow.
   - On the **Requested Approvals** tab, your request for the removal of you or your assignment group is displayed in the Requested state.

Result

The request is approved by using a default, one-level approval workflow. For more information, see Approve or reject an unassign request in Vulnerability Response.

- If your request is approved, the state change approval record and the requested approval record transition to the Approved state. You and your groups are removed from the **Assigned to** and **Assignment group** fields. `Unassigned` is displayed in the **Assignment type** field, and the remediation task and VITs are displayed in the list of the Unassigned module for each product.

  Notifications that records are unassigned are sent automatically to vulnerability managers or analysts in the Unassign notification group. To configure the approval flag, notifications, and default assignment group, see Removing assignments from vulnerable items and remediation tasks.

- If your request is rejected, the state of the change approval record and requested approval record transition to the Rejected state.

Note: As a vulnerability administrator, you can set the *`sn_vul.unassign_vr.approval_required`* system property to **false** to disable the approval process.

What to do next

Navigate to the Unassigned modules for the Vulnerability Response and Application Vulnerability Response Container Vulnerability Response applications, monitor any unassigned records for items that might fall under your scope, and reassign them to yourself.

Approve or reject an unassign request in Vulnerability Response

Approve requests for the removal of vulnerable items from an assignment group or an individual user in the Vulnerability Response application.

Before you begin

Role required: For unassign approvals, one approver is required in the Approver – Level 1 group.

- sn_vul.unassign_approver for AVITs and VITs
- sn_vul_container.unassign_approver for CVITs

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

By default, an approval configuration is provided and an unassign approval group is created. Users of the Unassign Approver - Level 1 group can approve the request. This group contains an unassign approver role, sn_vul.unassign_approver, by default. You can modify or create a new group and update the approval configuration. To configure an approval rule, select any of the following approval rule in the Approval Rules module and navigate to the approval configuration on the **Approval Configurations** tab:

- *`Vulnerable item field change request`* for a vulnerable item.
- *`Vulnerability field change request`* for a remediation task.
- *`Application vulnerability field change request`* for an application vulnerable item (AVIT).
- *`Approval for container management`* for a container vulnerable item (CVIT).

For more information on approval rules and configurations, see Approval workflow configurations for unassign request.

Important: You can approve or reject requests in the Vulnerability Manager Workspace.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **My Approvals** for VITs and AVITs.
   Alternatively, navigate to **All** > **Container Vulnerability Response** > **My Approvals** for CVITs.
2. Select a request from your queue.
3. Approve or reject the request by adding the appropriate comments.

Automatic closing of vulnerable items and detections

You can automatically close stale detections and vulnerable items (VIs) associated with retired CIs using the Auto-Close rules module.

You can automatically close stale detections and VIs in the following scenarios:

- Automatically close stale detections in Vulnerability Response
- Automatically close vulnerable items related to retired CIs

For information on working with retired configuration items, see Working with retired configuration items and Create auto-close rules.

Working with retired configuration items

Decommissioned configuration items (CIs) are moved to retired, archived, or deleted state in the Configuration Management Database (CMDB). Vulnerability Response contains vulnerable items (VIs) that are made up of CIs. When the state of a CI is updated to retired, the associated VIs are closed with the substate 'CI decommissioned'.

Note: Starting with v25.0.3 of Vulnerability Response, a new auto-close rule 'CI Decommissioned' is introduced to close the vulnerable items and detections related to decommissioned CIs.

If the CMDB changes the life cycle stage status of a CI to retired, you can choose to automatically close the associated VIs. For more information on automatically closing the associated VIs, see Automatically close vulnerable items related to retired CIs.

The retired CI is eventually archived or permanently deleted from the CMDB.

Impact of retiring the CIs:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Impact on discovered items:** When the CI is retired, the related discovered item (DI) is marked as 'CI decommissioned'.
- **Impact on vulnerable items:** When the state of a DI is updated to 'CI decommissioned', the associated VI is closed and the Notes section is automatically updated.

> **Note:** The state of a DI is automatically updated to 'CI decommissioned' whenever the life cycle state of a CI is updated. On the other hand, the state of a VI is updated to Closed only when the **Auto-close VIs linked to retired CIs** option is enabled. For more information on automatically closing the associated VIs, see Automatically close vulnerable items related to retired CIs.

The scheduled job *Close detections/VIs for decommissioned CIs* is run daily for the updated DIs. If the auto-close configuration option is enabled for retired CIs, it identifies the DI containing a decommissioned CI, and closes the related VI with the substate 'CI decommissioned'. If all the VIs in a remediation task are closed and their substate is CI decommissioned, the remediation task is also closed with the substate 'Canceled'. To view the decommissioned VIs, navigate to **Vulnerability Response** > **Vulnerable Items** > **Decommissioned**.

> **Note:** If a CI moves back to the original state from the 'Retired' state, the 'Discovered Items' entry is updated as well. VIs are automatically opened when data is ingested again from the scanner.

Automatically close vulnerable items related to retired CIs

If the Configuration Management Database (CMDB) changes the life cycle stage status of a configuration item (CI) to retired, you can choose to automatically close the associated vulnerable items (VIs) and detections.

Before you begin
Role required: sn_vul.admin

About this task
Starting with v22.0 of Vulnerability Response, to automatically close the associated VIs and detections, you must enable the system property *sn_vul_cmn.auto_close_vis_linked_retired_cis* to auto-close VIs that are associated with retired CIs. To enable the option, set the Value field to '1'. Conversely, to disable the option, set the Value field to '0'.

During an upgrade if the system property *sn_vul_cmn.auto_close_vis_linked_retired_cis* is selected in v21.0 of Vulnerability Response, then the value remains as '1'. When this option is enabled, any new or existing VIs and detections reported for the same CI, are automatically created or updated with a status of 'Closed'. This is based on the Asset ID in the scanner payload and status of the Discovered Items entry. For more information on the impact of retired CIs, see Working with retired configuration items

.

> **Note:**
>
> - The state of a DI is updated to 'CI decommissioned' whenever the life cycle state of a CI is updated. On the other hand, the state of a VI is updated to Closed only when the **Auto-close VIs linked to retired CIs** option is enabled.
> - The information provided in the following procedure is only applicable to versions prior to v22.0 of Vulnerability Response. Starting from v22.0 of Vulnerability Response, you have the option to configure additional search options. See Create auto-close rules for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Auto-Close Configuration** > **Configuration Item Lifecycle**.
2. To automatically close vulnerable items associated with the retired CIs, select the **Auto-close VIs linked to retired CIs** check box.
3. Select **Update**.

> **Note:** If a CI is already retired before the **Auto-close VIs linked to retired CIs** option is enabled, VIs are created only for new detections from scanners. The state of these VIs is Closed and the substate is CI Decommissioned.
>
> You cannot manually reopen VIs whose state is CI decommissioned, using the **Reopen** or **Bulk Edit** options.
>
> Closed VIs with a substate of fixed or stale are reopened if a new detection is created and the VIs can be matched with the new vulnerability. See Detections, remediation tasks, and vulnerable item states for more information.

Closing stale detections in Vulnerability Response

The Auto-Close Stale Detections module helps you automatically clean up older, stale vulnerable detections not recently found by your third-party integrations. Moving these detections to Closed reduces the number of active vulnerable items and remediation tasks in your ServiceNow AI Platform instance and helps you reconcile assets in your CMDB.

Overview and key terms

In order to more accurately roll-up detection data to your vulnerable items, the Auto-Close Stale Detections module helps you clean up older, stale vulnerable item detections not recently found by your third-party integrations. For more information about this feature, see the use case below.

In previous versions of Vulnerability Response, the Auto-Close Vulnerable Items module automatically transitioned vulnerable items not recently found or updated by your third-party scanner integrations to the Closed - Stale.

Before you enable the Auto-Close Stale Detections feature, review the following terms, how states roll up to vulnerable items and remediation tasks, and the prerequisites for your third-party integrations that import detection data.

To enable the feature, see Automatically close stale detections in Vulnerability Response.

Key terms

Stale detections

Refers to detections associated with vulnerable items in your ServiceNow AI Platform® instance that are aged and have not been found, updated, or detected by third-party integration scans for a significant amount of time.

Detections last found

This search option uses a date and time provided by the third-party scanner. This term refers to the most current, or latest date and time that detections were found again by the scanner.

Assets Last scanned

This search option uses a date and time provided by the third-party scanner. This term refers the most current date and time an asset was last scanned by a third-party scanner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use case

At times, assets (configuration items) may be decommissioned in your environment or purged by third party-scanners, and their associated detections are not updated by vulnerable item detections. As a result, the detections and their related vulnerable items are not updated in the Vulnerability Response application, and they become inactive (stale).

To close these aged detections that have unchanged vulnerable item data and next reduce the number of active VIs and remediation tasks (RTs), enable Auto-Close Stale Detections. This feature automatically closes vulnerable item detections not recently found or updated by your third-party scanner integrations based on search criteria and an age in number of days that you set.

As an example, suppose a particular configuration item (CI) has multiple asset IDs, and one of these IDs has not been imported on a detection from a third-party scanner in the last 90 days. This feature automatically closes this detection that has no new vulnerability data so the associated VI can be closed.

Since a VI can have more than one detection associated with it, this feature only transitions the detections determined to be stale by the parameters you set. For example, if a VI has four detections associated with it, and two detections are stale, that is, no new vulnerability data has been imported in the last 90 days, this feature only closes the stale detections. Before the VI can be closed, you must first remediate the other two open detections.

Rollup of detection states to VIs

To differentiate the auto-closed detections from detections closed by third-party scanners, a new value for the Status field, Stale, has been added. The possible values for this field are, Open, Closed, and Stale. Stale indicates that a detection closed by the auto-close detection feature.

State precedence: Open > Closed > Stale.

1. If any detections are Open, the associated VI state remains Open.
2. If no detections are Open, some are Closed, and some are Stale, the associated VI state transitions to Closed - Fixed.
3. If all the detections are Stale, the associated VI state transitions to Closed - Stale.

   Starting with Vulnerability Response 20.0, if the detection is Stale and its associate VI is in Closed state, the VI's state doesn't transition to Closed - Stale. This is to avoid the VI from reopening when a new detection is identified so that you can avoid going through the entire false positive request and approval process. To reverse this behavior, deselect the **Ignore stale detections for closed VIs** check box in the Auto-Close Configuration form. For more information, see Automatically close stale detections in Vulnerability Response.

Rollup of VI states to remediation tasks (VUL)

State precedence: Open > Closed - Fixed > Closed - Stale.

1. If any VIs in a VUL (remediation task) are Open, the VUL state is not changed.
2. If at least one VI is Closed - Fixed and the rest are Closed - Stale, the VUL state transitions to Closed - Fixed.
3. If all the VIs in a VUL are Closed - Stale, the VUL state transitions to Closed - Canceled.
4. If any VIs are closed as Closed – False Positive, the VUL does not auto-close.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on state rollup and rolldown scenarios, see, State roll-up and roll-down scenarios.

Auto-Close detections and third-party integration requirements

Microsoft TVM users and Auto-Close Stale Detections

Checklist item	Description
The Microsoft TVM Vulnerability Integration	With the Microsoft TVM Vulnerability Integration, if you select **Detections last found** to base your search on, this feature requires a successful run of the Microsoft TVM Machine Vulnerabilities Integration (Full import) within the last seven days. This integration runs weekly. If Auto-Close Stale Detections are enabled and configured for **Detections last found**, and the Microsoft TVM Machine Vulnerabilities Integration is disabled, or a data import is not successfully completed within the last seven days, the scheduled job to close detections still runs daily but some stale detections might not be closed as expected. If you select **Assets last scanned** to base your search on, the Microsoft TVM Machine Vulnerabilities Integration run is not required. To activate this integration: 1. Navigate to **Microsoft TVM Vulnerability Integration** > **Administration** > **Integration**. 2. Locate and enable the **Microsoft TVM Machine Vulnerabilities Integration (Full import)**.
(Optional) Deploy multiple instances of the Microsoft TVM integrations in your environment.	You can optionally deploy multiple instances of the integrations across your environment. Auto-Close Stale Detections is not instance-specific, and it is either enabled or disabled across your environment. Stale detections are automatically transitioned to Stale on instances that have successfully completed integration runs. If Auto-Close Stale Detections are enabled and you disable the integrations that run weekly in an instance, the scheduled job to close detections still runs daily, but some detections may not transition to Stale automatically as expected.

Qualys users and Auto-Close Stale Vulnerable Items

- Any activated Qualys third-party integrations that retrieve detection data can run with this module. There are no specific Qualys applications required.
- You can optionally deploy multiple instances of the Qualys integrations across your environment.
- Auto-Close Stale Detections is not instance-specific, and it is either enabled or disabled across your environment. Stale detections are automatically transitioned to Stale on all instances.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist item	Description
The Rapid7 Vulnerability Integration	If you select **Detections last found** to base your search on, this feature requires a successful run of one of the Rapid7 Comprehensive Vulnerable Item Integrations within the last seven days. These comprehensive integrations run weekly: • For Rapid7 Nexpose data warehouse, a successful run from the Rapid7 Comprehensive Vulnerable Item Integration is required. • For Rapid7 InsightVM, a successful run from the Rapid7 Comprehensive Vulnerable Item Integration - API is required. If Auto-Close Stale Detections is enabled and configured for **Detections last found**, and the Rapid7 Comprehensive Vulnerable Item Integrations are disabled, or a data import is not successfully completed within the last seven days, the scheduled job to close detections still runs daily but some stale detections might not be closed as expected. If you select **Assets last scanned** to base your search on, no comprehensive Rapid7 integration run is required. To activate these integrations: 1. Navigate to **Rapid7 Vulnerability Integration** > **Administration** > **Integration**. 2. Locate and enable the Rapid7 Comprehensive Vulnerable Item Integration you need. **Note:** In addition to these integrations that run weekly, Rapid7 Nexpose and Rapid7 InsightVM each have VI integrations that run daily, the Rapid7 Vulnerable Item Integration, and the Rapid7 Vulnerable Item Integration - API. If both the daily and weekly Rapid7 integrations are enabled, only one integration runs at a time. If one of these integration jobs is running, the job for the other integration is skipped until the next scheduled job.
(Optional) Deploy multiple instances of the Rapid7 integrations in your environment.	You can optionally deploy multiple instances of the comprehensive integrations across your environment. Auto-Close Stale Detections is not instance-specific, and it is either enabled or disabled across your environment. Stale detections are automatically transitioned to Stale on instances that have successfully completed integration runs. If Auto-Close Stale Detections is enabled and you disable the integrations that run weekly in an instance, the scheduled job to close detections still runs daily, but some detections may not transition to Stale automatically as expected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable Vulnerability Integration users and Auto-Close Stale Vulnerable Items

- Any activated integrations from the Tenable Vulnerability Integration that retrieve detection data can run with this module. There are no specific Tenable Vulnerability Integrations required.
- You can optionally deploy multiple instances of the Tenable Vulnerability Integration across your environment.
- Auto-Close Stale Detections is not instance-specific, and it is either enabled or disabled across your environment. Stale detections are automatically transitioned to **Stale** on all instances.

After you verify that your integrations are configured properly, see Automatically close stale detections in Vulnerability Response to enable the feature.

Upgrade information from Auto-Close Stale Vulnerable Items to Auto-Close Stale Detections

For the Auto-Close Stale Detections module, if you previously used Auto-Close Stale Vulnerable Items:

- The value for the number of days you entered for the **Assets last scanned** option from Auto-Close Stale Vulnerable Items is preserved automatically for **Assets last scanned** in Auto-Close Stale Detections.
- The value for the number of days you entered for the **Vulnerable items last found** option from Auto-Close Stale Vulnerable Items is preserved automatically for **Detections last found** in Auto-Close Stale Detections.
- Existing open detections with Vulnerable items as Closed - Stale will be transitioned to Stale as per the auto-close close configuration settings when the *`Auto-Close Stale Detections`* scheduled job runs after upgrade.

Rollup information

- If a Vulnerable item was Closed - Stale prior to the upgrade, and all its detections are marked as Stale after upgrade, then the VI state remains Closed - Stale.
- If a Vulnerable item was Closed - Stale prior to the upgrade, and only some of its detections are marked as Stale after upgrade and the rest were closed by the scanner, then the vulnerable item transitions to Closed - Fixed as per the rollup logic.

Automatically close stale detections in Vulnerability Response

Enable Auto-Close Stale Detections to automatically close stale vulnerable detections not recently found by your third-party integrations.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vuln.admin (deprecated), or a vulnerability manager with the sn_vul.manage_auto_close_stale_vi granular role.

For more information about this feature, key terms, and any setup that may be required for your third-party integrations that import detection data, see Closing stale detections in Vulnerability Response for more information.

Note: The information provided in the following procedure is only applicable to versions prior to v22.0 of Vulnerability Response. Starting from v22.0 of Vulnerability Response, you have the option to configure additional search options. See Create auto-close rules for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Vulnerability Response** > **Administration** > **Auto-Close Configuration** > **Stale Detections**.
   The Auto-Close Stale Configuration form is displayed.
2. Fill in the fields.
3. For the **Auto-close stale detections based on** field, choose one option for your search.

   Both searches match the age of older, stale detections in number of days to a date provided by your scanner.

   Note: Starting with v22.0 of Vulnerability Response, the options **Detections last found** and **Assets last scanned** are created as a list.

   - **Detections last found**. This option searches for the most current, or latest date that detections were found again by the scanner.

     Note: For Rapid7 and Microsoft TVM users, a warning message is displayed about requiring current detection information.

     If you select **Detections last found** to base your search on, this feature requires a successful integration run of one of the Rapid7 Comprehensive Vulnerable Item Integrations within the last seven days.

     If you select **Detections last found** to base your search on, this feature requires a successful integration run of the Microsoft TVM Machine Vulnerabilities Integration (Full import) within the last seven days.

   - **Assets last scanned**. This option searches for the most current date an asset was last scanned by a third-party scanner.
4. For Rapid7 and Microsoft TVM users only, verify that any required integrations are enabled. See Understanding the Rapid7 Vulnerability Integration and Understanding the Microsoft Threat and Vulnerability Management Vulnerability integration for more information.
5. To enable the module, click the Active check box to select it.
6. In the **Detections last found (days ago)** field, enter the age of older, stale detections in the number of days.

   Default is 90 days. You can enter any positive value for the number of days. This value is used to match a date provided by your scanner. With 90 and **Detections last found** displayed, any detections not found in the last 90 days are automatically closed. With 90 and **Assets last scanned** displayed, any detections associated with assets not scanned in the last 90 days are automatically closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

There is a relationship between the **Detections last found/Assets last scanned (days ago)** field for this feature and the **Import since** field on the Rapid7 Comprehensive Vulnerable Item Integration – API and the Microsoft TVM Machine Vulnerabilities integration.

For these integrations, the **Import since** field on the configuration pages is empty by default.

If you do not enter a value, or the field has no value, then the data for the number of days configured in the **Detections last found/Assets last scanned (days ago)** field is used.

For example, if the number of days defined in the auto-close configuration form is 90, and the **Import since** field is empty on the integration configuration pages, then the first integration run imports the data for the last 90 days. The **Import since** fields for the Rapid7 Comprehensive Vulnerable Item Integration - API and the Microsoft TVM Machine Vulnerabilities integration are editable, so you can also provide whatever values you want. The 90 days value is provided as a default if the field remains empty so that the auto-close feature doesn't close the false positives.

This relationship between these fields applies only to the first integration run. After that, changing the **Detections last found/Assets last scanned (days ago)** field on the Auto-Close Stale Vulnerable detections form doesn't affect the **Import since** field on the integration configuration pages. The field is changed to the first run's start time so that the subsequent integration runs import only the delta information.

7. **Optional:** Select the **Ignore stale detections for deferred VIs** check box to ignore stale detections that are mapped to deferred VIs or to VIs currently in review for deferral.

   (Optional) If you leave this option disabled, any detections that match your criteria will be closed that map to deferred VIs, or to VIs that are in review for deferral. The deferred VIs, or VIs that are in review that correspond to these detections are also automatically closed based on the rollup logic. For more information on roll up logic, see Closing stale detections in Vulnerability Response and State roll-up and roll-down scenarios.

   If you enable this option, any detections that match your criteria that map to deferred VIs, or to VIs that are in review for deferral, are skipped during auto-close.

8. **Optional:** Deselect the **Ignore stale detections for closed VIs** check box.

   (Optional) By default, this check box is selected so that the closed VI is not reopened when a new detection related to this closed VI is identified. For more information on the roll up logic, see Closing stale detections in Vulnerability Response and State roll-up and roll-down scenarios.

9. Click **Update** to save your changes.

   The *Auto-Close Stale Detections* scheduled job runs daily. The job determines whether you have selected the date when detections were last found or the date when assets were last scanned. It then transitions the corresponding detections to the Stale state. It's important to note that the Auto-Close Stale Detection feature only closes stale detections for active integration instances. Vulnerable items and detections associated with active integration instances are closed. Starting from v22.0 of Vulnerability Response the scheduled job has been modified to take into account the common table [sn_vul_cmn_auto_close_rule].

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the detections are marked as Stale, if the scanner reports finding that detection again, the Status field of the detections transitions to Open. The detection's corresponding vulnerable items are also reopened.

Additionally, if the detection is marked as Stale, and the scanner finds that it is Fixed, the detection transitions to Closed. The state also rolls up to the VIs.

Create auto-close rules

Use auto-close rules to close older detections automatically based on the filter conditions that you set.

Before you begin

Role required: sn_vul.manage_auto_close_stale_vi

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Auto-Close Rules**.

   The base system provides the following auto-close rules:

   - **Assets last scanned**: Detections associated with assets that haven't been scanned within the last 90 days are transitioned to **Stale** state.
   - **Manual detections last found**: Manual detections that haven't been found within the last 90 days. If you activate **Detections last found** record, then this feature requires a successful integration run of Rapid7 Comprehensive Vulnerable Item Integrations and Microsoft TVM Machine Vulnerabilities Integration (Full import) within the last seven days.
   - **Detections last found**: Detections that haven't been found within the last 90 days.
2. Select **New** to create a new auto-close rule.
3. Fill in the fields on the form.

Field	Value
Name	Name of the auto-close rule.
Active	Option to activate the rule. If activated, it closes any detections automatically that match its filter criteria.
Ignore deferred items	If selected, any detections that are mapped to the **In-review** or **Deferred** states are ignored and not closed. If you clear this option, any detections that match your criteria are closed.
Execution order	Unique value for the execution of the auto-close rule. This value determines the order of execution. The default value is 100.
Description	Description of the auto-close rule.
Condition	Filter conditions used to identify detections that should be closed.

4. Select **Submit**.

   The *Auto-Close Stale Detections* scheduled job runs daily. It identifies detections based on the specified conditions and transitions the matching ones to the **Stale** state. The job handles the following scenarios:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If all the detections within a vulnerable item (VIT) are marked as stale, the VIT is closed with the sub-state set as "Stale".
- If there is at least one detection that remains open within a VIT, while others are in the Stale status, the VIT remains open.
- In cases where there are detections with both "Closed" and "Stale" statuses within a VIT, the VIT is closed with the sub-state set as "Fixed".

When you upgrade to the latest version of Vulnerability Response, the conditions set in your auto-close rules also get updated accordingly. Additionally, if the rules are associated with different domains, the rules are created specifically within those domains.

Reclassify unclassed hardware

Reclassify unclassed hardware by updating the CI lookup rules.

Before you begin

Role required: sn_sec_cmn.admin

About this task

The Host Import Map [sn_sec_cmn_src_cmdb_map] table displays the payload's incoming variables and their corresponding assignments in the Discovered Items table. Occasionally, discrepancies in naming conventions between the scanner and Discovery can lead to the hardware being left unclassified. While creating a new Unclassed Hardware CI, ensure that the name in the payload contains only the Host Name. Later, when Discovery identifies the asset, it can be reclassified into the appropriate CI class. If needed, a script can be written to generate a derived value that aligns with the CIs name in both Discovery and the Configuration Management Database (CMDB).

If the Identification and Reconciliation engine (IRE) is activated, the reclassify option from Discovered Items isn't supported.

Procedure

1. Navigate to the Host Import Maps [sn_sec_cmn_src_cmdb_map] table.
2. Select **New**.
3. Select a source.
4. From the Target field list, select **Name**.
   The **Use script** check box becomes visible.

   Note:
   - The script is available only if **Name** is selected from the Target field list.
   - To add a script for other options in the Target field list, you must disable the UI policy by:
     - Disabling the 'Set Use script false'.
     - Disabling the 'Show or Hide Use Script'.
     - Removing the condition 'target field is name' in the 'Show or Hide Script policy'.
   - The Host Import Maps table is updated with two new columns: Script and Use script.

5. Select the **Use script** check box.
   The **Script** field displays the default script but you have an option to create a custom one. In this field, you can specify the source and derived values to align with the database's naming convention. The value generated by the script is stored in sourcePayload['DERIVED']

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

[rule.source_field]. Ensure that the CI lookup rules are adjusted to utilize source payload, derived, and targeted attribute values when checking in the corresponding tables.

6. To apply the script to older duplicate records, do the following:

   a. Navigate to **All** > **Vulnerability Response** > **Discovered Items**.

   b. Select the duplicate records.

   c. In the Action on selected rows list, select **Reapply CI Lookup rules**.
   It shows a match to an existing asset.

7. To apply the script for Tenable.io, do the following:

   a. Navigate to **Vulnerability Response Host Import Maps**.

   b. Select the script for the row with NetBIOS, HOSTNAMES, and FQDNS name as the **Source** field.

   c. Update the script for each element.

   Note: For Tenable.io, the scanner returns an array for NetBIOS, HOSTNAMES, and FQDNS name, for which the script doesn't work as expected.

   Because the Host Import Map for Tenable.io contains **netbios_name** in the **Source** field, you must write a script. During lookup, another source field **NETBIOS** is used, which has an array of values. So a new row is added in the table, and the same logic must be written in a loop in the script. Similarly, for **FQDNS** and **HOSTNAMES**.

8. To apply the script for Rapid7, do the following:

   a. Navigate to **All** > **Vulnerability Response Host Import Maps**.

   b. For Rapid7 rows with FQDN and HostName, update the Lookup Method to Script.

   Note: For Rapid7, the CI Lookup method is set to Field matching for FQDN and Hostname, which helps to prevent it from using the script.

Manually create a remediation task in Vulnerability Response

Creating a remediation task manually is done when you want to group vulnerable items by something other than the Remediation Task Rules criteria. For example, you can create tasks for a particular manager, or for active, new exploits, such as ransomware that include different vulnerabilities. You can also use it to group ungrouped vulnerable items.

Important: You can create host remediation tasks in the:

- Vulnerability Manager Workspace as a user with the sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin role.
- IT Remediation Workspace as a user with sn_vul.remediation_owner role.

Before you begin

Role required: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.

   Remediation task rules work the same way that vulnerability group rules previously worked, and they are still available to you. However, you might prefer to leave remediation task rules inactive as you get used to the features that are available to your security managers and IT teams in the workspaces.

2. Select one of the categories for tasks to open the list.
3. Click **New**.
4. Fill in the fields on the form, as appropriate.
   For information on specific fields, see Remediation task form fields.
5. Click **Submit**.
   When the task is created, using the **Condition** or **Filter Group** filter type the **Vulnerable Item** related list searches for and displays all matching vulnerable items.

   You can use the Related Link, **Re-scan for Vulnerabilities** to manually trigger a ServiceNow® - initiated scan. For information on how to configure a vulnerability scanner, see Configure and manage Qualys vulnerability scanners and scans.

   For a Qualys Vulnerability Integration, a default scanner is pre-installed in the **Vulnerability Scanners** module. This scanner is deactivated by default. Select the **Active** and **Default** check boxes to activate the Qualys scanner to work using the **Scan for Vulnerabilities** related link on the remediation task and vulnerable item forms.

   The **Update status** related link displays the date and time of the last update. It rolls up information from the VIs in the remediation task. See Remediation task form fields for more information. When a task is formed based on a specific vulnerability, that vulnerability is listed on the remediation task form.

   If you open an associated vulnerable item, any associated remediation task entries appear under the **Remediation Task** related list tab.

Add users to the Vulnerability Response group

When the Close/Defer feature is used to defer or close a vulnerable item without requiring a scan, the Vulnerability Response group is notified to approve or reject the request. You can assign the appropriate users.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. Open the Vulnerability Response group.
3. Click the **Group Members** related list and click **Edit**.
4. Select one or more name in the **Collection** list.
5. Click **Add**.
6. Click **Save**.

Related topics

Create a user

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Manage individual vulnerable items manually

Vulnerable items represent one configuration item (CI) with a given vulnerability. Vulnerable items are imported from third-party sources, or using the SAM NVD information (link) to compare vulnerability entries to software records retrieved from the Software Asset Management module.

Vulnerable items are contained in remediation tasks defined by vulnerability rules. Typically remediation tasks are the location where groups of vulnerable items are assigned and worked on.

Vulnerable items can be viewed and edited in bulk from the **Vulnerable Items** module. Vulnerable item records display information from the vulnerability in the **Vulnerability** tab. This tab can indicate whether there are public or active exploits for it. Also, it shows whether it can be remediated via a patch, configuration change, or combination of both. If there are IP addresses that are found during de-duplication, they appear in a related list.

If a CI is removed from the CMDB, any associated vulnerable items are removed as well.

When a vulnerable item is added to a remediation task, the group appears in the **Remediation Tasks** list of Vulnerable items.

When a task is created that affects a vulnerable item, the task appears in the **Affecting Tasks** related list of Vulnerable items.

Vulnerable items can be created manually. You can create security incidents or change requests and manually closed or defer them. Remediation task rules can be applied to manually created vulnerable items.

Remediation tasks and remediation task rules have been enhanced to take over task functionality. Vulnerable items cannot be linked as a parent task.

Create Vulnerability Response vulnerable items

Multiple methods create vulnerable items (VI). Most commonly, an integration to a vulnerability scanner is installed and configured to import results nightly. There are cases, like physical security vulnerabilities, when you might prefer to manually add vulnerable item records.

Before you begin

Role required: sn_vul.vulnerability_write

About this task

VIs that you create manually, and automatically-created VIs are automatically added and removed from remediation tasks by remediation task rules and group conditions.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items**.
2. Select a category to open the list.
3. Click **New**.
4. Fill in the fields on the form, as appropriate.
   For information on the vulnerable items fields see, Vulnerability Response vulnerable item form fields.
5. Right-click in the form header and click **Save**.

   The remediation task rules evaluate the vulnerable item and add it to an existing task or creates a new task. If the evaluation fails, then the vulnerable item is added to **Ungrouped Vulnerable Items** list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you save a new vulnerable item, all the enabled calculators run.

Note: Only one calculator per **Target field** is allowed to be active at a time. When you activate one, any others with the same **Target field** are deactivated.

6. You can click any of the related lists to view additional information.

   You can use the Related Link, **Scan for Vulnerabilities** to manually trigger a ServiceNow® -initiated scan. For information on how to configure a vulnerability scanner, see Configure and manage Qualys vulnerability scanners and scans.

   For a Qualys Vulnerability Integration, a default scanner is pre-installed in the **Vulnerability Scanners** module. This scanner is deactivated by default. Select the **Active** and **Default** check boxes to activate the Qualys scanner to work using the **Scan for Vulnerabilities** related link on the remediation task and vulnerable item forms.

   The following editing and remediation options become available from the header bar:

   - Update: Saves updates to the form.
   - Create Security Incident: Creates a security incident.
   - Close: Closes the item. If all items in its group are closed, the remediation task automatically closes.
   - Request Exception: Submits a request to defer an item.
   - Resolve: Resolves the item.
   - Delete: Removes the vulnerable item.

Related topics

Edit vulnerable items in bulk in Vulnerability Response

Defer a vulnerable item

If you determine that the issue associated with a vulnerable item (VIT) is of low risk and can be immediately deferred without further analysis, you can use the **Defer** feature.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

A scheduled job runs every day checking for deferred vulnerable items that have reached their reopen date. On the day the VI's deferral is set to expire, the record is reopened.

Starting with Vulnerability Response v20.0, before reopening a deferred VI, the `Check Vulnerable Item and Groups Deferment Expiration` scheduled job checks if any exception rule is applicable on a deferred VI and updates the **Reason** and **Until** fields as per the exception rule. The state of the VI remains Deferred till the latest expiry date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items**.
2. Open a vulnerable item.
3. Click **Request Exception**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Until	Select the date when the Deferred state expires and the remediation task is reactivated. **Note:** Starting with version 18.0 of Vulnerability Response (VR), if a deferred vulnerable item is closed and reopened by a scanner before the exception window expires, the state of the VIT reverts to deferred state honoring the active exception window. To enable this functionality, set the value of the system property sn_vul.auto_defer_vit_in_active_exception_window to true. Also, the deferred Until date persists even after the vulnerable item gets closed or the exception expires. The role required is sn_vul.manage_exception_configuration for both read and write. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerable item is set back to Open and a second email notification is sent out.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ False positive ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Submit**.
   The group is marked **In Review**. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **State Change Approvals** tab.

Request an extension for a deferred vulnerable item

Request an extension for a deferred vulnerable item before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task
You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items**.
2. Open a deferred vulnerable item.
3. Select **Request Extension**.

   Note: The Request Extension button is visible only when the state of the vulnerable item is Deferred.

4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the deferred vulnerable item must be extended for remediation.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   An email is triggered on submission of the request and subsequent action by the approver.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The request goes through two levels of approval.
- If a deferred exception rule is extended again, the extend deferral count increases in the backend.

6. After the request is approved, the Until, Reason, and Deferral notes are updated.

Refresh Vulnerability Response vulnerable items

The **Update status** related link is used to have vulnerable items inspected to see if there are any additional vulnerable items that belong to a remediation task. Use it if an update is warranted outside the scheduled job.

Before you begin

Role required: sn_vul.vulnerability_write or, sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

The **Update status** related link is only editable on the remediation task form in the **Open** or **Under Investigation** states, using a filter group or where the filter type is condition. This inspection is done regardless of the status of the **Automatically refresh vulnerable items** check box.

Starting with v22.0 of Vulnerability Response, the **Update Status** button is available in record view for remediation tasks in the Vulnerability Manager Workspace and IT Remediation Workspace.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
2. Open any record in the **Open** or **Under Investigation** states.
3. Click the **Update status** link.
   New vulnerable items appear under the **Vulnerable Items** tab.

Identify and escalate security issues in third-party software

You can view software vulnerabilities returned from third-party entries to determine remediation. Use this information to match the vulnerable software entries to a Software Asset Management discovery model.

Before you begin

Role required: sn_vul.vulnerability_write

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability** > **Libraries** > **Third Party**.
   A list of vulnerable software downloaded is shown.
2. Click a software record to view vulnerability information.
3. Click the following related lists to get more information for identifying vulnerabilities.

Related list	Description
Vulnerable Items	Lists any vulnerable items, which consist of pairings of a potentially vulnerable configuration item and software. To get more information about a pairing, click the information icon (ⓘ). **Note:** If software is removed, any associated vulnerable items are closed and removed from the **Vulnerable Items** related list.
Vulnerability Entries	Lists vulnerability entries for the selected software record. Click a record to view its details.

If vulnerabilities were identified and vulnerable items were created, you can Resolve remediation tasks, as needed.

Identify and escalate security issues using NVD

When Common Vulnerability and Exposures identifier (CVE-ID) records are downloaded from the National Vulnerability Database (NVD), they are compared to the software in your company network as identified by the Software Asset discovery model. When a CVE-ID matches vulnerable software or configuration item in your network, a vulnerable item is created. You use the information in the CVE-ID record to decide whether to escalate the vulnerable item for remediation.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Libraries** > **NVD**.
   A list of CVE-IDs that were downloaded from the NVD is shown. Updates from the NVD can be performed on-demand and by scheduled runs from the NIST National Vulnerability Database Integration records located at **All** > **Administration** > **Integrations**.
2. Click a CVE record to view the following information:
   - a summary for the CVE-ID.
   - a reference to a Common Weakness Enumeration (CWE) entry, if applicable.
   - the vulnerability score of the CVE-ID on the Common Vulnerability Scoring System (CVSS). For more information on the CVSS, see the National Vulnerability Database website.
3. Click the related lists for more information on vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability References

Name, description, and URL for the given vulnerability and where it is referenced.

Exploits

Details.

Weaknesses

List of CWE Weaknesses.

4. Click the following related lists to get more information for identifying vulnerabilities.

Related list	Description
Vulnerable Items	Lists any vulnerable items, which consist of pairings of a potentially vulnerable configuration item and software. To get more information about a pairing, click the information icon (ⓘ). **Note:** If software is removed, any associated vulnerable items are closed and removed from the **Vulnerable Items** related list.
Vulnerability Entries	Lists vulnerability entries for the selected software record. Click a record to view its details.

If vulnerabilities were identified and vulnerable items were created, you can Resolve remediation tasks, as needed.

Identify and escalate security issues using CWE

View the library of Common Weakness Enumeration (CWE) records from the National Vulnerability Database (NVD) to understand how they relate to the Common Vulnerability and Exposure (CVE) records. Then use this information to match the vulnerable software entries to a Software Asset Management discovery model.

Before you begin

Role required: sn_vul.vulnerability_write

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability** > **Libraries** > **CWE**.
   A list of vulnerable software downloaded is shown.
2. Click a CWE software record to view vulnerability information.
3. Click the following related lists to get more information for identifying vulnerabilities.

Related list	Description
Vulnerable Items	Lists any vulnerable items, which consist of pairings of a potentially vulnerable configura

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related list	Description
	tion item and software. To get more informa tion about a pairing, click the information icon ( ). **Note:** If software is removed, any asso ciated vulnerable items are closed and removed from the **Vulnerable Items** re lated list.
Vulnerability Entries	Lists vulnerability entries for the selected soft ware record. Click a record to view its details.

If vulnerabilities were identified and vulnerable items were created, you can Resolve remediation tasks, as needed.

View the remediation target status of a Vulnerability Response vulnerable item

When a vulnerable item has nearly reached (or passed) its remediation target date, as defined by a remediation target rule, the vulnerable item record is updated with a status. This information can help the analyst proactively monitor upcoming remediation activities.

Before you begin

Role required:

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [read only]

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

A scheduled job called **Evaluate remediation targets** runs once per day to compare the current date against the vulnerable item remediation date specified in the associated remediation target rule. When the current date falls within the number of days before the remediation is past due, a remediation status is added to the vulnerable item record.

For more information on remediation target rules, see Vulnerability Response remediation target rules.

Procedure

1. Navigate to **All** > **Vulnerability** > **Vulnerable Items**.
2. Click on the vulnerable item you want to review.
   If the remediation date for the vulnerable item is within range of the conditions set in the remediation target rule, the **Remediation Target Status** tab is visible.
3. Click on the **Remediation Target Status** tab.
4. Click on the remediation target status record to review it.

Note: To view the number of Vulnerable Items that are Approaching Target, In-flight and Past Target, see Using the default Vulnerability Response dashboards.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Create or edit a Vulnerability Response remediation target rule

Working with unmatched CIs

As a Vulnerability Manager and Analyst, you can view and reclassify unmatched Configuration Items (CIs), reconcile unmatched discovered items, reapply CI lookup rules on the selected discovered items, and de-duplicate existing CIs.

See the CI matching in Vulnerability Response knowledge base article [KB0998706] for more information about CI matching rule concepts and how CI matching works.

View and reclassify unmatched configuration items

Configuration items (CIs) that are not found in the Configuration Management Database (CMDB) are placed in a viewable list of discovered items. This list offers a convenient way to reclassify unmatched CIs.

Before you begin

Role required:
sn_vul.read (minimum to view Unmatched CIs)

and

itil or asset (to reclassify)

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task

As a Vulnerability Analyst you can view unmatched CIs.

The reclassify action is available only on *sn_sec_cmn_unmatched_ci* class CIs, when you have either the itil or asset roles. Once a CI has been reclassified, it cannot be reclassified using the UI. You can reclassify, from the CI form or the CI list view, by changing the **class** value. For more information, see Reclassify a CI.

Procedure

1. Navigate to **All** > **Security Operations** > **CMDB** > **Discovered Items**.
2. To review, click each item.
3. To make corrections to the information in the **Discovered Item** form fields, edit in this page, and right-click **Save**.
   Any data added to or left in these fields is transferred to the resulting **Configuration Item** when it is reclassified.
4. If everything looks correct, click **Reclassify**.
5. From the choice list, select a **Class Name** and click **Submit**.
   The **Discovered Item Class** is updated, the **State** field is changed to Reclassified, and all data is in the CMDB.

Reconcile unmatched discovered items

Create a scheduled job to reconcile unmatched discovered items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Roles required: admin

About this task
A vulnerable item (VI) consists of a vulnerability and a configuration item (CI). When a VI is created, the CI that is added to it at the time of creation might be an outdated one. Unmatched CI information is not reconciled if the information in the CMDB changes. To reconcile, apply configuration Item (CI) lookup rules on the items that are in an unmatched state when the CMDB is updated with the latest CIs.

You can run a scheduled job demand to reapply the CI matching rule for the discovered items in an unmatched state. If the CI changes after reapplying the lookup rules, the discovered items are updated with the new CI. Impacted detections and vulnerable items are also updated. For details, see CI changes for discovered items.

Procedure
1. Navigate to **All** > **Security Operations > Reconcile Unmatched Discovered Items**.
2. On the Background Jobs page, click **Create reconciliation job**.
3. On the form, fill in the fields.

Note: You can only edit the **Parameters** field.

Background Job form

Field	Description
Number	Unique job number.
Created by	User who created the job.
Parameters	Parameters to reconcile the unmatched discovered items: ○ limit: Maximum number of discovered items to be reconciled. If you do not enter a value, 10,000 discovered items are reconciled. ○ firstDiscovereditem: First discovered item that must be reconciled. If you do not enter a value, the reconciliation process starts from the first discovered item.
State	Current state of the background job.
State description	Description of the current state of the background job.
Job type	Type of job. The value is **Reconcile unmatched discovered items**.
Started at	Time when the job started.
Ended at	Time when the job was completed.
Job duration	Total time taken to complete the job.
Substate	Substate for the selected state.
Notes	Number of records that were processed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click **Submit**.

   Note:
   - To stop running the job, click **Cancel**.
   - You can't reconcile unmatched CIs or reapply CI lookup rules while you are importing hosts or vulnerable items.

5. Starting with Vulnerability Response v26.0.11, you can "Reapply Look up Rules" for selected or filtered items in the discovered items table view.

   Note: From the above mentioned version, the reconcile unmatched discovered items scheduled job is retired.

6. **Optional:** Select **All** > **Security Operations >Reapply Look up Rules** for selected or filtered items in the discovered items table.

   Note: If no filter is applied, the reapply option will be disabled.

   After reapplying, a background job URL or an error message will pop-up, once the integration is running.

Reapply CI lookup rules on selected discovered items

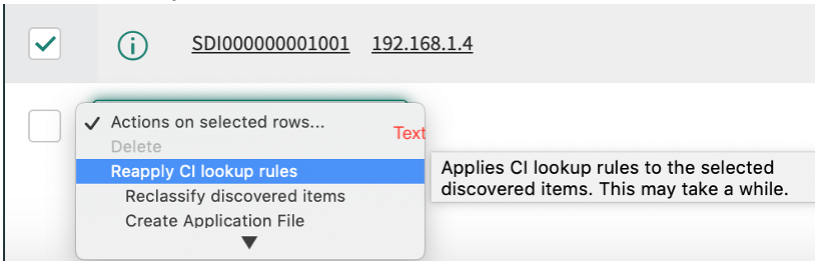
Reapply the configuration item (CI) lookup rules on selected discovered items from the discovered item list view select actions. If the CI changes after you reapply the rules, the discovered items are updated with the new CI and impacted detections. Vulnerable items are also updated.

Before you begin
Roles required: admin

About this task
For more information, see CI changes for discovered items.

For more information about the concepts of CI matching and the CMDB, discovered item lookup, rule-based identification, and other detailed information about how CI matching works, see the CI matching in Vulnerability Response [KB0998706] article in the HI Knowledge Base.

Procedure
1. Navigate to **All** > **Security operations** > **CMDB** > **Discovered Items**.
2. Select the required discovered items and click **Action on selected rows**.



3. From the list, select **Reapply CI lookup rules**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

Starting with Vulnerability Response v24.0.6, you can skip the reapplication of CI lookup rules on discovered items with the substate 'CI Decommissioned' by enabling the system property *sn_sec_cmn.skipItemsWithCIDecommissioned*.

The rules are reapplied on these discovered items.

4. Click **View status** in the message.

   The status displays on the background job form.

   Note: In the **Notes** field, the `Discovered items could not be process due to exception` attribute with a non-zero value indicates that there is an error or exception while reapplying a CI look up rule. Check the system logs for more details.

5. Reapply only applies to items scanned within the last 90 days based on the **last_scan_date, last_comp_scan_date, non_infra_last_scan_date, non_infra_last_comp_scan_date** column.

   Added ci_lifecycle_status_source (scope = sn_sec_cmn) system property for configuring Ci lifecycle status columns (e.g., Install Status, Operational Status). You can configure additional columns for retiring CIs.

   Columns are added to the background job list view:

   - Elapsed Time(ms): The time required for processing the background job.
   - Items Processed: The number of items processed till now.
   - Total Items to be Processed: The total number of items remaining to be processed.
   - Time Until Completion(ms): The time remaining until the background job is processed. These columns provide visibility into job progress, these columns are available for each form view for you to add as per requirement.

Reapply CI Lookup Rules Enhancements

Reapply the configuration item (CI) lookup rules on selected discovered items like os and netbios.

Before you begin

Role required: admin

About this task

- Values of os and netbios present in source data are populated before the configuration item while populating these fields in the discovered item.
- In case of empty values of OS and NETBIOS in source data, the values are taken from the configuration item while populating these fields in discovered items table.

Procedure

1. Navigate to **All** > **Security operations** > **CMDB** > **Discovered Items**.
2. Select the required discovered items and select **Action on selected rows**.
3. From the list, select **Reapply CI lookup rules**.

   The rules are reapplied on these discovered items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules

Take steps to help prevent duplicate or orphan records resulting from matching (configuration items (CIs) within the CMDB.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. Thorough testing and debugging of processing scripts in the rules helps alleviate the potential of issues later in the process.

Preventing duplicate or orphaned records

- Use small subsets of data that are specific to the CI Lookup Rule being tested.
  - Set all CI Lookup Rules, other than the one being tested, to Inactive.
  - Analyze the imported CIs to ensure that you are observing the expected behavior and matching is occurring properly.
- Review Matched CIs
  - Examine the count of matched vs unmatched CIs. Ensure that the percentage is acceptable. Don't just look at the first page, that is likely the first one inserted.
  - Manually search for some CIs.
  - Check to see if there are any naming or field problems (such as searching for a specific domain).

    If it seems appropriate, add additional matching rules.
- Review Unmatched CIs
  - Navigate to the Unmatched CIs table.
  - Group by Configuration Item class.
  - Review any classes that don't look right (certificates, network cards, images).
    - Figure out why didn't they match the correct CI?
    - Should the class be excluded?
    - Should the class be elevated to a related class?
- Review CI states such as **Retired**.
- Remove Test Data
  - Once you begin to observe the correct or expected behavior in CI matching, start over.
  - Start over by: Deleting the data used for testing: (see the **Deleting data from tables** section)
    - Discovered Items
    - Vulnerable Items
    - Remediation tasks
  - Manually rerunning all the CI Matching rules.

For more information on CI Lookup Rules and Qualys, see the KB0750656 article.

For more information on CI Lookup Rules and Rapid7, see the KB0818096.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deleting data from tables

Sometimes you have imported data and realize something is wrong. If something is wrong in a development or performance environment, you could reclone from a better environment, but that isn't always an option.

Note: Performing these actions requires ServiceNow expertise.

There are four options for deleting data from tables:

- Using **Delete All Records** on **Table Configuration**.
- Configure the **Table Cleaner** by navigating to **Auto Flushes** (sys_auto_flush.list) and creating a new **Auto-flush** record.
- Truncate the gs.truncateTable using a background script.

  Using *truncateTable* requires turning off the record for rollback check box in the background scripts. Otherwise, a copy of the table and related cascade tables are created, take too long, and most likely fail.

  Note: Never use *truncateTable* in a production environment. Consult you Support representative before executing large deletions in production or shared environments.

De-duplicating existing configuration items

Whenever configuration items (CIs) are updated through a deduplication task, the discovered items (DIs) that are related to those CIs are also updated. The vulnerable items (VIs) and detections are also updated with the CI.

For more information, see CI changes for discovered items.

Related topics

Remediate a de-duplication task

Working with unmatched CIs

As a Vulnerability Manager and Analyst, you can view and reclassify unmatched Configuration Items (CIs), reconcile unmatched discovered items, reapply CI lookup rules on the selected discovered items, and de-duplicate existing CIs.

See the CI matching in Vulnerability Response knowledge base article [KB0998706] for more information about CI matching rule concepts and how CI matching works.

Resolve remediation tasks

The flexibility inherent in Vulnerability Response allows you to remediate vulnerabilities in whatever way suits your security organization.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task

Once you are notified that a change request is resolved, move the remediation task state to Resolved and wait for the next scan. Rescans are triggered automatically by the third-party import schedule configured in the Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If state synchronization is activated, remediation tasks are automatically moved to the Resolved state after a change request associated with a remediation task (VUL) is implemented and in the Review state. See Change management for Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation tasks** > **Assigned to me**.
2. Click a record that is in the Open state.

   The Open state indicates that the record has not yet been worked on. The form displays:

   - Remediation task information
   - Group Configuration details
   - Notes
   - Associated vulnerable items
   - Task SLAs
   - Change Requests
3. Perform your analysis of the group.
4. When you are ready to start working on the record, choose any of the following options.

Option	Description
If the vulnerable item poses a risk to your IT environment, create a CHG record and es calate the issue to team.	Assign the group to the appropriate group or individual and click **Create Change**.
If the vulnerable item poses a potential secu rity risk to your organization, create a securi ty incident record and escalate the issue to the Security Incident Response team.	Click **Create Security Incident**. This button is displayed only when Security In cident Response is activated. A business im pact calculation is applied, the incident is as signed, and the security incident is created.

   After you create a change request, the appropriate record appears in the **Change Requests** related list on the Vulnerability Group form.
5. If you determine that the issue is of low risk and can be deferred, click **Request Exception**. For more information on how to defer a remediation task, see Defer a Remediation task.
6. If you determine that the issue can be immediately closed without further analysis, click **Close**. For more information on how to close a remediation task, see Close a remediation task. Starting with v23.0 of Vulnerability Response, the **Close** button has been removed for a remediation task.

   A third-party integration scheduled job automatically updates and scans records at a set interval. The vulnerable items are scanned at the next scheduled date and time. Alternatively, you can manually initiate a vulnerability scan using the **Scan for Vulnerabilities** related link.

   If the scan again finds the vulnerability on the configuration item and does not mark it Fixed, the vulnerable item returns to the Under Investigation state. Contact IT Operations to reopen the change request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the scan does not find the vulnerability and returns that the vulnerable item has been marked Fixed, the vulnerable item transitions to the Closed-Fixed state and is closed during import.

Only when all vulnerable items in a task are in the Closed-Fixed state, does the remediation task close automatically. Remediation tasks with vulnerable items in Closed states other than Fixed must be closed manually.

Defer a Remediation task

If you determine that the issue associated with a remediation task (VUL) is a low priority and can be immediately deferred without further analysis, you can use the **Request Exception** feature.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task

You can defer a remediation task from a remediation task record in the Vulnerability Response Workspaces. After you submit the request, it is sent for approval. See Request an exception in the IT Remediation Workspace.

A scheduled job runs every day checking for deferred remediation tasks that have reached their reopen date. On the day the task's deferral is set to expire, the task is reopened.

Note: You can manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move remediation tasks from the Closed or Deferred states.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
2. Open a record.
3. Click **Request Exception**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Until	Select the date when the Defer state expires and the remediation task is reactivated. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the remediation task is set back to **Open** and a second email notification is sent out.
Reason	Enter the reason for deferring the issue. Choices include:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Awaiting maintenance window ○ False positive ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Click **Submit**.
   The group is marked In Review. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **State Change Approvals** tab.

Request an extension for a deferred remediation task

Request an extension for a deferred remediation task (VUL) before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task
You can also request an extension from the Vulnerability Response Workspaces.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
2. Open a deferred remediation task.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date when the Defer state expires and the remediation task is reactivated.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select **Request Approval**.
   On approval of the request, the changes on the remediation task are rolled down to the vulnerable items as well, which are part of the remediation task. However, the vulnerable items should be in the deferred state and their current until data precedes the updated until date. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred remediation task is extended again, the extend deferral count increases in the backend.

Close a remediation task

If you determine that the issue associated with a remediation task can be immediately closed without further analysis, you can use the **Close** feature. Starting with v23.0 of Vulnerability Response, the **Close** button has been removed for a remediation task and the closure of a remediation task is driven by the scanner.

Before you begin

Role required: admin

About this task

In the Vulnerability Response Workspaces, a remediation task transitions through the same states as a remediation task prior did in previous versions of Vulnerability Response. When all the vulnerable items (VITs) in a remediation task are closed, the remediation task transitions to the Inactive state.

Important: You can manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move remediation tasks from the `Closed` or `Deferred` states.

Procedure

1. Open the record that you want to request a review for.
2. Select the **Close/Defer** button.
3. Fill in the fields on the form, as appropriate.

Field	Description
State	Select a state. Choices are: ○ Deferred ○ Closed
Until	Only available in the **Defer** state pop-up.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Select the date when the **Defer** state expires and the remediation task is reactivated. After the record is submitted, if email notifications are defined, members of the Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerable item is set back to **Open** and a second email notification is sent out.
Reason	Enter the reason for closing the issue.
Additional information	Enter any other relevant information.

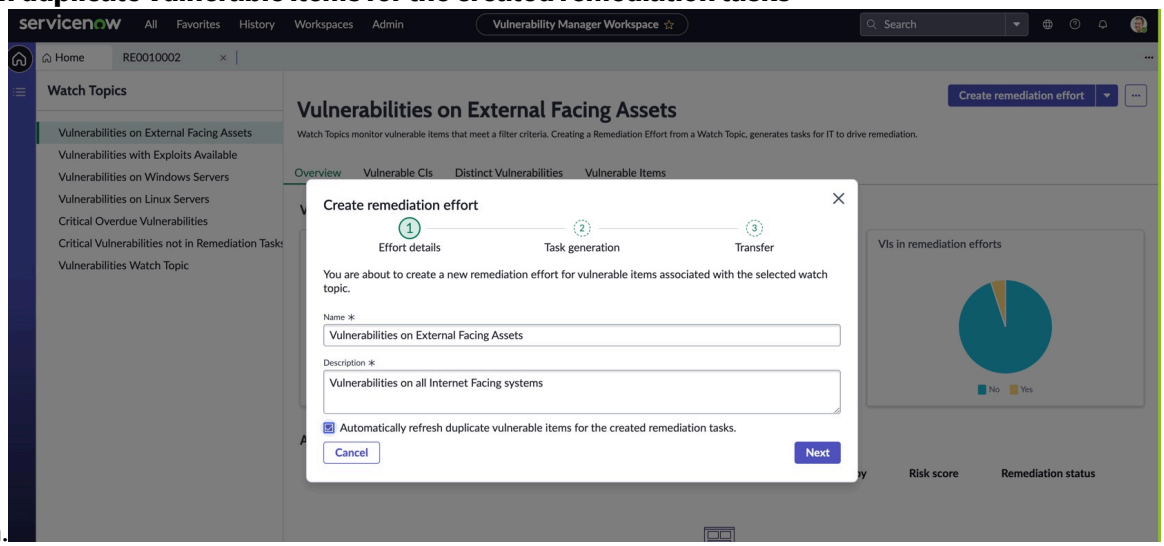
4. Select **Submit**.
   The remediation task is marked **Closed**.

Identifying duplicate vulnerable items from multiple scanners

If you are using multiple scanners on the same asset to detect vulnerabilities, multiple vulnerable items (VIs) might be created. You can identify these duplicate VIs to ensure that the duplicate vulnerabilities are not assigned to the remediation owners.

This resolution is possible only if the same vulnerabilities, such as the same Common Vulnerabilities and Exposures (CVEs) are detected. The vulnerability combination depends on the scanners being used. For example, Qualys and Tenable have their own vulnerability type, that is, third-party entries (TPEs), and other scanners such as Microsoft Defender for Endpoint detect vulnerabilities based on CVEs.

Starting from v 17.1, while creating a remediation effort, you can automatically refresh duplicate vulnerable items on the created remediation tasks. To automatically refresh the duplicate vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** option.



Show Duplicate VIs: Identify duplicate vulnerable items reported by multiple scanners in the system. You can mark the duplicate VI as Resolved. For more information, see Automatically resolve duplicate vulnerabilities. Duplicate entries are only shown when the combination

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

of vulnerabilities is created using CVEs. For more information, see Vulnerability Response remediation task and vulnerable item states.

Potential duplicates are identified for the following vulnerability combinations:

Scanner combination	Type of vulnerability
Scanner 1 and Scanner 2	CVE
Scanner 1 and Scanner 2	CVE and TPE

Automatically resolve duplicate vulnerabilities

Starting from Vulnerability Response (VR) v17.1, you can automatically resolve any duplicate vulnerabilities on an asset.

When an asset is scanned with multiple scanners, there's a chance of identifying the same vulnerability as duplicates by the different scanners. For example, if the Qualys and Microsoft scanners identify the same vulnerability, you can choose to automatically resolve the duplicate one.

Sample scenario

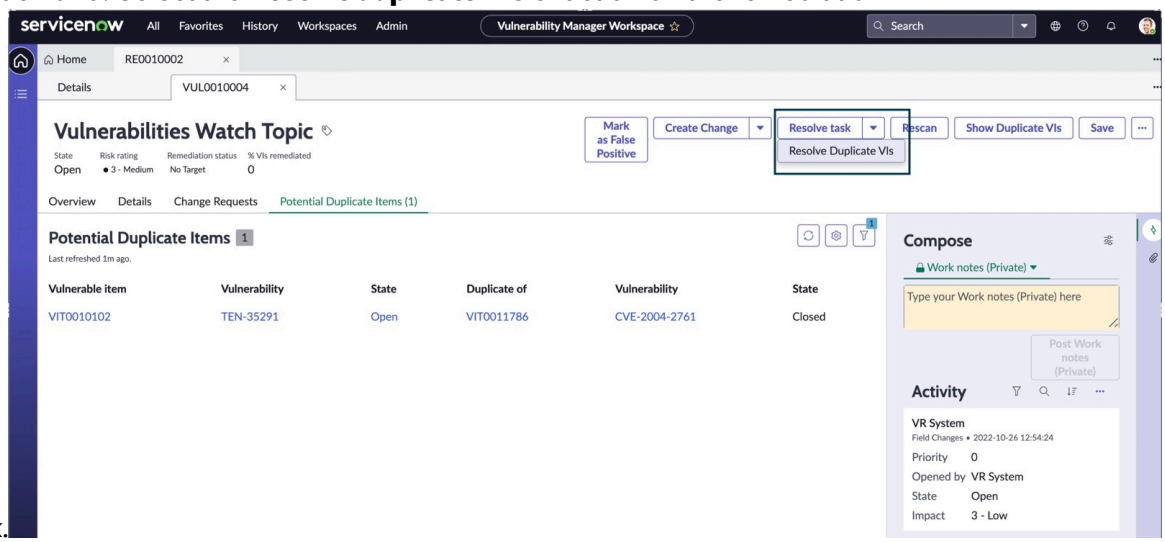
VR creates a record, VI1, for vulnerability 1 from the Microsoft Defender for Endpoint scanner. A second record, VI2, is created from the Qualys scanner for the same vulnerability. The remediation team applies the patches that might resolve the VI1 and VI2 records. If you configure the Qualys scan schedule beyond one day, by that time the Microsoft Defender gives the fixed vulnerability information and VR closes the VI1 record as Closed/Fixed.

In this scenario, VI2 record is still in Open state and VR waits for the Qualys scan results. In this situation, VI records from the second scanner remain in Open state even if the patch is applied and the VI is confirmed as fixed by the other scanner.

To address this situation, you may consider to resolve the duplicate vulnerability record based on the condition that the vulnerability is closed by the first scanner.

Resolve vulnerabilities in the following ways:

- On-demand: Select the **Resolve duplicate VIs** UI action on the remediation task.



- Automated: Enable the system property `sn_vul.auto_resolve_duplicate_vit` to automatically resolve duplicate vulnerable items. The daily scheduled job 'Refresh and resolve duplicate VITs on remediation task' automatically refreshes the duplicate items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The duplicate VIs are then marked as resolved.

Note: The resolved vulnerability item record is reopened if the scanner identifies it as **Not Fixed**.

Create and edit a classification group

Create groups so that the underlying rules of this group can classify the table records based on the conditions. The rules can be used to select any field in the corresponding table.

Before you begin

Role required: sn_vul.manage_classification_rule

Procedure

1. Navigate to the System Properties table.
2. In the *sn_sec_cmn.classificationTables* system property, add the name of the table for which you want to create the classification group.
3. Create a new business rule by adding the following code snippet to the business rule on the table defined in the group:

```
var classificationCalc = new
sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_gr
classificationCalc.calculate();
```

Note: Business rules are provided to execute the classification during ingestion for the Discovered items and Vulnerability Entry tables. For other tables, to have the classification rules on ingestion, you must add the business rules.

4. Navigate to **All** > **Vulnerability Response** > **Administration** > **Classification Rules**.
5. On the Classification Groups context menu, click **New**.
6. On the form, fill in the fields.

Vulnerability Classification Group form

Field	Description
Name	Name of the new classification group.
Active	Option to activate the group.
Description	Description of the new classification group.
Table	Table based on which the rules are executed. **Note:** The Vulnerability Response base system includes classification groups for discovered items and vulnerabilities.

Create and edit a classification rule

Create rules to automatically classify the incoming vulnerabilities to the correct teams for remediation.

Before you begin

Role required: sn_vul.manage_classification_rule

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

When created, these rules classify the vulnerabilities as belonging to either a platform or an application. You can configure these rules to replace the value of a specific field on the vulnerability entry.
Use these rules to move the calculation upstream to the Third-Party Vulnerabilities Entry table to enable the reuse of content.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Classification Rules**.
2. To view a classification group, click that group.
3. On the Classification Rules context menu, click **New**.
4. On the form, fill in the fields.

Vulnerability Classification Rule form

Field	Description
Name	Name of the new classification rule.
Active	Option to activate the rule.
Description	Description of the new classification rule.
Execution order	Order in which the rule should be executed.
Advanced view	Option to view additional fields on the tabbed sections.
When this condition is met	
Condition type	Type of condition for the rule. Choices are as follows: ○ **Filter**: Basic filter conditions for determining whether to use the rule or not. ○ **Filter group**: Set of multiple conditions that are used together. The rule is evaluated based on the conditions defined in the filter group. ○ **Script**: Scripted condition used to determine when to apply this rule. This field appears only when the **Advanced view** option is selected.
Condition	Condition for the rule. Define conditions based on the column selected on the required vulnerability entry column. You can add multiple conditions to refine the rule. This field appears only when **Filter** is selected from the **Condition type** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: When defining multiple conditions or templates, you can select only from a parent and a child table. You cannot select from two or more child tables.
Filter group	Group of filters. The group is defined when a set of conditions is used repeatedly in multiple places. Click the lookup using the list icon ( ) to select the filter group. For more information, see Create and define filter groups in Security Operations. This field appears only when **Filter group** is selected from the **Condition type** field.
Script	Script that is evaluated to determine when to apply this rule. You can write your code and set the response as either true or false. This field appears only when **Script** is selected from the **Condition type** field
Set these values	
Classification	Classification of the rule. To select an option, click the bulb icon ( ). The list displays the options for Platform and Application. Alternatively, you can enter your own classification that is not in the list.
Classification type	Type of classification. This field shows the filtered list of classification types based on your selected value for the **Classification** field.
Value type	Type of the value that is assigned by using this rule. Choices are as follows: ○ **Template**: Select a template. You can use a required template. ○ **Script**: Select a pre-existing script, or write your own custom script. This field appears only when the **Advanced view** option is selected.
Template	Another condition for the rule apart from the **Classification** and **Classification type** fields. Select a combination of fields and values that you want to set when the rule is evaluated. This field appears only when **Template** is selected from the **Value type** field.
Script value	Script to set values on the current record. This field defines what values to set on the fields in vulnerability entries. This field

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	appears only when **Script** is selected from the **Value type** field.

5. To create the new rule, click **Submit**.

Example:
Use VR classification rules to add the logic to upstream tables like Vulnerability and Discovered Items and calculate it. You can reuse the output multiple times, thereby improving the performance of rules such as assignment rules. For example, classify the Third-Party Entry (TPE) as Java and reuse the output in the assignment rules multiple times. Sample assignment rule:

```
VI.TPE.Classfication Type
          | IS | Java
```

Apply a rule to an existing vulnerability

When you change a classification rule, rerun all the active rules on all the vulnerability entries. You can also retrofit the existing vulnerabilities, by applying the newly created classification rules to the existing vulnerabilities.

Before you begin
Role required: sn_vul.manage_classification_rule

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Vulnerability Classification Rules**.
2. To select a rule, select the check box next to the rule.
3. Click **Apply Changes**.
4. Click **Reapply**.

Deactivate or delete a classification rule

Deactivate or delete a classification rule if it is no longer needed or relevant.

Before you begin
Role required: sn_vul.manage_classification_rule

About this task
When a classification rule is deactivated or deleted, the data that was populated in the **Classification** and **Classification_type** fields by that deleted rule remains in their respective tables.

If you want to clear this data, create a rule with empty values in the **Classification** and **Classification_type** fields and reapply the group. Once this new rule is reapplied, the changes are reflected on all the records that this rule is applicable for, based on the conditions of the rule.

Starting with v24.0.6 of Vulnerability Response, if a classification rule is deleted or deactivated, it's no longer applied to the discovered item or vulnerability entry and the data in the **Classification** and **Classification_type** fields get cleared.

Procedure

1. Navigate to **All** > **Vulnerability** > **Administration** > **Vulnerability Classification Rules**.
2. To select the rule that you want to delete, click the check box that is next to the rule.
3. To delete the rule, do one of the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- From the Action on selected rows list, click **Delete**.
- Select the rule and click the **Delete** button.

4. Click **Apply Changes**.

> **Note:** If you don't click this button, the rule continues to reside in the system. Vulnerabilities referenced by the rule continue to reference them.

Create an exclusion rule

Create a rule to filter or exclude detections from getting converted into vulnerable items (VITs) during ingestion.

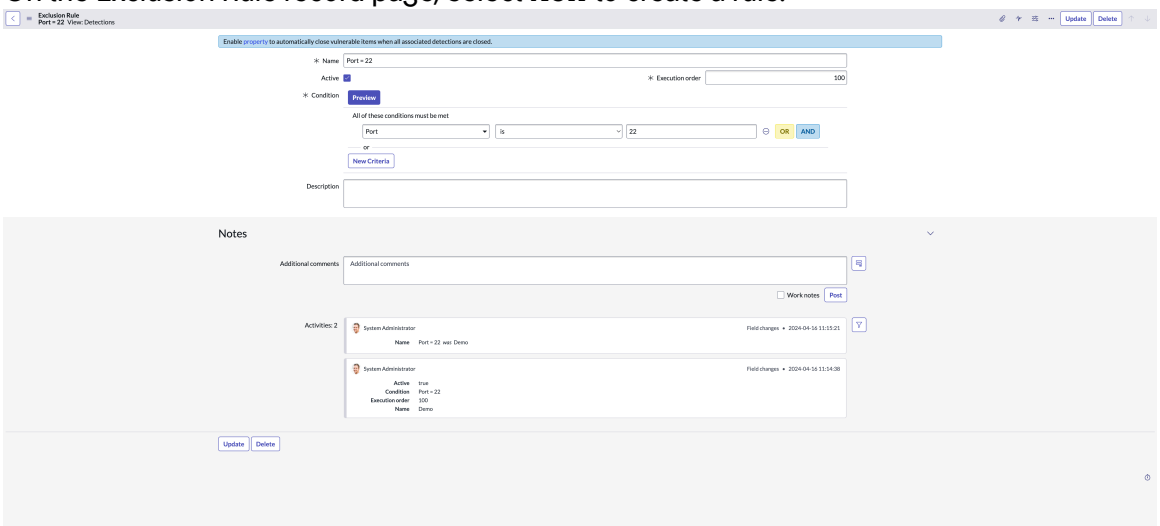
Before you begin

Role required: Vulnerability admin

About this task

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Exclusion Rules**.
2. On the Exclusion Rule record page, select **New** to create a rule.



A message saying 'Enable property to automatically close vulnerable items when all associated detections are closed' is displayed. By default, the property is inactive. To enable, select the property link and enter the value as True in the **Value** field.

3. On the form, fill in the fields.

Exclusion Rule form

Field	Description
Name	Name of the exclusion rule.
Active	Option to activate the exclusion rule.
Execution order	Unique order for each exclusion rule.
Condition	Filter conditions for the detections that can be defined while processing them.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: You can't select Exclusion rule or Vulnerability item field conditions.
Description	Description of the exclusion rule.

4. Select **Submit**.
   The activity is recorded in the system.

   Note: Once an exclusion rule is created, it takes effect on detections starting from the subsequent ingestion.

Change Management tasks for Vulnerability Response

From remediation tasks (RTs), create change requests, associate RTs to existing change requests, or split remediation tasks into new tasks with subsets of vulnerable items (VI).

Create and manage change requests directly from a remediation task if a manual and controlled process of any kind is required for modification or removal of supported configuration items (CIs) in your CMDB. Creating and managing change requests directly from a record helps you investigate and resolve vulnerabilities quickly.

See Change management for Vulnerability Response for an overview of how change management works with the Vulnerability Response application and the system requirements.

Refer to the following topics for how to create change requests, associate remediation tasks to existing change requests, and split remediation tasks. See State synchronization between change requests and remediation tasks for information about how state fields on change requests (CHG) automatically resolve remediation tasks.

Create a change request from a remediation task

As an IT remediation owner, create a change request (CHG) directly from a remediation task (VUL) for all the vulnerable items in the group. Create a change request with pre-populated information that includes the preferred solution to expedite your investigation for vulnerabilities that require manual intervention.

Before you begin

Roles required: For creating a change request: Any user with the itil role. The sn_vul.remediation_owner role is also automatically assigned when the itil role is assigned to a user.

Role required: For approval of change requests: users with itil, admin, sn_change_write, change_manager roles.

About this task

For information about how to create a change request from the Vulnerability Response workspaces, see Create a change request in the IT Remediation Workspace.

To create a change request from the classic environment, follow the steps listed below.

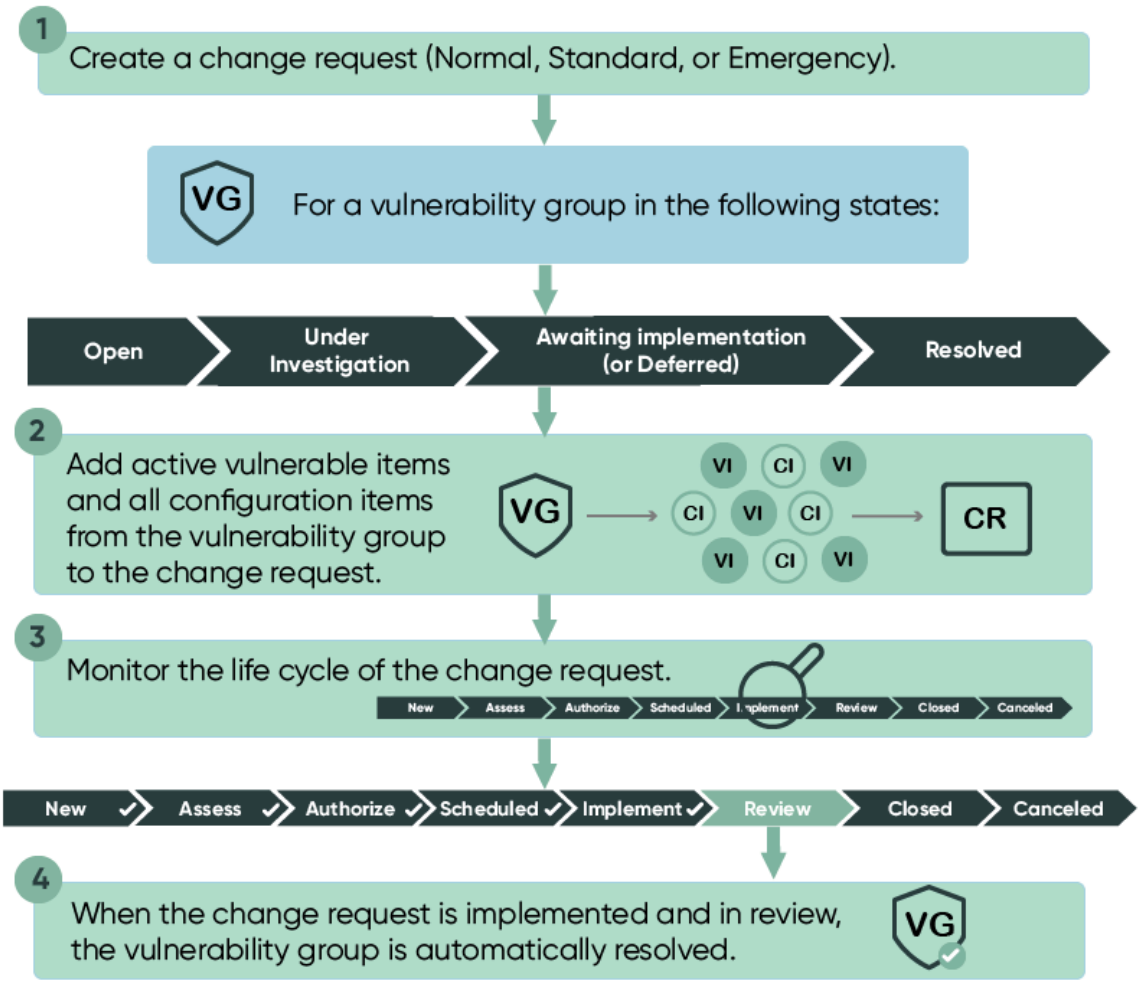
You can create, approve, implement, review, and close change requests directly from a remediation task. You can create three types of change requests with pre-populated information from a remediation task:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Standard. A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.
- Normal. Normal change requests follow a prescriptive process that requires two levels of approval before being implemented, reviewed, and closed.
- Emergency. A change to resolve a major incident.

The following image illustrates the basic flow for creating a change request from a VUL (remediation task). The detailed steps for this flow follow the image.

The remediation task record is referred to as a VUL in the following sections. In previous versions of Vulnerability Response, remediation tasks were called, vulnerability groups (VG)s. In the following images, VG= remediation task, or a VUL record.



Note: Key points about creating new change requests:

- You can create new change requests for any remediation task (VUL) in a state other than `Closed`.
- Verify that you have an approver for change requests other than Standard (pre-approved) that you create or associate to a VUL. This expedites moving the VUL to resolution. For more information on adding users, see Add users to the Vulnerability Response group.
- Before a remediation task can be resolved, all tasks on at least one CHG that is associated with the VUL must be completed so that the change request can be implemented and moved to the `Review` state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

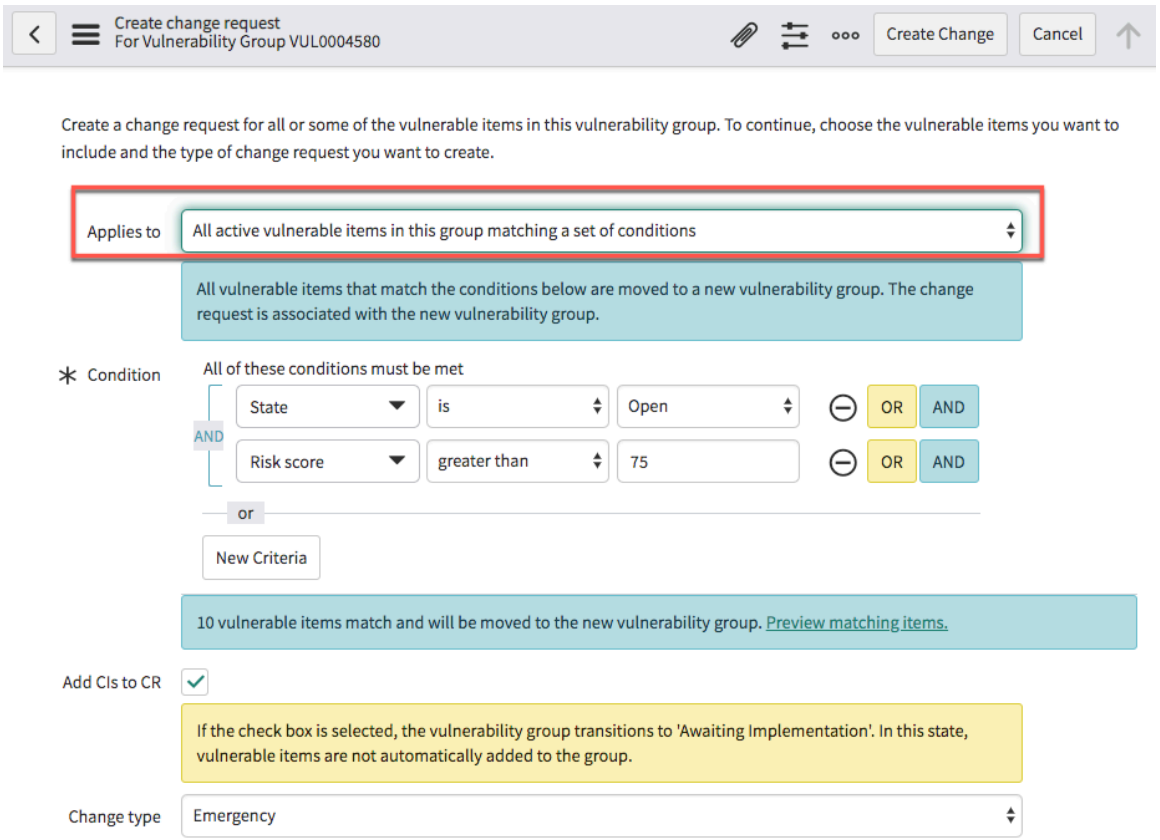
1. To create a complete change request from an existing remediation task record, navigate to **All** > **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**.
   The list of remediation tasks assigned to your assignment group is displayed.
2. **Optional:** Navigate to **All** > **Vulnerability Response** > **Remediation Overview** to view the Remediation Overview dashboard and locate a VUL assigned to you or your assignment group.
3. Alternatively, in the Number column, click a remediation task to open the record and view the details.
   The record is displayed.
4. With the VUL record displayed that you want to create the change request for, in the upper right of the record, click **Create Change**.
   The Create change request form is displayed.
5. Fill in the fields.

   a. From the choice list of the Applies to field, choose one to continue.

Option	Description
All active vulnerable items in this group	If selected, all active vulnerable items from this remediation task with a state other than Closed are added automatically to the change request after you click **Create Change**.
All vulnerable items in this group matching a set of conditions	If selected, the Condition builder is displayed as shown in the second figure below. Enter filter criteria to identify the vulnerable items that you want for the new change request. An example of a filter might include only vulnerable items that match specific search criteria: **State is Open** and **Risk score greater than 75**. After you enter your conditions, a message is displayed with the number of VIs that match your criteria (10). A link (**Preview matching items**) to preview the matching items is displayed. If no items match your filter conditions, a message is displayed below the Condition builder that instructs you to adjust your filter. After you click **Create Change**, all vulnerable items that match this condition filter are moved a new remediation task. This change request is associated with the new remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create change request form for vulnerable items in a task that match a set of conditions



b. Optional: If displayed on the form, click the **Preview matching items** link for a list of the VIs that match your filter criteria.
The Remediation Task List preview is displayed. You can select items on this preview list and perform UI actions on them, however, these actions are also performed on the VUL. For example, if you delete a VI from the preview list, that VI is also deleted from the VUL.

c. After you complete your preview, close the browser window to return the change request form.

d. For the Add CIs to CR check box, choose one to continue.

Option	Description
Add CIs to CR check box selected	Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this remediation task are added to this change request. The VUL automatically moves to the `Awaiting Implementation` state.
Add CIs to CR check box cleared	Clear the check box if you do not want the CIs from the active vulnerable items from this remediation task added to the new change request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	When disabled, the state of the change request is not synched to the VUL, and the VUL remains in its current state.

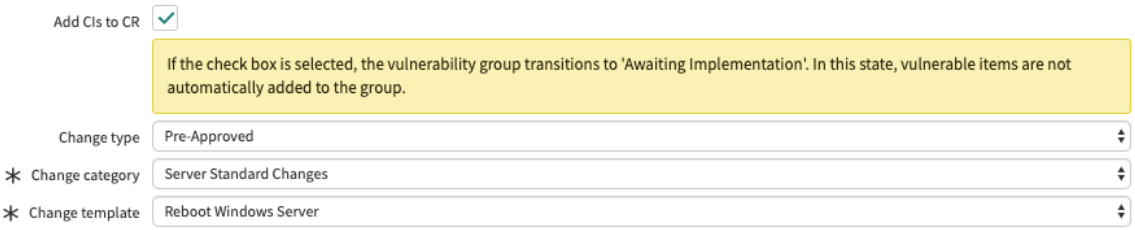
e. From the choice list for the Change type field, choose one to continue.

Change type	Description
Emergency	A change to resolve a major incident.
Normal	A change type that is used to implement any change to a service that is not a standard or emergency change.
Standard	A pre-authorized, low-risk change request that is frequently implemented. Approved standard change requests can be predefined in a catalog of templates to make accessing and requesting a standard change more efficient. If selected, two fields are displayed as shown in the following figure. Select one from each choice list to fill in these fields: ▪ Change category: Select a category for the change from your existing catalog, for example, `Hardware`, `Server Standard Changes`, `Software`. In this example, `Patching Standard Changes` is selected. ▪ Change template: Select one available template for change requests with pre-defined supporting tasks from your catalog. In this example, the `Microsoft Monthly Patching Cycle` template is selected. For more information on ITSM change request categories, templates, and change types, see Change types.

The feature automatically reads the types of change requests that you set up in your catalog in ITSM Change Management. For example, if you change the name for your Standard change requests in ITSM from `Standard` to `Pre-approved`, your new name is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

automatically displayed in the Change type choice list on the Create change request from as shown in the following figure.



The fields in the Change Request Preview section of the form are pre-populated with information from the VUL. If required, these field values can be edited. For example, review the values in the fields in the following figure:

Planned end date

This date (2019 - 10 - 10) is the same value that is displayed in the Remediation target date field of the VUL. This value is derived from the earliest remediation target date from the vulnerable items that belong to the VUL. If you are creating a change request for a critical issue that requires an earlier remediation date, you may prefer to edit this value and the value in the Priority field.

Justification

This field displays the number of CIs that are added to the CHG. If you want to add additional information, you may prefer to edit this text. For example, you may prefer to add a note in this field about the filter you used to create the new VUL, for example, `Risk score greater than 75`. This text can help you locate your new change request and vulnerability group.

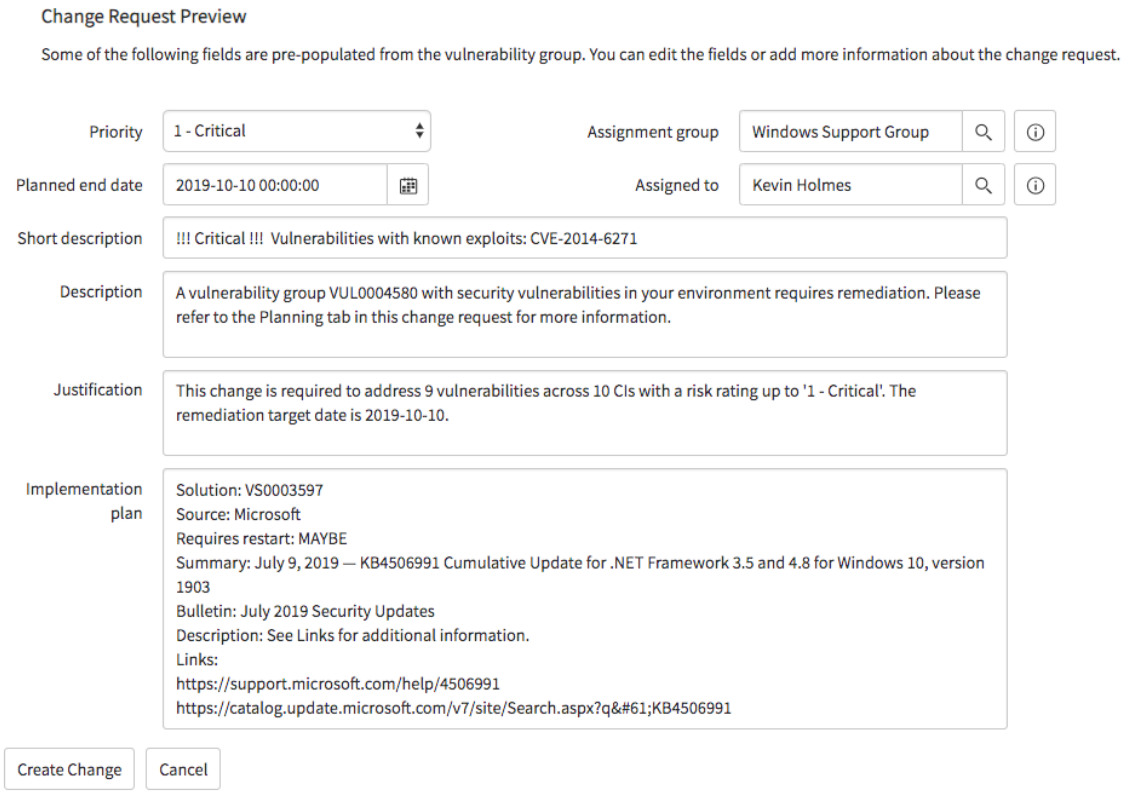
Implementation plan

This field displays the preferred solution for the vulnerability.

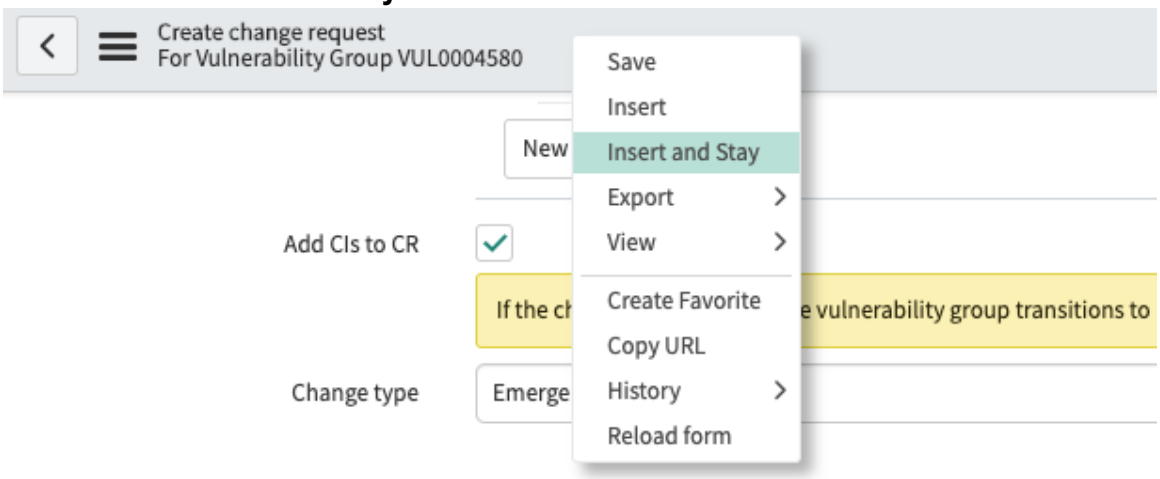
Assignment group and Assigned to

Edit these fields to change the assignment group or reassign this change request to a user in one of your assignment groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Continue to preview and edit the fields as required.
7. To save your changes and remain on this page, in the gray banner at the top of the form, right-click and select **Insert and Stay**.

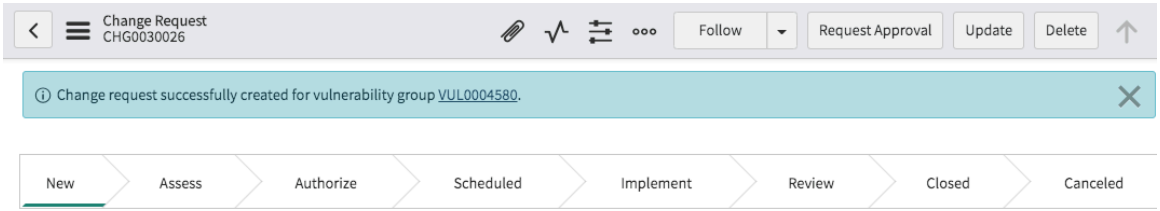


8. After you complete your edits, choose one to continue.

Option	Description
Create Change	Your change request is created and the new change request is displayed in the New state. At the top, messages are displayed that indi cate the change request is successfully creat ed with the number of vulnerable items that were added as shown in the following figure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	If state synchronization is enabled and the VUL is not already in `Under Investigation`, the VUL is automatically moved to `Under Investigation` and a work note is posted.
Cancel	The change request is not created and the VUL is displayed.



Note:

For a remediation task in the `Open` state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the task after you click **Create Change**. In addition, the Add CIs to CR check box must be selected. At the top of the VUL, a blue confirmation message is displayed that indicates this assignment.

What to do next

Monitor the change request and the change tasks to verify that they are completed and the change request is implemented. After this CHG is implemented and moved to the `Review` state, if state synchronization is enabled, the VUL automatically moves to `Resolved`. For more information on state synchronization, see State synchronization between change requests and remediation tasks.

Associate a remediation task to an existing change request

As an IT remediation owner, avoid creating duplicate change requests (CHG) as you work to resolve your remediation tasks by associating a remediation task (VUL) to a change request that is already available in your instance.

Before you begin

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: Any user with the itil role. The sn_vul.remediation_owner role is also assigned automatically to a user when the itil role is assigned.

About this task

For more information about associating a remediation task to an existing change request, see Create a change request in the IT Remediation Workspace.

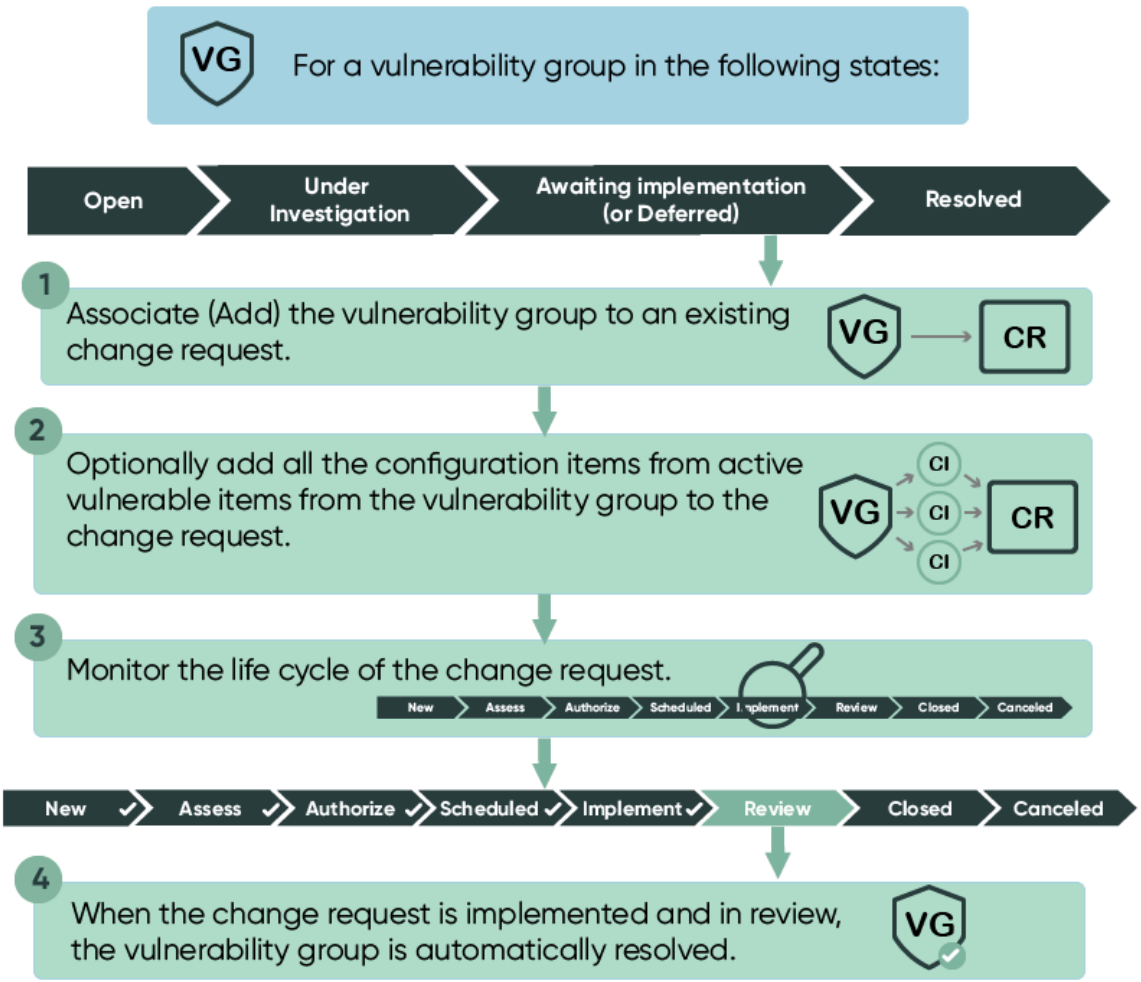
The remediation task record is referred to as a VUL in the following sections. In previous versions of Vulnerability Response, remediation tasks were called, vulnerability groups (VG). In the following images, VG= remediation task, or a VUL record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about associating a remediation task to an existing change request, see Create a change request in the IT Remediation Workspace.

As a remediation owner, you can associate remediation tasks that are assigned to you or your assignment group to existing change requests directly from the remediation task records. The following image illustrates the basic flow for associating a change request to an existing VUL (VG). The detailed steps for this flow follow the image.

Workflow for associating a remediation task to an existing change request



Note: You can associate an existing change request to a VUL in any state (Open, Under Investigation, Awaiting Implementation, Closed, and Deferred). When you associate a change request to an existing VUL, only the active VIs are added to the change request.

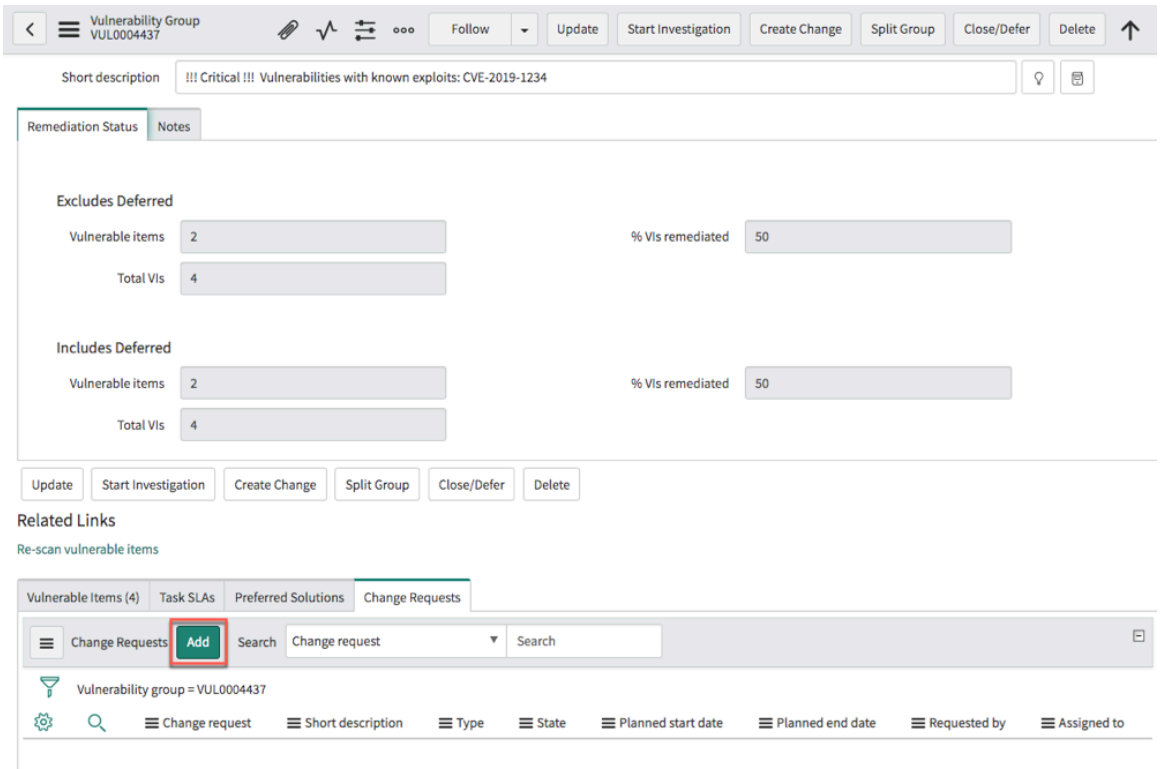
Before you begin, to avoid creating duplicate change requests, you might prefer to view any existing change requests already associated with a VUL. To easily track the number of change requests that are related to a specific VUL, refer to the CR count column on the Remediation Tasks list. If not displayed, click the settings icon ( ) in the upper right. Move the CR count column from Available to Selected and click **OK**.

To automatically populate the new column, for customers with existing data in this table, run the scheduled job: `Populate new CR Count Column`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

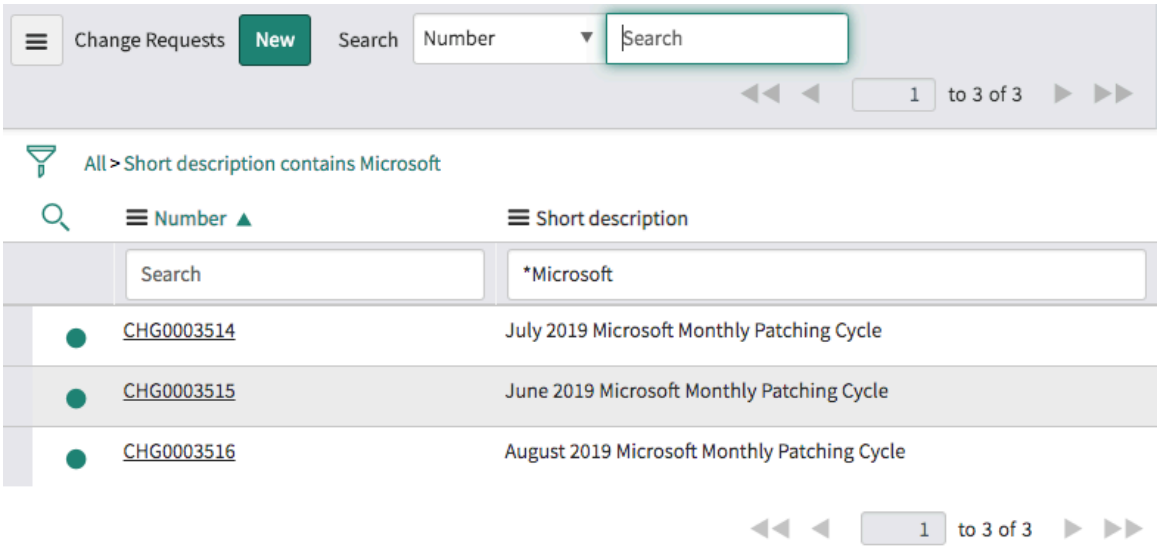
Procedure

1. To associate a remediation task to an existing change request, navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
2. Locate the remediation task you are working with.
3. **Optional:** Navigate to **All** > **Vulnerability Response** > **Remediation Overview** to view the Remediation Overview dashboard and locate a VUL assigned to you or your assignment group.
4. In the Number column, click a VUL record to open it.
   The VUL record is displayed.
5. With the open record displayed, if not already displayed, scroll to the Change Requests related list and select it.
   Any change requests associated with the VUL are displayed along with the **Add** button. In the following figure, there are no change requests already associated with this VUL.



6. To associate the VUL with an existing CHG, click **Add**.
   The Add Existing Change Request to Remediation Task form is displayed.
7. In the form, click the search icon.
   A list view of existing change requests is displayed in a new window as shown in the following figure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. Select an item from the displayed list, or, alternatively, click the filter ( ) and enter conditions to limit your search results.
9. For the Add CIs to CR check box, choose one to continue.

Note: This check box is displayed only for existing change requests in the New state.

Option	Description
Add CIs to CR check box selected	Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this remediation task are added to this change request. When selected, the state of the change request is synched to the VUL. For more information, see State synchronization between change requests and remediation tasks.
Add CIs to CR check box cleared	Clear the check box if you do not want the CIs from the active vulnerable items from this remediation task added to the new change request. When disabled, the state of the change request is not synched to the VUL, and the VUL remains in its current state.

10. With the change request number you want displayed in the Search for Change Request field, click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The VUL is displayed. At the top of the record, the blue confirmation message is displayed indicating that the change request you selected is successfully associated to the VUL.

Note: For a VUL in the Open state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the VUL after you click **Add**. In addition, the Add CIs to CR check box must be selected. At the top of the VUL, a blue confirmation message is displayed that indicates that the current user is assigned.

What to do next

Review the VUL record. In the Change Request column on the Change Requests related list, click link for the new CHG to view CR record. On the open CHG record, you can monitor the state of the change request. The affected configuration items (CI)s and the remediation tasks are displayed on the Affected CIs and remediation tasks related lists.

Split a remediation task

As an IT remediation owner, from an existing remediation task (VUL), identify a subset of vulnerable items (VI) that you want to move to a new group.

Before you begin

Note:

Use cases for splitting VIs from existing VULs into new remediation tasks might include the following examples:

- When you want to create a change request or change requests for a split task.
- When you reassign a split group to another user in your assignment group.
- When you request a deferral or exception for a split task, because you know that some vulnerabilities on specific configuration items (CI) cannot be remediated in a given time frame.

Role required: Any user with the itil role for splitting a VUL.

Note: The sn_vul.remediation_owner role is also automatically assigned when the itil role is assigned to a user.

About this task

For more information about splitting remediation tasks in the Vulnerability Response workspaces, see Split a remediation task in the IT Remediation Workspace.

To split a remediation task in the classic environment or for versions of Vulnerability Response.

You can split existing remediation tasks with more than one vulnerable item that are in the Open, Under Investigation, or Awaiting Implementation states. By creating a new VUL with vulnerable items that match specific criteria, you can work with a specific group of vulnerable items without impacting the original remediation task.

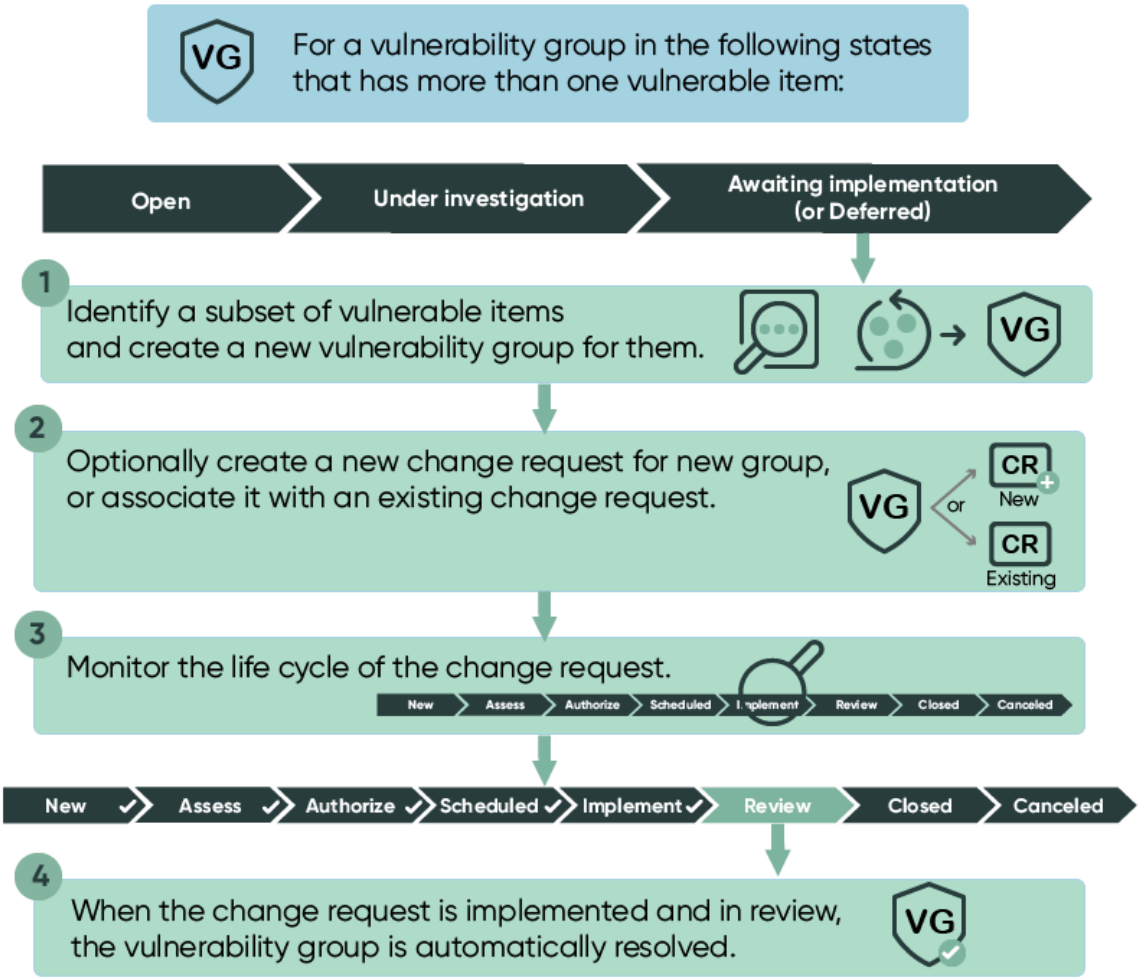
When you specify the conditions for the vulnerable items that you want to move to a new remediation task with the condition builder, only the active VIs that match your criteria are moved to the new group.

You are not required to create change requests (CHG) when you split a VUL. You have the option to split a VUL at the same time you create a change request, or, you can split a VUL without creating a change request. The following image illustrates the basic flow for splitting a vulnerability group. The detailed steps for this flow follow the image.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The remediation task record is referred to as a VUL in the following sections. In previous versions of Vulnerability Response, remediation tasks were called, vulnerability groups (VG). In the following images, VG= remediation task, or a VUL record.

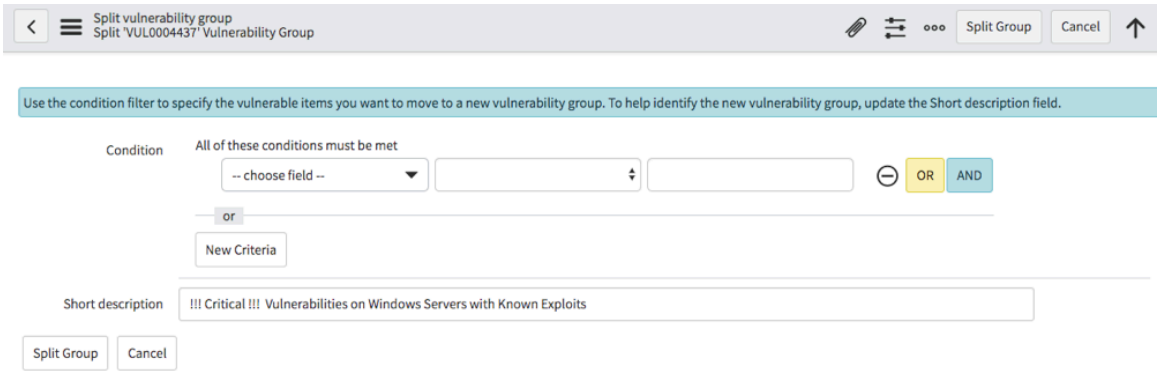
Workflow for splitting a remediation task



Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**.
   The remediation tasks list is displayed.
2. In the Number column, click a record to open it.
   The record is displayed.
3. On the upper right of the VUL, click **Split Task**.
   The Split remediation task form is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

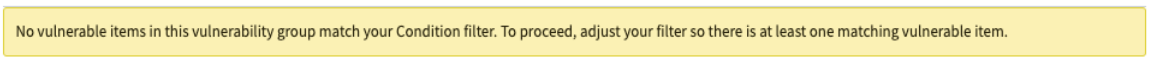


4. With the condition filter displayed, specify the conditions for the vulnerable items that you want to move to a new task.
   For example, you may prefer to filter out only vulnerable items that match the following conditions:
   - In Open states.
   - Risk scores greater than 80.
   - Configuration items that contain 'WINSV'.
   - Located in San Diego.

   As an example, for conditions, you might enter:
   - State - is - Open
   - Risk score - is greater than or is - 80
   - Configuration item . Name - contains - WINSV
   - Configuration item . Location - is - San Diego

   If vulnerable items match your filter after you enter the conditions, a message is displayed with the number vulnerable items that match.

   Note: If a message is displayed that no vulnerable items match your filter, adjust the conditions so at least one vulnerable item matches your filter criteria.

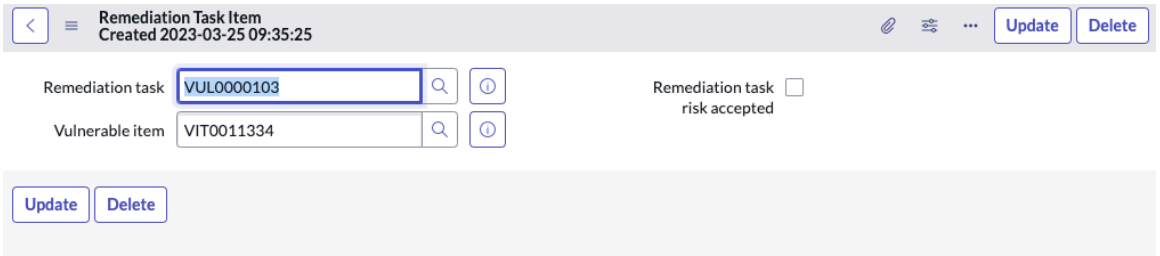
5. **Optional:** Adjust the filter as required.
6. **Optional:** To help you identify the new VUL after it is created, you may prefer to update the Short description field.
   If edited, use the short description field as search criteria for the new VUL to help you locate it after it is created, for example,LOCATED IN SAN DIEGO.
7. **Optional:** To preview details about the vulnerable items that match your filter criteria, follow these steps before you click **Split Task** to create the new VUL.
   These details include existing change requests that are already associated with this subset and VULs with these vulnerable items. Viewing this information on the preview may prevent you from creating duplicate VULs.

   a. In the blue confirmation message on the Split remediation task form, click **Preview matching items**.
   The Remediation Task Item list is displayed in a new window in your browser with a list of vulnerable items that match your conditions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. In the Number column, click an item to open the record.

c. In the record that is displayed, to the right of the vulnerability group or the vulnerability item fields, click the information icon for the Vulnerable item to view the records.



d. On the dialog that is displayed, click **Open Record**.
Information about the remediation target date is displayed. In the Related Lists section, click a related list to view more information about the VI.

8. When you are ready to create the new VUL with the VI(s) that meet your conditions, close the preview window to return to the split task form in the other window and, at the top of the form, click **Split Task**.

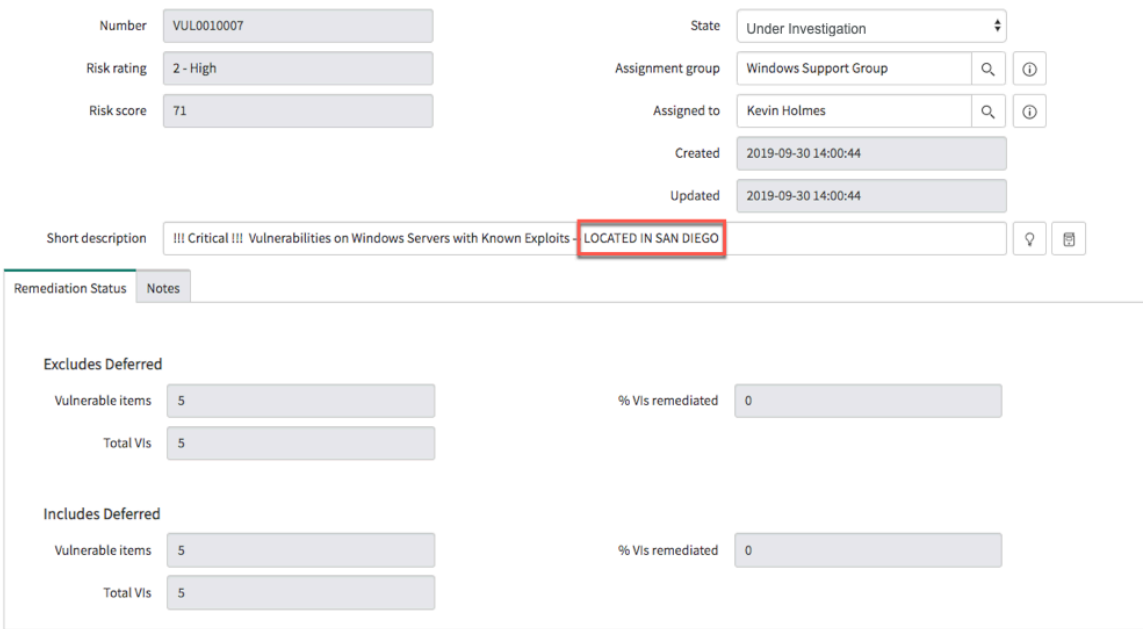
Note:

For under 200 VIs, the split operation is done synchronously.

For over 200 VIs, the split operation is done asynchronously in the background, and it may take a few seconds for the VIs to appear in the new group.

A confirmation message is displayed that shows all the active VIs that are moved to the new group. The new remediation task number is also displayed. If not already in Under Investigation, the VUL is moved to Under Investigation. Check the Short description field for the text you entered for the new VUL in the (`LOCATED IN SAN DIEGO`).

Roll-up calculations on the new group are performed to calculate its new Risk Score, Remediation Target Date, and other field values.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The vulnerable items, preferred solutions, and change requests are displayed on the Related Lists on the bottom of the record. Process and monitor this new task as you would with any remediation task.

9. **Optional:** Scroll to the **Notes** related list and click to select it.
   Confirm that the number of vulnerable items from the original remediation task have been moved to the new group in the activity stream.
10. **Optional:** On the new VUL, to select and split the VIs from the Vulnerable items related list once again, scroll to the bottom of the vulnerability group record, and, with the VIs you want to move selected in the Vulnerable item column of the Vulnerable Items related list, from the Actions on selected rows choice list, select **Split Task**.
    The Split remediation task form is displayed.
11. To split the group again and move the selected items to a new group, click **Split Task**.
    The selected VIs are moved to another remediation task, the confirmation message is displayed, and the new group is displayed.
12. Choose one to continue your investigation or remediation.

Option	Description
Create Security Incident	Create a security incident.
Create Change	Create a change request for this remediation task.
Split Task	If the new group has more than one VI, split this remediation task again to create another subset of vulnerable items.
Awaiting Implementation	If displayed, move the task from Under Investi gation to the Awaiting Implementation state.
Close or Request Exception	Close or defer the remediation task. A confir mation dialog is displayed with the following required fields: ○ State ○ Reason ○ Additional information Fill in the fields to close or defer the group and click **Submit**.
Delete	Delete this remediation task.
State	Move the record to another state displayed in the choice list and click **Update** to save your changes to the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Note: You can manually move the new VUL through the states of its life cycle. However, if state synchronization is en abled, and the system registers that a change request associated with the VUL has changed its state, or you add a CHG or remove it from the VUL, state synchro nization potentially can override your manual intervention. For more information, see State synchroniza tion between change requests and remedia tion tasks.
Assignment group	Reassign the VUL to an assignment group and click **Update** to save your changes to the record.
Assigned to	Assign the VUL to yourself or to a specific user in another assignment group and click **Update** to save your changes to the record.

What to do next

Monitor the state of the new VUL to expedite its resolution.

State synchronization between change requests and remediation tasks

There is a synchronized relationship between the State fields of remediation tasks (VULs) and the State fields of change requests (CHG) in the Vulnerability Response product. As a change request moves through its life cycle, it also moves the state of any related remediation tasks automatically.

Overview

The remediation task record is referred to as a VUL in the following sections. In previous versions of Vulnerability Response, remediation tasks were called, vulnerability groups (VG). In the following images, VG= remediation task, or a VUL record.

State synchronization is enabled by a system property (sn_vul.cr_state_synch) by default in your instance when you download the Vulnerability Response application.

When state synchronization is enabled, the CHG State field changes the remediation task State field automatically in the following cases:

- When a new CHG is created for a remediation task (VUL), if it is not in `Awaiting Implementation`, the VUL state moves forward to `Awaiting Implementation`.
- When an existing CHG is associated to a VUL, if it is not in `Awaiting Implementation`, the VUL state moves forward to `Awaiting Implementation`.
- After the tasks on a CHG are completed (`Implemented`), and the CHG is moved to the `Review` state, the VUL moves forward to `Resolved`.

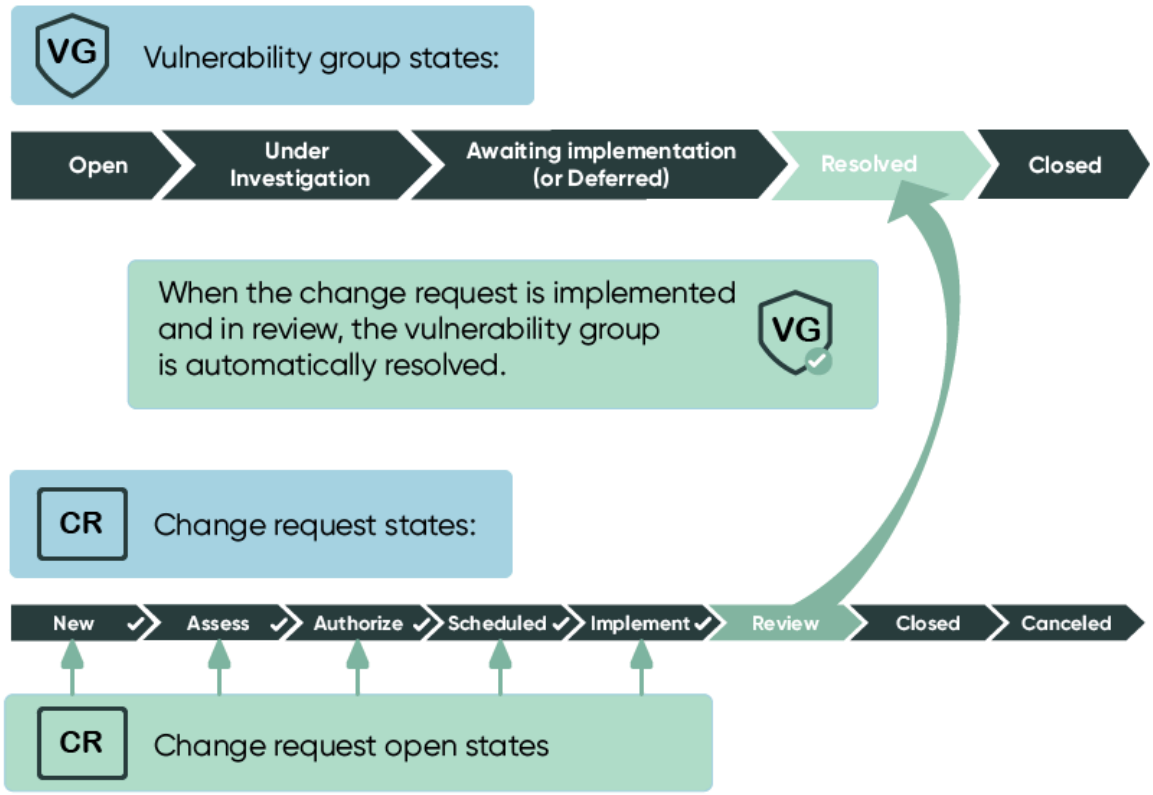
For more information and examples of state synchronization, see the following sections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can still manually move CHGs and VULs through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a VUL, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the VUL from the `Closed` or `Deferred` states.

Forward state synchronization

The following image illustrates how CHG states automatically move VUL states in a forward life cycle, that is, from `Open` to `Resolved`.



You can create new change requests for any remediation task in a state other than `Closed`. State synchronization automatically moves the VUL bi-directionally through the `Open`, `Under Investigation`, `Awaiting Implementation`, and `Resolved` states. This movement is based on certain values of the state field on the change request. State synchronization between the change request and the remediation task is invoked automatically unless the check box (`Add CIs to CR`) is displayed on a form and you choose to clear the check box.

The VUL does not move forward to `Resolved` when a CHG is in its open states. Any CHG in states prior to `Review` in its life cycle such as, New, `Assess`, `Authorize`, `Scheduled` or `Implement` as shown in the preceding figure are considered open states for the CHG. Open states do not move the state field on the VUL, because investigations or tasks on the CHG are not completed. State synchronization is invoked when a CHG is created for, or associated to, the VUL, or the state of an existing relationship changes on the CHG. The completed CHG states are `Review` and successfully `Closed`. When a CHG is closed successfully, its closed codes are: `Successful`, or `Successful with issues`, in which case the VUL moves forward to `Resolved`.

Backward state synchronization

As a CHG is processed during its life cycle, it may be canceled at some point. In this case, if the CHG is `Cancelled`, or `Closed` (with a close code of `Unsuccessful`), the VUL automatically

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

moves back to Under Investigation. The VUL moves back to Under Investigation, because there is no active plan to remediate the vulnerability.

If a VUL is in a Resolved state, and you create a new CHG or associate it to an existing CHG in one of the initial open states, the VUL automatically transitions back to Awaiting Implementation. The VUL moves back to this state, because more work is now assigned to the CHG.

VULs with more than one CHG

If a VUL in Awaiting Implementation has more than one CHG associated with it, state synchronization is based on the status of the CHG in the earliest state of its life cycle. For example, a VUL has four CHGs associated with it, CHG1, CHG2, CHG3, and CHG4 as shown in the following table.

CHG number	CHG state
1	Implement
2	Canceled
3	Closed (close code of Unsuccessful)
4	Closed (close code Successful)

State synchronization between the CHG and the VUL in this case is based on CHG1, which is in the earliest state of the four CHGs, (Implement). In this case, the VUL remains in Awaiting Implementation.

In another example, if a VUL is in the Resolved state and has an existing CHG that has been implemented and is in the Review state, and a new CHG is created, the VUL moves back from Resolved to Awaiting Implementation. State synchronization is based on the CHG in the New state, which is the CHG in the earliest state.

CHG number	CHG state
1	Review
2	New

Additionally, when VULs have more than one CHG, the state of the VUL transitions automatically in the following cases:

- When a CHG moves forward to Review, if all other CHGs associated with the VUL are in Review or Closed states (with a successful close code), the VUL automatically transitions to Resolved. Any other related CHGs that are canceled or closed unsuccessfully are ignored.
- When a CHG moves to Cancelled or Closed (close code of Unsuccessful), if all other CHGs associated with the VUL are in the same state, then the VUL automatically transitions back to Under Investigation.

For more information about remediation task states and what you can do in each state, see Vulnerability Response remediation task and vulnerable item states.

Assess your exposure to vulnerable software

You can provide the publisher and product information in the Exposure Assessment module to assess your zero-day (current day) exposure of your assets to vulnerable software using the ITSM Software Asset Management (SAM) Foundation application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: You can perform the exposure assessment by software and Common Vulnerabilities and Exposures (CVE) to leverage the additional capabilities in the Vulnerability Assessment Workspace. For more information, see Explore the Vulnerability Assessment workspace.

Before you begin

Role required: vulnerability admin (sn_vulnerability_write)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Have the following information available about the vulnerable software that you want to assess:

- Publisher
- Version
- Product
- Edition

About this task

For more information on system requirements, see Configure the Vulnerability Exposure Assessment.

View the software exposure assessment module and create and edit exposure assessment records on-demand for vulnerable software in your ServiceNow AI Platform® instance.

You manage the vulnerability response activities for a large operation responsible for many assets. The Security Operations Center (SOC) in your operation contacts you about a version of software that they've learned is vulnerable. You discover that a scan of your assets was recently completed and didn't find this vulnerability. The SOC team learned about this vulnerability from a reliable source outside of the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or the other third-party libraries in your instance, and you're concerned that your vulnerability scanner hasn't yet added the plugin for it.

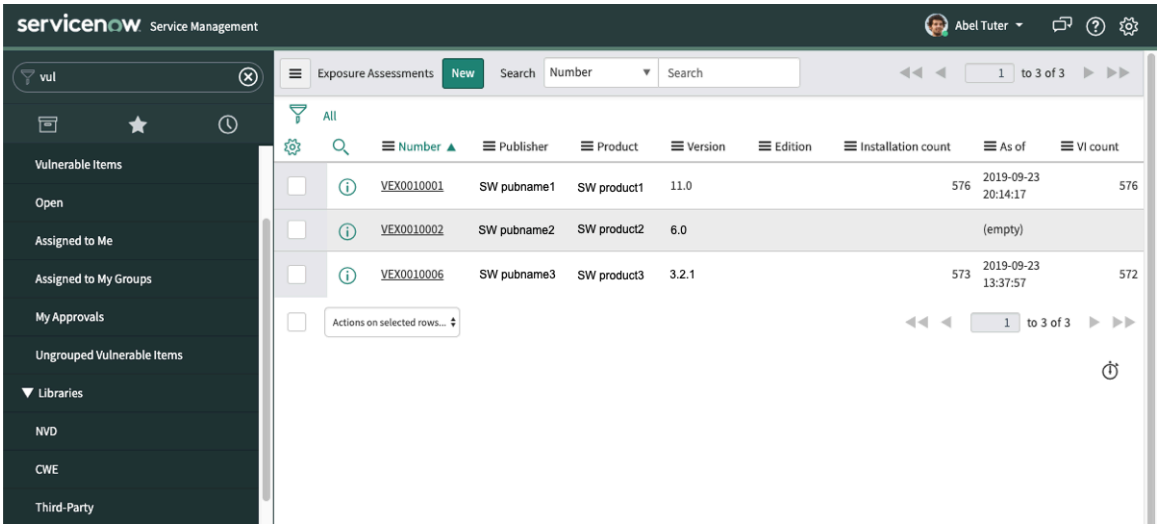
You are confident that the data for this vulnerability will be updated in the NVD and imported soon so that your scanner can catch this vulnerability in the next scan, but because you are concerned about the scope of your potential exposure, you want to determine today if you have assets in your network that have this software installed.

Starting with v23.0 of Vulnerability Response, if you have the Pro or Enterprise subscription, you are redirected to the **Exposure Assessment** page in the Workspaces based on your role on selecting the **Exposure Assessment** link in the **All** menu. For more information, see Configure the Vulnerability Exposure Assessment.

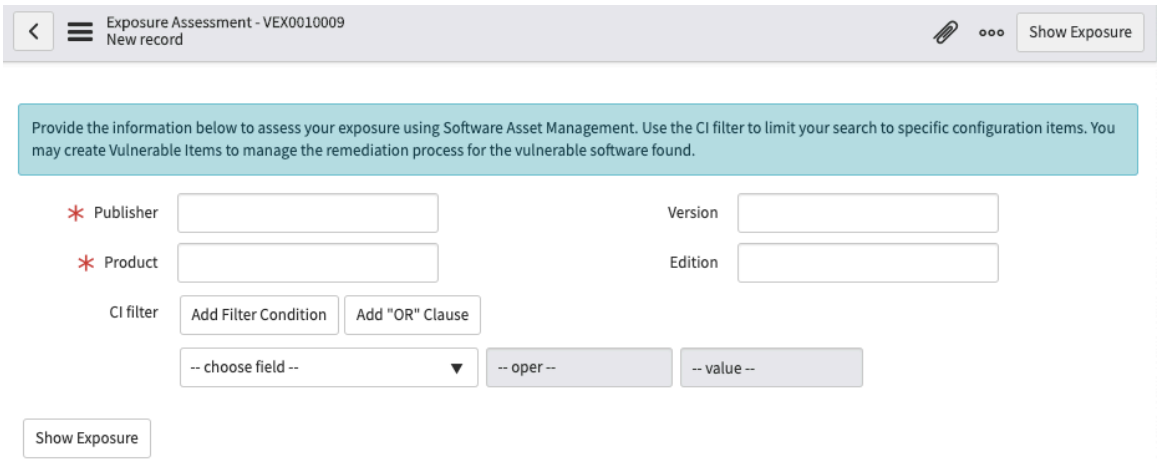
Procedure

1. To create a new exposure assessment, navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Exposure Assessment**.
   The Exposure Assessments list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Select **New**.
   The Exposure Assessment form is displayed.

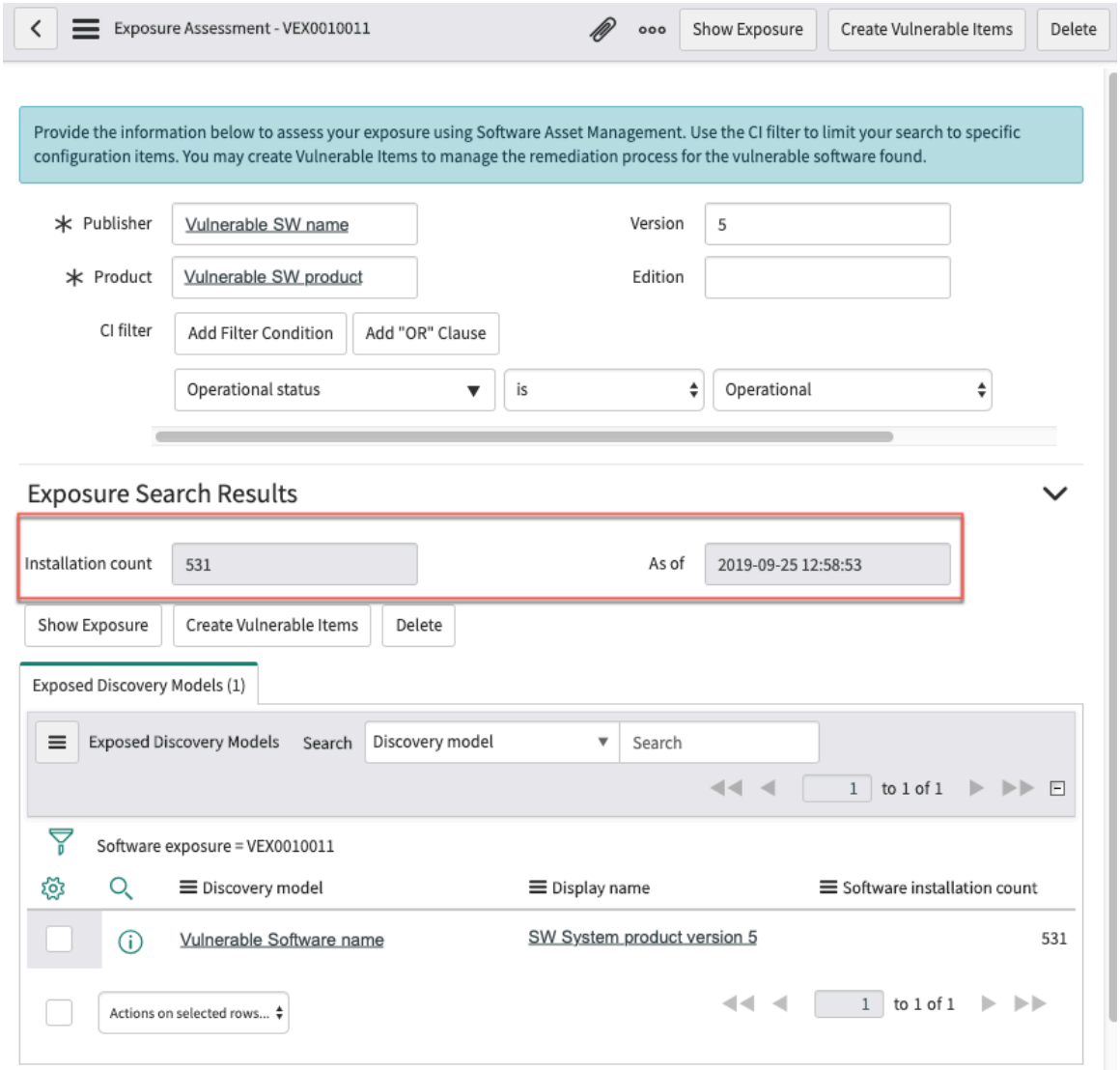


3. Fill out the form.

Field	Description
Publisher	Name of the software publisher.
(Optional) Version	Enter the version number to help you narrow the search on your assets.
Product	Name of the software product.
(Optional) Edition	Enter the edition to help you narrow the search on your assets.
CI filter	Use the choice lists for the Configuration Item (CI) filter to limit your search to specific configuration items (assets). For example, you can submit a query for only active assets that may have this software installed: `Operational status is Operational`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **Show Exposure**.
   The Exposure Assessment record with your discovery model and the software installation count on your assets as of the specific date is displayed.



5. Choose one to continue.

Option	Description
Show Exposure	Add additional CI filter conditions and select **Show Exposure** to further refine your search results.
Create Vulnerable Items	Create vulnerable items for the configuration items from your search results. If vulnerable items are successfully created, a remediation task is created for all the vulnerable items and displayed on the exposure assessment record.
Delete	Delete this record and return to the Exposure Assessments list. A confirmation dialog is dis played.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. **Optional:** Create a vulnerable item for your search result.

   Note: After you create vulnerable items, you cannot alter the search criteria for this exposure record.

7. Alternatively, revise your filter conditions and further refine your search results.
8. To create vulnerable items, follow these steps:

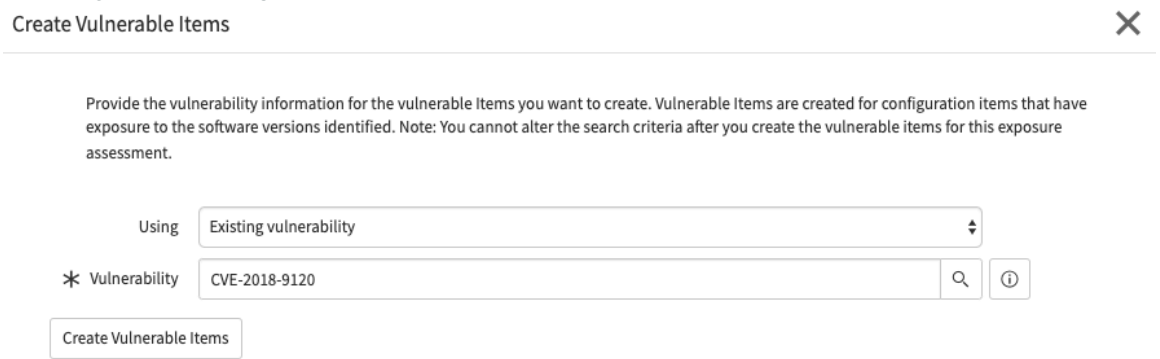
   a. Select **Create Vulnerable Items**.
   The Create Vulnerable Items dialog is displayed.

   b. Fill in the fields.

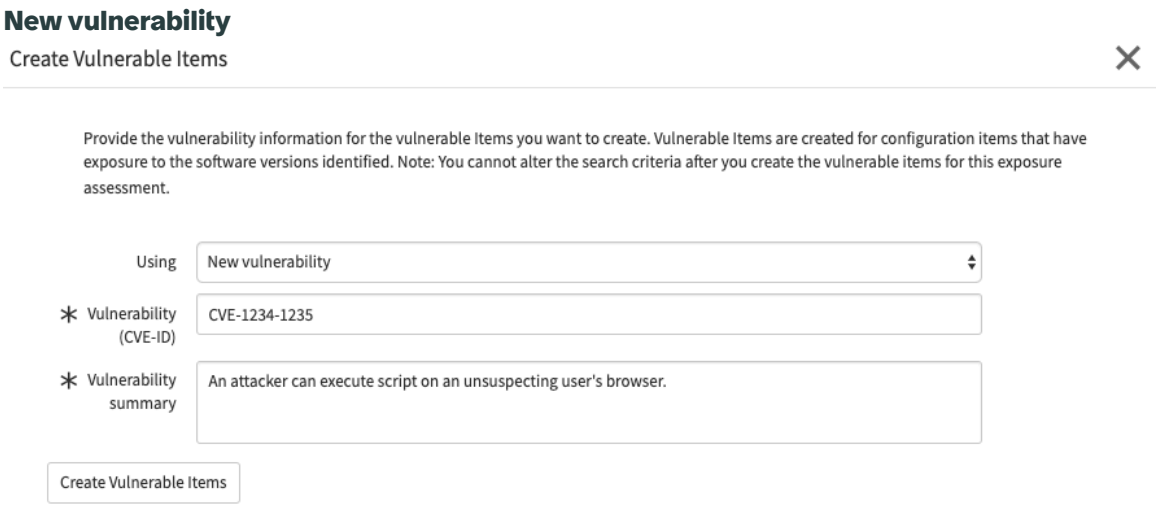
Field	Description
Using	Form the choice list, choose one to continue. ▪ **Existing vulnerability**. To the right of the Vulnerability field, click the search icon. In the list that is displayed, select the CVE-ID, or enter search criteria to locate the existing CVE-ID, for example, CVE 2018-9120. **Note:** This can be a CVE-ID from a vulnerability database other than the NVD. ▪ **New vulnerability**. Enter the CVE-ID for your new vulnerability in xxxx-xxxx, xxxx-xxxxx, or xxxx-xxxxxxx format.
Vulnerability summary (for new vulnerability only)	Enter a summary for the new vulnerability, for example, `An attacker can execute script on an unsuspecting user's browser`.

The following images show examples of the completed form for an existing vulnerability and a new vulnerability.

Existing vulnerability



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

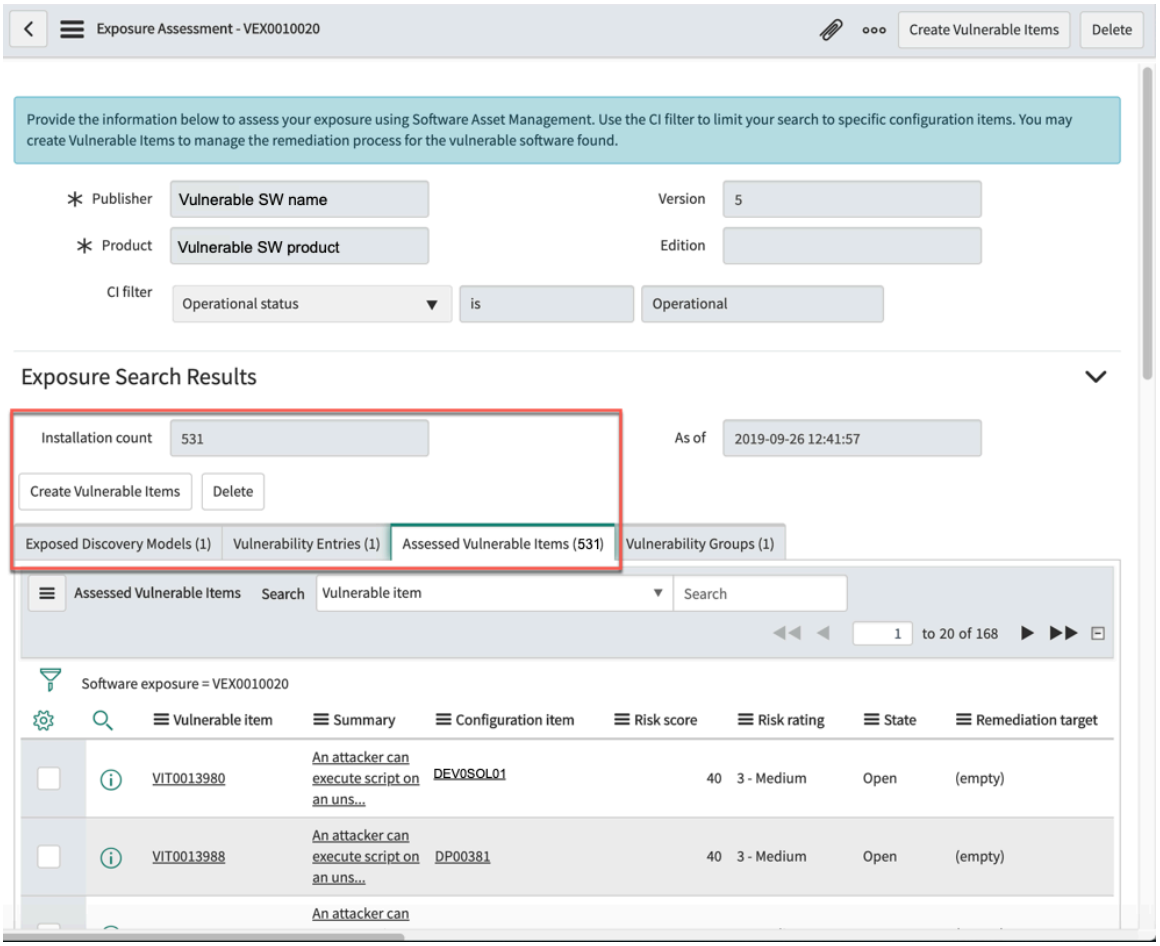


c. Select **Create Vulnerable items**.
The Exposure Assessment record is displayed with a status message which indicates that vulnerable items are being created.

d. After a few seconds, at the top of the form, right-click in the gray banner to reload the page.
The new vulnerable items are displayed as shown in the following figure on the Assessed Vulnerable Items tab (531). The new remediation task created for these vulnerable items is displayed on the remediation task tab (1).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

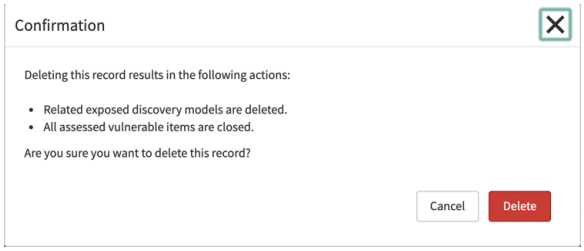
Note: For this example, a remediation task is created according to the group rules and conditions from the remediation task rule called, Vulnerability. This group rule is the default remediation task rule that is installed with the Vulnerability Response product in your ServiceNow AI Platform® instance. In this example, the conditions of this group rule placed all the vulnerable items into a single remediation task. If you prefer to create more than one remediation task for the vulnerable items that match your exposure assessment search results, you may prefer to set up additional remediation task rules. Creating more remediation tasks may help you prevent creating remediation tasks with large numbers of vulnerable items. For more information about remediation task rules, see Vulnerability Response remediation tasks and remediation task rules overview and Create or edit Vulnerability Response remediation task rules.



9. Choose one to continue.

Option	Description
Remediation tasks	With the Remediation Tasks tab selected, in the number column, click to open the record and review and assign the task for remediation. For more information on assignment groups, see Creating groups.
Assessed Vulnerability Items	With the Assessed Vulnerable Items tab selected, in the Vulnerable item column, click to open the records and review and assign individual vulnerable items.
Delete	Delete the exposure assessment record. A confirmation dialog is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Note: If you delete the exposure record after you create vulnerability items, any vulnerable items that you create for this record that aren't related to another exposure record are automatically moved to the `Closed` state. The reason for closure is `Cancelled`.
	

What to do next

Respond to any zero-day (current day) threats based on your exposure assessment. For more information about remediation tasks and change management for Vulnerability Response, see Vulnerability Response remediation tasks and remediation task rules overview and Change management for Vulnerability Response.

Viewing assignment recommendations

An assignment group is usually allocated to a vulnerable item by using assignment rules. These rules are configured by the vulnerability administrator to allocate the correct assignment groups that are based on the data received from third-party scanners.

For more information, see Vulnerability Response assignment rules overview. If a matching assignment group is not available or is incorrect, you can use Vulnerability Assignment Recommendations to view alternative assignment groups.

Use Vulnerability Assignment Recommendations to do the following actions:

- Request assignment group recommendations for a vulnerable item.
- Request assignment group recommendations for multiple vulnerable items.
- Request assignment group recommendations for a remediation task.

Request assignment group recommendations for a vulnerable item

Request Vulnerability Assignment Recommendations so that you can view assignment group recommendations. You can request recommendations if a matching assignment group is not available or is incorrect for a vulnerable item (VI).

Before you begin

Role required: sn_vul.remediation_owner

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items** and open a VI.
   The item must be in the Open, Deferred, Under investigation, or Awaiting implementation state.
2. Click the recommend icon ( ) next to the **Assignment group** field for assignment suggestions for that VI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. From the Assignment Group Recommendations dialog box, select a recommendation that is based on the confidence score.
   The confidence score predicts how relevant the match is for the VI. For more information, see Machine Learning solutions for Vulnerability Response.
4. Click **Assign**.

Result

The selected group appears in the **Assignment group** field and the Assignment type changes to Recommendation.

Request assignment group recommendations for multiple vulnerable items

Use Vulnerability Assignment Recommendations to view the assignment group recommendations for multiple vulnerable items (VIs) using a bulk edit. When multiple VIs are selected, a prediction is performed on a random sample of the selected VIs.

Before you begin

Role required: sn_vul.remediation_owner

About this task

The recommendations and their confidence scores may differ slightly between invocations, based on the samples taken from the selected VIs. The confidence score evaluates whether the system is confident that the recommended assignment group is suited to resolve the vulnerability. Use the `assignment_recommendation_batchsize` system property to set the batch size when you request Vulnerability Assignment Recommendations for remediation tasks (VULs) and VIs using the bulk edit option. The default value of this system property is set for optimum prediction performance.

Note: If you increase the default value, the response time for Vulnerability Assignment Recommendations for these cases might change.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Item** and select multiple VIs.
   The items must be in the Open, Under investigation, or Awaiting implementation state.
2. Click **Bulk Edit**.
3. On the form, fill in the fields.

Bulk Vulnerable Items form

Field	Description
Record selection	Records to be selected for bulk edit.
Assignment group	Assignment group to set for the selected vulnerable items. To view the recommended assignment groups, click the recommend icon ( ) next to the field. Select a recommendation that is based on the confidence score and click **Assign**.
Work notes	Notes to be added.

4. Click **OK**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The selected group appears in the **Assignment group** field and the Assignment type changes to Recommendation for all the selected VIs.

Request assignment group recommendations for a remediation task

Use Vulnerability Assignment Recommendations to view assignment group recommendations for a remediation task (VUL).

Before you begin
Role required: sn_vul.remediation_owner

About this task
Use the `assignment_recommendation_batchsize` system property to set the batch size when you request Vulnerability Assignment Recommendations for VULs and vulnerable items (VIs) using the bulk edit option. The default value of this system property is set for optimum prediction performance.

Note: If you increase the default value, the response time for Vulnerability Assignment Recommendations for these cases might change.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks** and select a VUL.
   The group must be in the Open, Under investigation, or Awaiting implementation state.
2. Click the recommend icon ( ) next to the **Assignment group** field for the assignment group recommendations for the selected VUL.
   The Assignment Group Recommendations dialog box displays the recommended assignment groups with the average confidence score for all the VIs in that group.
3. Select a recommendation from the Assignment group list based on the confidence score.
   The confidence score predicts how relevant the match is for the selected VUL.
4. Click **Assign**.
   The selected group appears in the **Assignment group** field.
5. Save the remediation task with the updated information.

Result
All the VIs with the same assignment group as the VUL are assigned to the selected assignment group. The Assignment type changes to Recommendation for the VUL, as well as all the modified VIs.

Requesting and approving an exception

You can request to defer the remediation of a vulnerable item or remediation task for a specified period. For example, as a remediation owner, you can request an exception if a patch is not available for a machine. Approvers who have access can approve requests from other users.

You can request exceptions from the Vulnerability Response Workspaces. See Request an exception in the IT Remediation Workspace.

- Request an exception for a vulnerable item
- Request an exception for a remediation task
- Request a bulk exception

You can also request policy exceptions using GRC: Policy and Compliance Management:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Request an exception using GRC: Policy and Compliance Management
- Request a bulk exception using GRC: Policy and Compliance Management

Note:

Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested.

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Request an exception for a vulnerable item

Request an exception for a vulnerable item (VI) that can't be remediated immediately. For example, as a remediation owner, you can request an exception if a patch isn't available for a machine.

Before you begin

Role required: sn_vul.remediation_owner

About this task

Important: You can request exceptions from the Vulnerability Manager and IT Remediation Workspaces. For more information, see Request exceptions for remediation tasks and records from the Vulnerability Manager Workspace and Request an exception in the IT Remediation Workspace.

You can also request exceptions for VIs in the classic environment.

Note:

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **Vulnerability Response** > **Vulnerable Items** > **All**.
2. Select the item that you want to request an exception for.
   The selected item must be in Open, Under Investigation, or Awaiting Implementation state.
3. On the Vulnerable Item form, click **Request Exception**.
4. If Vulnerability Response is selected in the Exception Management screen, fill in the fields in the Request Exception form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the duration selected in the **All** > **Vulnerability Response** > **Administration** > **Exception Management** screen. When the exception request expires, the group reverts to the Open state. **Note:** Starting with version 18.0 of Vulnerability Response (VR), if a vulnerable item was deferred for remediation by using the exception management feature, then in case it is reopened by the scanner, the deferral date set on the vulnerability will still persist. To enable this functionality, set the value of the system property *sn_vul.auto_defer_vit_in_active_exceptio* to true. Also, the deferred **Until** date persists even after the vulnerable item gets closed or the exception expires. The role required is sn_vul.manage_exception_configuration for both read and write.
Reason	Reason for the request. Choices are: ○ Risk Accepted ○ Awaiting Maintenance Window ○ Fix Unavailable ○ Mitigating Control in Place ○ Other To see how to add new reason choices, see Define policy reason mapping.
Additional information	Details that are related to the reason why this request is being made. This required field is to be updated by the remediation owner.

5. Submit the exception request by clicking **Request Approval**.

Result

The state of the vulnerable item changes to In Review. Use the **State Change Approval** tab to track the status of the exception request.

Request an exception for a remediation task

Request an exception to defer a remediation task for a specified period if it can't be resolved immediately.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Important:

You can request the exceptions from the Vulnerability Manager and IT Remediation Workspaces. See Request an exception in the IT Remediation Workspace.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.remediation_owner

You can also request exceptions for remediation tasks in the classic environment.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation tasks** > **All**.
2. Select the group that you want to request an exception for.
   The selected task must be in the Open, Under Investigation, or Awaiting Implementation state.
3. On the remediation task record (VUL), select **Request Exception**.
4. On the form, fill in the fields.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the exception duration that is defined in the configuration.
Reason	Justification for requesting an exception.
Additional information	Details that are related to the reason why this request is being made. This field is to be updated by the remediation owner.

5. Click **Request Approval**.

Request a bulk exception

Use the bulk edit option to request an exception for multiple vulnerable items (VITs) instead of manually selecting each item.

Before you begin

Role required: sn_vul.vulnerability_analyst

About this task

When multiple VITs are selected, a remediation task (VUL) is formed with these items. See Edit vulnerable items in bulk in Vulnerability Response for more information on editing multiple VITs.

Important: You can request an exception for:

- a VIT from the Vulnerability Manager Workspace and IT Remediation Workspace. For more information, see Request an exception in the IT Remediation Workspace.
- multiple VITs from the Vulnerability Manager Workspace. For more information, see Request bulk exception in the Vulnerability Manager Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Vulnerability Response** > **Vulnerable Items** > **All** and select the items that you want to request an exception for.
   The selected items must be in the Open, Under Investigation, or Awaiting Implementation state.
2. Click **Bulk Edit**.
3. On the form, fill in the fields.

Vulnerable Item Bulk Edit form

Field	Description
Record selection	Records that you selected for a bulk edit.
State	State of the vulnerable item. Select the Deferred state to request an exception for the selected items.
Reason	Substate for the State that you selected.
Short description	Name of the remediation task that you are creating.
Until	Ending date that you specify for your exception request.
Additional information	Further details that you want to mention to inform the approver about the reasons for your request.
Preferred solution	Solution that is targeted for remediating all the vulnerable items that you selected for a bulk edit.
Assignment group	Assignment group for the VI. You can select a group manually or use Assignment Recommendations if that feature is enabled.
Work notes	Notes to be added.

4. Click **OK**.
   A remediation task is created containing the VIs that you selected. This remediation task is submitted for approval.

Request an exception using GRC: Policy and Compliance Management

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Vulnerability Response.

Before you begin

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Role required: sn_vul.remediation_owner

You can also request exceptions in the classic UI:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.
2. On the selected form, click **Request Exception**.
3. On the form, fill in the fields.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you are requesting an exception for.
Control objective	Control objectives that are associated with the policy you selected. If a policy is not selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date cannot be in the past.
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid cannot exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.

4. Click **Submit**.
   For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

Request a bulk exception using GRC: Policy and Compliance Management

Select a group of vulnerable items and submit a bulk exception.

Before you begin

Before you can use the Policy Exception Integration to request bulk exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Note: To use this feature, you must upgrade GRC: Policy and Compliance Management before upgrading Vulnerability Response. If you have already upgraded Vulnerability Response before GRC: Policy and Compliance Management, and want to use this feature, you must perform the upgrade procedures again in the correct order.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.remediation_owner

You can also request exceptions in the classic environment in Vulnerability Response.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable Items** > **All** and select the items that you want to request an exception for.
   The selected items must be in Open, Under investigation, or Awaiting implementation state.
2. Click **Bulk Edit**.
3. On the form, fill in the fields.

Vulnerable Item Bulk Edit form

Field	Description
Record selection	Records that you selected for a bulk edit.
State	State of the vulnerable item. Select the Deferred state to request an exception for the selected items.
Short description	Name of the task that you are creating.
Preferred solution	Solution that you are targeting for remediating all the vulnerable items that you selected for bulk edit.
Assignment group	Assignment group for the VI. You can select a group manually or use Assignment Recommendations if that feature is enabled.
Work notes	Notes to be added.

4. Click **OK**.
   A remediation task is created with the selected vulnerable items.
5. On the form, fill in the fields.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you are requesting an exception for.
Control objective	Control objectives that are associated with the policy that you selected. If a policy is not selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date cannot be in the past.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid cannot exceed the **Maximum exception duration (days)** that you set for the policy in GRC: Policy and Compliance Management. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.

6. Click **Submit**.
   For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

Approve or reject an exception request in Vulnerability Response

Approve or reject the exception requests for vulnerable items or remediation tasks that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

Important:

You can approve or reject the exception requests in the Vulnerability Manager Workspace.

Before you begin

Role required: sn_vul.exception_approver
You can also approve exception requests in the classic environment.

Note:

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Working with an exception rule

You can request an exception for vulnerabilities, vulnerable items (VIs), or configuration items (CIs) that can't be remediated or deferred immediately. By automating the VI deferral process, you can defer the matching VIs based on the rule when the system identifies them.

You can perform the following tasks for an exception rule:

- Create an exception rule
- Approve an exception rule request
- Activating an exception rule
- Reopen an exception rule
- Update an approved exception rule
- Delete an exception rule

Note:

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Create an exception rule

Create a rule to automatically request an exception for a specific condition for a group of vulnerable items (VIs), such as a rule with a condition that is based on the vulnerability severity of these VIs. With this rule, you can defer new and existing VIs automatically if they match the approved rule condition.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

The rule is applied from the "Valid from" until the "Valid to" date. The remediation task (VUL) is created when the rule is approved. The grouping method for this VUL is known as exception rules. The VUL is created in the Deferred state. You can't close, reopen, or delete this VUL. New and reopened VIs are deferred and added to this VUL from the "Valid from" date until the group expires on the "Valid to" date.

Note:

Email notifications are sent at every stage of the exception rule work flow. These emails provide the status and other details of a request. For example, when an exception rule is requested, the requester receives an email that confirms that the request is submitted.

Note: If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Rules**.
2. On the Exception Rule new record page, click **New** to create a rule.
3. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception Rule form

Field	Description
Name	Name of the exception rule.
Valid from	Date from which this rule is active to defer the VIs.
Valid to	Date from which the remediation task stops accepting new VIs.
Reason	Reason to create this exception rule.
Assignment group	Group that the remediation task that was created for tracking the deferred VIs is assigned to.
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.
Condition	Filter condition for the VIs that can be defined while processing the VIs.
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run.
Workflow stage	Current approval status of the exception rule.
State	State of the exception rule.
Execution order	Unique order for each exception rule.
Deferred until	Date until when the VULs and VIs are deferred. On this date, the created VUL is closed, all the VIs move out of the group, and group rules are reapplied.

4. Add the assignment group when you are creating the rule.
5. Submit the form for approval.
   The status of the request changes to In review. Until you submit the exception rule, it remains in the Draft state.

Approve an exception rule request

Assess exception rule requests from users so that you can approve or reject these requests.

Before you begin

Role required: sn_vul.exception_approver

About this task

Exception approver level 1 user group members can approve the level 1 exception rule requests. Similarly, exception approver level 2 user group members can approve the level 2 exception rule requests. Both the user groups inherit the exception approver role by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with and explain why you approved or rejected the request. After an exception rule is approved, a remediation task (RT) is created in the Deferred state by default. Starting from the "Valid from" date, this rule runs on all the VIs that are created and also on the ones that are moved from the Closed to the Open state. VIs that match the defined conditions are added to the RT and deferred for the specified period.

Note: If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

Activating an exception rule

A rule is activated on its "Valid from" date. After activation, it automates the exception process for vulnerable items (VIs).

The exception rule follows this life cycle:

1. The new vulnerable items (VIs) that you create or reopen, and that meet the specified condition, are deferred. If you enable the Execute on existing data option when you run the exception rule for the first time, all the active and non-deferred VIs that match the exception rule condition are moved to the newly created remediation task (RT) and its state is changed to Deferred.
2. If a newly created VI matches the exception rule condition, it is moved to the deferred RT that is associated with the rule and the group rule is not run on it.
3. On the "Valid from" date, existing VIs are added if you enable the Execute on existing data option.
4. The RT stops accepting new VIs when the rule expires on the "Valid to" date. The RT remains in existence until the "Deferred until" date.
5. The exception rule expires on the "Valid to" date.

Request an extension for an exception rule

Request an extension for a deferred exception rule before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.exception_approver

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Exception Rules**.
2. Select an approved exception rule.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the exception rule must be extended.
Reason	Enter the reason for deferring the exception rule. Choices include: ○ Risk accepted ○ Awaiting maintenance window ○ Fix unavailable ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the Deferred until, Reason and Additional information fields get updated on the exception rule and the associated remediation tasks and vulnerable items. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred exception rule is extended again, the extend deferral count increases in the backend.
- Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Reopen an exception rule

Reopen an exception rule that has been rejected, but you want to resubmit. Reopening the rule moves it to the Draft state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
You can then update and resubmit the rule for approval.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Rules**.
2. Find the rule that you want to reopen and click **Reopen**.
3. Update the form and resubmit it for approval.

Update an approved exception rule

Cancel an approved rule to be able to update it. For example, before you can modify any dates or add a condition to an approved rule, you must cancel it so that the remediation task (VUL) is deleted, and the vulnerable items (VIs) move to the Open state.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Group rules are reapplied to these VIs. Submit the rule after making the changes so that it goes through the approval process once again.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Rules**.
2. Open the exception rule that you want to cancel and click **Cancel**.
3. In the Cancel Rule dialog box, click **Cancel rule**.
   The rule moves back to the Draft state and the associated VUL is deleted. The related VIs are reopened, and group rules are applied to the individual VIs.

Delete an exception rule

Delete an exception rule that is not required anymore. For example, you can delete a rule if you don't want to defer a vulnerable item (VI) during ingestion.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Deleting a rule cancels the associated remediation task (VUL). The related VIs are reopened, and group rules are applied to the individual VIs.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Exception Rules**.
2. Open the exception rule that you want to delete and click **Delete**.
3. In the Delete Rule dialog box, click **Delete rule** to delete the selected rule.
   The associated remediation task is also deleted. The related VIs are reopened, and group rules are applied to the individual VIs.

Marking and approving a false positive

Vulnerable items (VIs) and remediation tasks (VULs) can be marked as false positives. Approvers with write access can approve such requests from other users.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Mark as a false positive
- Bulk edit for false positive
- Approve or reject a false positive

Note:

Email notifications are sent at every stage of the false positive workflow, providing the status and other details of a request. For example, when a VI or remediation task is marked as a false positive, the requester receives a confirmation email. Simultaneously, the approver receives an email stating that a VI or remediation task has been marked as a false positive.

Starting from v21.0 of Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Mark as a false positive

Mark a vulnerable item (VI) or remediation task (VUL) as a false positive if the warning given by the scanner is not actually an issue. For example, if a configuration item has been decommissioned but the scanner is still raising an issue related to it, mark it as a false positive.

Before you begin

Role required: remediation owner

You can request false positives from the Vulnerability Response Workspaces. See Request a false positive in the IT Remediation Workspace.

You can also request false positives in the classic environment:

Procedure

1. Navigate to **Vulnerability Response** > **Vulnerable Items (or Remediation Tasks)** > **All**.
2. Open the VI or VUL you want to mark as a false positive and click **Mark as False Positive**.
   The VI or VUL must be in an **Open** state.
3. On the False Positive form, enter details in **Additional information** and click **Request Approval**.
   The request is sent for approval and the State of the VI or VUL changes to **In Review**.

Bulk edit for false positive

Use bulk edit to mark multiple vulnerable items (VITs) as false positive. If multiple VITs are selected, a remediation task is formed with these items.

Important: As an admin or analyst, you can use the bulk edit feature in the Vulnerability Manager Workspace to mark multiple VITs as false positive. For more information, see Bulk edit for false positive in the Vulnerability Manager Workspace.

Before you begin

Role required: remediation owner

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

You can also request false positives in the classic environment:

Procedure

1. Navigate to **Vulnerability Response** > **Vulnerable Items** > **All** and select the items you want to mark as false positive.
   The selected items must be in Open, Under investigation, or Awaiting implementation state.
2. Click **Bulk Edit**.
3. On the form, fill in the fields.

Vulnerable Item Bulk Edit form

Field	Description
Record selection	Records to be selected for bulk edit.
State	State of the vulnerable items. Select Closed to mark as false positive.
Reason	Substate for the State that was selected. If you selected Closed as the State, select False Positive here to mark as false positive.
Unassign	Submit a request to clear the Assigned to and Assignment group fields.
Preferred solution	Solution targeted for remediating all the vulnerable items selected for bulk edit.
Assignment group	Assignment group for the VI. Select manually, or using Assignment Recommendations if it is enabled.
Work notes	Notes to be added.

4. Click **OK**.
   A new remediation task is created containing the selected VIs, and this task is sent for approval.

Approve or reject a false positive

As a false positive approver, you can approve or reject false positive requests from other users.

Important:

You can approve or reject the false positive requests in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.false_positive_approver for vulnerable items
- sn_vul.app_false_positive_approver for application vulnerable items

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerabilities** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Note: A false positive can be time bound. Only the approver can set the end date.

Analytics and Reporting Solutions for Vulnerability Response

Monitoring vulnerability remediation involves viewing trends, managing risk, and monitoring assignment groups. You can review high risk issues, assignment group workloads, deferrals and, reoccurring vulnerabilities. Vulnerability Response offers tools, reports, and procedures to make that process more productive and efficient.

Data visualizations in the Vulnerability Response Workspaces

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Vulnerability analysts can also use default Vulnerability Response dashboards at **All** > **Vulnerability Response** > **Overview**.

Important:

Starting with version 19.0 of Vulnerability Response, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Vulnerability Response remediation process

Most vulnerability remediation is done from the remediation task record from within the Vulnerability Response Workspaces. From the remediation tasks (RTs) in the Under Investigation state, you can perform several tasks.

- Create change requests.
- Add work notes and descriptions of vulnerabilities within the remediation task.
- Defer the remediation task and the vulnerable items in it until a later date.
- Close the remediation task.
- Track new regulatory compliance obligations, which are usually time sensitive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Log in to your Vulnerability Response instance.
- Review your Vulnerability Management and third-party dashboards and reports to locate problem areas. For example, view dashboards that show remediation task (RT) aging by states or high risk vulnerable items (VIs) past their remediation target date.
- Review the state of remediation tasks, in order of risk.
- Revise the prioritization for the tasks by adjusting your risk score calculators if the risk score is not being calculated correctly or deferring VIs or RTs, as needed. See Vulnerability Response calculators and vulnerability calculator rules or Defer a Remediation task for more information on these options.
- Review deferred vulnerable items about to reopen and take further action as required. If you want to initiate and track change activities on your assets, remediation tasks, and their corresponding vulnerable items, for more information, see Change management for Vulnerability Responsefor further action.
- Review feedback from IT Operations.

  Once you are notified that a change request is resolved, wait for the next scan. Scans are triggered automatically by the third-party import schedule configured in the Setup Assistant.

- After a scan, if the state is Fixed, vulnerable items are automatically closed during import. The group closes when all vulnerable items in the group are fixed.
- After the scan, if the state is not Fixed, the VI is automatically moved back to Under Investigation.

- Vulnerable items set to 'Resolved' in your instance but not transitioned to 'Closed/Fixed' by the third party integration runs are reopened if they are detected during rescans.

  For Qualys detections, if the scanner continues to find VIs that were set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans, these VIs move back to 'Open' when the last found date is later than the Resolved date.

  For Rapid7 detections, an option is now available on the Rapid7 configuration page in your instance to reopen resolved VIs by age. If enabled, VIs set to 'Resolved' but then not transitioned to 'Closed/Fixed' by subsequent scans transition back to 'Open' after the number of days that you enter.

Vulnerability Solution Management Deployment Progress

Comprehensive deployment metrics for remediation tasks and vulnerability entries are included in Vulnerability Solution Management under **Remediation Status** in vulnerabilities, vulnerable items. Easily identify which remediation task or vulnerability is slowing resolution progress. Drill down into how the vulnerability is identified, or what aspects of the affected assets may be causing the remediation issue. Update the status of your metrics using the **Update status** related link in the vulnerability, solutions, and remediation task forms.

Using the default Vulnerability Response dashboards

The Vulnerability Response overview dashboard (Vulnerability Management) provides an executive view into vulnerabilities and vulnerable items, helping the Vulnerability Admin pinpoint areas of concern quickly. The Vulnerability Response remediation dashboard (Vulnerability Remediation) allows a remediation specialist to focus on the remediation tasks and vulnerable items they own.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data visualizations in the Vulnerability Response Workspaces

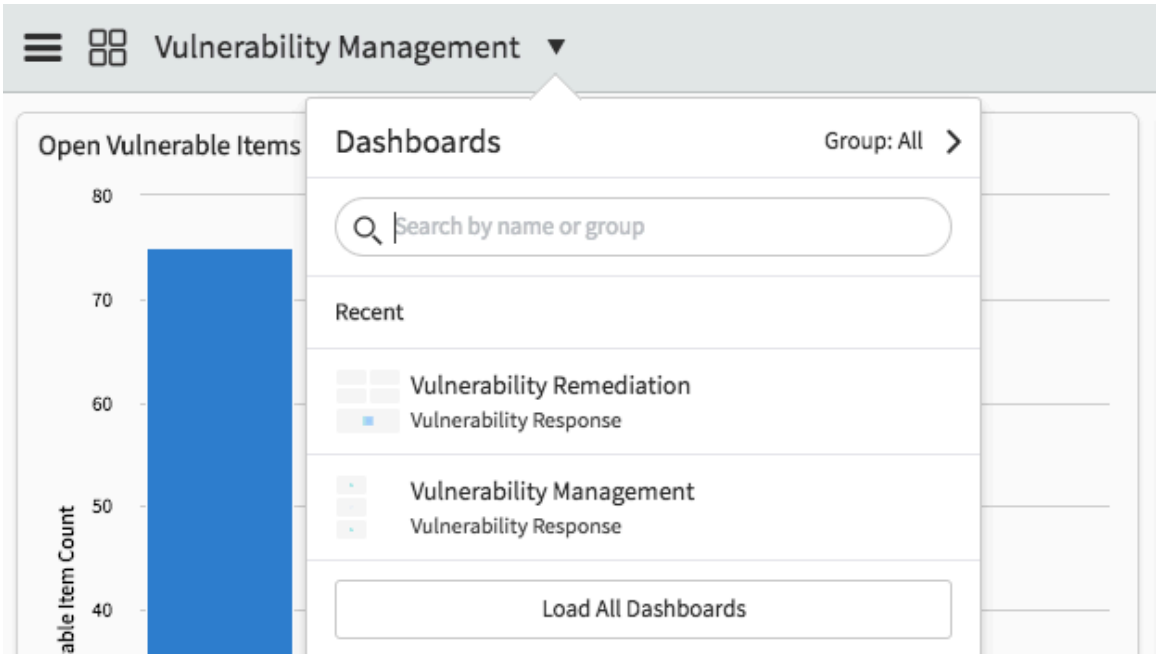
The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Response Workspaces, Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Vulnerability analysts can also use default Vulnerability Response dashboards.

Roles required: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst, and users with sn_vul.vulnerability_read (or who inherit the sn_vul.vulnerability_read role), and pa_viewer.

The default Vulnerability Response dashboards in the legacy environment

These reports are included as part of the Performance Analytics for Vulnerability Response application and do not require a separate subscription. To open one, select the choice list to expand it and choose a dashboard. Alternatively, enter the name of a dashboard in the search field.



Note:

When the Performance Analytics Content Pack for Vulnerability Response application is installed and activated, the Vulnerability Management (PA) dashboard, is displayed automatically in the Overview module. This dashboard contains reports covering all stages of the vulnerability management life cycle.

For information on the reports included in the Performance Analytics Content Pack for Vulnerability Response, see Vulnerability Management [PA] dashboard.

For information about the CISO dashboard and Scan Coverage reports, see Vulnerability Management CISO dashboard.

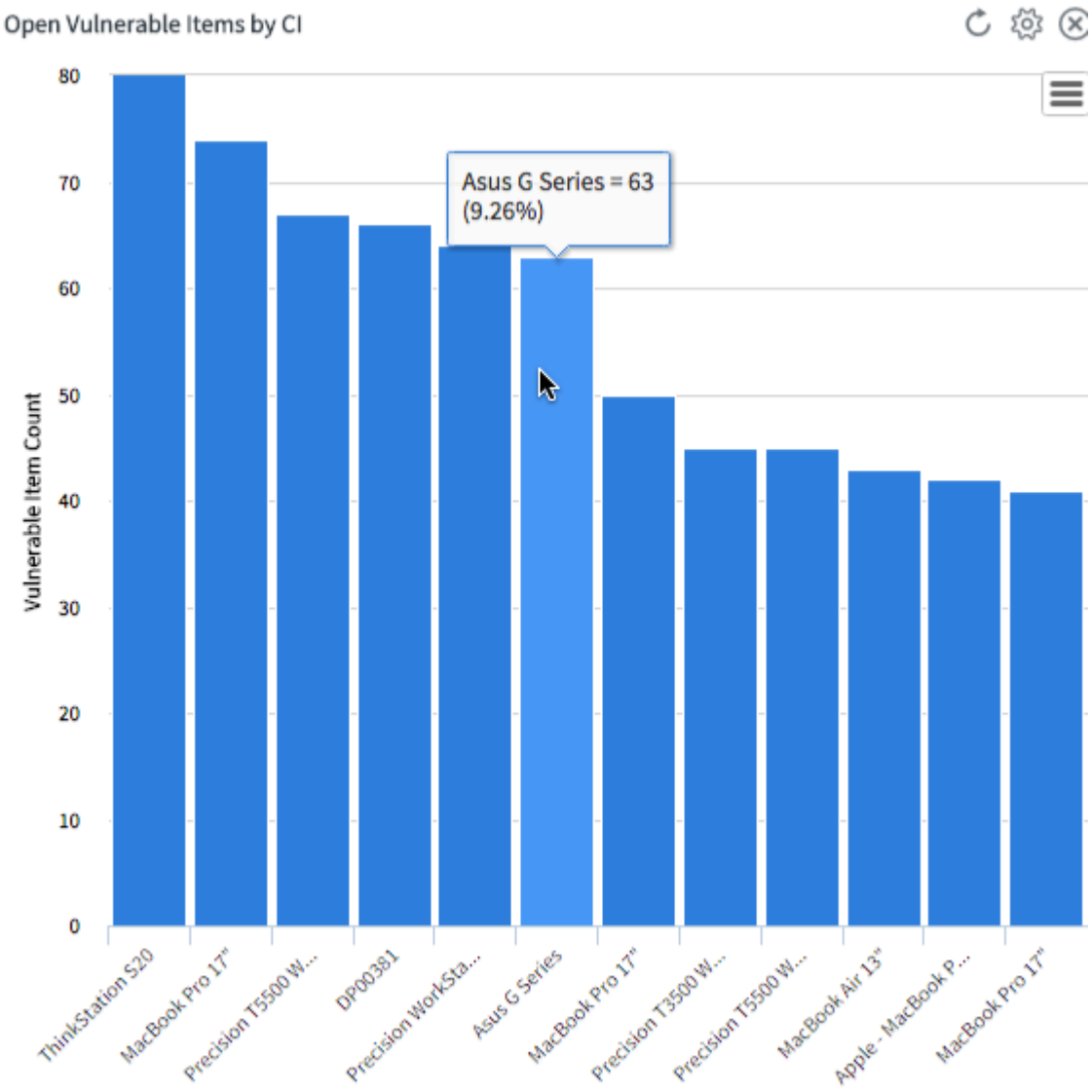
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Management dashboard

In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

Note:

If customized dashboards are needed, see Create and use dashboards for more information.



Vulnerability Overview reports

Name	Visual	Description
Open Vulnerable Items by CI	Bar	Displays the number of open vulnerable items recorded for each configuration item (CI), from most to least.
Vulnerable Items by Remediation Target Status	Bar	Displays the number of Vulnerable Items that are Approaching Target, In-flight, and Past Target.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Overview reports (continued)

Name	Visual	Description
		Note: Items in the Deferred, Resolved, or Closed state are not included.
Deferred Vulnerable Items Expiring this Week	Graph	Displays the number of deferred vulnerable items scheduled to be reactivated within seven days.
Open Vulnerable Items by Vulnerability	Bar	Displays the number of open vulnerable items for each vulnerability, from most to least.
Vulnerabilities by Model	Bar	Displays the number of vulnerable items recorded for each model (CI class), from most to least.
Vulnerabilities by Week	Trend	Displays the number of vulnerability entries recorded each week.
Most Vulnerable Models	Donut	Displays models (CI classes) with the most vulnerable items.
Vulnerabilities by Publisher	Bar	Displays the number of vulnerable items recorded for each publisher, from most to least.
Vulnerabilities by Impact	Bar	Displays the number of vulnerability entries for impacted network types.
Most Vulnerable Publishers	Donut	Displays publishers with the most vulnerable items.
Most Vulnerable CIs	Donut	Displays CIs with the most vulnerable items.
Vulnerabilities by Score	Bar	Displays the number of vulnerability entries by vulnerability scores.
Reopened Vulnerable Items	List	Lists the reopened vulnerable items and their age.
Most Vulnerable CIs by Class	Donut	Displays CIs with the most vulnerable items.
Vulnerable Item Age	List	Lists the number of days since vulnerable items were last opened.
CIs with Vulnerability by Date	List	Lists configuration items that have been scanned within the last 30 days.
CIs not Scanned	List	Lists configuration items that have never been scanned for vulnerabilities.

Vulnerability Remediation dashboard

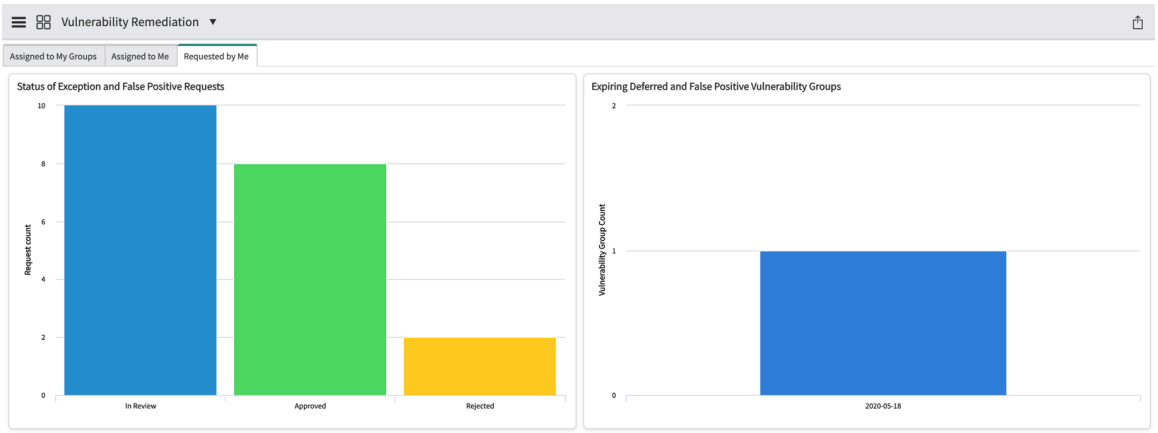
Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

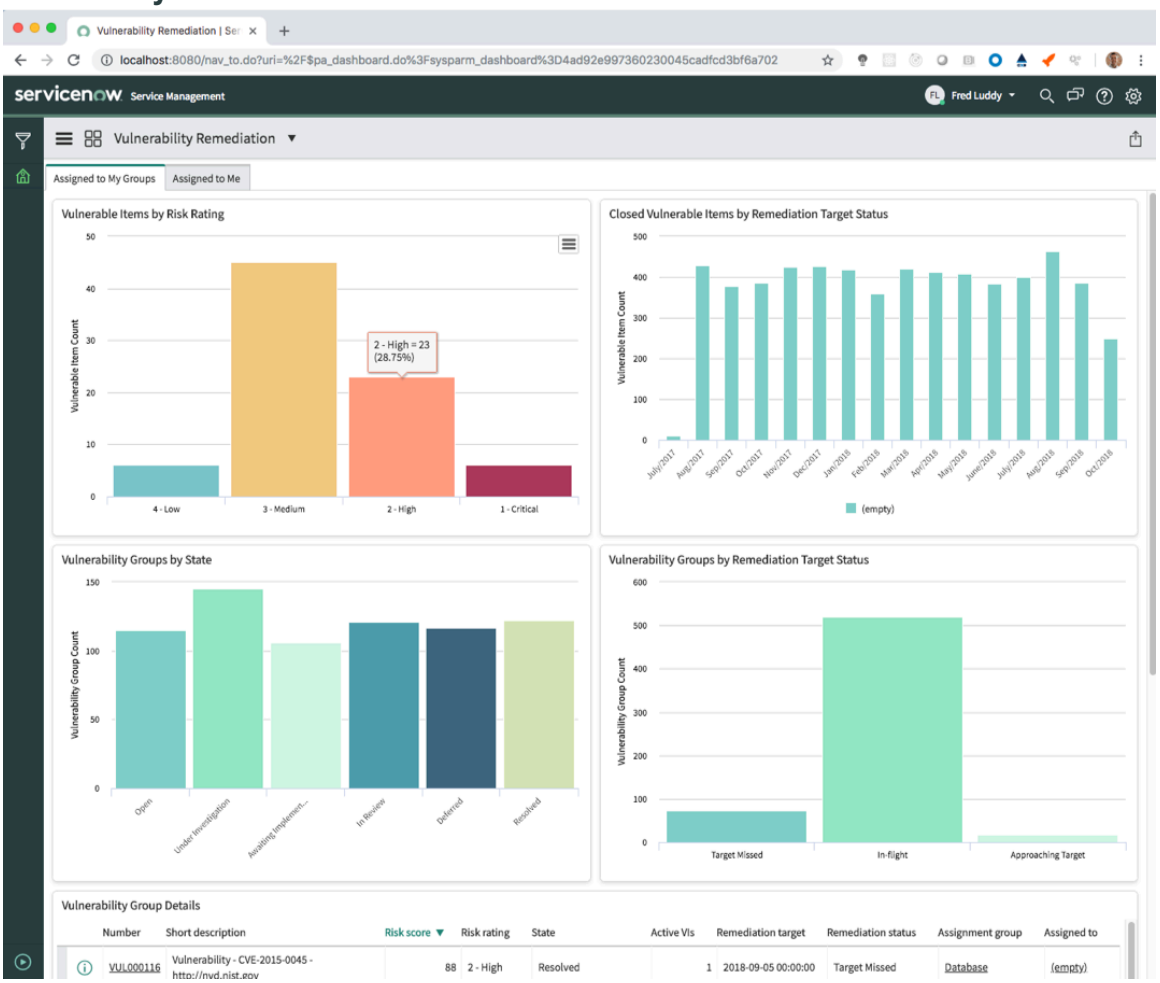
The Vulnerability Remediation dashboard contains the following tabs: **Assigned to My Groups**, **Assigned to Me**, and **Requested by Me**. The Assigned to My Groups and Assigned to Me tabs show the same reports. The former tab reports by the assignment groups you belong to, and the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

latter by vulnerable items or remediation tasks that are assigned to you. The Requested by Me tab reports the false positives and exceptions you requested.



Vulnerability Remediation dashboard



Reports

Assigned to My Groups and Assigned to Me

Name	Visual	Description
Vulnerable Items by Risk Rating	Bar	Number of active vulnerable items grouped by risk rating over the selected time span.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assigned to My Groups and Assigned to Me (continued)

Name	Visual	Description
Closed Vulnerable Items by Remediation Target Status	Bar	Number of Closed vulnerable items grouped by remediation target status over the selected time span.
Remediation Tasks by State	Bar	Number of active remediation tasks (RTs) grouped by state.
Remediation Tasks by Remediation Target Status	Bar	Number of active RTs grouped by remediation target status. This report excludes deferred vulnerable items.
Remediation Task Details	List	Remediation task record details in a list.

Requested by Me

Name	Visual	Description
Status of Exception and False Positive Requests	Bar	Number of active requests from you.
Expiring Deferred and False Positive Remediation Tasks	Bar	Number of Deferred and False Positive Remediation Tasks (RTs), grouped by Until date.

Vulnerability Approvals dashboard

The Vulnerability Approvals dashboard contains the following reports for exception and false positive approvers.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Name	Visual	Description
Exception and False Positive Requests by Age Pending My Approval	Bar	Number of approvals pending for you, grouped by created date.
My Approval and Rejected Exception and False Positive Requests	Bar	Number of approval requests approved or rejected, grouped by approval state.
All Remediation Tasks by Risk Rating Pending Approval	Bar	Number of remediation tasks pending approval, grouped by risk rating.
All Pending and False Positive Approval Requests Grouped by Reason	Bar	Number of pending approval requests grouped by reason.

Platform Analytics Solutions for Vulnerability Management

Platform Analytics Solutions contain prepackaged Performance Analytics and Reporting content for use with other ServiceNow AI Platform products. This Analytics and Reporting Solution permits you to track the volume, performance and progress of vulnerabilities from initial analysis

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and detection to containment, or remediation. You can filter reports by assignment group, exploits, risk rating, or state.

The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application. It is available on the ServiceNow Store as a separate subscription.

Performance Analytics for Vulnerability Response contains two dashboards:

- Vulnerability Management (PA) dashboard
- Vulnerability Management Chief Information Security Officer (CISO) dashboard

Required roles, installation, and viewing the dashboards

The following roles and tasks are associated with this Solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Analytics and Reporting Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the indicators, breakdowns, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.

To install this application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

Note: Set up and test Analytics and Reporting Solutions on a non-production instance before enabling them in production.

Analytics and Reporting Solutions provide all the configuration records required to analyze default applications. Customize these records for use in your production environment. For more information, see Configure Analytics and Reporting Solutions.

To view the vulnerability Management (PA) dashboard, navigate to **Vulnerability Response** > **Overview** > **.**

To view the Vulnerability Management CISO dashboard, navigate to **Vulnerability Response** > **CISO Dashboard** > **.**

Key terms

Performance analytics (PA)

Solution that creates management dashboards, reports on KPIs and metrics, and answers key business questions to help increase quality and reduce costs.

Vulnerable item (VI)

A security vulnerability reported by a third-party vulnerability scanner that is present on a configuration item (CI).

Remediation task

Remediation tasks are created and assigned automatically to IT teams based on the group that is associated with the vulnerable items in a remediation effort. IT teams and remediation owners view remediation tasks in the IT Remediation Workspace. See Vulnerability Response Workspaces for more information

.

PA indicator

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior, for example, Non-Deferred Overdue Critical Vulnerable Items.

PA indicator source

Data sets that filter records from one table or database view, for example, VI Active.

View data visualizations in real-time

To see what is happening today with the most critical items in your Vulnerability Response application, you can view certain reports on the Vulnerability Management (PA) dashboard in real-time. Viewing these reports on-the-fly helps you manage your most important vulnerable items (VIs) and remediate them quickly. You can view the following reports in real time:

- Overview tab - Vulnerable Items by Assignment Group
- Vulnerable CIs tab
  - Vulnerable Configuration Items (CIs) without Owners
  - Retired or Stolen CIs with Active VIs
- Exceptions tab
  - Deferred Vulnerable Items by Reason
  - Deferral Requests About to Expire
  - Deferred Vulnerable Items by CIO Manager
- Remediation tab - Unassigned Vulnerable Items

For more information, see View Performance Analytics for Vulnerability Response [PA] reports in real time.

Related topics

Analytics and Reporting Solutions

Vulnerability Management CISO dashboard

With the Vulnerability Management CISO dashboard, view data such as Key Performance Metrics (KPIs) for vulnerability remediation, see the highest risks, verify scan coverage, and learn how to lower risks.

Required ServiceNow AI Platform roles

- sn_vul.vulnerability_ciso to view the dashboard.
- sn_vul.ciso_write to edit the dashboard.

Activating the CISO dashboard

To activate the CISO dashboard, you must install Performance Analytics for Vulnerability Response and activate the corresponding Performance Analytics job. For more information, see Analytics and Reporting Solutions for Vulnerability Response.

Use cases

User	Dashboard use
Chief Information Security Officers (CISOs)	Chief Information Security Officers (CISOs) can use the CISO dashboard to gain insight

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User	Dashboard use
	into the vulnerability management program for their organizations. The dashboard provides data to help them identify data at-a-glance how they can use to lower the vulnerabilities to their environments.

Using the CISO dashboard

Executive users, like the Chief Information Security Officers (CISOs) in your organization, can view the CISO dashboard for Vulnerability Response to understand how effective their vulnerability management program is. You can view the CISO dashboard by navigating to **Vulnerability Response** > **CISO Dashboard**. Use the top-level filters to filter reports by Risk Rating, Age Range, or Internet Facing. Some reports display trending data over a period of time. You can view how the important metrics are trending on a regular basis, analyze the overall business security risk, and identify the areas that need improvement.

Starting with version 19.0 of Vulnerability Response, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Running the scheduled jobs

Run the scheduled jobs in this order to update the data in the reports:

1. Update dashboard tables
2. [PA VR] CISO Dashboard

Scheduled jobs for CISO dashboard

Scheduled job name	Description
Update dashboard tables	Daily scheduled job that you must run before the [PA VR] CISO Dashboard job so that you can collect the CISO data. By running this scheduled job, you update the Scan Coverage reports. The information updated includes the operational configuration items (CIs) that are scanned in the last 90 days, their classes, and the total number of operational CIs that correspond to these classes. Running this scheduled job updates the reports in the **Recommended Actions** tab as well.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled jobs for CISO dashboard (continued)

Scheduled job name	Description
	Note: Operational CIs refer to the CIs that have an operational status as `Operational`.
[PA VR] CISO Dashboard	After the Update dashboard tables scheduled job is complete, run this scheduled job to populate all the reports in the **CISO Overview** tab.

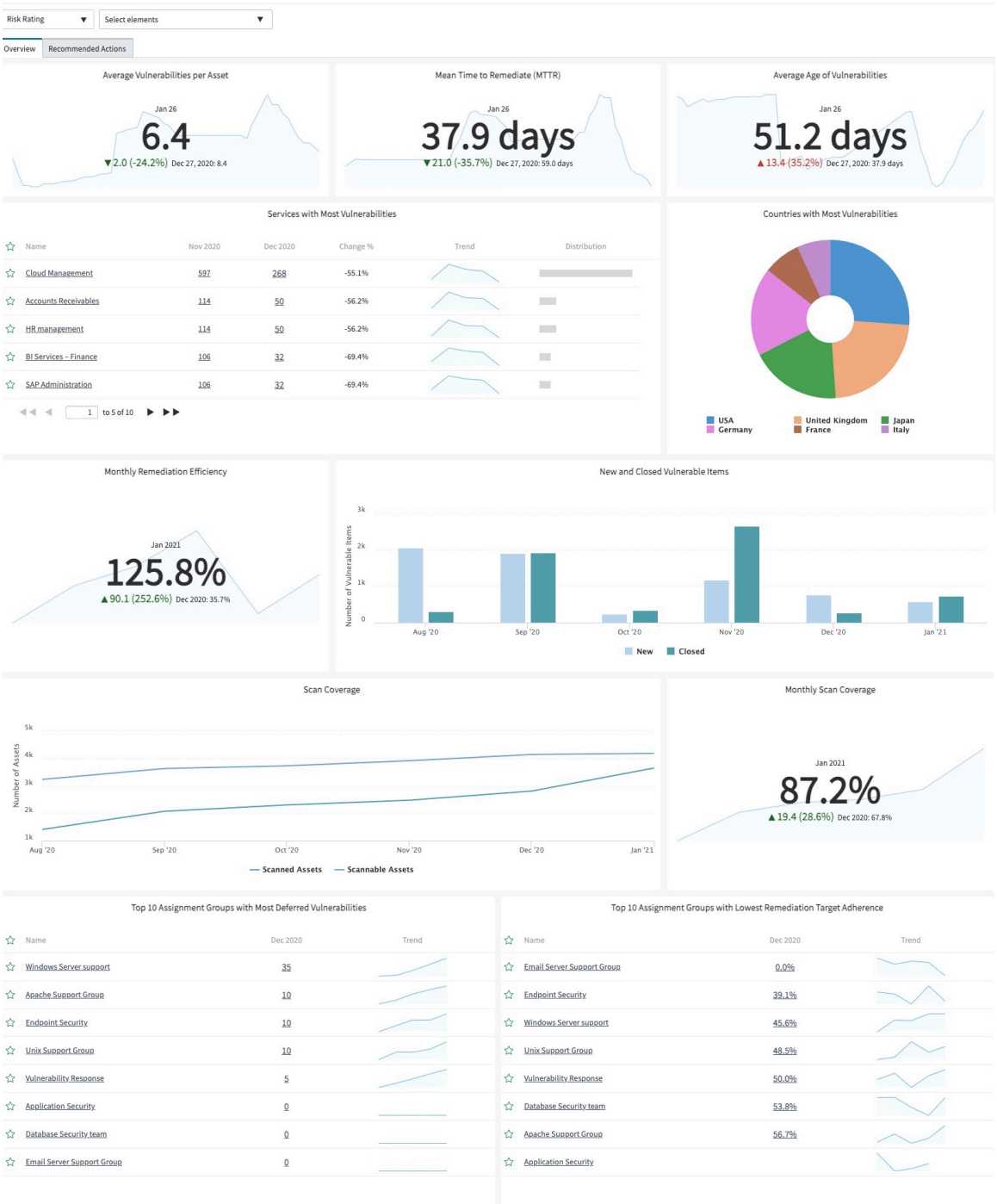
CISO dashboard tabs

This dashboard provides an insight into the risks present in Vulnerability Management. You can view vulnerabilities and their related data by region, age, services, and other breakdowns.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab

The Overview tab contains reports that provide the security posture of your organization at a glance.

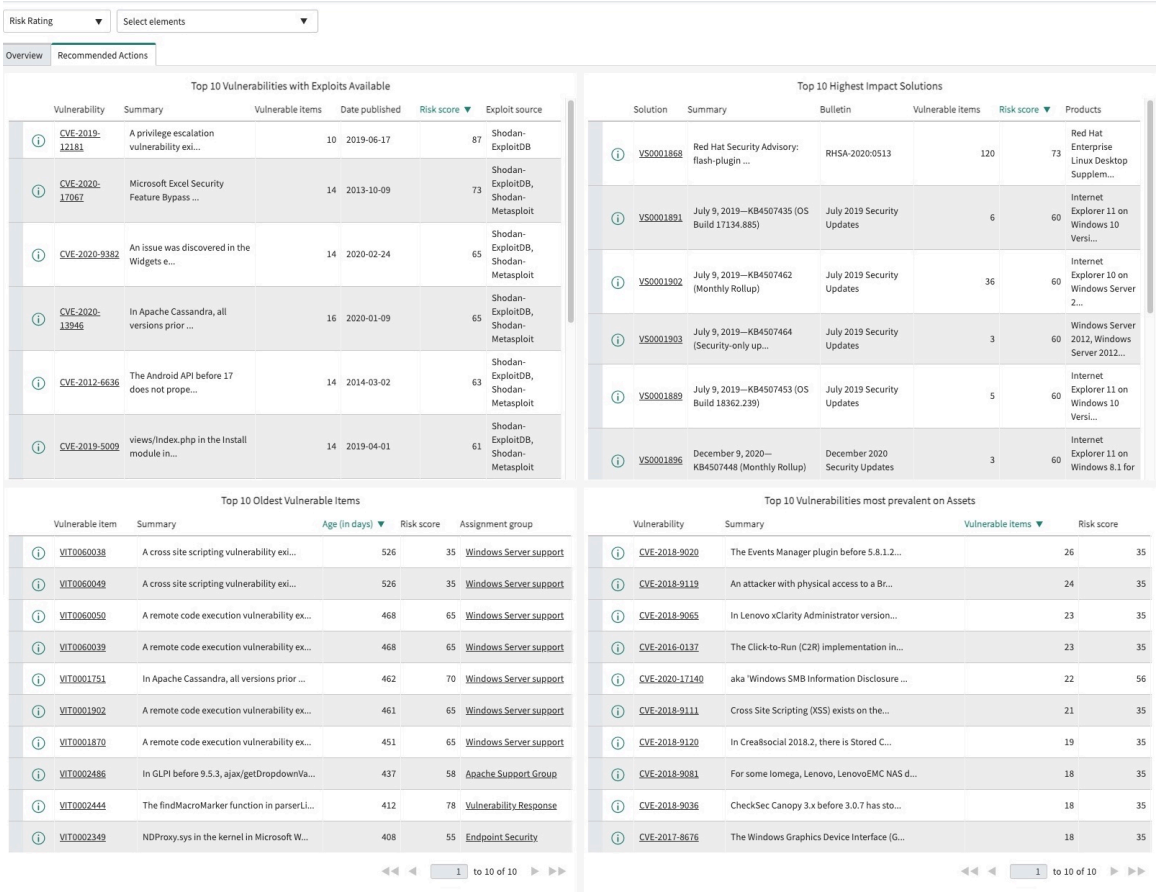


Note: The top-level filter can only be used for some reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recommended Actions tab

The Recommended Actions tab contains reports that provide insights into exploitable, aging, and prevalent vulnerabilities. It also contains solutions that recommend actions to reduce the risks. Run the **Update CISO dashboard tables** scheduled job to update the reports in this tab.



Indicators

To view the indicators, navigate to **Performance Analytics** > **Indicators**.

1. On the Indicators page, search for the required indicator name in the Name column.
2. Click the indicator name to open the record and view its details.

The indicators for the CISO dashboard do not collect records by default. You can choose to collect records by selecting the Collect records check box.

Total Duration of Closed Vulnerable Items

Total Duration of Closed VIs is measured daily as Days. The goal of this indicator is to minimize the score.

Scannable Assets

Scanned Assets is measured daily as unit #. The goal of this indicator is to maximize the score.

Services with Most Vulnerabilities

Services with Most Vulnerabilities is measured daily as unit #. The goal of this indicator is to minimize the score.

Average Vulnerabilities per Asset

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

[[Active Vulnerable Items]] / [[Active Vulnerable Configuration Items]

Closed Vulnerable Items

Closed Vulnerable Items is measured daily as unit #. The goal of this indicator is to maximize the score.

Vulnerable Items Mean Time to Remediate

[[Summed Duration of Closed Vulnerable Items]] / [[Closed Vulnerable Items]]

Current Scan Coverage

Calculates the current scan coverage as percentage.

Scanned Assets

Scanned Assets is measured daily as unit #. The goal of this indicator is to maximize the score.

Closed Vulnerable Items (Target Met)

Closed Vulnerable Items (Target Met) is measured daily as unit #. The goal of this indicator is to maximize the score.

% of Closed Vulnerable Items that Met Target

[[Closed Vulnerable Items (Target Met) / By month SUM]] / [[Closed Vulnerable Items / By month SUM]] *100

Active Vulnerable Items

Active Vulnerable Items is measured daily as unit #. The goal of this indicator is to minimize the score.

Average Age of Vulnerable Items

Average Age of Active VIs is measured daily as unit Days. The goal of this indicator is to minimize the score.

Active Vulnerable Configuration Items

Active Vulnerable CIs is measured daily as unit #. The goal of this indicator is to minimize the score.

Monthly Remediation Efficiency

[Number of vulnerable items closed during a month] / [Number of new or reopened vulnerable items in the same month]

New Vulnerable Items

New Vulnerable Items is measured daily as unit #. The goal of this indicator is to minimize the score.

Deferred Vulnerable Items

Deferred VIs is measured daily as unit #. The goal of this indicator is to minimize the score.

Breakdowns

- Assignment Group: Applies to some VI reports.
- Risk Rating: Applies to VI reports.
- Age Range: Applies to VI reports.
- Age Closed: Applies to reports for closed VIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Internet Facing: Indicates whether the CI belongs to the hardware class and is internet facing.
- Region: The CMDB CI parameter used is Location. This location indicates the country of origin of the configuration item.

Data visualizations

Name	Type	Description
Average Vulnerabilities per Asset	Single Score	Average number of active vulnerable items for each configuration item.
Mean Time to Remediate (MTTR)	Single Score	The mean time to remediate (close) a vulnerable item, displayed as a 30-day running average. **Note:** The value for Age Closed is calculated when data is collected. The value is the difference between the Last Opened date and the date and time of the collection job.
Average Age of Vulnerabilities	Single Score	Average age of active vulnerable items in days.
Services with Most Vulnerabilities	List and Line	Monthly average of active vulnerable items for services in the organization. **Note:** For information on defining the service classifications that you want to display in Vulnerability Response reporting and related lists, see the Services tab in Vulnerability Management [PA] dashboard.
Countries with Most Vulnerabilities	Donut	Top 10 countries with the highest number of vulnerable items.
Monthly Remediation Efficiency	Single Score	Percentage of closed vulnerable items divided by new vulnerable items in the current month.
New and Closed Vulnerable Items	Bar	Number of new vulnerable items imported and number of vulnerable items closed in a month.
Scan Coverage	Line	Number of scanned assets compared to the total number of scannable assets, shown over time. The CI Classes included in the widget are specified in the Scan Coverage Configuration module. For information on configuring the Scan Coverage module, see Configure the Scan Coverage reports.
Monthly Scan Coverage	Single Score	Percentage of scanned assets divided by the total number of scannable assets for the current month. For information on configuring the Scan Coverage module, see Configure the Scan Coverage reports

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Type	Description
Top 10 Assignment Groups with Most Deferred Vulnerabilities	List and Line	Top 10 assignment groups with the highest number of deferred vulnerable items, deferred based on the monthly average.
Top 10 Assignment Groups with Lowest Remediation Target Adherence	List and Line	Top 10 assignment groups whose vulnerable items have the lowest adherence to their remediation targets.

Recommended Actions

Name	Type	Source table	Description
Top 10 Vulnerabilities with Exploits Available	List	Vulnerability Top Item [sn_vul_analytics_top_item]	Active vulnerabilities with exploits available for all the threat intelligence vendors that use the VR exploit framework.
Top 10 Highest Impact Solutions	List	Vulnerability Top Item [sn_vul_analytics_top_item]	Preferred solutions or patches with the highest risk scores for active vulnerable items. This report uses the capabilities of Vulnerability Solution Management (VSM), which correlates patches from Microsoft and Red Hat to vulnerabilities in the environment. VSM helps identify the preferred solution for vulnerabilities.
Top 10 Oldest Vulnerable Items	List	Vulnerability Top Item [sn_vul_analytics_top_item]	Active vulnerable items with the highest age. Resolve these items to lower the average vulnerability age on the Overview tab.
Top 10 Vulnerabilities Most Prevalent on Assets	List	Vulnerability Top Item [sn_vul_analytics_top_item]	Active vulnerable items available for the highest number of assets.

Configure the Scan Coverage reports

Enable your users to run scan coverage reports from the CISO dashboard. With these reports, your users can see what the organization's scan coverage is over a period of time.

Before you begin

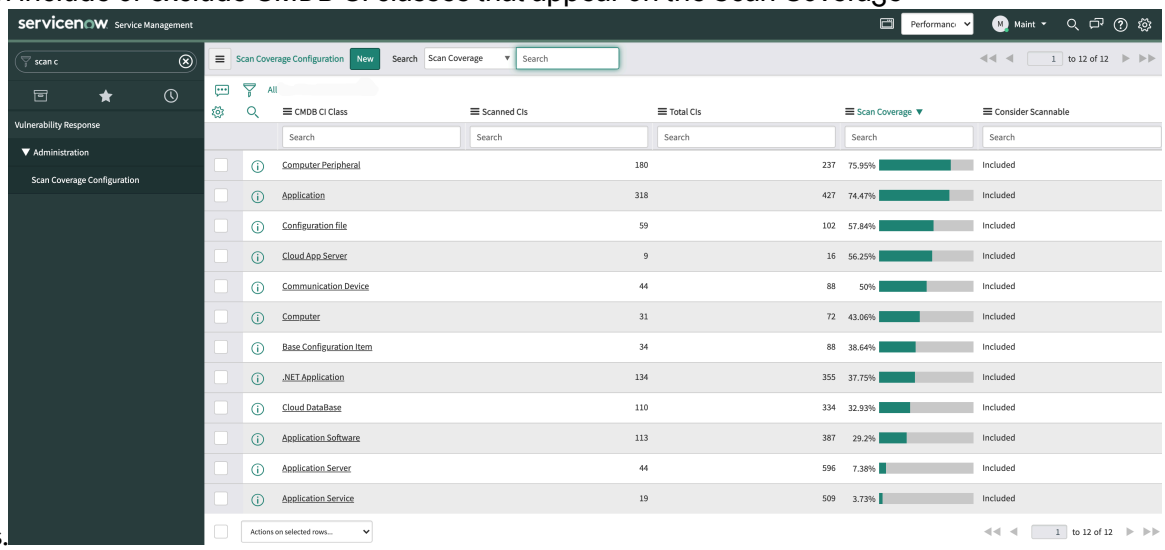
Role required: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

About this task

The scan coverage shows the number of assets that are being scanned by the vulnerability scanners for the various classes over the last 90 days. These assets are compared to the number of scannable assets in the Configuration Management Database (CMDB). By default, the Scan Coverage Configuration module includes CMDB CI classes, to which at least one scanned asset has been matched. You can add a CI class from the CMDB to the Scan Coverage report that is displayed on the CISO dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can include or exclude CMDB CI classes that appear on the Scan Coverage reports.



Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Scan Coverage Configuration**.
2. Click **New**.
3. On the form, fill in the fields.

Scan Coverage Configuration form

Field	Description
CMDB CI Class	CI class that must be added to the Scan Coverage Report on the CISO dashboard. **Note:** If a CI class already exists in the Scan Coverage Configuration module, it is not included in this list.
Consider Scannable	Option to define if the CI class must be included or not. Include a CI class if you want its data to be added to the scan coverage reports. If excluded, the data for that CI class is not added.

4. Click **Submit**.

Configure the PA indicators for the CISO Dashboard

Monitor the automated and formulated CISO indicators so that you can manage the vulnerability data in your instance.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

Vulnerability Response has both automated and formulated indicators.

Key terms

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Indicator

Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior. An example is an Active Vulnerable Item.

Indicator source

Data sets that consist of records filtered from one table or database view for increased efficiency. An example is VI.Active (Internet facing).

Breakdowns

Breakdowns filter and group indicator scores using qualitative attributes such as Priority, Category, and Assignment Group.

Scheduled jobs

Scheduled jobs are run to populate the indicator source data. The [PA VR] CISO Dashboard daily scheduled job is disabled by default. You must activate it to collect indicator scores for the CISO dashboard.

Procedure

1. Navigate to **All** > **Performance Analytics** > **Indicators** and choose one of the following:
   - Automated Indicators
   - Formula Indicators

   For more information on indicators, see Performance Analytics Indicators.
2. On the Indicators page, search for the required indicator name in the Name column.
3. Click the indicator name to open the record and view its details.

   The indicators for the CISO dashboard do not collect records by default. You can choose to collect records by selecting the **Collect records** check box.

   Note: Activating collect records in an indicator may cause performance issues such as taking a lot more time and memory that is required to run the data collection job.

   The maximum number of rows that you can fetch for an indicator source is 1,000,000.

SecOps Vulnerability Response Health dashboard

The Vulnerability Response Health dashboard is a tool designed to empower organizations with comprehensive insights into the implementation and usage of their Vulnerability Response applications.

The overall health assessment is determined by aggregating various critical factors across configuration, implementation, integration, performance, data, and process. View the aggregate dashboard for each category for the following applications:

- Vulnerability Response
- Application Vulnerability Response
- Container Vulnerability Response
- Configuration Compliance

Installing the SecOps Vulnerability Response Health Dashboard

To install and configure the SecOps Vulnerability Response Health Dashboard for Vulnerability Response applications in your ServiceNow AI Platform instance, navigate to the ServiceNow® Store and activate the SecOps Health Analytics (sn_sec_analytics) plugin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required ServiceNow AI Platform roles

Roles required: sn_sec_analytics.admin, sn_sec_analytics.read

Scheduled job

To view the scheduled job, navigate to **All** > **System Scheduler** > **Scheduled Jobs** > **Collect health dashboard metrics**. The 'Collect health dashboard metrics' scheduled job is run daily at 00:00 hours. It generates the data for the SecOps Vulnerability Response Health dashboard. You can choose to run the scheduled job manually as well.

Use cases

For examples of how people in your organization would use this dashboard, see these use cases.

User	Dashboard use
Vulnerability admin	Helps you gain an understanding of the health score of the Vulnerability Response applications. It's also helpful to highlight the areas that need improvement. The Vulnerability Response Health Dashboard deals with the implementation and usage health only. It doesn't assist with management of vulnerabilities or assets.
Support admin	Helps you to identify the performance, customization, and configuration issues using KPIs. Based on the application health, you can perform an extra analysis or provide a recommendation to the users.
Implementation partner	Helps you to evaluate the Vulnerability Response implementation health for configurations, add-ons, customizations, and integrations, and provide improvement recommendations for the users.

The SecOps Vulnerability Response Health Dashboard tabs

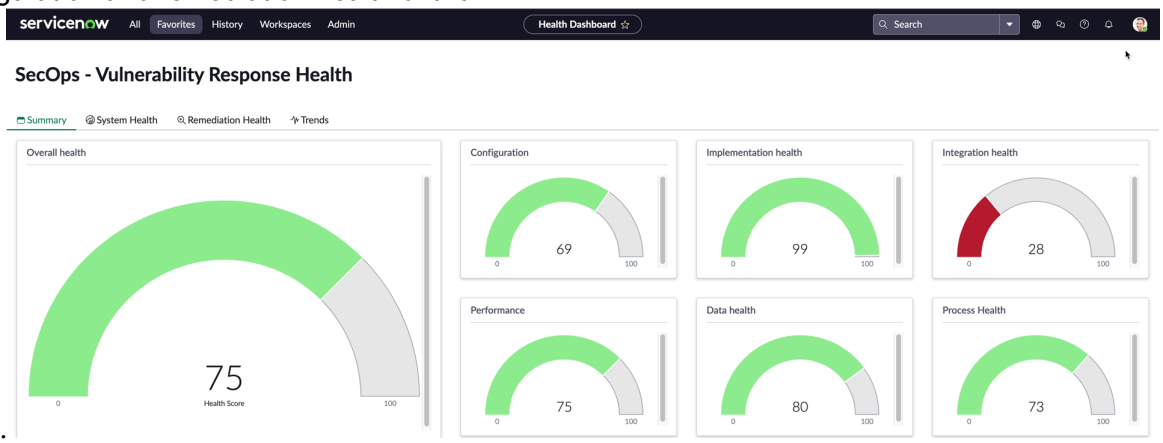
To view the SecOps Vulnerability Response Health dashboard, navigate to **Security Operation Health** > **Vulnerability Response Health**. Each color in the dashboard represents the following:

- Green: Safe
- Yellow: Warning
- Red: Critical

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

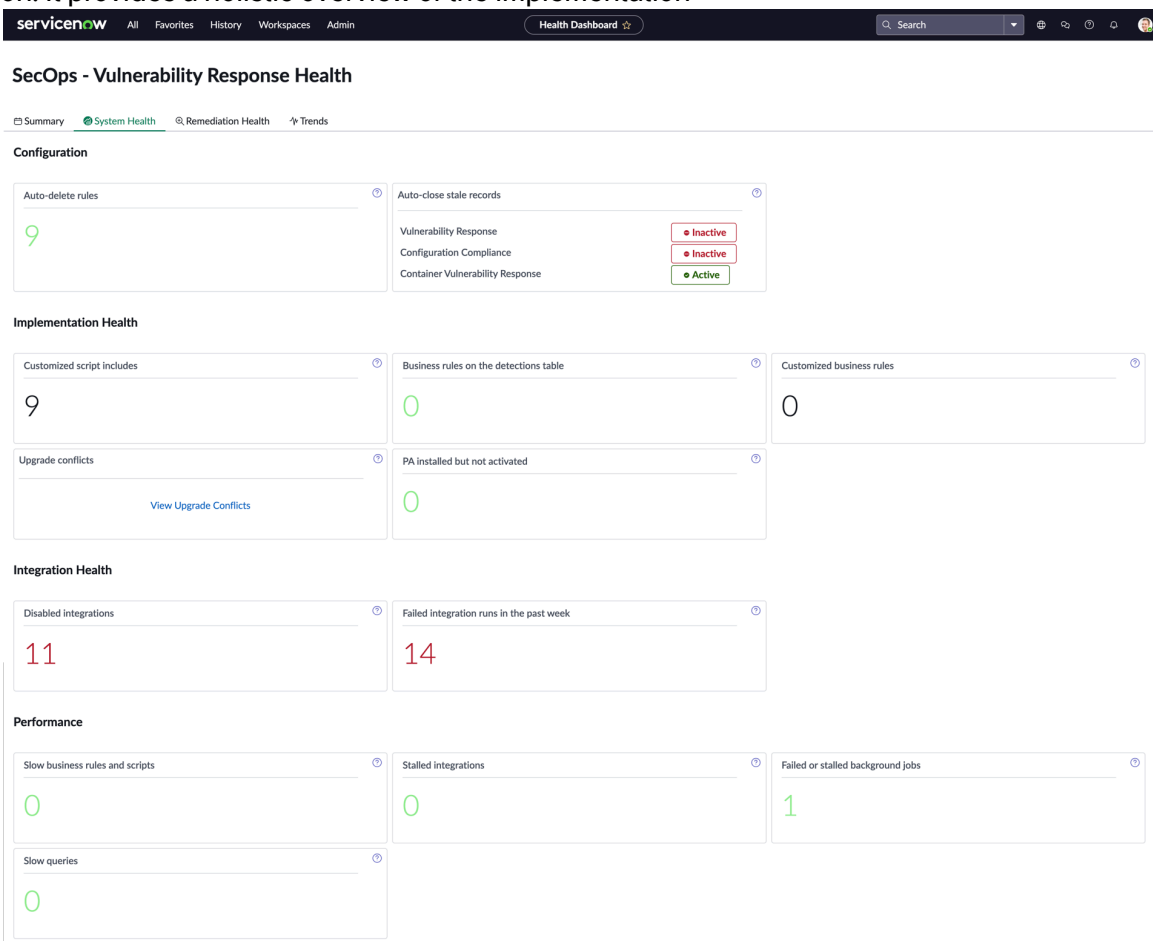
Summary tab

This dashboard communicates the overall health score for the configuration and remediation health of the VR applications.



System Health tab

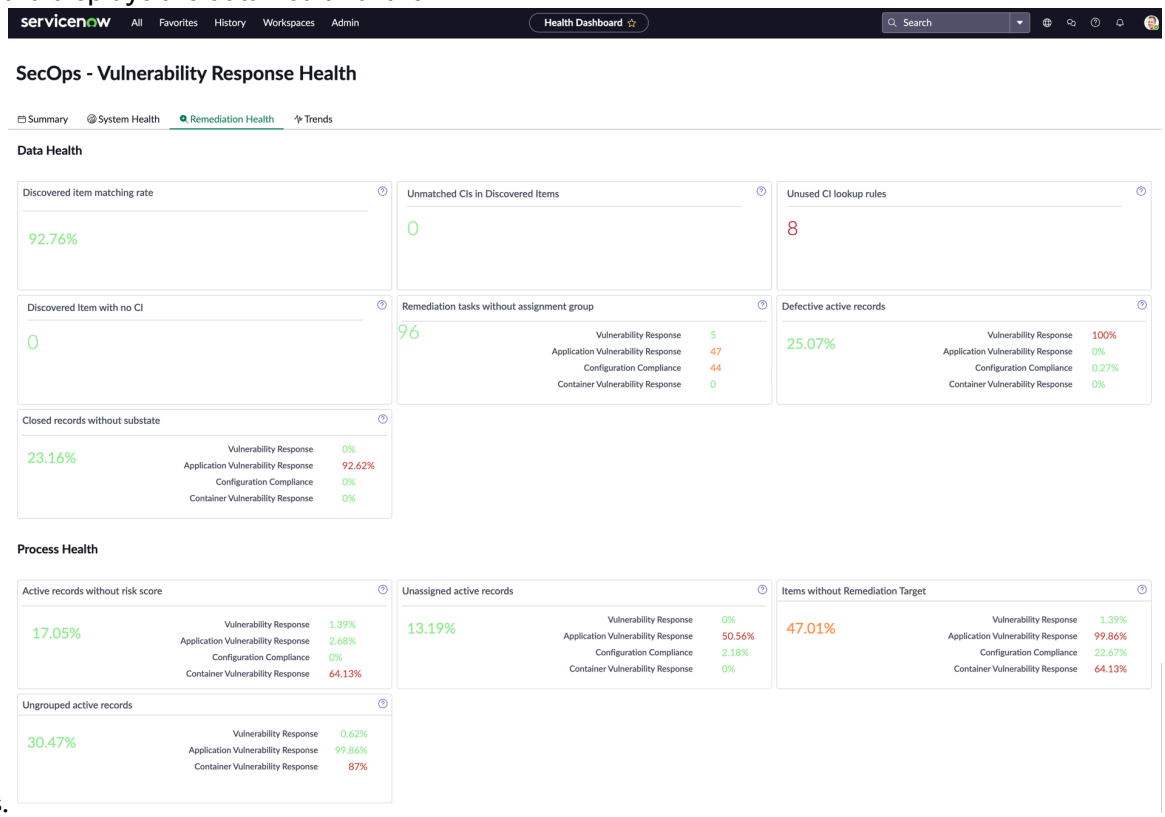
This dashboard displays the configuration and integration health of your implementation. It provides a holistic overview of the implementation performance.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

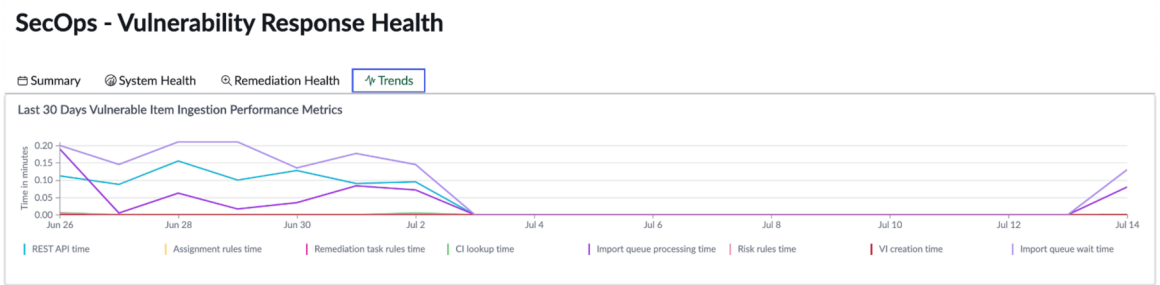
Remediation Health tab

This dashboard displays the data health of the VR applications.



Trends tab

This dashboard displays the trends for the vulnerable item ingestion performance metrics for the past 30 days for the VR applications.



Reports

Note: The threshold values are a part of the base system. You can configure the values based on your requirements.

Summary

Title	Description
Overall health	Overall health score for the VR applications. For more information, see the reports for the metrics.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Summary (continued)

Title	Description
Configuration	Overall configuration health of the VR applications.
Implementation health	Overall implementation health of the VR applications.
Integration health	Overall integration health of the VR applications.
Performance	Overall performance health score of the VR applications.
Data health	Overall data health of the VR applications.
Process health	Overall process health score of the VR applications.

System Health

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Configuration				
Auto-delete rules	Displays the number of enabled auto-delete rules.	Review and resolve the inactive auto-delete rules.	3	1
Auto-close stale records	Closes stale detections automatically. For more information, see the 'Automatically close stale detections in Vulnerability Response' topic in servicenow.com/docs.	Reduce the volume of stale detections. Enable this option to close the stale detections that aren't closed by the scanners.	3	1
Implementation health				
Customized script includes	Number of 'script includes' customized.	Minimize customized 'script includes' for easier upgrades.	10	12
Business rules on the detections table	Number of customized business rules	Minimize business rules for easier upgrades.	4	8

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
	in the detection table.			
Customized business rules	Number of customized business rules before creation of records in the CMDB.	Use the default business rules on records.	5	8
Upgrade conflicts	Conflicts such as business rules and scripts identified on an upgrade.	Review and resolve the upgrade conflicts.	10	15
PA installed but not activated	Indicates if the Performance Analytics dashboard is not enabled.	Activate the PA dashboard.	10	15
Integration health				
Disabled integrations	Number of integrations that have been disabled.	Review and enable the required integrations.	6	9
Failed integration runs in the past week	Number of integration runs that weren't successful in the past week.	Review and resolve the cause of the failed integration runs.	9	12
Performance				
Slow business rules and scripts	Business rules and scripts whose average execution time greater than 10 ms and execution count greater than 10,000.	Review and resolve the slow-running business rules.	10	15
Stalled integrations	Number of integrations that were timed-out before completion.	Review and resolve the cause of the stalled integrations.	10	15
Failed or stalled background jobs	Failed or timed-out background	Review and resolve the cause of the failed jobs.	5	10

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
	jobs in the past week.			
Slow queries	Queries whose average execution time is greater than 10 ms and execution count is greater than 10,000.	Review and resolve the slow-running business rules.	10	15

Remediation Health

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
Data Health				
Discovered item matching rate	Number of discovered items matched to existing CIs.	Review the health of your CMDB and the CI lookup rules logic.	50	20
Unmatched CIs in discovered items	Discovered items in unmatched state.	Review the health of your CMDB and the CI lookup rules logic.	9	12
Unused CI lookup rules	CI lookup rules that aren't associated with any discovered item.	Change the status of the unused CI lookup rules to inactive.	4	6
Discovered item with no CI	Discovered item with no configuration item.	Review and reapply CI lookup rules.	9	12
Defective active records	Records without a configuration item or vulnerability.	Retire the CIs using the CMDB CI Lifecycle Management option.	40	60

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Health (continued)

Title	Description	Considerations for improving performance	Threshold warning	Threshold critical
		Note: Deleting CIs directly can result in orphan VITs.		
Remediation tasks without assignment group	Active remediation tasks whose assignment group is yet to be assigned.	Assign remediation tasks to an assignment group and review the existing assignment rules.	40	60
Closed records without substate	Records that are closed without a substate.	Provide information in the Reason field while closing the records.	40	50
Process Health				
Active records without risk score	Active records with a risk score of 0 or with no risk score assigned.	Review and resolve the risk rules.	40	60
Unassigned active records	Records without an assignment group.	Assign a group to the records and review the existing assignment rules.	30	50
Items without Remediation Target	Items without a remediation target date.	Review and resolve the remediation target rules. These rules must include all the records.	30	50
Ungrouped active records	Records that aren't included in a remediation task rule.	Review the remediation task rules.	40	60

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Trends

Title	Description
Last 30 days vulnerable item ingestion performance metrics	Average time taken to ingest vulnerable items and process multiple rules in the past 30 days.

Modifying the threshold values

You can modify the threshold values for the SecOps VR Health dashboard data based on your preferences.

Before you begin
Role required: admin

Procedure

1. Navigate to **Security Operation Health** > **Configuration** > **Metrics**.
2. On the Health Dashboard Data page, open the record you want to modify.
3. Update the record and save.

Vulnerability Management (PA) dashboard

Track the volume, performance and progress of vulnerabilities from initial analysis and detection to containment, or remediation. You can filter reports by assignment group, exploits, risk rating, or state, for example. Quickly gain insight into your vulnerability exposure and which business services are affected.

Required ServiceNow AI Platform roles

Role required: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst, and users with sn_vul.vulnerability_read (or who inherit the sn_vul.vulnerability_read role), and pa_viewer.

Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

User	Dashboard use
It managers, IT analysts, vulnerability remediation owners	Help your organization deal with increasing security incidents due to exploited vulnerabilities by efficiently determining which vulnerable items present the most risk. These dashboards provide a graphical view into vulnerable item activity and help design remediation plans and status progress. You can focus on the KPIs associated with critical affected assets and high-visibility vulnerabilities.

To view the Vulnerability Management (PA) dashboard, navigate to **Vulnerability Response** > **Overview**.

See reports that show trending data over time. Reports with real-time data are listed below. View trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

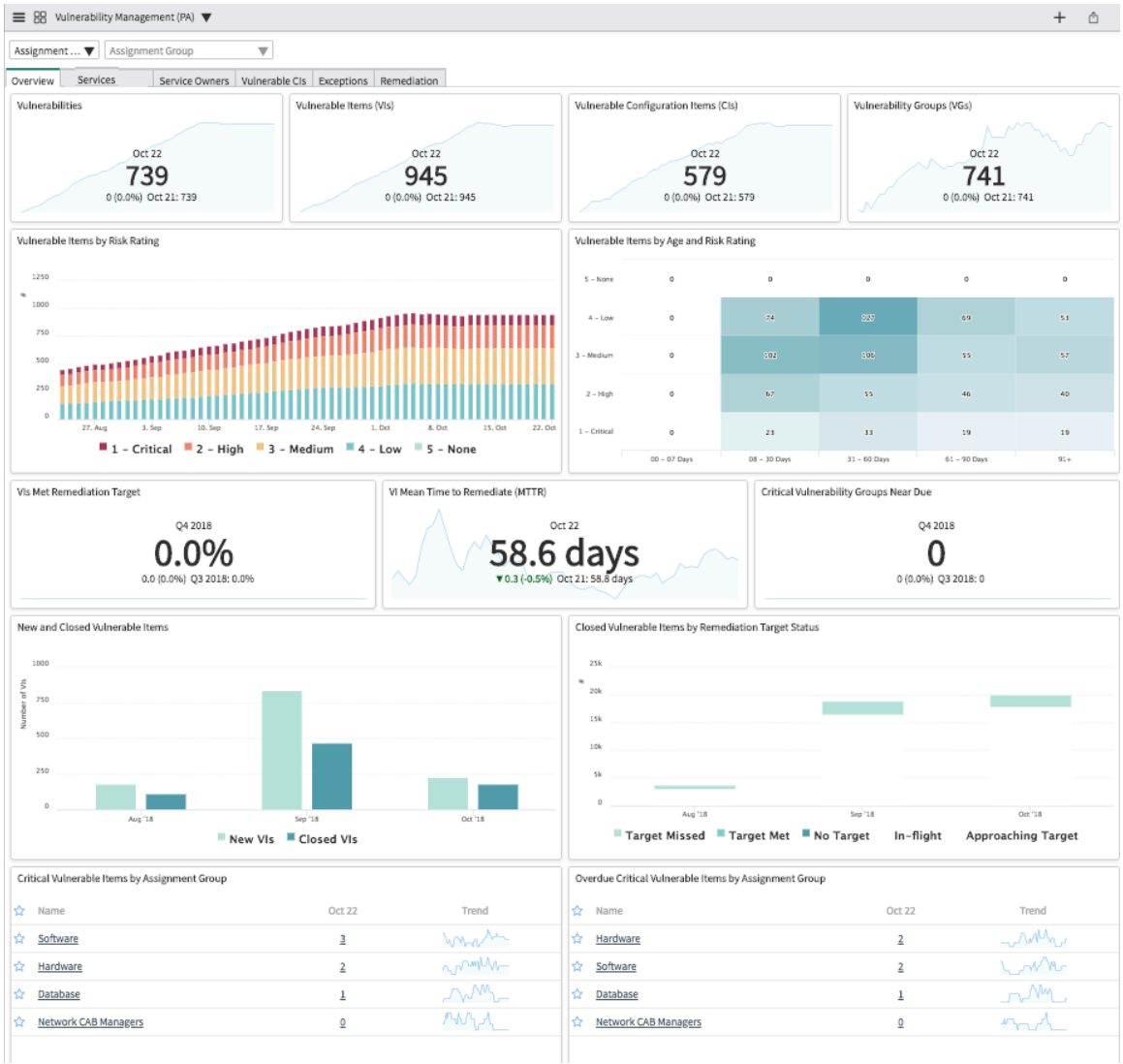
For more information about how to view your PA reports with real-time scores, see View Performance Analytics for Vulnerability Response [PA] reports in real time.

The Vulnerability Management [PA] dashboard tabs

Overview tab

This dashboard communicates KPIs for vulnerability risk and prevalence, affected assets, remediation target adherence, and remediation progress.

On the Overview tab, you can view the Critical Vulnerable Items by Assignment Group report that is run based on the scheduled job.

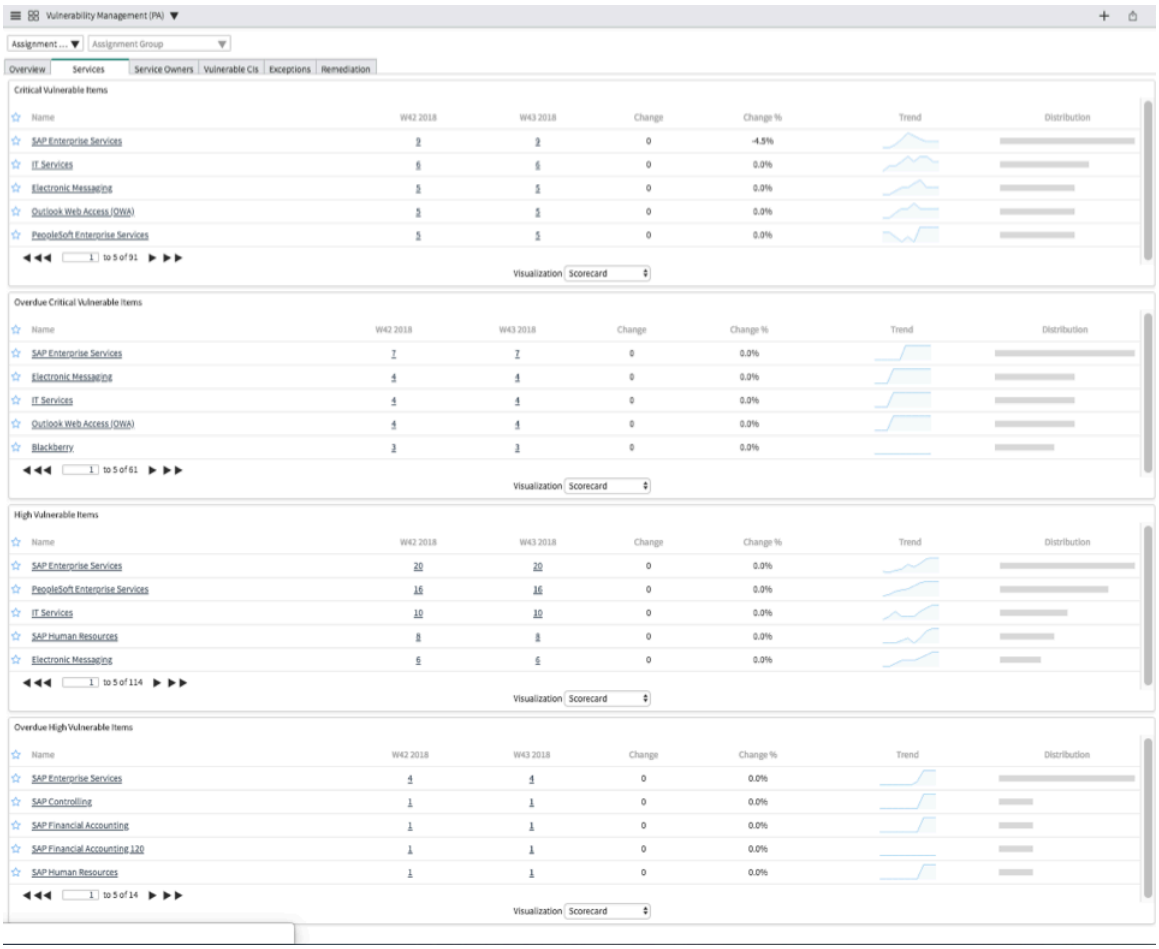


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Business Services tab

This dashboard exposes vulnerability risk at the business service level. Sharing this information across the organization can assist service managers to remediate vulnerabilities promptly and proactively, and drive the organization toward a shared responsibility model of information security.

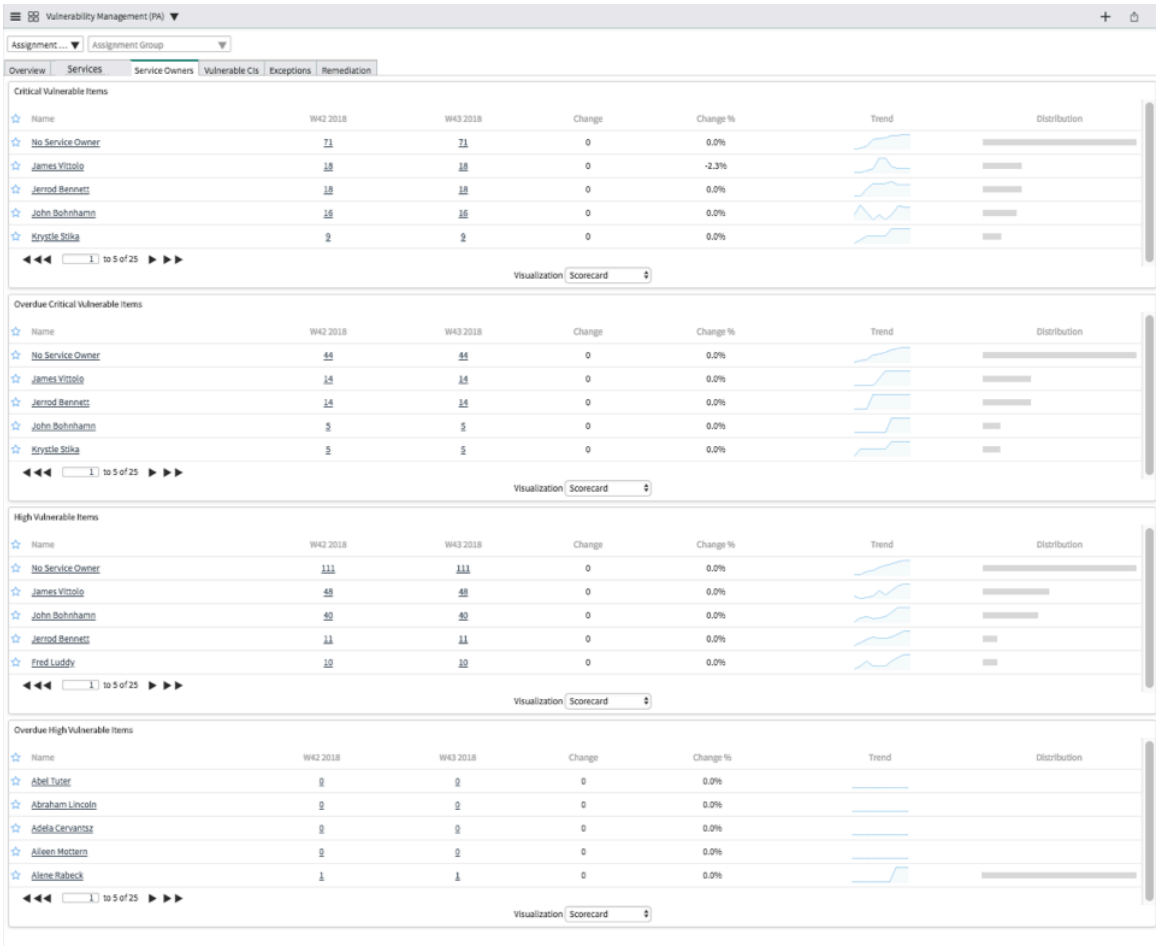
You can change the service class to technical or application services using the system property `sn_vul.service_classifications`.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Service Owners tab

This dashboard aggregates the vulnerability risk from the business service level to the service owners — the executives responsible for those business services. It shows which executives are assuming the most vulnerability risk and which may require the most help encouraging prompt remediation activities.

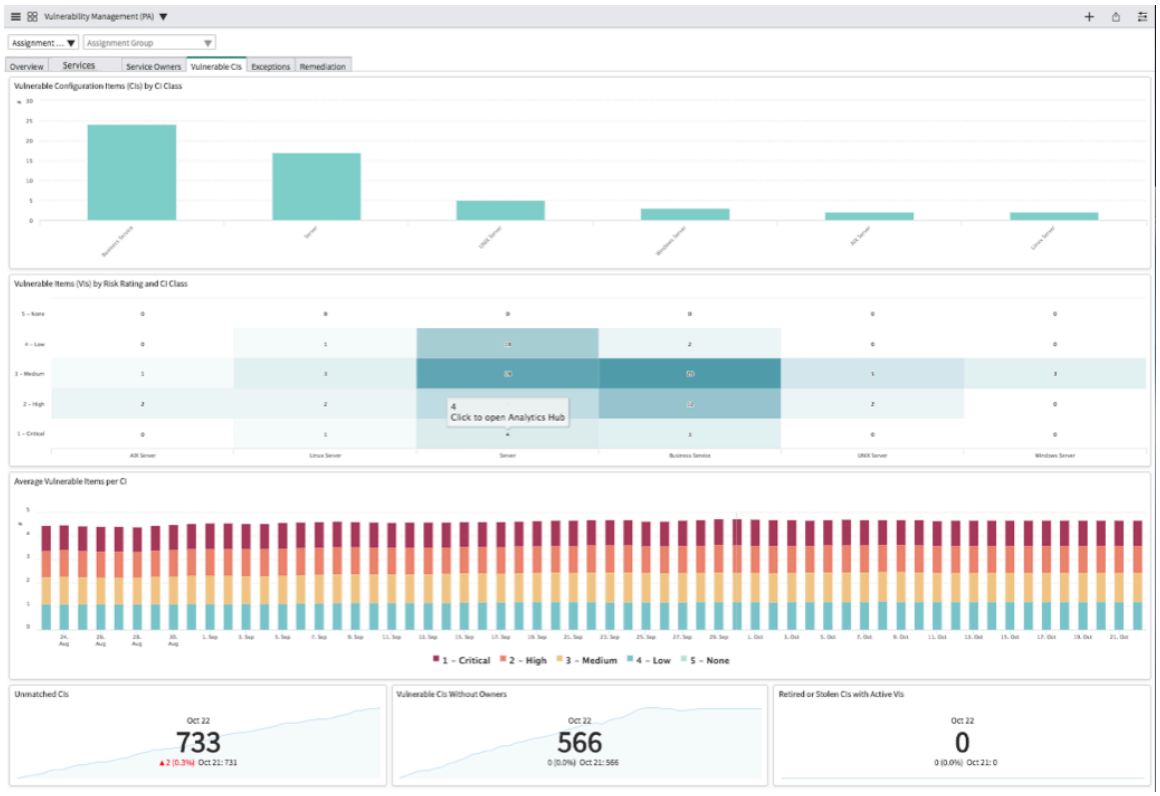


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable CIs tab

This dashboard shows the scope and composition of CIs with active vulnerabilities, and which categories of CIs need the most attention. Identify decommissioned assets with active vulnerable items and confirm that the assets have been decommissioned. View the number of vulnerable CIs that lack ownership information, so that you can proactively identify owners for these assets before a critical vulnerability affects those systems.

On the Vulnerable CIs tab, you can view the Vulnerable CIs Without Owners and Retired or Stolen CIs with Active VIs reports in real-time.

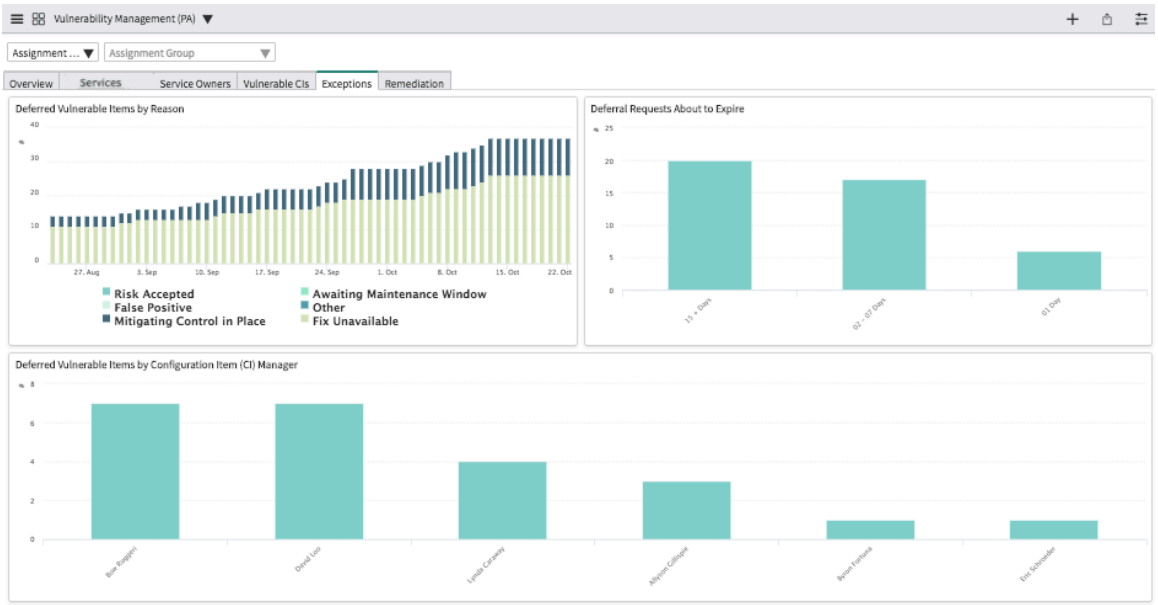


Exceptions tab

This dashboard help you understand where your organization is taking risk due to potentially excessive deferrals and reconsider remediation options.

You can view Deferred Vulnerable Items by Reason, Expiring Deferral Requests, Exceptions for Critical Vulnerable Items by Assignment Group, and Exception Requests by Requester reports.

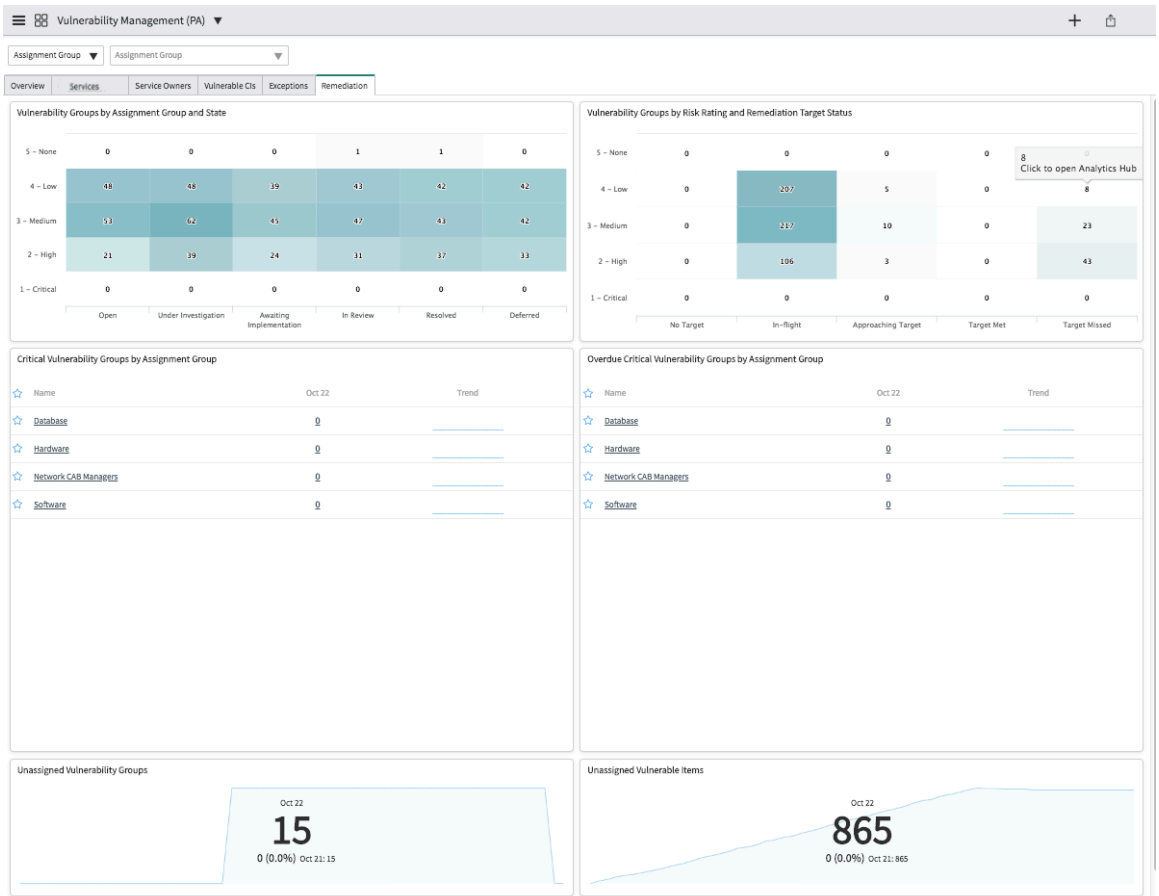
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Remediation tab

This dashboard helps you understand the progress of your remediation actions, and which support teams need the most assistance with their completion.

On the Remediation tab, you can view Unassigned Vulnerable Items report in real-time.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Indicators

Vulnerability Response indicators

There are a number of indicators used to measure and track the progress of your vulnerability remediation in the Vulnerability Response application.

The collect records option for the indicators is disabled by default for the Vulnerability Response application. This option is disabled so that certain reports can be viewed in real-time. Trending information used by these indicators is still available if you prefer to enable collect records manually and view the records that make up the scores.

Distinct Vulnerabilities

Distinct Vulnerabilities with count_active_vi > 0. Goal is to minimize.

Non-Deferred Overdue Critical Vulnerable Items

It is the count on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

% Vulnerable Items Met Remediation Target

`([[Closed Vulnerable Items > Remediation Target = Target Met]] / [[Closed Vulnerable Items]]) * 100`. Goal is to maximize.

Unassigned Vulnerable Items

All active Vulnerable Items where both the Assignment Group and Assigned To fields are empty. Goal is to minimize.

Critical Vulnerable Items (Services)

It is the count on data source Active VIs (Services), which is using the table: sn_vul_analytics_business_services_vi. Goal is to minimize.

High Overdue Vulnerable Items (Services)

It is the count on data source Active VIs (Services), which is using the table: sn_vul_analytics_business_services_vi. Goal is to minimize.

Unassigned Remediation Tasks

All active remediation tasks where both the Assignment Group and Assigned To fields are empty. Goal is to minimize.

Critical Vulnerable Items

It is the count on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Vulnerable Items

It is the count on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

New Vulnerable Items

It is the count on data source VI.New, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Vulnerable Configuration Items

It is the count distinct on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Summed Duration of Closed Vulnerable Items

It is the sum on data source VI.Closed, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Non-Deferred Remediation Tasks

It is the count on data source VG.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

Vulnerable Item Mean Time to Remediate

`[[Summed Duration of Closed Vulnerable Items]] / [[Closed Vulnerable Items]]`

Critical Overdue Vulnerable Items (Services)

It is the count on data source Active VIs (Services), which is using the table: sn_vul_analytics_business_services_vi. Goal is to minimize.

Retired Configuration Items

It is the count distinct on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Deferral Requests

It is the count on data source Active Deferral Requests, which is using the table: sn_vul_change_approval. Goal is to minimize.

Vulnerable Items by Configuration Items

It is the count on data source CIs with Active VIs, which is using the table: sn_vul_analytics_vi_ci_class. Goal is to minimize.

Closed Vulnerable Items

Closed Vulnerable Items is measured daily as unit #. The goal is to maximize.

Unmatched Configuration Items

Lists the hosts discovered by 3rd party vulnerability scanners that don't match any existing CIs in the CMDB.

Non-Deferred Overdue Critical Remediation Tasks

It is the count on data source VG.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

Vulnerable Configuration Items Without Support Group

It is the count on data source VI.Open, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Non-Deferred Critical Remediation Tasks

It is the count on data source VG.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

Deferred Vulnerable Items

It is the count on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

High Vulnerable Items (Services)

It is the count on data source Active VIs (Services), which is using the table: sn_vul_analytics_business_services_vi. Goal is to minimize.

Distinct Configuration Items with Active Vulnerable Items

It is the count distinct on data source CIs with Active VIs, which is using the table: sn_vul_analytics_vi_ci_class. Goal is to minimize.

Average Number of Vulnerable Items per Configuration Item

`[[Active Vulnerable Items]] / [[Vulnerable CIs]]`. Goal is to minimize.

Remediation Tasks

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

It is the count on data source VG.Active, which is using the table: sn_vul_vulnerability. Goal is to minimize.

Critical Deferred Vulnerable Items

It is the count on data source VI.Active, which is using the table: sn_vul_vulnerable_item. Goal is to minimize.

Deferral Requests (created)

It is the count on data source Closed.Requests, which is using the table: sn_vul_change_approval. Goal is to minimize.

Breakdowns

The following breakdown names apply to the indicators on the dashboard:

- Age
- Age Closed
- Assignment Group
- CI Class
- CI Manager
- Deferral Age
- Deferral Reason
- Exception Requesters
- Exploit Attack Vector
- Exploit Exists
- Exploit Skill Level
- Remediation Target Rule
- Remediation Target Status
- Remediation Target Status (Closed)
- Risk Rating
- Service
- Service Criticality
- Service Owner
- Severity
- State

Breakdown source

- Assignment Group: Applies to VI or and RT reports
- Exploit Exists: Applies to VI reports.
- Exploit Attack Vector: Applies to VI reports.
- Exploit Skill Level: Applies to VI reports.
- Remediation Target Status: Applies to VI and RT reports.
- Risk Rating: Applies to VI and RT reports.
- State: Applies to VI and RT reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data visualizations

Title	Type	Description
Vulnerabilities	Single Score	Number of vulnerabilities associated with one or more active vulnerable items.
Vulnerable Items (VIs)	Single Score	Number of active (non-closed) vulnerable items.
Vulnerable Configuration Items (CIs)	Single Score	Number of configuration items (CIs) associated with one or more active vulnerable items.
Remediation Tasks	Single Score	Number of active (non-closed) remediation tasks.
Vulnerable Items by Risk Rating	Bar	Number of active vulnerable items grouped by risk rating over the selected time span.
Vulnerable Items by Age and Risk Rating	Heatmap	Number of active vulnerable items grouped by risk rating and age (in days).
VIs Met Remediation Target	Single Score	Percentage of closed vulnerable items that have met their remediation target dates in the current and previous quarters. Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments).
VIs Mean Time to Remediation (MTTR)	Single Score	The mean time to remediate (close) a vulnerable item, displayed as a 30-day running average. **Note:** The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
Critical Remediation Tasks Near Due	Single Score	Number of active remediation tasks approaching their remediation target date. The remediation target date of a remediation task is set to the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Title	Type	Description
		closest due date belonging to an active vulnerable item in the group. Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments). This report excludes deferred remediation tasks.
New and Closed Vulnerable Items	Bar	Number of New and Closed vulnerable items over the selected time span. **Note:** The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
Closed Vulnerable Items by Remediation Target Status	Bar	Number of Closed vulnerable items grouped by remediation target status over the selected time span. **Note:** The value for Age Closed is calculated when data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
Critical Vulnerable Items by Assignment Group	List and Line	Number of active vulnerable items with a critical risk rating grouped by assignment group.
Overdue Critical Vulnerable Items by Assignment Group	List and Line	Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by assignment group. Remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Title	Type	Description
		This report excludes deferred vulnerable items.

Business Services

Name	Type	Description
Critical Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a critical risk rating, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.
Overdue Critical Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.
High Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a high risk rating, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.
Overdue High Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a high risk rating and past their remediation target dates, grouped by business service. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Service Owners

Name	Type	Description
Critical Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a critical risk rating, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.
Overdue Critical Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a critical risk rating and past their remediation target dates, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.
High Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a high risk rating, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard.
Overdue High Vulnerable Items	List, Line, and Distribution Bar 	Number of active vulnerable items with a high risk rating and past their remediation target dates, grouped by business service owner. Displays a weekly average from the current and prior week, the difference between the two weeks (in count and percent), and a trend. The distribution bar displays the difference between all values on the current page of the scorecard. This report excludes deferred vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable CIs

Name	Type	Description
Vulnerable Configuration Items (CIs) by CI Class	Bar	Numbers of configuration items with active vulnerabilities, grouped by CI class in the CMDB.
Vulnerable Items (VIs) by CI Class	Treemap	Number of active VIs broken down by CI class.
Average Vulnerable Items per CI	Bar	Average number of vulnerable items belonging to a configuration item, grouped by risk rating.
Unmatched CIs	Single Score	Number of imported configuration items that do not match any existing CI in the CMDB.
Vulnerable CIs Without Support Group	Single Score	Number of vulnerable configuration items that do not have an assigned support group.
Retired or Stolen CIs with Active VIs	Single Score	Number of configuration items marked **Retired** or **Stolen** in the CMDB that have active vulnerable items.

Exceptions

Name	Type	Description
Deferred Vulnerable Items by Reason	Bar	Number of deferred vulnerable items grouped by deferral reason.
Deferral Requests About to Expire	Bar	Number of deferral requests associated with remediation tasks or vulnerable items that are about to be reopened for review. They are grouped by the number of days left until they reopen. If email notifications are defined, an email is sent.
Deferred Vulnerable Items by Configuration Item (CI) Manager	Bar	Number of deferred vulnerable items grouped by the manager for the associated configuration item.

Remediation

Name	Type	Description
Remediation Tasks by Risk Rating and State	Heatmap	Number of active remediation tasks grouped by risk rating and state.
Remediation Tasks by Risk Rating and Remediation Target Status	Heatmap	Number of active tasks grouped by risk rating and remediation target status. This report excludes deferred vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation (continued)

Name	Type	Description
Critical Remediation Tasks by Assignment Group	List and Line	Number of active remediation tasks with a critical risk rating grouped by assignment group. This report excludes deferred remediation tasks.
Overdue Critical Remediation Tasks by Assignment Group	List and Line	Number of active remediation tasks with a critical risk rating and past their remediation target dates, grouped by assignment group. This report excludes deferred remediation tasks.
Unassigned Remediation Tasks	Single Score	Number of active remediation tasks without an assignee or assignment group.
Unassigned Vulnerable Items	Single Score	Number of active vulnerable items without an assignee or assignment group.

View Performance Analytics for Vulnerability Response [PA] reports in real-time

To manage your most important vulnerable items (VIs) and help you remediate them quickly, view reports on-demand, in real-time on the Vulnerability Management (PA) dashboard. The Performance Analytics for Vulnerability Response application is available with a separate subscription from the ServiceNow Store.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

For more information about the reports for Performance Analytics for Vulnerability Response, see Vulnerability Management [PA] dashboard.

For more information about the setup and installation of the Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

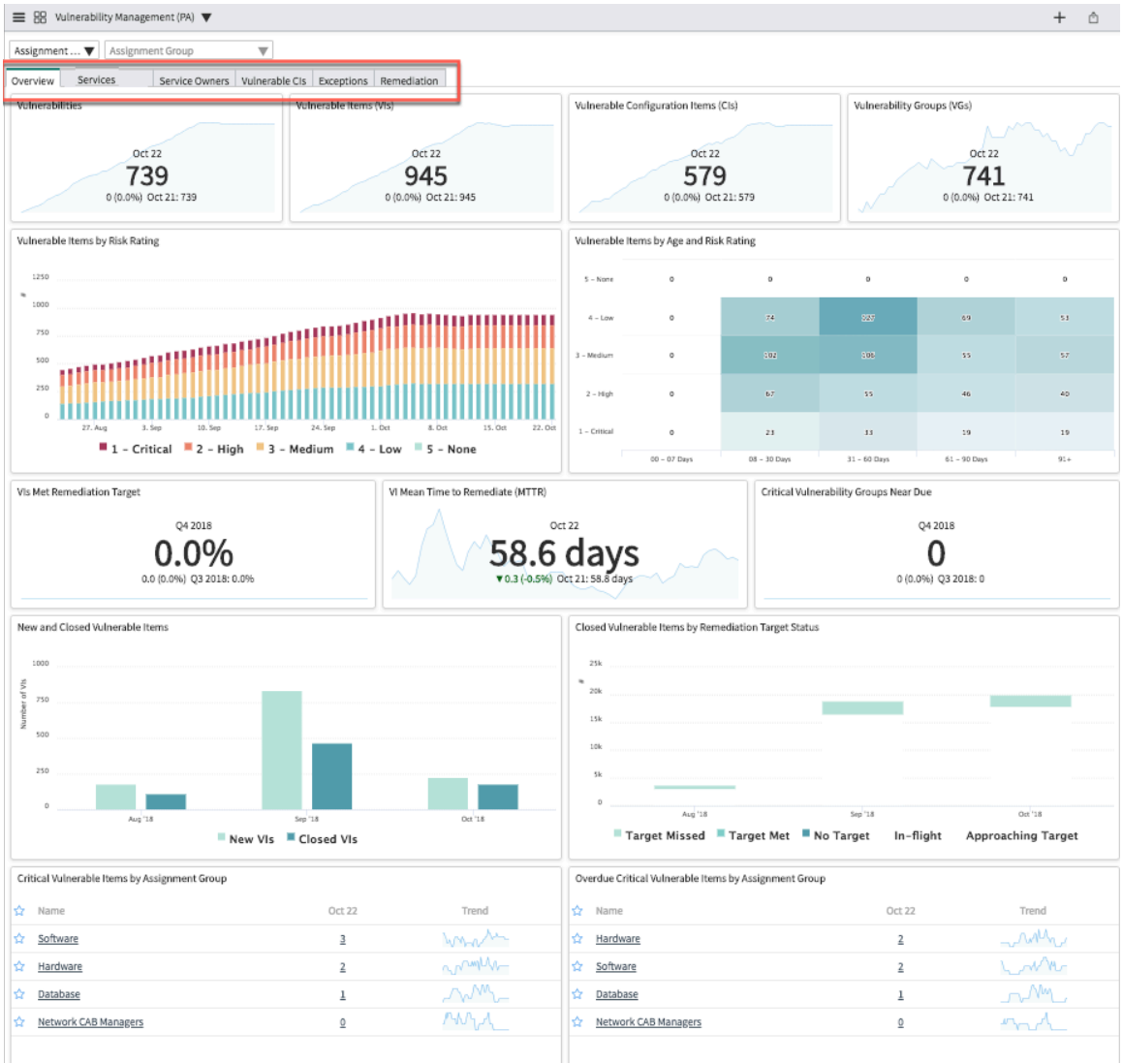
If not displayed, to view the dashboard, navigate to **Vulnerability Response** > **Overview**. At the top of the dashboard the report tabs are displayed.

Starting with version 19.0 of Vulnerability Response, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab



View the following reports on the tabs of the Vulnerability Management (PA) dashboard in real-time.

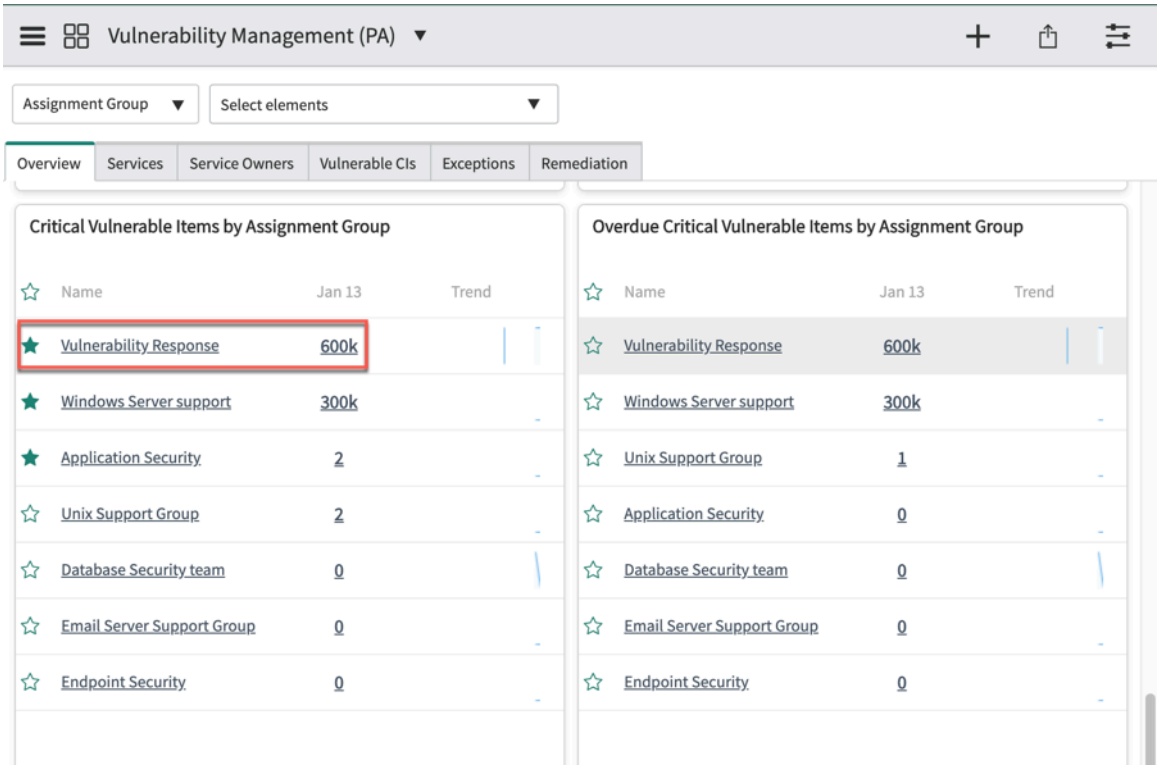
- Overview tab
  - Critical Vulnerable Items by Assignment Group
- Vulnerable CIs tab:
  - Vulnerable CIs Without Owners
  - Retired or Stolen CIs with Active VIs
- Exceptions tab:
  - Deferred Vulnerable Items by Reason
  - Deferral Requests About to Expire
  - Deferred Vulnerable Items by CIO Manager
- Remediation tab:
  - Unassigned Vulnerable Items

To view real-time scores, with one of the tabs selected that contains real-time reports, follow these steps:

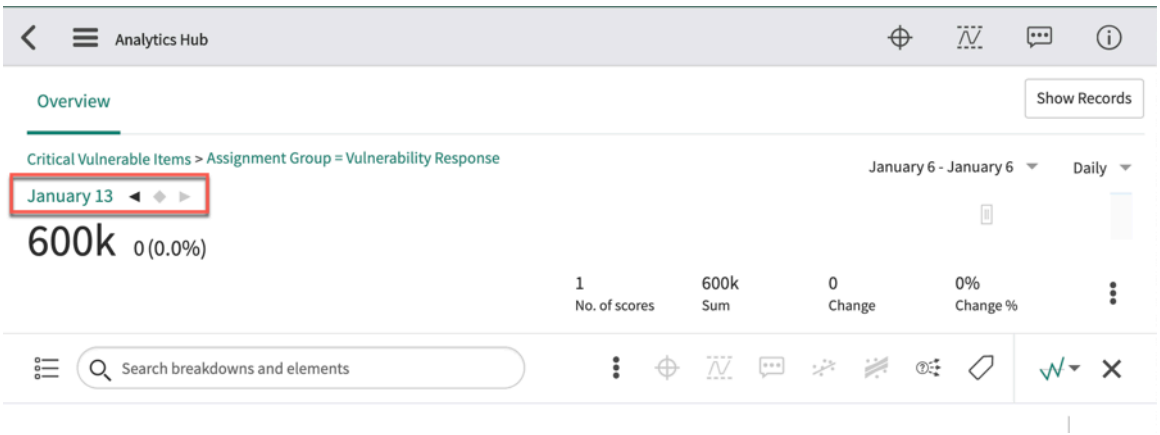
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the report, for example, Critical Vulnerable Items by Assignment Group, click one of the links that is displayed.



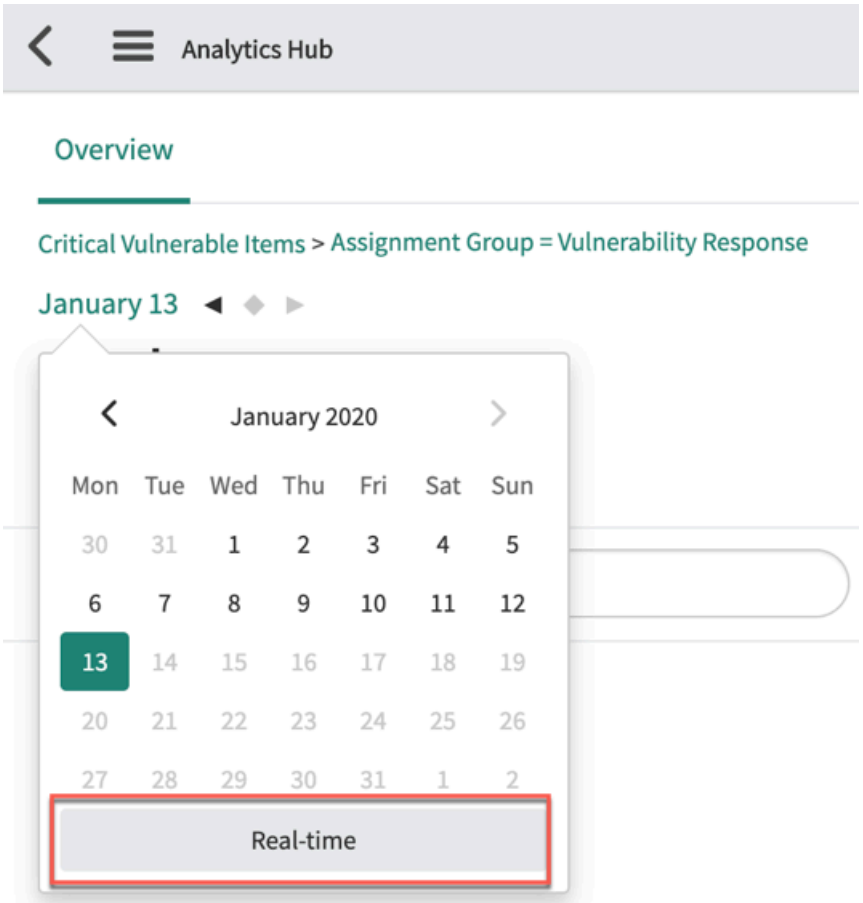
2. In the record that is displayed, click the date.



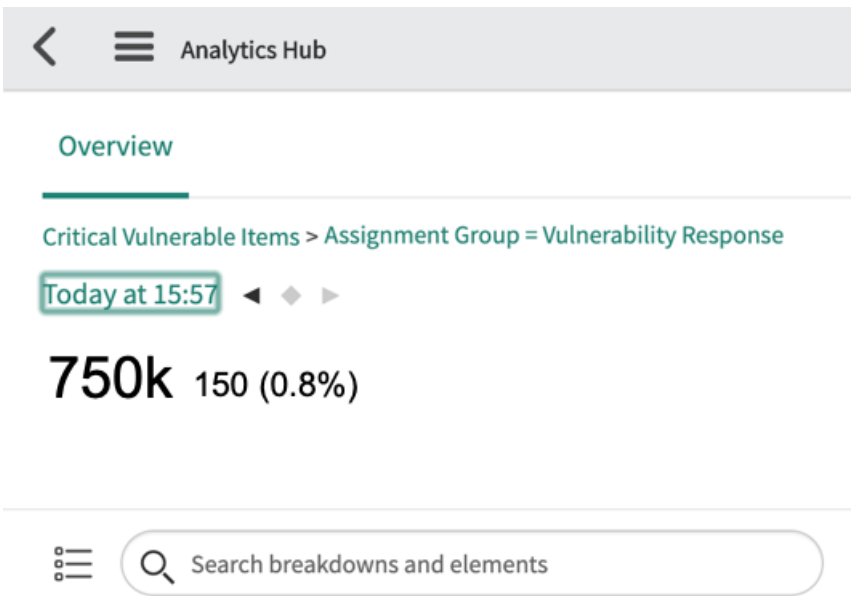
3. In the calendar that is displayed, click Real-time.

   If a report does not support a real-time score, the Real-time button is not displayed on the calendar.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



It may take a few moments for the value to update. The current date, the records, the number of new records since the last report, and the percent change from the last report are also displayed.



4. **Optional:** To view the records that make up the report, with the real-time report displayed, in the upper right, click **Show records**.
   A list of records that make up the score is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View the Performance Analytics indicators for Vulnerability Response [PA]

View automated and formulated Performance Analytics indicators representing the vulnerability data in your instance.

Before you begin

The collect records option for the indicators is inactive by default for the Performance Analytics - Content Pack Vulnerability Response application. This option is disabled so that certain reports can be viewed in real time. Trending information used by these indicators is still available if you prefer to enable collect records manually and view the records that make up the scores.

Note: Activating collect records in an indicator may impact your performance and considerably lengthen the time and memory required to run the data collection job.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated), or pa.viewer

About this task

Vulnerability Response has both automated and formulated indicators.

Key terms

PA indicator

Defines a performance measurement taken at regular intervals of a business service, activity, or organizational behavior, for example, Non-Deferred Overdue Critical Vulnerable Items.

PA indicator source

Data sets that filter records from one table or database view, for example, VI Active.

Collect records

When enabled, stores records in memory and provides access to Analytics Hub.

Breakdowns

Breakdowns filter and group collected records. Breakdowns may increase memory use, especially as their number and diversity increase.

Breakdown exclusions

Exclusions remove certain breakdowns, which may reduce memory consumption.

Procedure

1. For automated indicators, navigate to **Performance Analytics** > **Indicators** > **Automated Indicators**.
2. For formulated indicators, navigate to **Performance Analytics** > **Formula Indicators**.

   For detailed information on indicators, see Performance Analytics Indicators.
3. In either case, search on **Application** > **Performance Analytics**.

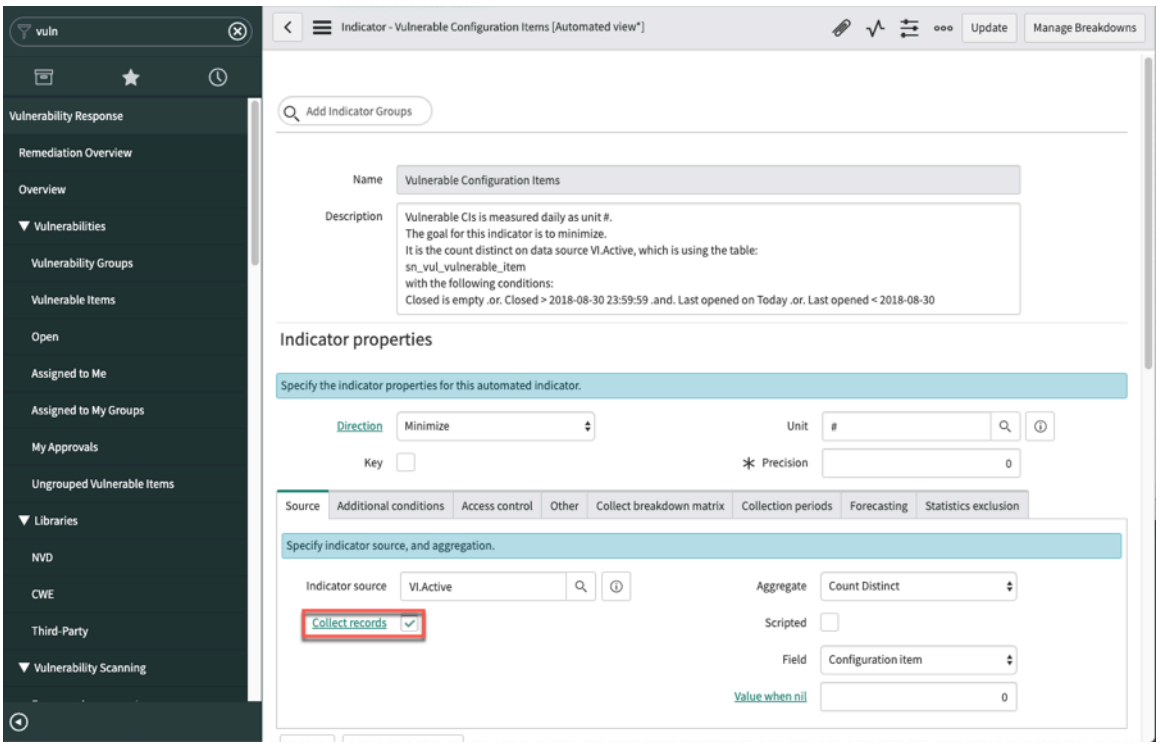
   Note: If it is not in your default view, add the **Application** column using the gear icon ( ) in the upper left corner of the page. The Application column is then displayed in your Search drop-down menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. **Optional:** To enable Collect records on a Performance Analytics for Vulnerability Response indicator, follow these steps:

   a. With the list of automated indicators displayed, in the Name column, click the indicator you want to enable collect records for.
   The indicator record is displayed.

   b. In the Indicator properties section with the Source tab selected, select the Collect records check box.



   c. Choose one to continue.

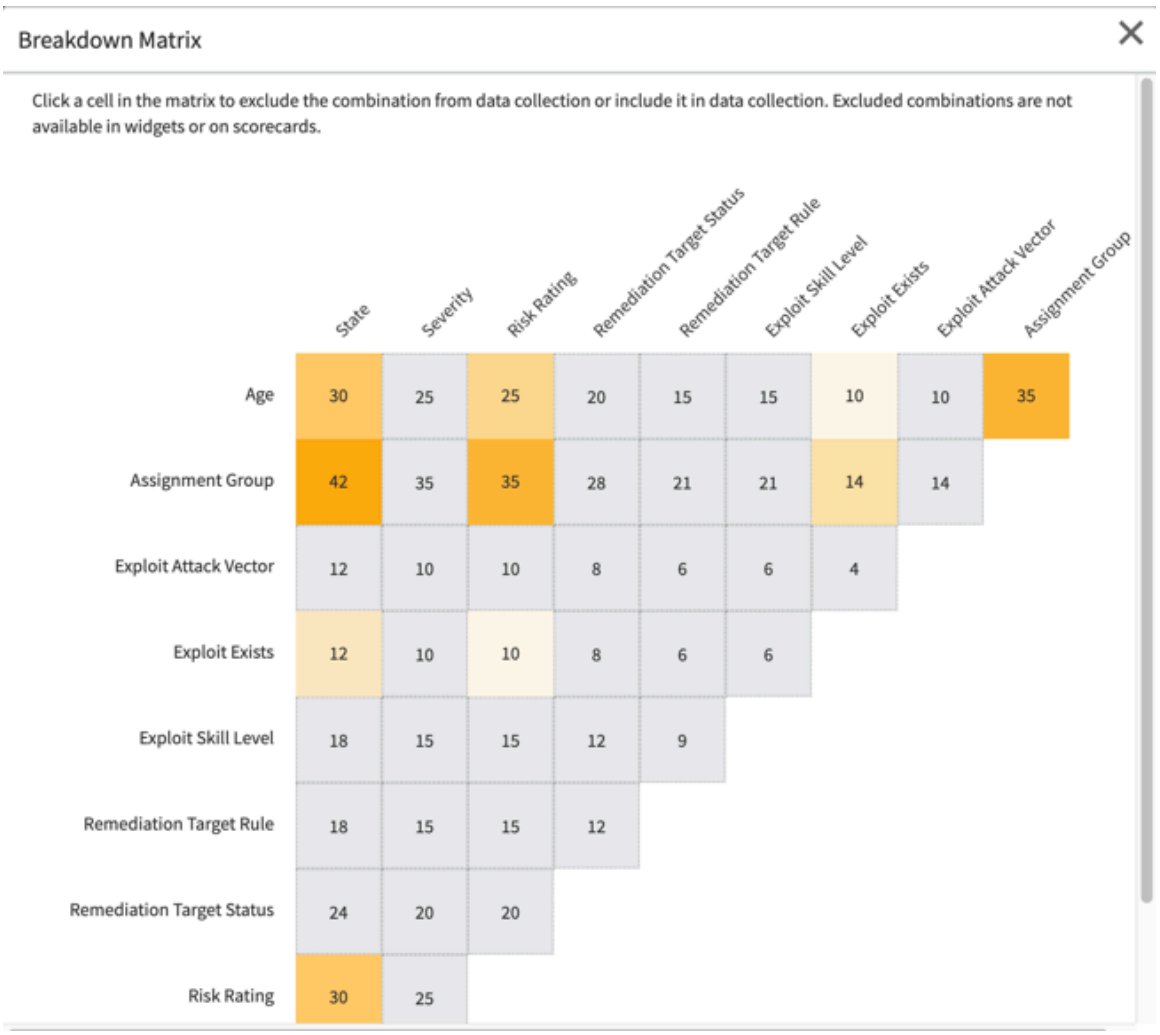
Option	Description
Update	Save your edits and return to the Indicators list.
Manage Breakdowns **Note:** If you choose to reactivate second-level breakdowns, you may significantly increase your memory consumption and slow the data collection job. By default, second-level breakdown exclusions have been applied to the following indicators:	Reactivate second-level breakdowns for the listed indicators, or, edit breakdowns for other indicators. (Optional) For more information on Performance Analytics breakdowns, see Performance Analytics Breakdowns.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
▪ Vulnerable Configuration Items ▪ Retired CIs ▪ Deferred VIs	

d. Click **Manage Breakdowns**.

e. In the form that is displayed, click **Configure Breakdown Matrix**.
The Breakdown Matrix form is displayed. Excluded combinations are selected and displayed with colors, as shown in the following figure.



f. To remove the exclusion and reactive an excluded combination, click a selected cell.

g. In the upper right of the form, click **Close** to return the Manage Breakdown form.

h. Click the back arrow to return to the indicator record.

i. Click **Update** to save your edits and return to the Indicators list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Aggregated reports framework

Using aggregated reports framework, you can create reports for the data that involves complex and long-running on-the-fly queries for better performance.

The aggregated reports framework improves the performance by:

- using lesser resources and rendering reports faster,
- aggregating the data and reusing aggregations and breakdowns (Group By) and
- reducing the queries to the database

When you have more than one million vulnerable items, use the framework provided in Vulnerability Response Common alongside standard reports.

Required roles

The following roles and tasks are associated with this solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Platform Analytics Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the aggregations, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.
- Admin (sn_vul_cmn.admin): Create aggregations.
- VR write(sn_vul_cmn.write): Edit the data in the Aggregations and Aggregated Results.
- VR read (sn_vul_cmn.read): Review the data in the Aggregations and Aggregated Results.
- Vulnerability analyst (sn_vul.vulnerability_analyst): Review Aggregated Results.

Related topics

Configure an aggregation for source data

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Create a report using an aggregation

Configure an aggregation for source data

To analyze the performance of a specific facet in a business process that is recorded in a ServiceNow table, create an aggregation specific to the facet and create a report for this aggregation.

Before you begin

Role required: sn_vul_cmn.admin

Procedure

1. Navigate to **All** > **Aggregated Reports** > **Aggregation definitions** > **All** and click **New**.
2. In the **Name** field, give the aggregation a descriptive name.
3. In the **Description** field, provide a brief description about the aggregation.
4. In the **Source** tab, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source tab fields

Field	Description
Table	Table from which you want to fetch the data for the report. This drop-down contains app sec common, app-vul, app-vulc, app-vul-container, and application vulnerability tables only.
Aggregate function	Function to be applied to the column selected in **Field**. ○ **Count**: Number of records. ○ **Sum**: Total sum of the values in the column selected in **Field**. ○ **Average**: Average of all the values in a column selected in **Field**. ○ **Maximum**: Maximum value in the column selected in **Field**. ○ **Minimum**: Minimum value of the column selected in **Field**. ○ **Count Distinct**: Unique values in the column selected in **Field**.
Field	Column on which you want to apply the function. **Note:** This field doesn't appear when you select **Count** in the **Aggregate function** field.

5. In the **Additional Conditions** tab, provide the condition in the **Conditions** field to select a particular set of records for which you want to get the aggregated results.
6. In the **Group By** tab, select the columns of the table by which you want to group or stack the data.
   You can select up to two breakdowns.

   If you select the **date** column in any group by field, the **Trend by** field appears. You can get the aggregation results that are categorized by week, day, minutes, etc by selecting the options in the **Trend by** field.
7. In the **Schedule** tab, select or create an aggregation schedule, which defines the frequency at which you can execute the aggregation to fetch the data.
   To create an aggregation schedule, see Run multiple aggregations simultaneously.

   Note: You cannot schedule the aggregation run for an inactive aggregation definition.
8. Click **Submit** to create the aggregation.
   The aggregation appears in the Aggregation list. At the predefined frequency, the aggregation is executed, and a record is created along with an execution date and time in the Scheduled Runs related list for every execution.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Navigate to **All** > **Aggregated Results** and open your aggregation to see the Aggregated Results and Scheduled Runs.
   The aggregated results are listed in the **Aggregated Results** related list. If the aggregation run fails, see the **Notes** column in the **Scheduled Runs** related list for more information.
10. **Optional:** Select **Execute Now** to collect the aggregation results irrespective of the aggregation schedule.
    If you terminate the scheduled run when it is in progress, then no changes are made to the aggregated results. You can also delete or deactivate an aggregation.

What to do next

Create a report using your aggregation. For more information about creating a report using an aggregation, see Create a report using an aggregation.

Related topics

Aggregated reports framework

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Create a report using an aggregation

Run multiple aggregations simultaneously

You can schedule the execution of multiple aggregations using a single Aggregation schedule.

Before you begin

Role required: sn_vul_cmn.admin

About this task

Suppose you want to execute six aggregations at the same time. Create an aggregation schedule and add all the aggregations to it. These aggregations are executed at the defined frequency and time.

Procedure

1. Navigate to **All** > **Aggregated Reports** > **Schedule**.
2. Select **New**.
3. On the Aggregation schedule form, fill in the fields.

Field	Description
Schedule name	Name of the aggregation schedule.
Schedule job	Scheduled Script Execution that defines the frequency at which the aggregations must run. You can create a schedule job by selecting the **New** button.

4. Select **Submit**.
   The aggregation schedule appears in the Aggregations schedule list.
5. Open your aggregation schedule.
6. Select **Edit**, add the aggregations to the **Aggregation List**, and select **Save**.
   The selected aggregations appear in the Aggregations related list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you add an inactive aggregation to a schedule, the scheduled run will not be commenced.

7. Select **Update**.
   These aggregations are executed at the frequency defined in the aggregation schedule.

Related topics

- Aggregated reports framework
- Configure an aggregation for source data
- Configure the number of aggregations that can run simultaneously
- Create a report using an aggregation

Configure the number of aggregations that can run simultaneously

A new processor or a background job, Aggregated Reporting Framework Processor is shipped with the base system, which executes the scheduled jobs that are related to the Aggregated Reports Framework table. This enables the entire subsystem to run in the background, and it allows better utilization of system resources when they're available.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **Background Job Configuration – Vulnerability Response Common-Aggregation Result Calculator**.
2. Define the number of aggregations that you want to execute simultaneously in the **Max concurrent threads** filed and select **Save**.
   By default, four aggregations are executed simultaneously.
3. Navigate to the Background Job Processor Pools list, **sn_sec_cmn_background_job_processor_pool.list**, and select **New** to create a background job processor for Aggregated Reports Framework.
   For more information on how to create a background job processor pool, see Advanced parallel processing for background jobs in Vulnerability Response.

Note: The number of background job processors must be equal to the number of maximum concurrent threads provided in the **Background Job Configuration – Vulnerability Response Common-Aggregation Result Calculator** form. See Step 2.

Related topics

- Aggregated reports framework
- Configure an aggregation for source data
- Run multiple aggregations simultaneously
- Create a report using an aggregation

Create a report using an aggregation

To visualize and analyze the data specific to an aggregation that you created, generate a report by providing a condition for the aggregation in the condition builder.

Before you begin
Role required: pa_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Reports** > **Create New**.
2. In the **Data** tab, fill in the fields.

Data tab fields

Field	Description
Report name	Name of the report.
Source type	Type of the source from which data is fetched. Select **Table**.
Table	Name of the table for which the aggregation is created. Select the aggregated results table, **Aggregated Result [sn_vul_cmn_aggregate_result]**.

3. In the condition builder, set the condition for your aggregation for which you want to generate a report.

Condition in the condition builder

Part	Description
Field	Select **Aggregation**.
Operator	Select **is**.
Value	Name of the aggregation.

4. In the **Data** tab, click **Next**.
5. In the **Types** tab, select how you want to visualize the data and click **Next**.
   To know more about report types, see Creating Reports.

   The supported visualizations are bar chart, pie chart, and heatmap. You can modify the line graphs and other trends visualisations to make use of the supported visualisations with aggregated result to represent the same data. List view is not supported.
6. In the **Configure** tab, fill in the fields.

Field	Description
Group by	Select **Grouped by 1** that you selected in the **Group By** tab for the aggregation.
Stack by	Select **Grouped by 2** that you selected in the **Group By** tab for the aggregation.
Aggregation	Apply **Minimum** or **Maximum** function on **Value**.

7. In the **Style** tab, fill in the fields as appropriate and click **Run**.
   For more information about the fields in **Configure** and **Style** tabs, see the Creating a report video.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. In the condition builder, set the condition for your aggregation for which you want to generate a report and click **Run**.

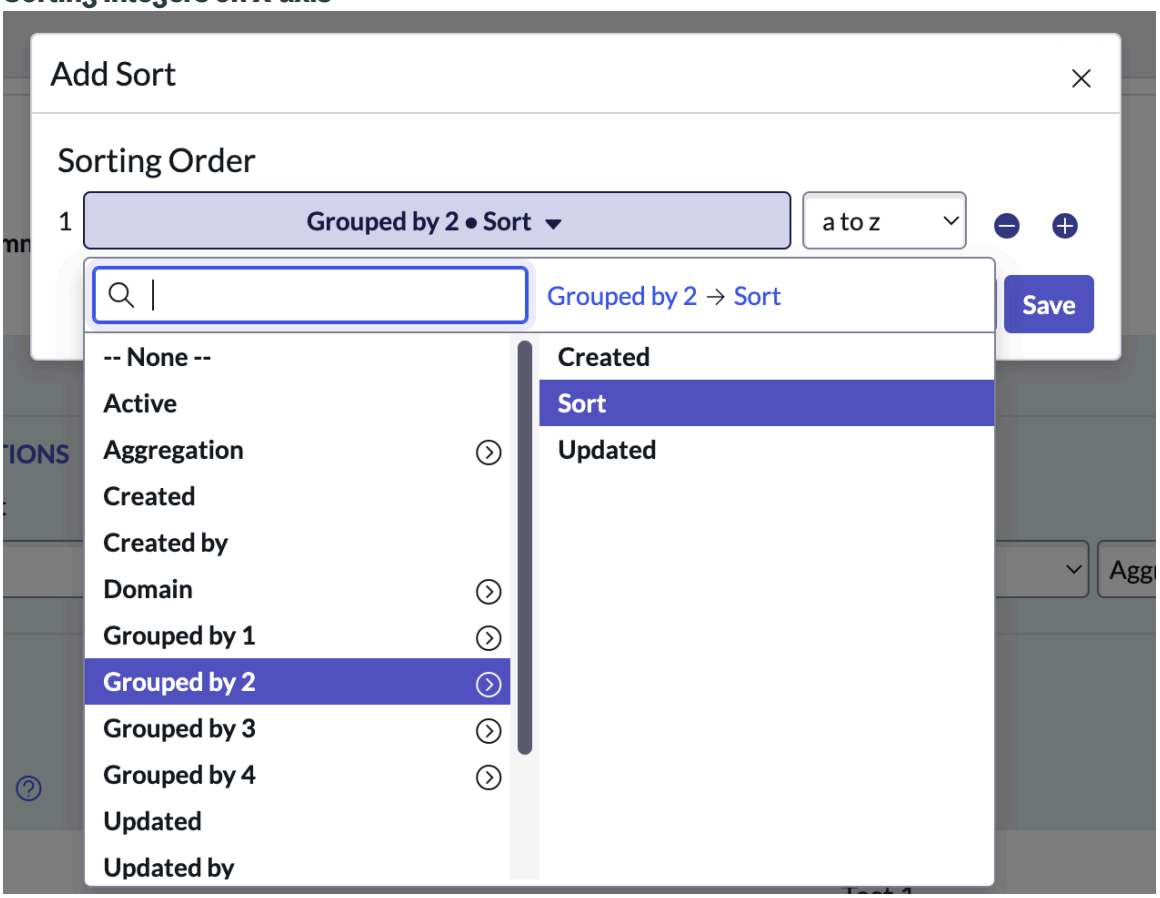
   The report displays.

9. To sort the values on the x-axis, select **Add sort**.

   a. For strings, provide the condition as **Grouped by > a-z or z-a** to sort the strings in an alphabetical order.

   b. For integer and date data type values, provide the condition as **Grouped by.sort > a-z or z-a** to sort the values in ascending and descending order respectively.

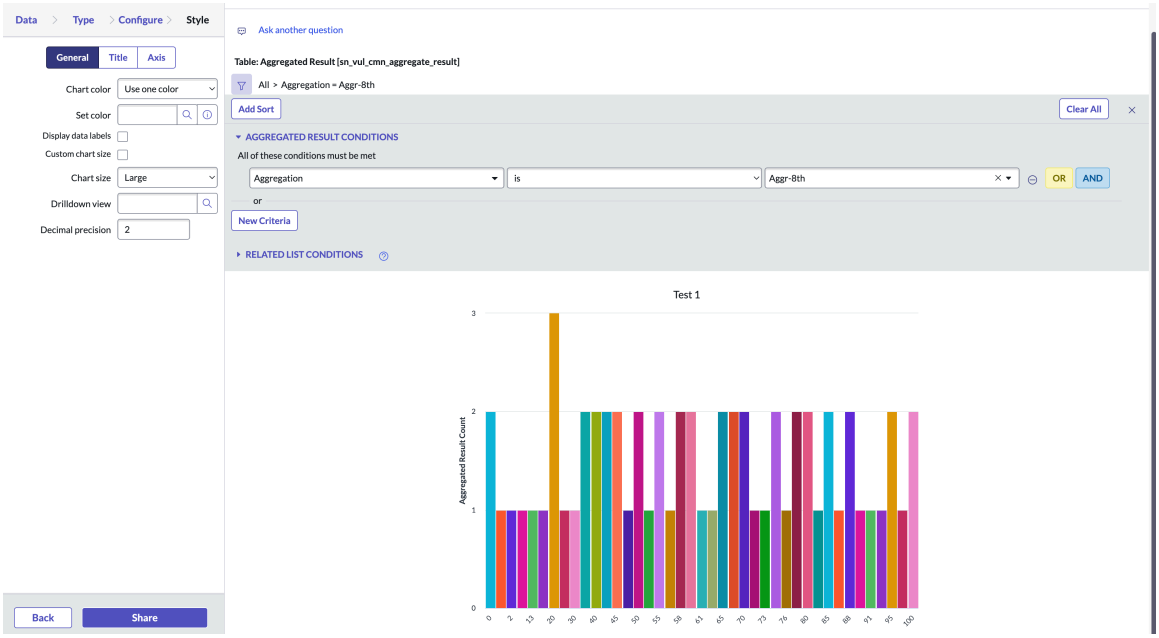
Sorting integers on X-axis



   c. Select **Run**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The integer and date values get sorted on the X-axis.



10. Click **Save** to save your report.
    The report that is generated for an aggregation displays in the **Results** tab of the respective **Aggregation** form.
11. **Optional:** Add your report to a dashboard.
    For more information on how to add a report to a responsive dashboard.

    The **Vulnerability Management[Aggregated]** dashboard consisting of reports created using the cached reporting framework is shipped with the base system. To view this dashboard, navigate to **All** > **Performance Analytics** > **Dashboards** > **All** > **Vulnerability Management[Aggregated]**. The active aggregations corresponding to the reports in this dashboard are shipped with the base system.
12. Share your report with other users.
    For more information on how to share reports, see Distribute reports.

Related topics

Configure an aggregation for source data

Aggregated reports framework

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Vulnerability Response reference information

The following topics provide you with links, reference information, troubleshooting, and knowledge articles, in addition to field data on the forms and records found in Vulnerability Response.

Listed below are some links to other resources you might find helpful, starting with a link to the Knowledge base links for Support and Troubleshooting VR/CC article in the HI Knowledge Base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Knowledge base links for Support and Troubleshooting VR/CC
- For more information about applications and compatibility, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes.
- Security Operations videos
- Developer training
- Developer documentation
- Work with an implementation specialist to achieve your desired business outcomes with the Customer Success Center.
- Take a Vulnerability Response course to build expertise and realize ROI faster. To sign up, see ServiceNow training and certification.
- Find components installed with an application
- Vulnerability Response Orchestration
- Tips for writing integrations
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Implementation checklist for the Vulnerability Response application

This checklist lists the steps required for a basic implementation of the Vulnerability Response application on your ServiceNow AI Platform® instance. When you have completed these tasks, the base system is ready for operation and verification.

Before you begin

Roles required: admin for downloading and activating applications and assigning roles, sn_vul.vulnerability_admin for configuring Vulnerability Response.

Procedure

1. Consider creating and printing a PDF of this checklist so that you can check off tasks as you complete them.
2. To generate a PDF, click the **Save As PDF** icon ( ) at the top of the topic and click Selected topic.

Vulnerability Response basic implementation checklist tasks for admin

Item	Description
☐	As a user with the admin role, verify that you have the obtained any entitlements and downloaded (**Install**) the following applications from the ServiceNow® Store onto your ServiceNow AI Platform instance: ○ Vulnerability Response ○ Vulnerability Response Integration with the NIST National Vulnerability Database ○ Qualys Integration for Security Operations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
	a. To verify the applications are available on your instance, navigate to **All** > **System Applications** > **All Available Applications** > **All** and search for [sn_vul], [sn_vul_nvd], and [sn_vul_qualys]. **b.** If you can't locate the applications, see Security Operations and the ServiceNow Store for more information about getting entitlement and downloading the applications.
☐	As a user with the admin role, navigate **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Application Installation** and activate (**Install**) the Vulnerability Response application along with its dependencies on your ServiceNow AI Platform instance. **Note:** During installation of the Vulnerability Response application, you have the option to install demo data. Demo data is required if you want to run automated tests to confirm that your instance works after installation. Run tests only on development, test, and other non-production instances to avoid data corruption and outage. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production. The Setup Assistant for Vulnerability Response is installed automatically along with the application. The Setup Assistant is required to configure the Vulnerability Response application. Additionally, it is used to install and configure the Qualys Integration for Security Operations application used in this example, as well as other applications that support and are compatible with Vulnerability Response. For more information about installing the Vulnerability Response application, see Install Vulnerability Response.
☐	As a user with the admin role, in Setup Assistant, navigate to **All** > **Vulnerability Response Users and Groups** and assign users with the required Vulnerability Response persona roles. **a.** From within Setup Assistant, view existing users and any roles that are already assigned by clicking the **User Administration module** link. **b.** From the list, click a user name to open the record and click the **Roles** related list. All the roles assigned to this user are displayed. **c.** Navigate back to **Vulnerability Response Users and Groups** in Setup Assistant and follow the prompts to assign the sn_vul.vulnerability_admin role. **Note:** The sn_vul.vulnerability_admin role is required to continue with the configuration. Alternatively, you can continue with the configuration as a user with the admin role. (Optional) You can also assign the Configuration Item (CI) Manager [sn_vul.ci_manager] and Exception Approver [sn_vul.exception_approver] roles, but these personas are not required for the remaining setup tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
	For more information about assigning the persona roles using the Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information on users and assigning roles to users and groups, see User administration.
☐	**a.** Navigate to **All** > **Administration** > **Integrations** and verify the **CWE Comprehensive 2000 Integration** is activated and run the scheduled job to import data. **b.** As a user with the admin role, navigate to **System Applications** > **All Available Applications** and activate (**Install**) the Vulnerability Response Integration with NVD application. Run the NVD and CWE integrations as part of your initial setup of Vulnerability Response and prior to importing vulnerability data into your instance with a third-party scanner product. See Importing data with the NVD and CWE integrations and managing third-party libraries and Configure and run the scheduled job for updating CWE records for more information about installing, configuring, and viewing the NVD and CWE libraries.
☐	As a user with the admin role, navigate **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration Application Installation** and activate the Qualys Integration for Security Operations application. Before you install and run a third-party scanner product like Qualys that has a library, you must first install and run the NVD and CWE Integrations to ingest vulnerability data. For more information, see Install Vulnerability Response third-party applications using Setup Assistant.
☐	(Optional) As a user with the admin role, if you installed demo data with the Vulnerability Response application, you can run the Vulnerability Response ATF Test Suite to verify the applications successfully installed. **Note:** Run tests only on development, test, and other non-production instances to avoid data corruption and outage. For more information, see Run the Automated Test Framework (ATF) test suite for Vulnerability Response. For more information about automated tests, see Automated Test Framework (ATF).

3. Continue with the configuration of the applications starting in the Vulnerability Response Settings section.

   Reviewing these settings helps you understand how Vulnerability Response works as you continue to set up your environment. For the scanner integration used in this example, you are required to edit the settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The concepts you use in this configuration example for the Qualys product apply to other scanner applications.

Your Qualys credentials are required to configure the application. Verify you have any account names, passwords, and other service information required by Qualys products so that you have access to them.

Roles required: sn_vul.vulnerability_admin or, alternatively, admin.

Vulnerability Response basic implementation checklist tasks for vulnerability admin

Task	Description
☐	Review the Vulnerability Assignment Rules. Assignment rules automatically assign vulnerable items (VIs) to the appropriate assignment group. For more information, see, Vulnerability Response assignment rules overview. For more information about configuring Vulnerability Response using the Setup Assistant, see Configuring Vulnerability Response using the Setup Assistant.
☐	Review the remediation task rules. Remediation task rules automatically group vulnerable items (VIs) as they are imported based on certain conditions. For more information, see Vulnerability Response remediation tasks and remediation task rules overview.
☐	Review the Risk Calculators. Risk calculators score vulnerable items for prioritization. You can configure calculators to incorporate characteristics of the configuration item (CI), exploit availability, and vulnerability severity reported by your vulnerability assessment (scanner) vendor. For more information, see Vulnerability Response calculators and vulnerability calculator rules.
☐	Review the Remediation Target Rules. Remediation Target Rules define remediation time lines for VIs and remediation tasks. For more information, see Vulnerability Response remediation target rules.
☐	In the Integration Configuration section, review the Qualys application settings and define and schedule your data imports. **a.** Click **Scanner Integrations**. **b.** On the Installed Applications page, click **Edit**. **c.** Enter your credentials and click **Next**. **d.** Read the descriptions for the KnowledgeBase Configuration. **e.** Review the Host Detection Configuration page for Import Settings, CI Lookup Rules, and Import Schedules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	f. After you are satisfied with the settings on this page, click **Execute Now** to import data. Click the **View details** link that is displayed to view vulnerability integration run status. **g.** (Optional) Continue to edit configuration settings. **h.** Click **Finish** to complete the installation and configuration in Setup Assistant. For more information about configuring the Qualys application, see Configure the Qualys Vulnerability Integration using Setup Assistant.

What to do next

Congratulations! You successfully installed the Vulnerability Response application and configured it and a scanner application using the Setup Assistant. The base system is now ready for operation.

To download, install, and configure other applications for Vulnerability Response, follow the same steps and concepts you completed for the preceding checklist. Refer to specific topics provided for each application for more information.

For more information about supported applications available that are available to you from the ServiceNow Store for Vulnerability Response, see Installation of Vulnerability Response and supported applications.

For more information about how to use Vulnerability Response, see Exploring the Vulnerability Response application.

Vulnerability Response remediation task states

Third-party integrations import vulnerable item detection data that create new vulnerability items (VITs) or update existing VITs. Detection states update VIT states in so far as they're Open or Closed.

For more information on how a detection's state affects a VIT's state, see the Detections, remediation tasks, and vulnerable item states.

With Change management for Vulnerability Response, there's a synchronized relationship between the state fields of the remediation tasks and the state fields of the change requests (CHG) in the Vulnerability Response product. As a change request moves through its life cycle, it also moves the state of any related remediation tasks automatically. After a change request is implemented, the remediation task is automatically resolved. See State synchronization between change requests and remediation tasks for more information.

Note: Starting with v23.0 of Vulnerability Response:

- the **Remediation Task State Approval** workflow is deprecated and replaced by flow Remediation Task State Approval in the flow designer.
- the **Close** button has been removed for a remediation task and the closure of a remediation task is driven by the scanner.

The following table lists the remediation task states and the actions that you can perform on a remediation task at the respective state:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task states

State	Description
Open	State upon creation. From this state you can: **Show Duplicate VIs** Identify duplicate VIs reported by multiple scanners in the system. You can mark the duplicate VI as Resolved or Closed. Duplicate entries are only shown when the combination of vulnerabilities is created using Common Vulnerabilities and Exposures (CVE). For more information, see Vulnerability Response remediation task and vulnerable item states. **Start Investigation** Assign this remediation task to a person or group to start investigating. **Mark as false positive** Mark an item or group as false positive if the scanner reports that a vulnerability exists in the system, but in reality there's no vulnerability. **Request exception** Request an exception, a reopen (Until) date, a reason, and optionally, provide additional information. Defers the remediation of the item or group until the date that an exception is requested. **Resolve** Mark as Resolved to move the item or group to a resolved state. **Create Change** Create a change request or associate a remediation task to an existing change request. For more information, see Create a change request from a remediation task and Associate a remediation task to an existing change request. **Split Remediation task** For a remediation task with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a remediation task. The items that you select are automatically moved to a new remediation task. For more information, see Split a remediation task in the IT Remediation Workspace. **Defer** Select the Deferred state, a reopen date, a reason and, optionally, provide addition information. Defers the remediation task state until the reopen date. **Delete** Confirm the deletion. Removes the group.
Under Investigation	Triggered by the **Start Investigation** button. From this state, you can: **Create a Security Incident**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task states (continued)

State	Description
	For more information, see Create a security incident. **Create Change** Create a change request or associate a remediation task to an existing change request. For more information, see Create a change request from a remediation task and Associate a remediation task to an existing change request. **Split Task** For a remediation task with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a remediation task. The items that you select are automatically moved to a new remediation task. For more information, see Split a remediation task. **Create a Change Request** For more information, see Create a change request from a remediation task. **Awaiting Implementation** Changes state to Awaiting Implementation. This state indicates that remediation tasks have been referred outside a Vulnerability Response. **Defer** Select the Deferred state, a reopen date, a reason and, optionally, provide additional information. Defers the remediation task state until the reopen date. **Delete** Confirm the deletion. Removes the remediation task.
Deferred	Triggered by the **Request Exception** button. As part of the approval workflow, the Deferred state is In Review and can't be closed until approved. From this state, you can: **Create Change** Create a change request or associate a remediation task to an existing change request. For more information, see Create a change request from a remediation task and Associate a remediation task to an existing change request. **Split Task** For a remediation task with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new VG. See Split a remediation task. **Create a Security Incident** For more information, see Create a security incident. **Reopen**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task states (continued)

State	Description
	Transition back to an Open state. **Delete** Confirm the deletion. Removes the remediation task. Deferment information appears under the **Close/Defer** tab. On the defer date, the group reopens for remediation.
Awaiting Implementation	Triggered by the **Awaiting Implementation** button. From this state, you can: **Create a Security Incident** For more information, see Create a security incident. **Create Change** Create a change request or associate a remediation task to an existing change request. For more information, see Create a change request from a remediation task and Associate a remediation task to an existing change request. **Split Task** For a remediation task with more than one vulnerable item, use a set of conditions to filter out a subset of vulnerable items and split a vulnerability group. The items that you select are automatically moved to a new remediation task. For more information, see Split a remediation task. **Create a Change Request** For more information, see Create a change request from a remediation task. **Defer** Select the Deferred state, a reopen date, a reason and, optionally, provide addition information. Defers the remediation task state until the reopen date. **Resolve** Add notes. The state becomes Resolved. Notes appear under the **Resolution** tab. **Delete** Confirm the deletion. Removes the remediation task.
Resolved	Triggered from the **Resolve** button. From this state you can: **Create a Security Incident** For more information, see Create a security incident. **Create Change** Create a change request or associate a vulnerability group to an existing change request. For more information, see Create a change request from a remediation task and Associate a remediation task to an existing change request. **Reopen** Transition back to an Open state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task states (continued)

State	Description
	Delete Confirm the deletion. Removes the remediation task. Notes appear under the **Notes** tab. Resolution information appears under the **Resolution** tab.
Closed	Triggered by the scanner. From this state, you can: **Create a Security Incident** For more information, see Create a security incident. **Reopen** Transition back to an Open state. **Delete** Confirm the deletion. Removes the remediation task. Closure information appears under the **Close/Defer** tab.

- The remediation owner can only mark a vulnerable item or remediation task as resolved. Based on the confirmation from the scanner, this resolved item or remediation task can be marked as Closed or reopened.
- The **Delete** button is available for the administrator when there are multiple vulnerable items created manually, and these need to be closed or deleted.
- If you determine that the items are a low risk, waiting for a change window, or a patch, you can change their remediation task to the Deferred state for a defined amount of time. You can request an exception using the **Request Exception** option.

  Note: When remediation tasks are deferred or closed, you can specify resolutions to further define the reasons for doing so.

- When a VIT is reopened, either manually or automatically, the following happens:
  - The VIT state changes to Open. The original remediation task state doesn't update.
  - The VIT is reevaluated and put into a new or existing remediation task that is based on the active Remediation Task Rules.

  This preserves its history while enabling further remediation.
- When a remediation task is created (automatically or manually), or split, then its **State**, **Reason**, and **Until** fields are evaluated. In case of the split action, these fields are evaluated for both the old and new remediation tasks. When a VIT is updated, then the **State**, **Reason**, and **Until** fields of all its associated remediation tasks are evaluated.
  - If all the VITs in a remediation task are deferred and have the same reason, then the remediation task's state changes to **Deferred** and the VITs' reason is assigned to the remediation task. If the VITs differ in reason, then the remediation task's reason changes to **None**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The closest **Until** date of all the VITs is updated in the **Until** field of the remediation task.
- If you reopen any VIT, then the state of the remediation task changes to **Open**.

This evaluation is done by the *Rollup vulnerability item values to vulnerability and group* scheduled job, which runs every 15 minutes.

Detections, remediation tasks, and vulnerable item states

Third-party integrations retrieve the vulnerable item detection data. Detections are distinct occurrences of vulnerabilities as reported by the scanners.

Detection data are paired with vulnerable items (VIs, VITs) and the VI state is updated based on the state of the detections. If a VI isn't found, a new one is created. Detections are only opened or closed by the data that is found directly by a scanner.

If all detections are closed for a vulnerable item, that vulnerable item is closed. On the VI record, the state is Closed/Fixed. When all VIs are closed for a remediation task, the remediation task is closed. The state flow otherwise remains the same.

Closed VIs with a substate of fixed or stale are reopened if a new detection is created and the VIs can be matched with the new vulnerability.

Starting with version 20.0 of Vulnerability Response, if a detection is Stale and the associated VI is in Closed state, the VI's state doesn't transition to Closed - Stale. This is to avoid the VI from reopening when a new detection is identified so that you can avoid going through the entire false-positive request and approval process. To reverse this behaviour, deselect the **Ignore stale detections for closed VIs** check box on the Auto-Close Configuration form. For more information, see Automatically close stale detections in Vulnerability Response.

As per the script include, *DetectionBase*, method *_shouldReOpenVI()*, if the VI was earlier Closed with a substate of Fixed, Stale, or CI Decommissioned, it is reopened, and the detection is mapped to the existing VIT.

For example, let's say that a VI's closed date is later than the lastfound date of a detection. You would expect these VI records to remain closed. However, if you see that a previously closed VI has reopened, it means that the VI was closed by an earlier detection and the vulnerability was found again in a later scan. When a new detection is found that matches the closed VIT that has the same vulnerability on the VI's configuration item, the VI is reopened.

Remediation tasks and vulnerable item states

Remediation tasks and vulnerable items states can affect each other. Most of the time, a remediation task state updates the vulnerable item state, with the highest precedence task state used to update the vulnerable items in the group.

The state precedence is as follows.

Closed > **Deferred** > **Resolved** > **In Review** > **Awaiting Implementation** > **Under Investigation** > **Open**

- When a group of vulnerable items are in one remediation task and aren't altered at an individual level, they have the same state as their remediation task.
- When the remediation task goes from the Open state to Awaiting Implementation, all the VIs in the remediation task move to the Awaiting Implementation state.
- When the remediation task is deferred, the VI is likewise deferred. Starting with version 16.5, you can track the number of times that a vulnerable item, application vulnerable item, container vulnerable item, or a remediation task is deferred. The scheduled job, *set deferral counts*, runs daily to post counts for the records that are deferred more than

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

once in the Deferral count column in the Multiple deferrals modules for VR, AVR, and CVR. All counts for VIs that are associated with a remediation task are collected and posted if a remediation task is deferred more than one time.

Vulnerable items updated only by remediation tasks

Items match the state of the remediation task, if they haven't been updated individually, with these exceptions:

- If the remediation task state changes to Closed, and its resolution to Canceled or Fixed with Exception, the item is not affected and takes on the state of any other remediation task that contains it. If the vulnerable item is in no other remediation task, it reverts to the Open state.
- If the vulnerable item state is Closed/Fixed (updated by a scan or import), then when the remediation task changes its state, the vulnerable item remains in the Closed/Fixed state. This condition is true no matter what state the remediation task is in.

Vulnerable items in states set individually

Vulnerable items, in a state updated on the item, such as those items closed or deferred individually, don't match the state of the remediation task automatically. Instead, it compares its state to all associated groups to find the state with the highest precedence to apply.

Note: The Closed/Fixed state is a special case. For the vulnerable items that are set to the Closed/Fixed state, if all vulnerable items within a remediation task are set to Closed/Fixed — such as when a scanner finds that all the vulnerabilities have been remediated — the remediation task is automatically marked as Closed/Fixed.

Remediation tasks contain empty assignment fields

If the state of the VIs in a remediation task changes from Resolved to Open, the state of the remediation task is also updated from Resolved to Under Investigation.

However, if both the **Assigned to** and **Assignment group** fields in the remediation task are empty, the remediation task remains in the Resolved state and does not move to Under Investigation.

Assignment group for vulnerable items is not always updated when their remediation task is updated

If the assignment group for a VI in Open state is updated manually, it is not updated again when the assignment group for its remediation task is updated. This information is not overwritten because the assignment group for the VI has been updated intentionally, and might be a part of another remediation task.

State roll-up and roll-down scenarios

State roll-up and roll-down scenarios automatically sync the status of remediation tasks (RTs) and vulnerable items (VITs), ensuring real-time updates across both. This dynamic interaction reduces manual tracking, enhances accuracy, and provides users with an up-to-date view of progress, making vulnerability management more efficient and helping users make informed decisions quickly.

Roll-up behavior

When vulnerable item (VIT)states change, these changes may propagate up to the remediation task (RT)level. The following table summarizes key roll-up scenarios where changes in vulnerable

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

item (VIT) state may influence the associated remediation task (RT) state, based on closure conditions, reassignments, and deferrals.

Roll-up scenarios

VITs State	Condition	RT State
Open → Under Investigation / Awaiting Implementation (any sub-state) / In Review / Closed–False Positive / Closed–Invalid / Closed–Result Invalid / Resolved	VIT transitions to any non-final or non-actionable state	Remains Open
Open → Closed	All associated VITs have the same sub-state	Closed – <same sub-state as VITs>
Open → Closed	All associated VITs have different sub-states	Closed – <no sub-state>
Open → some Closed VITs and some Deferred VITs	All associated Deferred VITs have the same sub-state	Deferred – <same sub-state as VITs> (Until date = earliest of all VITs)
Open → some Closed VITs and some Deferred VITs	All associated Deferred VITs have different sub-states	Deferred – <no sub-state> (Until date = earliest of all VITs)
Open → Closed–Fixed (after next scan) → Resolved	VITs marked as fixed but pending verification	Remains Open
Closed–Fixed → Open	VIT reopens after being Closed–Fixed	Remains Closed–Fixed
Closed–Stale → Open	VIT reopens after being Closed–Stale	Remains Closed–Cancelled
Under Investigation → Closed–CI Decommissioned	Multiple RTs (e.g., RT1, RT2) exist for related VITs	Each RT transitions to Closed–Cancelled
Resolved → Open	If a resolved VIT reopens and the previously associated RT was assigned to a user	Resolved → Under Investigation
Resolved → Open	If a resolved VIT reopens and the previously associated RT was unassigned to a user	Resolved → Open

Roll-down behavior

When the state of a remediation task changes, the state is often propagated to the associated VITs unless overridden by manual updates or specific exceptions. The following table summarizes key roll-down scenarios where changes in remediation task (RT) state may affect the associated vulnerable item (VIT) state, based on precedence rules and special conditions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roll-down scenarios

RT State	Condition	VIT State
Open → Under Investigation / In Review / Closed–False Positive	RT transitions to a non-final or non-actionable state	Mirrors RT state change (Open → <same state as RT>)
Open → Deferred (Sub-state: Reason Given)	RT deferred with a specified reason	Open → Deferred (Sub-state: Reason Given)
Open → Resolved	RT marked as resolved	Open → Resolved
Open → Closed–Cancelled / Closed–Fixed with Exceptions	RT closed without full resolution	Remains Open
RT1: Open → Under Investigation; RT2: Open	One RT moves to Under Investigation while another remains Open	Open → Under Investigation
RT1: Open → Under Investigation → Awaiting Implementation; RT2: Under Investigation	One RT progresses to Awaiting Implementation	Open → Under Investigation → Awaiting Implementation
RT1: Awaiting Implementation → Deferred; RT2: Awaiting Implementation	One RT deferred while another remains Awaiting Implementation	Awaiting Implementation → Deferred
RT1: Awaiting Implementation → Closed–Cancelled; RT2: Under Investigation	One RT cancelled while another is Under Investigation	Awaiting Implementation → Under Investigation
Open → Closed–Fixed with Exceptions	Mixed outcome: one VIT closed as fixed with exceptions, another remains open	VIT1: Open → Closed–Fixed; VIT2: Remains Open
Open → Resolved	Mixed outcome—one VIT closed as fixed and another resolved	VIT1: Open → Closed–Fixed; VIT2: Open → Resolved
Resolved → Open	RT reopens after resolution	VIT2 reopens; VIT1 remains Resolved

Remediation task state for Vulnerable Items (VITs) in multiple groups

When a VIT is in multiple remediation tasks, (RT in the following tables), and its own state has not been set, the higher precedence group state determines the state of that VIT, as shown in the following table.

Vulnerable item states examples

Remediation task state	Vulnerable item state
RT 1: **Open** > **Under Investigation** RT 2: **Open**	**Under Investigation** When RT 1 is Under Investigation and RT 2 is Open, the VI changes to Under Investigation. After the search, between RT 1 and RT 2, RT 1 has the state with the highest precedence.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable item states examples (continued)

Remediation task state	Vulnerable item state
RT 1: **Under Investigation** RT 2: **Open** > **Under Investigation**	**Under Investigation** When RT 2 is Under Investigation and RT 1 is Under Investigation, the VI stays as Under Investigation. After the search, between RT 1 and RT 2, they have the state with the same precedence.
RT 1: **Under Investigation** RT 2: **Under Investigation** > **Awaiting Implementation**	**Awaiting Implementation** When RT 2 is Awaiting Implementation and RT 1 is Under Investigation, the VI changes to Awaiting Implementation. After the search, between RT 1 and RT 2, RT 2 has the state with the highest precedence.
RT 1: **Under Investigation** > **Deferred** RT 2: **Awaiting Implementation**	**Deferred** When RT 1 is Deferred and RT 2 is Awaiting Implementation, the VI changes to Deferred. After the search, between RT 1 and RT 2, RT 1 has the state with the highest precedence.

Vulnerable item in multiple groups special cases

Remediation task State	Vulnerable Item State
RT 1: **Under Investigation** RT 2: **Awaiting Implementation** > **Closed (Fixed or Cancelled)**	**Under Investigation** When RT 2 is Closed/Fixed or Closed/Cancelled, and RT 1 is Under Investigation, the VI changes from Awaiting Implementation (previously the highest precedence) to Under Investigation (currently the highest precedence).
RT 1: any state RT 2: any state	If the vulnerable item source status is Fixed (updated by a scan or import), then when the group changes its state, the vulnerable item changes its state to Closed/Fixed. This condition is true no matter what states the other associated groups are in. The vulnerable item search for the group state does not occur.

When a VI state is set individually, its state is considered when evaluating precedence, as with any other remediation task. When a VI belongs to more than one remediation task, the following table lists the updates that are made.

Vulnerable item state set individually special cases

Vulnerability item state within a group	Vulnerable item final state
RT 1 state: **Under Investigation**	**Awaiting Implementation**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable item state set individually special cases (continued)

Vulnerability item state within a group	Vulnerable item final state
RT 2 state: **Under Investigation** > **Awaiting Implementation** Original VI state: **Under Investigation** > **(set on the VI)**	When RT 2 moved to Awaiting Implementation, and RT 1 remained Under Investigation, the VI changes to Awaiting Implementation (the highest precedence).
RT 1: **Under Investigation** RT 2: **Under Investigation** > **Awaiting Implementation** Original VI state: **Deferred** > **(set on the VI)**	**Deferred** When RT 2 moved to Awaiting Implementation, and RT 1 remained Under Investigation, the VI remains in the Deferred state (the highest precedence).

The following table shows that when two remediation tasks with common vulnerable items are deferred, the state is deferred until the latest date is reached.

Vulnerable item deferred state special cases

Vulnerability item state within a group	Vulnerable item final state
RT 1 state: **In Review (until April 10)** RT 2 state: **Under Investigation** > **In Review (until April 30)** Original VI state: **In Review (until April 10)** > **(set on the VI)**	**Deferred (until April 30)** When RT 2 moved to Deferred (until Apr-30), and RT 1 remains Deferred (until Apr-10), the VI changes from Deferred (until Apr-05) to Deferred state (until Apr-30).
RT 1: **In Review (until July 15)** RT 2: **Under Investigation** > **In Review (until July 10** Original VI state: **Deferred** > **(until July 15)**	**Deferred (until July 15)** When RT 2 moved to Deferred (until Jul-10), and RT 1 remains Deferred (Jul-15), the VI remains in Deferred (until Jul-15).

Additional settings for domain separation

For precise execution and results, the following precautions and settings are required for domain separation in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance.

Don’t modify the business logics and processes in the global domain to avoid any issues so that all the latest changes are updated for every upgrade. Duplicate all the business logics and processes in each domain separately and ensure that they are inactive in the global domain. Otherwise, the business logics and processes in the global domain take precedence over the child domain. Suppose, you created a risk rule in a child domain and the global domain also has a similar risk rule then the global domain's rule takes precedence over the child domain's rule.

Reevaluation of calculators and rules

Prior to v20.0, when you reapply calculators or rules, the `rerun` flag is set to true and a business rule is triggered to run a schedule job that reapplies the calculators and rules. Starting from v20.0, you need not depend on the `rerun` flag. When you click on the **Reapply Calculator**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

button, a background job is triggered that reapplies the calculators and rules. This enables you to create calculators and rules for all the domains.

Settings for rollup calculators

In a domain, only one roll up calculator must be active for a table. For example, consider the Remediation Task table, *sn_vul_vulnerability* with the roll up calculator, **Remediation Task Rollup** in the global domain. If you duplicate this roll up calculator by changing the weights for the same table in the same domain, there will be discrepancies in the roll up calculations. Therefore, ensure to activate only one rollup calculator if there are two or more roll up calculators for a table in the same domain.

Discovered Items form fields

Assets are automatically matched to configuration items (CIs) in the Configuration Management Database (CMDB) when they're imported using the CI Lookup Rules. Records for unmatched CIs are automatically created during third-party vulnerability integration imports and included in Discovered Items. However, for cloud assets that aren't present in CMDB CI, the record is created in the cloud resource class.

Discovered Items fields

The information in these records is ingested from the third-party records and classified during import.

These fields are found on records listed in the Discovered Items [sn_sec_cmn_src_ci] table.

To view imported data in the fields listed in the following tables, you must have, at a minimum, the sn_vul.read_all role.

Field	Description
Number	Identifier assigned to the record.
Configuration Item	Configuration item that is imported from the third-party source integration. Starting from v12.0, Configuration Item is the latest CI from the list of CIs after filtering the decommissioned ones.
Class	Class assigned to the CI during import by Vulnerability Response.
Source	Source that is imported from the third-party source integration.
CI matching rule	The CI matching rule that was used to create the item.
V18.0: Matching type for the DI	Matching type used to create the discovered item. Options are: • Created by VR • Created by IRE • Matched by CI lookup • Matched by IRE • Matched manually (Starting with v24.0.6 of Vulnerability Response, you can view this additional option. This option is set automatically if you manually update a CI on the Discovered Item form.) This information is only available for data that is populated for Vulnerability Response v18.0 and later. On existing data, this column doesn't contain any value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If you reapply the CI lookup rules, some CIs on DIs might be updated, resulting in this column being populated.
Other matched CIs	List of the other configuration items matching the CI lookup rule.
State	State of the CI that is determined during import. Choices are: • **Matched**: A matching configuration item was found in the CMDB. • **Unmatched**: No match was found in the CMDB. A placeholder record is created.
Created	Date when the Discovered Item record was created.
Updated	Date when the Discovered Item record was updated.
Updated by	User who updated the data.
Host tag	Host tags assigned to this discovered item during import. You can have up to 31 host tags per discovered item.
Fully qualified domain name	Data associated with this CI found in the CMDB.
MAC Address	Data associated with this CI found in the CMDB.
Operating System	Operating system associated with this CI.
NetBIOS	NetBIOS imported from the third-party source integration.
IP address	Data associated with this CI found in the CMDB.
Source data	Latest data associated with this CI from the source.
V16: Initial source data	Initial data associated with this CI from the source.
V16: Reevaluate CI	Receives data from the scanner. If there's updated data, the value is set to true. **Note:** The source data values are recalculated according to the latest source data. When updated data is retrieved from the scanner, the source data is updated. The existing source data value is moved to the initial source data field. To reevaluate the discovered items, activate the `Re-apply CI Lookup Rules on the Changed Discovered items` scheduled job.
Agent exists	Indicates `true` if the agent is installed on the asset. If the `hostUID` and UUID values in the Source data column are empty, this value populates as `true`. **Note:** This field appears starting from v19.0 of Vulnerability Response.

Starting with v23.0 of Vulnerability Response, the **Test Result Compliance % (CI)** column shows the percentage of test results that are compliant for the corresponding CI. To obtain this value, you must set the `calcTRComplianceForCI` to `true` in the **Update remediation metrics** scheduled job.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Test Result Compliance % (CI)** value populates only for the Discovered Items which have a non-empty value in either the **Last Configuration Compliance scan date** or **Non-infra last compliance scan date** columns.

Starting with version 18.0 of Vulnerability Response, Qualys, Tenable for Vulnerability Response and Rapid7 scanners can receive the following additional metadata for cloud assets.

Field	Description
Cloud service provider	Name of the cloud service provider that offers cloud computing services. For example, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).
Cloud region	Location where the resource has been hosted.
Cloud account	Account provided by cloud service providers such as AWS, GCP, and so on to access cloud computing services.
Cloud resource type	Types of assets present in the cloud such as Amazon Elastic Compute Cloud (EC2) machine, AWS S3 buckets and so on.
Resource ID	Unique identifier that is assigned to a resource in a cloud computing environment. This ID is used to identify and manage the resource.
Resource name	User-defined name used to identify and manage a resource in a cloud computing environment.
Image	Virtual machine image or a server image, is a pre-configured virtual machine that contains an operating system, applications, and other software. For example, Amazon Machine Image.

A new CI Lookup Rule, 'Cloud Resource ID', has been introduced to match the cloud CIs based on the cloud metadata.

Vulnerability Response vulnerability form fields

Vulnerabilities are created automatically when records are downloaded from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-party integrations and stored under **Libraries** in Vulnerability Response.

NVD entry fields

To view imported data in the fields listed in the following tables, you must have, at a minimum, the sn_vul.read_all role.

These fields are found on records listed in the National Vulnerability Database Entries [sn_vul_nvd_entry] table.

Field	Description
ID	Identifier for this vulnerability entry.
Risk rating	(Hidden when no VITs are associated with the vulnerability) Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see Vulnerability Response calculators and vulnerability calculator rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This base **Risk rating** is not the same as the Solution record **Risk rating.**
Risk score	(Hidden when no VITs are associated with the vulnerability) Calculated amount of risk the vulnerable item poses to your environment. **Note:** This base **Risk score** is not the same as the Solution record **Risk score.** For more information, see Vulnerability Response calculators and vulnerability calculator rules.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.
Exploit exists	Yes, if at least one exploit is associated with this vulnerability.
Exploit skill level	Lowest skill level required to exploit this vulnerability.
Exploit attack vector	Most vulnerable attack vector of the exploits for this vulnerability. Available when SAM NVD is enabled.
Active VIs	(Hidden when no VITs are associated with the vulnerability) Number of vulnerable items associated with this vulnerability, not in the Closed state. If there are no active VIs for this vulnerability, **Risk Rating** and **Risk Score** are not displayed.
CWE entry	Reference to the Common Weakness Enumeration element that this vulnerability best fits into.
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Summary	Description of the vulnerability.
Threat intel (starting with Vulnerability Response version 20.0)	Threat intelligence provided by Qualys. With this data, you can understand a threat actor's motives, targets and attack behaviors.
Vulnerability Details	
CVSS v2	Imported CVSS v2 data
CVSS v3	Imported CVSS v3 data, not available prior to 2015.
Preferred solution	(Hidden when no VITs are associated with the vulnerability) Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	can be overwritten on subsequent imports. Setting this value manually should be done on the vulnerable item.
CISA Exploit (This tab is available only when the CISA application is installed.)	
CISA due date	Deadline to resolve the vulnerability.
Date added	Date when the vulnerability was added to the CISA catalog.
Product	Product on which the vulnerability was identified.
Vendor/Project	Vendor associated with the identified vulnerability.
Known ransomware Starting from v21.0 of Vulnerability Response.	Selected when the field **Known To Be Used in Ransomware Campaigns** is ingested from the CISA Known Exploited Vulnerabilities (KEVs) catalog. The flag is set at the Common Vulnerabilities and Exposures (CVE) level and rolled up to the third-party entry (TPE).
Remediation Status (Hidden when no VIs are associated with the vulnerability)	
Excludes Deferred	
Vulnerable items	Number of active vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
Total VIs	Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
Includes Deferred	
Vulnerable items	Number of active vulnerable items with this vulnerability.
Total VIs	Total number of vulnerable items with this vulnerability.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability.
Related Links	
Update status	Displays date and time of the last update. Updates the following: • Remediation task state • Risk score and rating • Metrics such as Active VITs, Total VITs from the Remediation Status section
Related Lists	
Vulnerable Items	(Hidden when no VITs are associated with the vulnerability)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Vulnerable items associated with this vulnerability.
Vulnerability References	Information about the vulnerability from external sources, cited by NVD.
Exploits	Exploits associated with this vulnerability.
Solutions	(Hidden when no VITs are associated with the vulnerability) All Vulnerability Solution Management integration solutions associated with this vulnerability.
Weaknesses	Imported **Weakness** data associated to a Common Vulnerabilities and Exposures (CVE).
Vulnerable Software	(Hidden when software is associated with the CVE) Imported Common Platform Enumeration (CPE) data associated with the vulnerability.
Vulnerability Malware Kits	Malware imported from various scanner sources, for a vulnerability.

CWE vulnerability entry fields

These fields are found on records listed in the CWEs [sn_vul_cwe] table.

Field	Description
CWE-ID	Identifier for this vulnerability entry. This identifier is used for both Categories and Weaknesses, and are unique between the two datasets.
Name	Descriptive name assigned to this CWE-ID.
Likelihood of exploit	How likely the weakness is to be exploited, on a qualitative scale. One of: • Unknown • Low • Medium • High
OWASP Top 10 Position	This vulnerability's numerical position in the OWASP top 10 list.
SANS To 25 Position	This vulnerability's numerical position in the SAN top 25 list.
Class	Type of weakness
Status	One of: • Incomplete • Draft • Stable

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	• Deprecated • Obsolete • Unstable
Abstraction	One of: • Variant • Class • Base • Compound
Updated	Last time the record was updated in the instance.
Functional areas	List of functional areas affected. For example, **File Processing**. Only populated for 24/862 weaknesses.
Affected Resources	List of affected resources. For example, **File** or **Directory**. Only populated for 51/863 weaknesses.
URL	Knowledge base article associated with this vulnerability.
Description	Description of the vulnerability.
Integration run	The integration run this CWE was imported in.
Sections	
Additional details	Software concept descriptions that further explain the weakness. Includes: • Extended description • Background details • Notes
Detection methods	Details on how you might detect this weakness in an application.
Modes of introduction	The phases in which the weakness is introduced for example, **Implementation**, **Architecture and Design**, and so on.
Demonstrative examples	Code examples of the weakness with accompanying descriptions.
Potential mitigations	Details on how to prevent the weakness, including which phase of the application lifecycle it occurs in, and effectiveness of the mitigation.
Related Lists	
Relationships	CWEs associated to this vulnerability. Lists relationships between this CWE and others. Can include parent/child, follows/precedes, requiredby/requires (for composite weaknesses), CanAlsoBe, PeerOf, MemberOf .
Observed Examples	Some CVEs that are representative of this weakness.
Common Consequences	Consequences of a successful exploit, in terms of scope and impact. For example:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Scope: Confidentiality Impact: Read Application Data
Memberships	CWE memberships with this vulnerability.
Applicable Platforms	Platforms associated with this vulnerability.
Application Vulnerability Entries	Other application vulnerability entries associated with one.
External References	Information about the vulnerability from external sources.

Third-party vulnerability entry fields

These fields are found on records listed in the Third-party Vulnerability Entries [sn_vul_third_party_entry] table.

Field	Description
ID	Identifier for this vulnerability entry.
Version 16.0: CVEs	Multiple Common Vulnerability and Exposures (CVEs) associated with this third-party vulnerability.
Source	Origin of the vulnerability — whether a scanner or physical test.
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low and None. For more information on risk ratings see, Vulnerability Response calculators and vulnerability calculator rules. **Note:** This base **Risk rating** is not the same as the Solution record **Risk rating**
Risk score	Calculated amount of risk the vulnerable item poses to your environment, based on risk score. **Note:** This base **Risk score** is not the same as the Solution record **Risk score.** For more information, see Vulnerability Response calculators and vulnerability calculator rules.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.
Exploit exists	Yes, if at least one exploit is associated with this vulnerability.
Exploit skill level	Lowest skill level required to exploit this vulnerability.
Exploit attack vector	Most vulnerable attack vector of the exploits for this vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active VIs	Number of vulnerable items associated with this vulnerability, not in the Closed state.
Category	Classification provided by the third-party integration. Aids in assignment.
Remediation type	Types of remediation actions. • Patch • Configuration change • Patch and Configuration change • Countermeasure
CWE entry	Reference to the Common Weakness Enumeration element that this vulnerability best fits into.
PCI	When the checkbox is selected, the vulnerability is flagged for significant risk for exposure of payment information.
PCI severity	Level of risk for exposure of payment information. [Qualys only.]
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Summary	Description of the vulnerability.
Vulnerability Details	
CVSS v2	Imported CVSS v2 data
CVSS v3	Imported CVSS v3 data, not available prior to 2015.
Threat	Description of the threat from this vulnerability.
Preferred Solution	Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually can be overwritten on subsequent imports. Setting this value manually should be done on the vulnerable item.
Remediation notes	Description of the remediation solution pulled from the vendor.
Remediation Status	
Excludes Deferred	
Vulnerable items	Number of active vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
Total VIs	Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
Includes Deferred	
Vulnerable items	Number of active vulnerable items with this vulnerability.
Total VIs	Total number of vulnerable items with this vulnerability.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Related Links	
Update status	Displays date and time of the last update. Updates the following: • Remediation task state • Risk score and rating • Metrics such as Active VIs, Total VIs from the Remediation Status section
Related Lists	
Vulnerable Items	Vulnerable items associated with this vulnerability.
Vulnerability References	Information about the vulnerability from external sources, cited by NVD.
CVEs	Common Vulnerability Enumeration (CVE) record associated with this vulnerability.
Categories	Categories associated with this vulnerability.
Exploits	Exploits associated with this vulnerability.
Vulnerability Malware Kits	Malware kits associated with this vulnerability.
Solutions (Rapid7)	Solution information from the Rapid7 solution integrations. Displayed when available.
Exploit Frameworks	Exploit frameworks associated with this vulnerability.
Solutions	Vulnerability Solution Management solutions associated with this vulnerability.
CISA Exploit	
CISA exists	CISA exploit exists for the Third-Party Vulnerabilities Entry table.
CISA due date	Deadline to resolve the vulnerability.

Remediation target rule fields

Use remediation target rules to define how remediation timelines are calculated and maintained for findings. Administrators can configure base target dates and recalculation behavior when risk ratings change. The following table describes all fields available in the remediation target rule form.

Field	Description
Name	Name of the rule.
Target (days)	Number of days within which the vulnerable items should be remediated, since last opened.
V17.1: Target from (date)	Date from when the target SLAs are computed. You can specify only the date or the date and time type fields. Default value is Last opened date. To customize the values for this field, see KB1642413.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	Option to mark the remediation target rule as active. If this check box is cleared, this rule doesn't apply to new vulnerable items created in the system.
Notify (days before due)	Number of days prior to the targeted remediation time for a notification to be sent. The notification date calculated using this value is used to show the remediation status and color coding. If the date is before the notification date, the remediation status is "In flight." If it's past the notification date and before the remediation target date, the status is shown as approaching target. **Note:** If this field is set to 0, only a **Target Missed** notification is sent.
Description	Text describing the remediation target rule.
Condition	Using the condition filter, select the criteria for applying the rule to the vulnerable items. To prevent performance impact, test your conditions at full production scale. Testing enables you to determine how long the **Evaluate remediation targets** job takes to execute, given the conditions and the size of your Configuration Management Database (CMDB). Case sensitivity for the search text you enter in the condition builder isn't supported on this record or form.
Recalculate target date	
Recalculation method	Method for recalculating the remediation target (RT) date when a vulnerable item's risk rating changes. You can choose to retain the existing target date, reset it based on the latest risk change date, or reset it to the earliest applicable date. By default, recalculation applies only to items that aren't overdue at the time of the risk rating change. To include overdue findings in the recalculation, enable the `sn_sec_cmn.evaluate_targetmissed_records` property. For more information, see Recalculate a remediation target date.
Notifications **Note:** The count shown in the notification email doesn't include vulnerable items in the **Deferred**, **Resolved**, or **Closed** state.	
Users	The people to notify when the selected vulnerable item is approaching or passes its targeted remediation target time.
Group	The group to notify when the selected vulnerable item is approaching or passes its targeted remediation target time.
Update History	
	Unused for initial creation of a rule. Subsequently, system work notes are logged here.

Remediation task form fields

Using remediation tasks, the analyst can monitor progress and drive the mediation process more efficiently.

These fields are found on records listed in the Remediation Task [sn_vul_vulnerability] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To view imported data in the fields listed in the following tables, you must have, at a minimum, the sn_vul.read_all role.

Remediation task fields

Field	Description
Number	The automatically generated vulnerable item (VI) number for this record.
Risk rating	Rollup of vulnerable item risk scores separated into ranges: Critical, High, Medium, Low and None. For more information on risk ratings see, Vulnerability Response calculators and vulnerability calculator rules. **Note:** This base **Risk rating** is not the same as the Solution record **Risk rating.**
Risk score	Rollup of the risk scores of all of the vulnerable items associated with this remediation task. Amount of risk the vulnerable items, collectively, pose to your environment. **Note:** This base **Risk score** is not the same as the Solution record **Risk score.**
Remediation target	Date by which the vulnerable items should be remediated, since first identified. For more information on remediation targets see Vulnerability Response remediation target rules.
Remediation status	Status of the remediation for the task. It is determined by the vulnerable item with the nearest due date. For open groups states include: • In-flight • Approaching Target • Target Missed For closed groups states include: • No Target • Target Met • Target Missed For calculated remediation target dates, if the task is closed, the overall remediation status of all of the closed vulnerable items is shown in the task. Those determine whether the task met its date or not. A closed task's remediation Status is **No Target** if none of its closed items had a remediation target date. It is **Target Missed** if any of its closed items missed their target date. It is **Target Met** if at least one closed VI met its target and none of the others missed it.
State	Progress status of the task. States include:

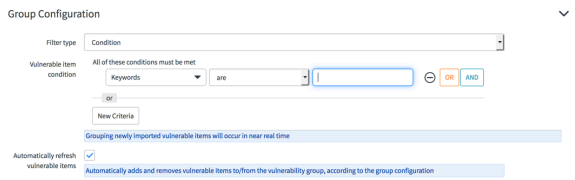
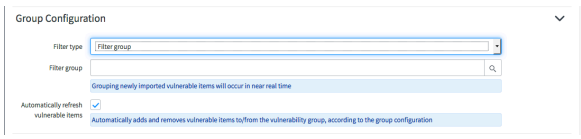
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task fields (continued)

Field	Description
	• Open • Under Investigation • Awaiting Implementation • Deferred • In Review • Resolved • Closed For more information on states, see Vulnerability Response remediation task and vulnerable item states.
Until date for Risk reduction	Date on which compensatory controls applied to the remediation task expire. **Note:** This field appears only when the value is available.
Assignment group	Group selected to work on this remediation task.
Assigned to	Individual from the selected assignment group that works on this vulnerability.
Created	Date this remediation task was created.
Updated	Date this remediation task was last updated.
Vulnerability	Vulnerability applicable to the task. (Visible when the group is formed based on a single vulnerability.)
Short description	Brief description of this remediation task.
In Review (visible when the RT is in the In Review state)	
Requested by	Individual who requested the deferral.
Desired reason	Reason for deferral.
Desired state	The state requested from the approver.
Desired substate	The reason requested from the approver.
Deferral(visible when the task is in the Deferred state)	
Deferred by	Individual who deferred the task.
Defer expiration	Date the deferral expires.
Reason to defer	Reason for the deferral.
Resolution (visible when the RT is in the Resolved state)	
Resolved by	Individual who resolved the remediation task.
Resolution date	Date the remediation task was resolved.
Resolution notes	Additional information.
Close (visible when the RT is in the Closed state)	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task fields (continued)

Field	Description
Closed by	Individual who resolved the remediation task.
Closed	Date the remediation task was closed.
Close notes	Additional information.
Group Configuration (visible in all states)	
Filter type	Type of filtering used to select vulnerabilities for the group: **Condition**  **Note:** Refreshes once an hour. **Filter group**  **Note:** Refreshes once an hour. **Manual** 
Remediation Status	
Excludes Deferred	
Vulnerable items	Number of active vulnerable items within this task. This count excludes deferred vulnerable items.
Total VIs	Total number of vulnerable items within this task. This count excludes deferred vulnerable items.
%VIs remediated	Percent complete for remediation of vulnerable items within this task. This count excludes deferred vulnerable items.
Includes Deferred	
Vulnerable items	Number of active vulnerable items within this task.
Total VIs	Total number of vulnerable items within this task.
%VIs remediated	Percent complete for remediation of vulnerable items within this task.
Notes (visible in all states)	
Description	Description of the group or remediation actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task fields (continued)

Field	Description
Additional comments	Additional information.
Activities	System notes.
Related Links	
Re-scan vulnerable items	Triggers a re-scan of the vulnerable items to determine if they are fixed.
Update Status	Displays date and time of the last update. Rolls up the following from the VIs in the task: • Remediation task state • Risk scores and risk ratings • Remediation target date and status (if applicable) • Metrics such as Active VIs, Total VIs from the Remediation Status section
Related Lists	
Vulnerable items	Vulnerable items in this task.
Task SLAs	Platform SLAs associated with this task.
Preferred Solutions	Preferred solutions of the vulnerable items in this task.
Change Requests	Change requests associated with this task.
Requested Approvals	(Visible when the task is in the In Review state.) List of approvers. Once the deferral is approved, the remediation task moves to the Deferred state.

Questionnaire Configuration form fields

You can define distinct questionnaire for a distinct collection of vulnerabilities or remediation tasks by filtering the vulnerabilities or remediation tasks respectively in the VR Questionnaire Configuration section of Settings for VR Exception Management form.

The Questionnaire Configuration form appears when you select the **New** button in the VR Questionnaire Configuration section of Settings for VR Exception Management form.

Questionnaire Configuration form fields

Field	Description
Name	Name of the questionnaire.
Approval rule	Approval rule for which the questionnaire is applicable. • **Exception request for vulnerability groups** • **Exception request for vulnerable items** • **False positive for vulnerability groups** • **False positive for vulnerable items**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Questionnaire Configuration form fields (continued)

Field	Description
	• **Questionnaire for compensating controls for vulnerable groups** for remediation task's risk reduction requests. • **Questionnaire for compensating controls for vulnerable items** for vulnerable item's risk reduction requests.
Description	Short description for the questionnaire configuration.
Order	Questionnaire with lowest order appears during the requests.
Active	Enabled by default, signifying that the questionnaire is in use.
Table	Table for which the approval rule is applicable. • Vulnerable Item [sn_vul_vulnerable_item for the approval rules related to vulnerable items. • Remediation Task [sn_vul_vulnerability] for the approval rules related to remediation tasks.
Condition	Condition for the records for which the questionnaire must appear. You can apply condition on all the fields of a vulnerable item and remediation task except **Reason**.
Questionnaire	Questionnaire that appears when a remediation owner is requesting an exception, false positive or risk reduction.

Related topics

Configure Exception Management for Vulnerability Response

Configure questionnaire for risk reduction

Vulnerability Response vulnerable item form fields

Vulnerable items are automatically created during third-party vulnerability integration imports.

Vulnerable item fields

To view imported data in the fields listed in the following tables, you must have, at a minimum, the sn_vul.read_all role.

These fields are found on records listed in the Vulnerable Items [sn_vul_vulnerable_item] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you have enabled SAM NVD vulnerability scanning, the records are compared to the software in your Configuration Management Database (CMDB) and matches are found with vulnerable software or configuration items (CIs).

Field	Description
Select security tag	Security tag to add metadata to the record or identify who should have access to this security incident record. This field appears only after the vulnerable item has been saved.
Number	Automatically generated vulnerable item number for this record.
Source	Scanner that found this vulnerable item.
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see Vulnerability Response calculators and vulnerability calculator rules. **Note:** This base **Risk rating** isn't the same as the Solution record **Risk rating.**
Risk score	Calculated amount of risk the vulnerable item poses to your environment. **Note:** This base **Risk score** isn't the same as the Solution record **Risk score.** For more information, see Vulnerability Response calculators and vulnerability calculator rules.
Vulnerability	ID of the vulnerability associated with this vulnerable item.
Configuration item	Affected asset.
State	This field defaults to **Open**, but you can change it to **Under Investigation** if the vulnerability is ready for immediate remediation.
Until date for risk reduction	Date on which compensatory controls applied to the vulnerable item expire. **Note:** This field appears only when the Original risk score value is available.
Assignment group	Group selected to work on this remediation task.
Assigned to	Individual from the selected assignment group that works on this vulnerability.
Created	Date this vulnerable item was created in your instance.
Last opened	Date the vulnerable item was most recently opened in your instance. Initially, this is the same as the creation date of the vulnerable item, however, if it was closed, then reopened the Last opened date contains the date and time reopened.
Updated	Date of the last scan.
Age	Duration for which the VI has been active since the date it was last opened. If the VI is closed, the value of the Age field is set to zero.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For more information on the Age field, see Vulnerable item age calculation and display. For more information on how to customize the calculation of Age duration, see the KB1703270 article.
Vulnerability	
Summary	Description of the vulnerability.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Create a Vulnerability Response severity map.
Vulnerability score (v3)	CVSS v3 score.
Vulnerability score (v2)	CVSS v2 score.
Exploit exists	Yes, if at least one exploit is associated with the vulnerabilities associated with this vulnerable item.
Exploit attack vector	Most vulnerable attack vector of the exploits for the vulnerabilities associated with this vulnerable item.
Exploit skill level	Lowest skill level required to exploit the vulnerabilities associated with this vulnerable item.
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Threat	Relevant information about the threat. Pulled from the vulnerable entry record. **Note:** Any changes made here update the vulnerable entry record.
Remediation notes	Relevant solution to the threat, pulled from the vulnerable entry record.
Remediation Available only with Vulnerability Solution Management.	
Preferred solution	Preferred solution imported from the vulnerability record. **Note:** Any manual changes made here don't change the vulnerability record and remain unchanged on the VI upon subsequent imports.
Summary	Imported Summary from the solution record.
Solution type	Potential or Preferred solution.
Initial Detection	
DNS name	Name of the Domain Name Service name. If a CI isn't provided, this field is used to look up a matching CI, if one exists.
NetBIOS name	Name of the NetBIOS. If a CI isn't provided, this field is used to look up a matching CI, if one exists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
IP Address	IPv4 or IPv6 address. If a CI isn't provided, this field is used to look up a matching CI, if one exists.
Port	Address of the port
Protocol	Name of the protocol.
SSL	Whether SSL encryption is used or not.
Detections	
Status	State of the detection.
First found	Date the third-party source first found the detection on this asset.
Last found	Date the third-party source last found the detection on this asset.
DNS name	Name of the Domain Name Service name. If a CI isn't provided, this field is used to look up a matching CI, if one exists.
NetBIOS name	Name of the NetBIOS. If a CI isn't provided, this field is used to look up a matching CI, if one exists.
IP Address	IPv4 or IPv6 address. If a CI isn't provided, this field is used to look up a matching CI, if one exists.
Port	Address of the port
Protocol	Name of the protocol.
SSL	Whether SSL encryption is used or not.
Times found	Number of times this vulnerability has been detected on this asset by the third-party source.
Integration run	Integration run that imported the detection.
Close Available once the vulnerable item has been remediated and closed. Items in this section are read-only.	
Closed by	Who closed the vulnerable item.
Closed	Date the vulnerable item was closed.
Close notes	Information included in the closure.
Age closed	Time period after which the VI was closed. If the VI is reopened, the value of the Age closed field is set to zero. For more information on how the Age closed field, see Vulnerable item age calculation and display. For more information on how to customize the calculation of Age closed duration, see the KB1703270 article.
Notes	
Additional comments/Work notes	Any relevant information. Select the check box to add Additional comments. Starting with Vulnerability Response v20.0, you can add work notes in the Notes section for a deferred vulnerable item.
Activity	Only appears when a work note has been created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Related Links	
Calculate Risk Score	When either the **Vulnerability Severity** or **Risk Score** calculators is enabled, the **Risk Score** field is updated.

The following are the vulnerable items related lists.

Related List	Description
Remediation Tasks	Tasks associated with this vulnerable item.
Affecting Tasks	Tasks associated with this vulnerable item.
Associated IP Addresses	Available if the Qualys Vulnerability Integration Vulnerability Integration application is installed. IP addresses that are found during de-duplication.
Impacted Services	Business services impacted by this vulnerable item. Shown when this information is available in the cmdb record. This information can be entered manually or using the ServiceNow® Service Mapping application. See Service Mapping for more information. If an affected CI associated with the vulnerable item is added or updated, information in this related list is automatically updated when the record is saved.
State Change Approvals	Status of change requests and other approval information associated with the VIT.
Qualys Tickets	Qualys ticket integration information associated with this vulnerable item.

Solution form fields

Solutions are created automatically when records are downloaded from third-party solution integrations and stored under **Solutions** in Vulnerability Response.

Solution integration entry fields

The imported fields in this table are read-only.

Field	Description
Number	Identifier assigned to the solution.
Source	Origin of the solution.
Source ID	Source identifier for this solution.
Risk rating	Separates Solution record **Risk score** into ranges from Critical to None. For more information on solution **Risk rating**, see Vulnerability Solution Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: Solution **Risk rating** is not the same as the **Vulnerable Item**, **Third-party Vulnerability Entry**, and **Remediation Task** records **Risk rating**.
Risk score	Weighted calculation based on the **Risk score** and count of vulnerable items with this solution as their **Preferred solution**. For more information on solution risk score, see Vulnerability Solution Management. **Note:** Solution record **Risk score** is not the same as the **Vulnerable Item**, **Third-party Vulnerability Entry**, and **Remediation Tasks** records **Risk score**. Available when SAM NVD is enabled, but if there are no active vulnerable items (VI) associated with a vulnerability the solution **Risk score** is set to zero.
Highest-supersedence	Indicates that no solution supersedes it.
Solution type	What kind of solution it is. Choices are: • Workaround • Mitigation • Vendor Fix • Patch • Rollup • Entitlement • Will Not Fix • None available
Requires restart	Restart needed. Choices are: • Yes • No • Maybe
Date published	Date the vulnerability was published by source.
Last modified	Date the vulnerability was last modified by source.
Summary	Remediation summary of the solution.
Bulletin	Security Bulletin associated with the solution.
Product Categories	Product categories to which the solution applies.
Products	Products to which the solution applies.
Solution Details	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	If no content is available from the solution source, you are directed to another relevant section or solution for more information.
Links	Imported internet resources associated with the solution.
Vulnerability Details	
Vulnerability notes	Summary of vulnerabilities remediated by the solution.
Remediation Status	
Preferred Solution Targets Remediation status for vulnerable items and their unique configuration items (CIs), for which this is the preferred solution. **Note:** A unique CI is one that is counted only once, regardless of how many VIs it is associated with.	
Vulnerable Items	Number of active (non-closed) vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
Total VIs	Number of active and closed vulnerable items for which this solution is preferred for remediation. This count excludes deferred vulnerable items.
% VIs remediated	Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred. This count excludes deferred VIs.
Remaining CIs	Number of unique CIs associated with one or more active vulnerable items for which this solution is preferred for remediation. This count excludes the CIs of deferred vulnerable items.
Total CIs	Number of unique CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation. This count excludes the CIs of deferred vulnerable items.
% CIs remediated	Percent complete of unique CIs remediated (meaning all VIs for that CI and this solution are remediated). Determined by the number of remediated CIs over the total unique CIs associated to vulnerable items with the preferred solution. This count excludes the CIs of deferred vulnerable items.
Preferred Solution Targets (Includes Deferred) Remediation status for vulnerable items and their unique CIs, including deferred, for which this is the preferred solution.	
Vulnerable Items	Number of active (non-closed) vulnerable items for which this solution is preferred for remediation.
Total VIs	Number of active and closed vulnerable items for which this solution is preferred for remediation.
% VIs remediated	Percent complete for vulnerable item (VI) remediation. Applies to VIs for which this solution is preferred.
Remaining CIs	Number of unique CIs associated with one or more active vulnerable items for which this solution is preferred for remediation.
Total CIs	Number of unique CIs associated with one or more active and closed vulnerable items for which this solution is preferred for remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
% CIs remediated	Percent complete of unique CIs remediated (meaning all VIs for that CI and this solution are remediated). Determined by the number of remediated CIs over the total unique CIs associated to vulnerable items with the preferred solution. This count excludes the CIs of deferred vulnerable items.
Potential Solution Targets Remediation status for vulnerable items and their unique CIs, with a vulnerability related to this solution.	
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is a potential solution for remediation. This count excludes deferred vulnerable items.
Remaining CIs	Number of unique CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation. This count excludes deferred vulnerable items.
Potential Solution Targets (Includes Deferred) Remediation status for vulnerable items and their unique CIs, including deferred, with a vulnerability that can be remediated by this solution, including preferred solution counts.	
Vulnerable items	Number of active (non-closed) vulnerable items for which this solution is a potential solution for remediation.
Remaining CIs	Number of unique CIs associated with one or more active vulnerable items for which this solution is a potential solution for remediation.
Notes	
Internal notes	Editable field provided for the remediation specialist.
Related Links	
Update status	Date and time when the Remediation status was last updated. Updates the following: • Remediation task state • Risk score and rating • Metrics from the Remediation Status section
Related Lists	
Vulnerable Items	Vulnerable items associated with this solution as the preferred solution for remediation.
Third-Party Vulnerabilities	Third-party vulnerabilities associated with this solution.
CVEs	Common Vulnerability and Exposure (CVE) vulnerabilities associated with this solution.
Remediation Tasks	Remediation tasks that contain related vulnerable items with this solution preferred for remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Preceding Solutions	Earlier solutions which resolve one or more of this solution's vulnerabilities.
Superseding Solutions	Later solutions that resolve all of this solution's vulnerabilities. This list is empty when the **highest-supersedence** box is checked.

Approval workflow configurations for unassign request

You can design the approval workflow for the removal of assignments from vulnerable items (VIs, VITs), remediation tasks, application vulnerable items (AVITs), and container vulnerable items (CVITs) for you and your group.

VIT, remediation task, AVIT, and CVIT have a default approval rule each. Each approval rule has a default approval configuration. Each approval configuration has a default approver level. The approval rules for VITs, remediation task, AVIT, and CVIT are enabled by default. As an admin, you can perform the following actions by navigating to **All** > **Vulnerability Response** > **My Approvals** > **Approval Rules** and selecting the appropriate approval rule.

- enable or disable an approval rule.
- create and update an approval configuration.
- define conditions for vulnerable items and remediation tasks for which the approval rules apply.
- create and update multiple approver levels.

The following table shows the default approval rules, approval configurations, and approver levels for a VIT, remediation task, AVIT, and CVIT which are shipped with the base system.

Default approval rules, approval configurations, and approver levels

Type	Approval Rule	Approval configuration	Approver levels
VIT or VI	Vulnerable item field change request	Vulnerable item field change request	Level-1 Unassign Request for VI
Remediation task	Vulnerability Group field change request	Vulnerability field change request	Level 1 - Unassign Request for VG
AVIT	Application vulnerable item field change request	Application vulnerability field change request	Unassign app vulnerability item
CVIT	Approval for container management	Default Configuration Unassign CVIT	CVIT unassign approval level - 1

For more information on how to approve unassign requests, see Approve or reject an unassign request in Vulnerability Response.

Vulnerability Response remediation task rule examples

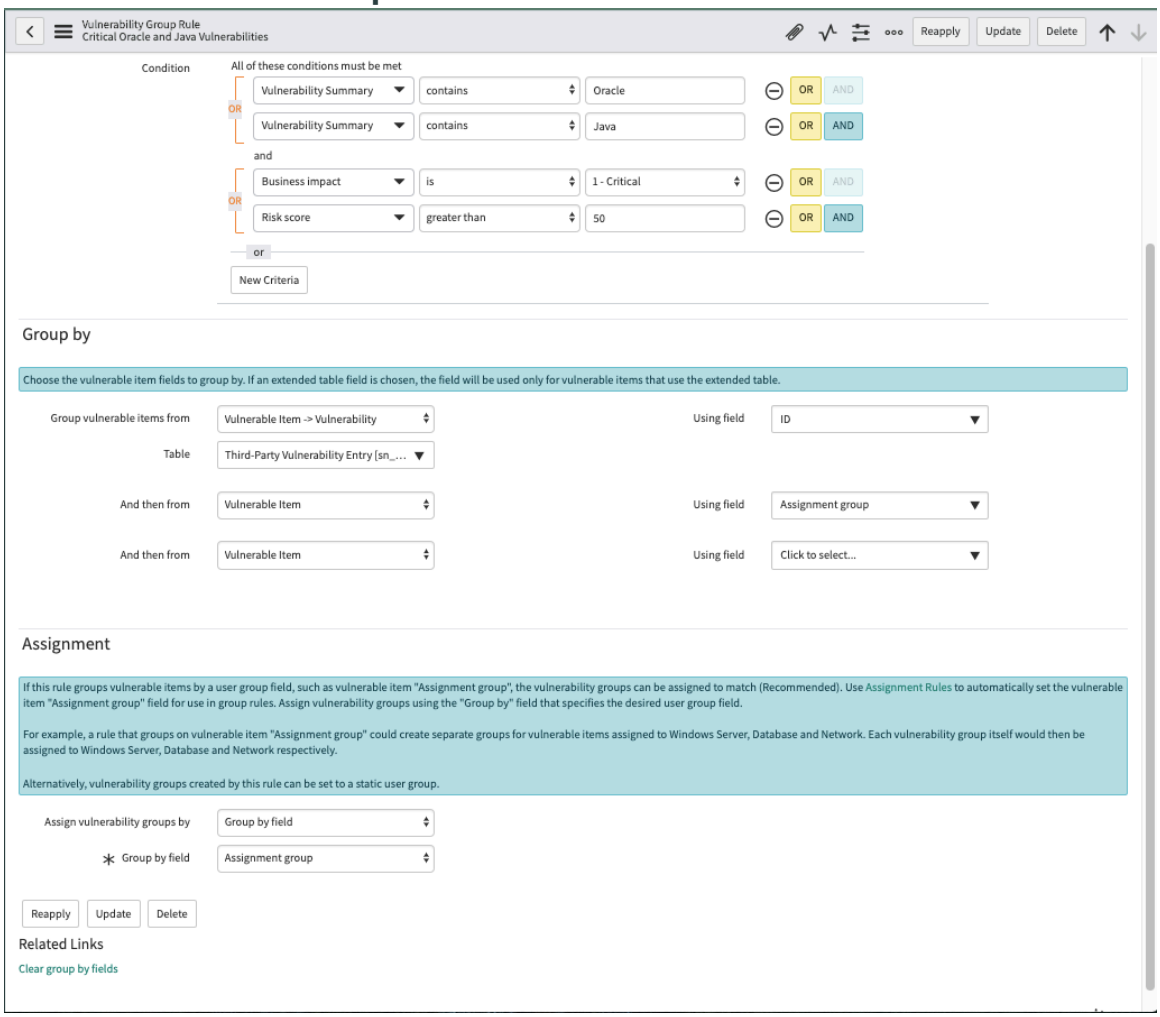
Examples of remediation task rules using vulnerability and risk, or impact, or configuration item (CI).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task rule to group high risk Java and Oracle vulnerable items

This example shows a walk-though of the rule that groups Java and Oracle vulnerable items by vulnerability and assigns them to their respective support groups.

Remediation Task Rule example

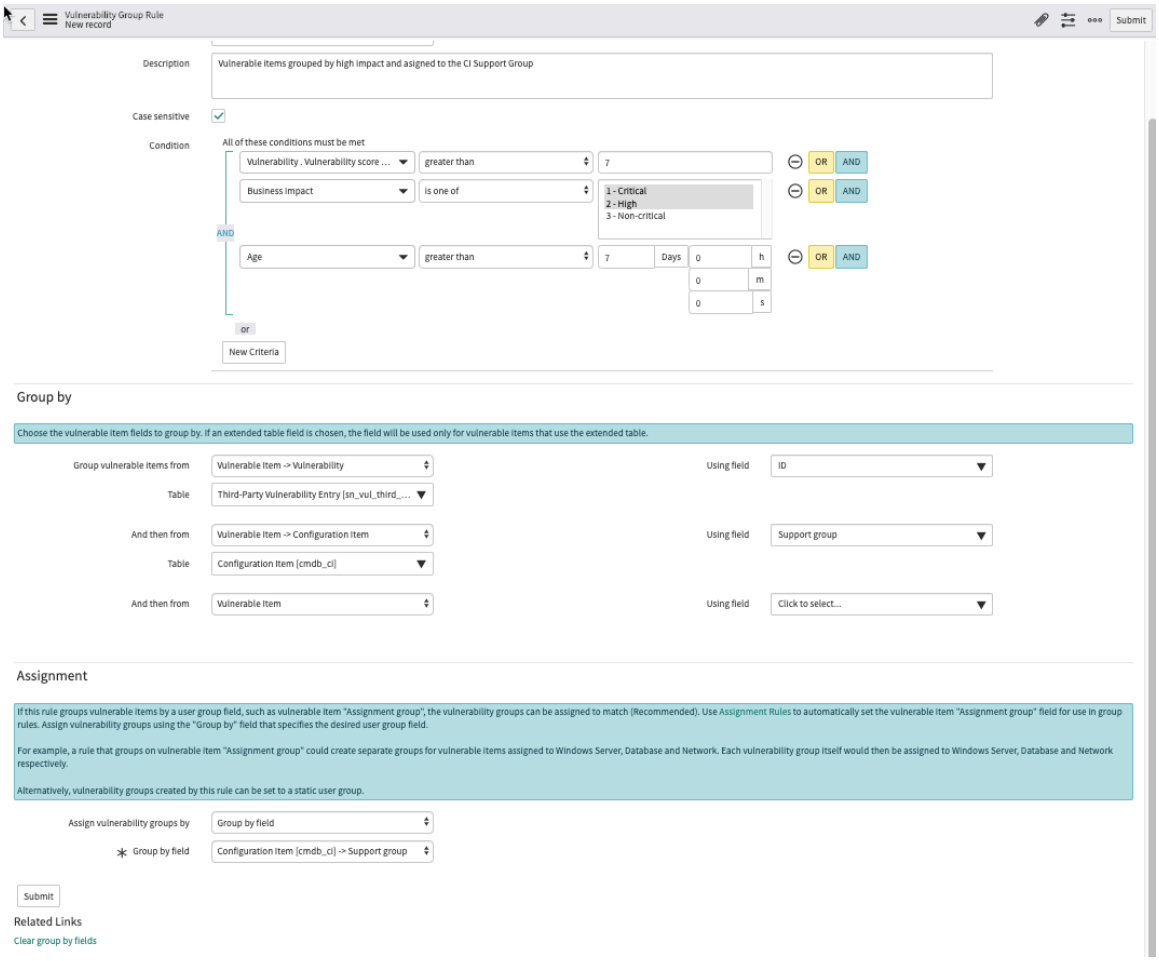


Right-click in the header to **Save**.

Remediation task rule to group all high impact vulnerable items by Vulnerability and CI support group

This example shows the form field settings for a group rule for high impact vulnerable items that assigns them to the CI support group.

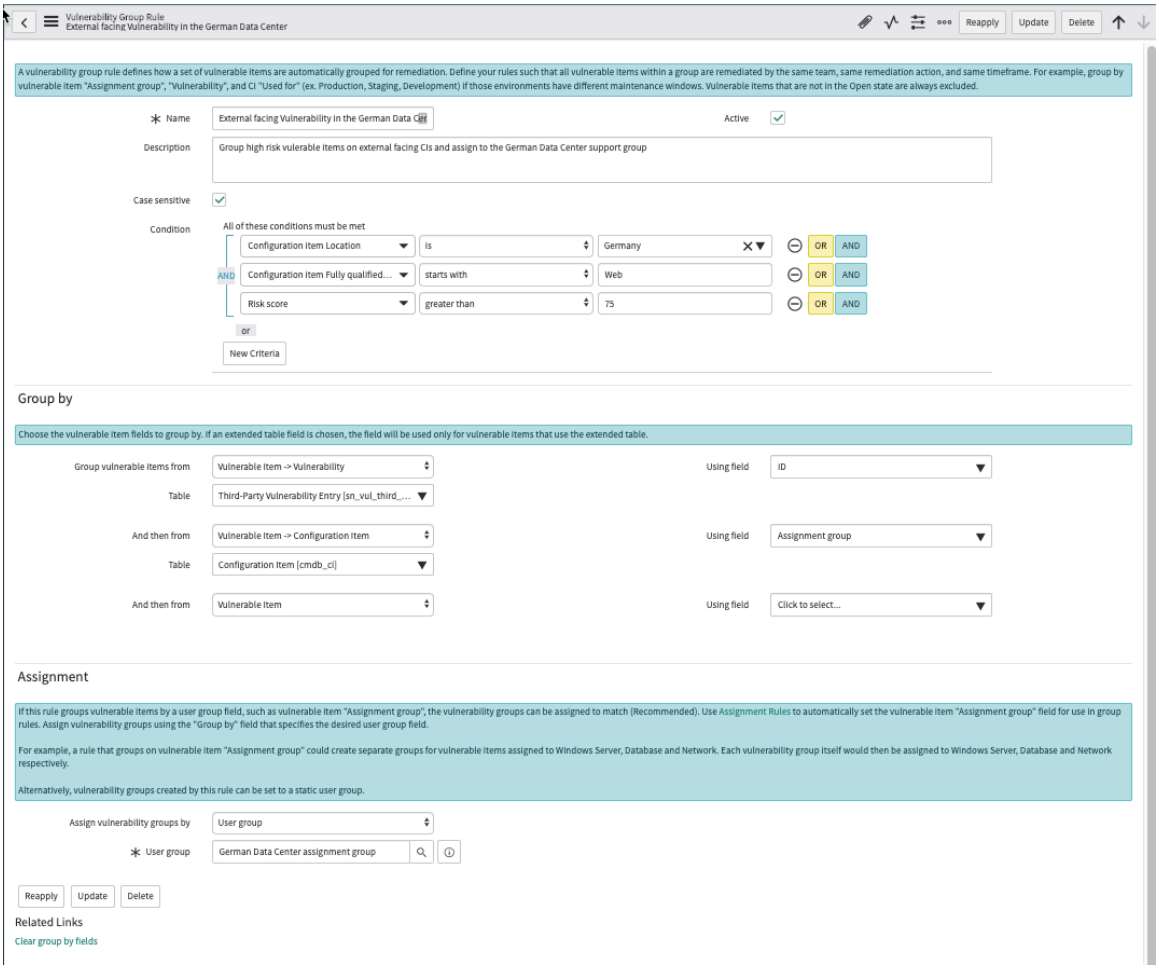
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Remediation task rule to group all the high risk vulnerabilities on an external-facing CI in a German data center

This example shows the form field settings for a group rule for high risk vulnerabilities on external facing CIs in a German data center. They are assigned to the German data center assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Risk score calculation example for Vulnerability Response

You can determine the risk score calculators to generate risk scores that use the vulnerability and asset data unique to your organization.

Example of determining risk rule calculators scores

The following example demonstrates how scores for risk rule calculators are determined.

Assume that a risk rule calculator is configured with the fields in this table:

Field	Weightage	Weight breakdown
Vulnerability.Severity	50	Default: 20 1 - Critical: 100 2 - High: 80 3 - Medium: 60 4 - Low: 40 5 - None: 20
Vulnerability.Exploit Exists	50	Default: 50

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Weightage	Weight breakdown
		Yes: 100 No: 0

Also, assume that the vulnerable items that are shown in this table are present in the system:

ID	Vulnerability severity	Vulnerability exploit exists
VIT00001	1 - Critical	1 - Yes
VIT00002	2 - High	1 - Yes
VIT00003	3 - Medium	2 – No
VIT00004	4 - Low	2 – No
VIT00005	5 - None	2 – No

The risk score calculation for the vulnerable items is calculated based on the formula:

```
Risk Score = (W(severity) * FV (severity). + W(exploitexists) *
FV(exploit exists)) / 100
```

where **W** is the weight and **FV** is the weight percentage of the field value.

The resulting risk score for these vulnerable items is described in this table:

ID	Vulnerability severity (50%)	Vulnerability exploit exists (50%)	Resultant risk score
VIT00001	1 – Critical (50% x 100)	1 – Yes (50% x 100)	100
VIT00002	2 – High (50% x 80)	1 – Yes (50% x 100)	90
VIT00003	3 – Medium (50% x 60)	2 – No (50% x 0)	30
VIT00004	4 – Low (50% x 40)	2 – No (50% x 0)	20
VIT00005	5 - None (50% x 20)	2 – No (50% x 0)	10

Note: For VIT00005, because the value of the severity is empty, the default weightage is applied.

If the weightage percentage is changed for one of the field values, see this table for the results:

Field	Weightage	Weight breakdown
Vulnerability.Severity	50	• Default: 20 • 1 - Critical: 100 • **2 - High: 70** *revised value

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Weightage	Weight breakdown
		• 3 - Medium: 60 • 4 - Low: 40
Vulnerability.Exploit Exists	50	• Default: 50 • Yes: 100 • No: 0

The risk score for the vulnerable items after reapplying the calculator is shown in this table:

ID	Vulnerability severity (50%)	Vulnerability exploit exists (50%)	Resultant risk score
VIT00001	1 – Critical (50% x 100)	1 – Yes (50% x 100)	100
VIT00002	**2 – High (50% x 70)** *revised value	1 – Yes (50% x 100)	**85** *revised value
VIT00003	3 – Medium (50% x 60)	2 – No (50% x 0)	30
VIT00004	4 – Low (50% x 40)	2 – No (50% x 0)	20
VIT00005	5 - None (50% x 20)	2 – No (50% x 0)	10

Error handling for detections

Errors are logged while creating detections, or creating and updating vulnerable items, while processing the attachments. If a vulnerability integration process fails, errors are logged in the 'Vulnerability Integrations Log' tab.

These errors are logged, with one of the following categories.

Field	Description
VI creation	Error while creating or updating the detection.
Detection	Error while creating a detection.

Mobile experience for Vulnerability Response

As a remediation owner, you can access the Vulnerability Response (VR) application on your ServiceNow AI Platform® instance with your Android or iOS mobile device.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response

To familiarize yourself with the concepts of vulnerability response and how this product can help your organization, see Understanding Vulnerability Response.

Note: Before you install the Vulnerability Response Mobile app mobile, familiarize yourself with the Mobile Agent.

Overview

As a user with the remediation owner role (sn_vul.remediation_owner), the Vulnerability Response Mobile app allows you to view and search the vulnerabilities, remediation tasks, and assignments on your ServiceNow AI Platform instance directly from your Android or iOS mobile device.

You are notified when remediation tasks (RTs) or VIs have been assigned to you or your assignment group. This app gives a remediation owner the flexibility to reassign, edit fields, and begin remediation without being tied to the desktop.

You have access to vulnerabilities, vulnerability items, modules, and all solutions. You can perform the following tasks on your mobile device:

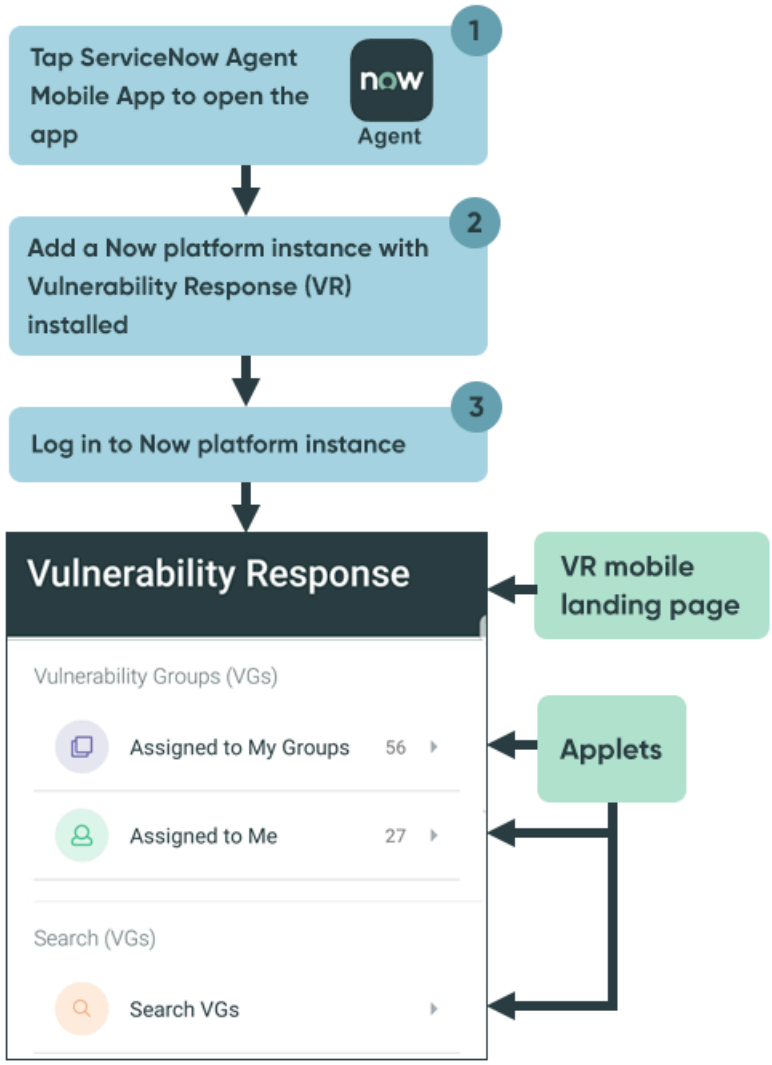
- View and update remediation tasks.
- View change requests.
- Reassign a remediation task or vulnerability item to another member of an assignment group.
- View notifications when a critical remediation task is assigned to you or one of your assignment groups.
- Edit a subset of fields on remediation task records.
- Search for remediation tasks that match specific search criteria.

The following figure illustrates how you log in to your ServiceNow AI Platform instance from your mobile device and the landing screen of the Vulnerability Response Mobile app that is displayed after you log in.

For step-by-step instructions about how to set up your ServiceNow AI Platform instance and install the Vulnerability Response Mobile app, see Set up checklist for the Vulnerability Response Mobile app. For instructions about how to log in, see Log in to the Vulnerability Response Mobile app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response Mobile app



Applications

Applications are the ServiceNow software components such as Security Incident Response (SIR), Vulnerability Response (VR), Governance, Risk, and Compliance (GRC) and other ServiceNow products that provide specific features and functionalities within your ServiceNow AI Platform instance. After you install core applications that have mobile apps on your ServiceNow AI Platform instance, these applications are displayed as icons on the bottom of your mobile device.

Vulnerability Response icon on mobile device

Folders

Each ServiceNow® mobile application contains folders that separate the applets by categories. In the preceding image, remediation tasks and Search (VGs) are the folders for the Vulnerability Response Mobile app.

Applets

Applets are the different options within the application. In the preceding image, the icons under remediation tasks and Search (VGs) are the available applets for the Vulnerability Response Mobile app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See the following topics for more information about the applets of the Vulnerability Response Mobile app.

Set up checklist for the Vulnerability Response Mobile app

The following checklist includes the set up tasks that you are required to complete in your ServiceNow AI Platform® instance and on your mobile device prior to using the Vulnerability Response Mobile app.

Before you begin

More information follows each step in the right column. Estimated time to complete this task: 15-20 minutes.

Roles required: admin, sn_vul.remediation_owner

You have successfully set up your mobile device for the Vulnerability Response Mobile app. The next step is to log in to the Vulnerability Response Mobile app and add a ServiceNow AI Platform instance to your mobile device.

Procedure

1. As an option, print this checklist and use it to guide you through the tasks that are required to install the Vulnerability Response Mobile app.
2. Verify that each item on the list is completed so that you can log in to the Vulnerability Response Mobile app and add a ServiceNow AI Platform instance.

Mobile checklist

Item	Description
☐	As a user with the admin role, verify that you have the Vulnerability Response core application installed on a ServiceNow AI Platform instance. This is the ServiceNow AI Platform instance that you view on your mobile device. **Note:** The Vulnerability Response core application and the ServiceNow AI Platform instance should be from the same family release. **a.** To verify the core application is installed on your instance, navigate to **Plugins** and search for Vulnerability Response. **b.** If the Vulnerability Response core application is not already installed, click **Install** to install it. For more information about installing the Vulnerability Response core application, see Install Vulnerability Response. For more information about obtaining the Vulnerability Response core application on the ServiceNow Store, getting entitlement, installing core applications, and activating dependencies, see Security Operations and the ServiceNow Store.
☐	As a user with the admin role, verify that you have the Vulnerability Response Mobile app installed on the ServiceNow AI Platform instance that you want to view on your mobile device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
	Note: The Vulnerability Response Mobile app and the ServiceNow AI Platform instance should be from the same family release. The Vulnerability Response Mobile app and the Vulnerability Response application should be compatible. For more information on Vulnerability Response application compatibility, see Vulnerability Response and Configuration Compliance Compatibility Matrix. Download and install the Vulnerability Response Mobile app from the ServiceNow Store on your ServiceNow AI Platform instance. When you install the Vulnerability Response Mobile app, its dependencies, com.glide.sg and com.glide.sg.agent_native_client, are also installed. To verify that these dependencies are installed: **a.** Navigate to **All** > **Plugins**. **b.** Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client). **c.** If they are not activated, activate these plugins. These plugins are required for the Vulnerability Response Mobile app. For more information about obtaining the Vulnerability Response Mobile app application on the ServiceNow Store, getting entitlement, installing applications, and activating dependencies, see Security Operations and the ServiceNow Store.
☐	As a user with the admin role, in your ServiceNow AI Platform instance, verify that you have assigned mobile users with the required ServiceNow AI Platform roles. **a.** To view the roles that are assigned to a user, navigate to **All** > **Administration** > **Users**. **b.** Select the user name followed by the roles related list. All roles assigned to this user are displayed. **c.** Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, update and close change requests and remediation tasks. Only users with the itil role can have tasks assigned to them. **d.** Verify a user is assigned, or assign a user with the remediation owner role (sn_vul.remediation_owner). Users with the sn_vul.remediation_owner role can read vulnerability and solution records. This role is automatically added when you assign the itil role. **e.** Verify you have created any required assignment groups and assigned mobile users to these groups. **Note:** If you have a large number of users for the mobile application, you alternatively can assign the sn_vul.remediation_owner role to a group. Each user you add to the group inherits this role. For more information about assignment rules and groups, see Vulnerability Response assignment rules overview.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
	For more information on users and assigning roles to users and groups, see User administration.
☐	As a user with the remediation owner role (sn_vul.remediation_owner), download the most current ServiceNow® Agent app on your mobile device.  The most current Agent app is available on the Apple iOS App Store and the Google Play Store.
☐	As a user with the sn_vul.remediation_owner role, verify notifications are enabled on your mobile device and in your ServiceNow AI Platform instance. Notifications inform you when critical remediation tasks are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the Vulnerability Response Mobile app and navigate directly to the record. To enable notifications in your ServiceNow AI Platform instance so they are displayed on your mobile device, follow these steps. **a.** Verify you have downloaded and installed the Vulnerability Response Mobile app on your ServiceNow AI Platform instance. **b.** In System Settings in your ServiceNow AI Platform instance, under Notifications, verify you have enabled the **ServiceNow Mobile Application**. For more information about setting notifications, see Setting notification preferences in Core UI. ServiceNow AI Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device.

Log in to the Vulnerability Response Mobile app

Open the Vulnerability Response Mobile app and add a ServiceNow AI Platform instance with Vulnerability Response to your mobile device.

Before you begin

Verify that you have completed the setup steps described in Set up checklist for the Vulnerability Response Mobile app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



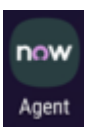
Role required: Remediation owner (sn_vul.remediation_owner)

About this task

Time to complete this task: 5-7 minutes.

Procedure

1. On your mobile device, tap the **ServiceNow Agent** app.



   If you are not already logged in to a ServiceNow AI Platform instance, the Instances screen is displayed.

2. If the ServiceNow AI Platform instance with the Vulnerability Response core application is not already added to your mobile device, follow these steps to add it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. On the Instances screen that is displayed, tap the plus icon ().
A screen is displayed that prompts you to enter and save an address of a ServiceNow AI Platform instance.

b. Fill in the fields.

Field name	Description
Enter the instance address or scan a QR code.	Choose one to continue: ▪ Before the `.service-now.com`, enter the name of your ServiceNow AI Platform instance, for example, `vrmobilenewyorkagent`. ▪ Enter an address. This address is the URL of your ServiceNow AI Platform instance that you want to view on your mobile device. ▪ Scan a QR code.
(Optional) Enter nickname	Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a ServiceNow AI Platform instance.

c. Tap **Save and Login**

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the ServiceNow AI Platform instance that you want to add and tap **Login**.
The Vulnerability Response landing screen is displayed. You have successfully logged in to the Vulnerability Response Mobile app !
4. After you log in, verify notifications are enabled in the Vulnerability Response Mobile app.

a. On the landing screen on the bottom, tap **Notification**.

b. On the Notifications screen, tap **Enable Notifications** if not enabled.
Notifications from the ServiceNow AI Platform are displayed on the Notifications screen in the Vulnerability Response Mobile app.

5. After you login to an instance on your mobile device, it is the default ServiceNow AI Platform instance on the device.
If you want to view another ServiceNow AI Platform on the device, you must log out of the default instance. To log out:

a. Tap the **Settings** icon.

b. Tap **Logout**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Instances screen is displayed with any ServiceNow AI Platform instances you have added to the mobile device.

c. **Optional:** Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

Result

If the instances screen for the Vulnerability Response Mobile app is not displayed after you tap the **ServiceNow Agent** app on your device, verify that the **ServiceNow Agent** is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings and general device management on your device and tap the option (Trust app, etc.) to permit access.

If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the ServiceNow AI Platform instance is correct.

If you have problems viewing the landing screen, verify your network connection.

If you cannot view the Instances screen after you tap the **ServiceNow Agent** app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.

View, assign, and edit remediation tasks with the Vulnerability Response Mobile app

View, assign, or edit the fields on remediation task (RT) records assigned to your group. Navigate through vulnerabilities, vulnerability items, and solutions records and related lists to view solutions, deployment metrics, and items to address.

Before you begin

Role required: Remediation owner (sn_vul.remediation_owner)

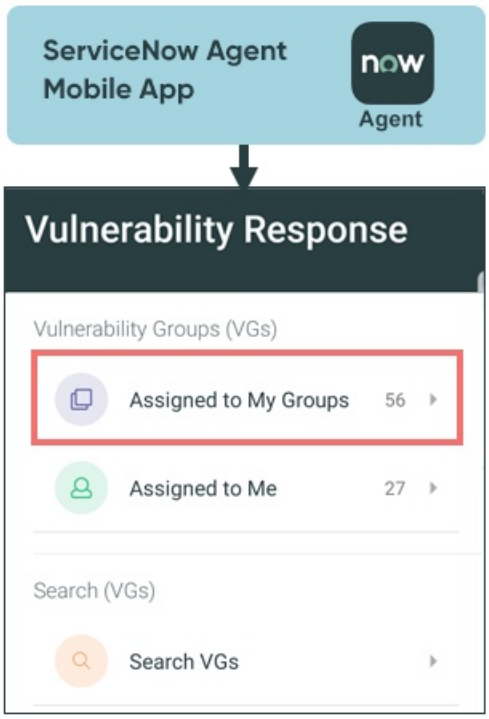
About this task

Assign RT (VUL) records to yourself or reassign them to another member of your group. Alternatively, view the details of active remediation task records, Vulnerable Items (VI), NVD vulnerabilities, and solutions prior to editing, assignment or remediation. Time to complete this task: 5-10 minutes.

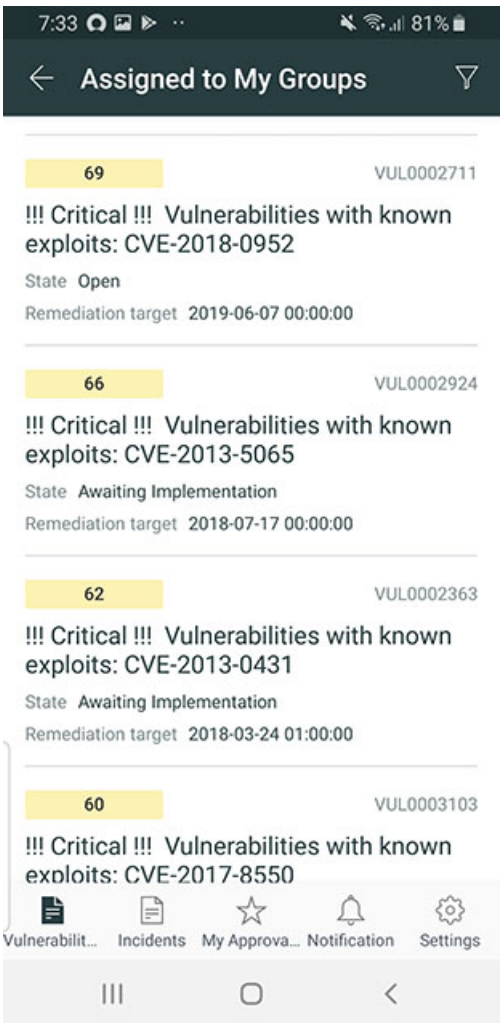
Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.
2. With the Vulnerability Response landing screen displayed, tap **Assigned to My Groups**.
   If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

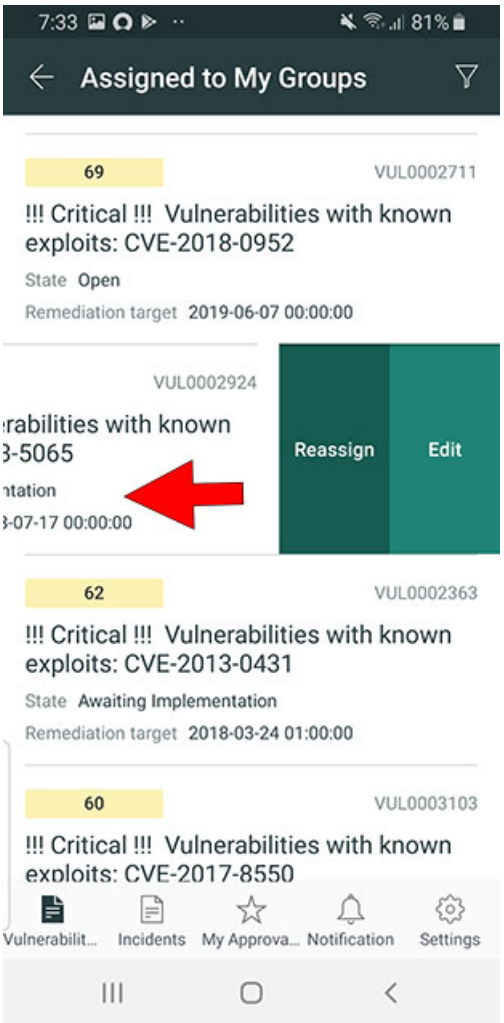


The list of open records assigned to your group is displayed.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. **Optional:** Refer to Search for remediation tasks with the Vulnerability Response Mobile app to search for records that match specific criteria.
4. Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list.
   Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.
5. To reassign or edit a record directly from the list, with the list of open records displayed, swipe left on a record to open the menu.



6. Choose one from the menu that is displayed to continue.

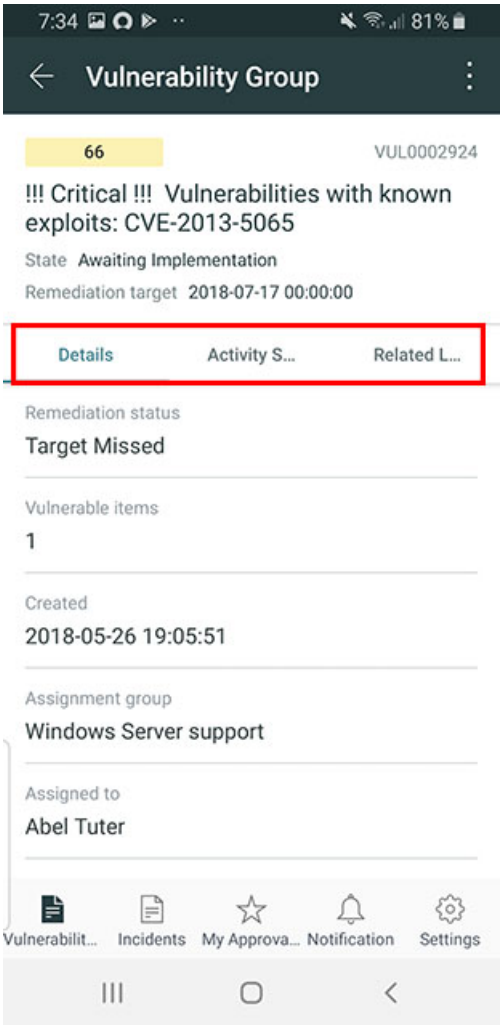
Option	Description
Assign to me	If the RT record is already assigned to you, this option is not displayed. Tap **Assign to Me** to assign the RT to yourself. Your name is displayed in the Assigned to field on the record. A message is displayed that confirms the as signment.
Reassign	To reassign the RT to an assignment group:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	a. Tap **Assignment group**. **b.** From the list, tap a group or enter text in the search field. To assign or reassign the RT to a member of an assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed or enter text in the search field. Tap the send icon () or **Submit** to save and submit your changes.
Edit	**a.** Tap **Edit**. **b.** Expand the fields and select an option from the list that is displayed or enter text in the Search field. Tap the send icon () or **Submit** to save and submit your changes.

7. Alternatively, to view the details of an open vulnerability record and to see more associated records and related lists, with the Assigned to My Groups screen displayed, tap a record on the list.
8. On the open remediation task record that is displayed, choose one option from the following table to the view work notes or the related lists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Option	Description
Details tab	With the Details tab selected, review the fields of the RT record. Tap the menu icon ( ) on the upper right of the screen to view the available options. The options that are displayed in this expanded menu vary. The remediation actions you can take on your vulnerable items vary and depend on the value that is displayed in the State field of the record. For more information about the State field and your remediation options, see Vulnerability Response remediation task and vulnerable item states.
Activity Stream tab	With the Activity Stream tab selected, choose one to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ View the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon ( ) to add a work note or at tach a file. ○ Tap the menu icon ( ) on the upper right of the screen to view the available remedia tion options.
Related Lists	With the Related Lists tab selected, view any of the related lists of the RT record that are populated. ○ Tap **Vulnerable Items**. Tap a Vulnerable item (VI) record and navigate to the pre ferred solution record. Refer to the figure that follows the table for a navigation map and more details. ○ Tap **Change Requests**. View a list of the change requests that are associated with this record. ○ When displayed, tap the menu icon ( ) on the upper right of a screen to view the available remediation options.

The following image illustrates the navigation path from the remediation task record to the preferred solution record for the selected vulnerability. Navigate through the records and related lists to view solutions, deployment metrics, and items to address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Navigation path from remediation task through a Solution record



9. After reviewing, editing, or remediation, choose one to continue.

Option	Description
Tap an icon on the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Vulnerability Response icon to re turn the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Vulnera bility Response Mobile app. ○ Tap **Settings** and choose one to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

View, reassign, and edit remediation tasks assigned to you with the Vulnerability Response Mobile app

View, assign, or edit the fields on remediation tasks records that are assigned to you. Navigate through records and related lists to view solutions, deployment metrics, and items to address.

Before you begin

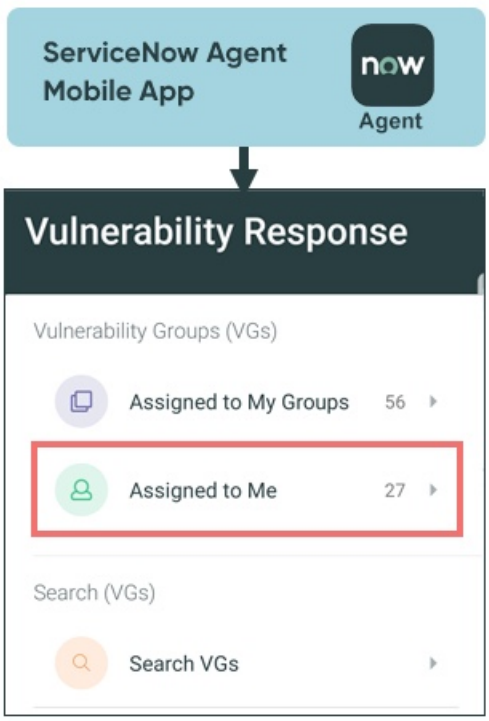
Role required: Remediation owner (sn_vul.remediation_owner)

About this task

Reassign or edit records assigned to you. View the details of active remediation tasks records, Vulnerable Items (VI) records, Vulnerabilities, and Solutions prior to editing, assignment or remediation. Time to complete this task: 5-10 minutes.

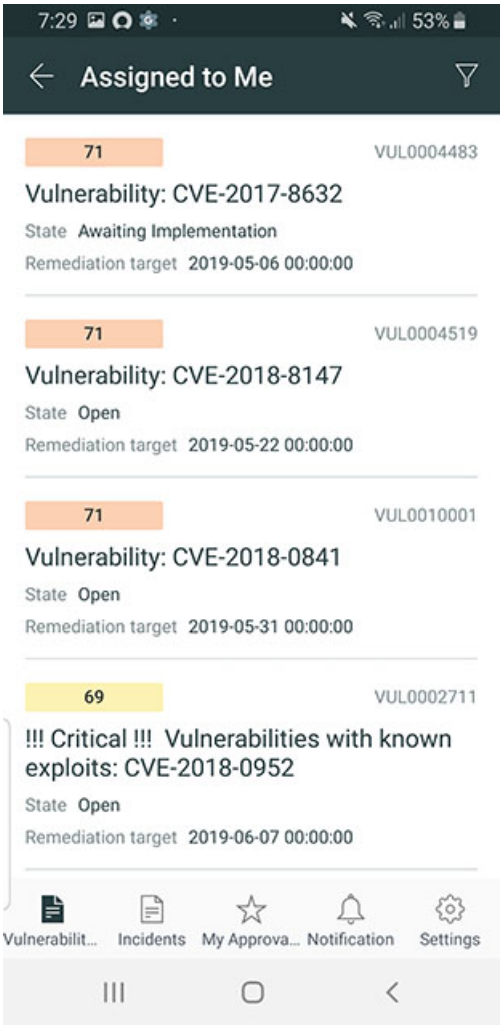
Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.
2. With the **Vulnerability Response** landing screen displayed, tap **Assigned to Me**.
   If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



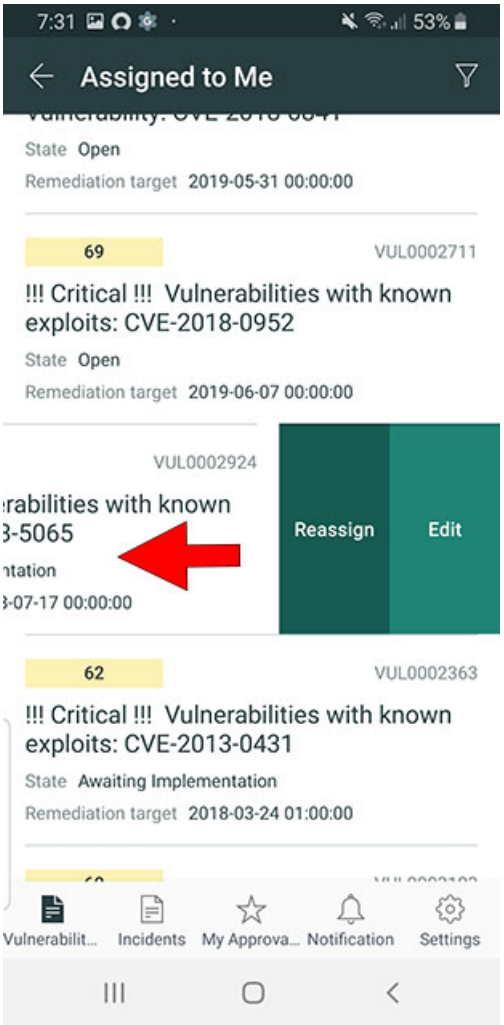
The list of remediation task records that are assigned to you is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for remediation tasks with the Vulnerability Response Mobile app to search for records that match specific criteria.
4. Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list.
   Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.
5. To reassign or edit the record directly from the list, with the Assigned to Me screen displayed, swipe left on a record to open the menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



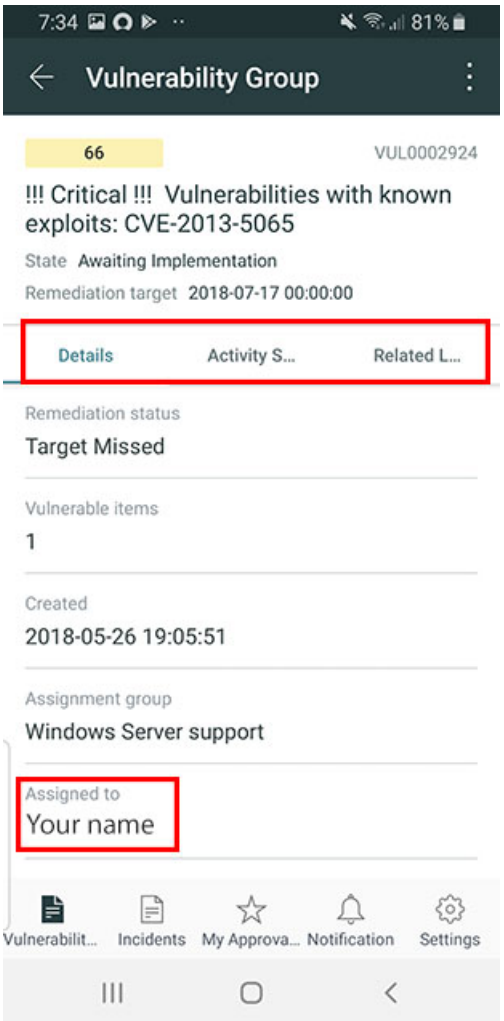
6. Choose one to continue.

Option	Description
Reassign	To reassign the task to another assignment group: **a.** Tap **Assignment group**. **b.** Tap a group from the list that is displayed or enter text in the search field. To assign or reassign the RT to a member of an assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed or enter text in the search field. Tap the send icon ( ) or **Submit** to save and submit your changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Edit	**a.** Tap **Edit**. **b.** Expand the fields and select an option from the list that is displayed or enter text. **c.** Tap the send icon ( ) or **Submit** to save and submit your changes.

7. Alternatively, to view the details of an open record and to see more associated records and related lists, with the Assigned to Me screen displayed, tap a record on the list.
8. On the open remediation task record that is displayed, choose one option from the following table to the view work notes or the related lists.



Option	Description
Details tab	With the Details tab selected, review the fields of the remediation task record. Tap the menu icon ( ) on the upper right of the screen to view the available options. The options that are displayed in this expand ed menu vary. The remediation actions you can take on your vulnerable items vary and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	depend on the value that is displayed in the State field of the record. For more information about the State field and your remediation options, see Vulnerability Response remediation task and vulnerable item states.
Activity Stream tab	With the Activity Stream tab selected, choose one to continue. ○ View the audit trail of work notes, activities, and additional comments of the record. Tap the plus icon ( ) to add a work note or attach a file. ○ Tap the menu icon ( ) on the upper right of the screen to view the available remediation options.
Related Lists tab	With the Related List tab selected, view the related lists of the record that are populated. ○ Tap **Change Requests**. View a list of the change requests that are associated with this record. ○ Tap **Vulnerable Items**. Tap a Vulnerable item (VI) record and navigate to the preferred solution record. Refer to the figure that follows the table for a navigation map and more details. ○ When displayed, tap the menu icon ( ) on the upper right of the screen to view the available remediation options.

The following image illustrates the navigation path from the remediation task record to the preferred solution record for the selected vulnerability. Navigate through the records and related lists to view solutions, deployment metrics, and items to address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Navigation path from RT through a Solution record



9. Choose one to continue.

Option	Description
Tap an icon on the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Vulnerability Response icon to re turn the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Vulnera bility Response Mobile app. ○ Tap **Settings** and choose one to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance. To log, tap **Logout**.

Search for remediation tasks with the Vulnerability Response Mobile app

Search for remediation tasks that match specific search criteria that you select.

Before you begin

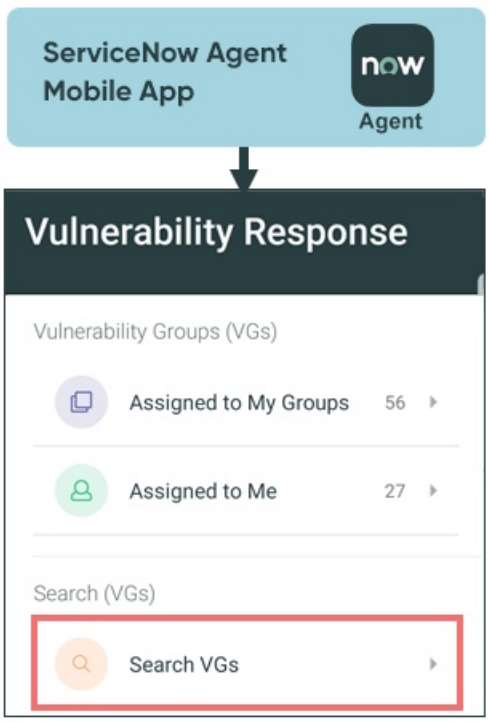
Role required: Remediation owner (sn_vul.remediation_owner)

About this task

Time to complete this task: 5-7 minutes.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Vulnerability Response Mobile app.
2. With the **Vulnerability Response** landing screen displayed, tap **Search RTs**.
   If you navigate away from the Vulnerability Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



3. On the Search screen that is displayed, tap the fields and fill out the form with your desired search criteria.

   Follow the instructions after the table to edit search criteria, clear search criteria, or submit a search.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tap this Field	To add an entry on Android devices	To add an entry on iOS devices
Number	Tap the screen and enter a RT number, for example, (VUL0002372) This number is displayed on the upper right of the RT record. Tap the check mark icon to add your entry and return to the Search RTs screen. Tap the close icon (X) to cancel your entry and return to the Search RTs field.	Enter a RT number, for example, (VUL0002372). This number is displayed on the upper right of the RT record. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.
Risk rating	Tap one or more items followed by the check mark icon to add your entry and return the Search RTs screen. Tap the close icon (X) to cancel your entry and return to the Search RTs field.	To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.
Remediation status	Tap one or more items followed by the check mark icon to add your entry and return the Search RTs screen. Tap the close icon (X) to cancel your entry and return to the Search RTs field.	To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.
State	Tap one or more items followed by the check mark icon to add your entry and return the Search RTs screen. Tap the close icon (X) to cancel your entry and return to the Search RTs field.	To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.
Reason	Tap one or more items followed by the check mark icon to add your entry and return the Search RTs screen. Tap the close icon (X) to cancel your entry and return to the Search RTs field.	To add an entry, tap one or more items, or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tap this Field	To add an entry on Android devices	To add an entry on iOS devices
Assignment group	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.
Assigned to	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.
Short description	Tap the screen and enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap the check mark icon to add your entry and return to the Search RTs screen.	On the screen enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the Search RTs screen.
Description	Tap the screen and enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap the check mark icon to add your entry and return to the Search RTs screen.	On the screen enter text. The feature recognizes text strings and partial text strings in this field, but wildcards (*) are not accepted. Capital letters are not required. Tap **Done** to return to the Search RTs screen. From the expanded field, tap **Cancel** to clear the entry and return to the SearchRTs screen.

For Android devices, with the Search RTs screen displayed and all your criteria entered, choose one to continue.

Option	Description
Clear or modify search criteria prior to exe cuting a search	To clear all entered criteria, with the Search RTs screen displayed, tap the back arrow to clear all the fields and return to the Vulnera bility Response landing screen. The search is not submitted and the search criteria are cleared. Alternatively, to edit a field, ○ With the Search RTs screen displayed, tap a field with search criteria to expand it. ○ Tap an item to deselect it. Tap All to select all items. Tap **All** again to clear all items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**. ○ Tap the check mark icon to save the changes and return to the Search RTs screen.
Submit a search	With the Search RTs screen displayed with your entered search criteria, tap the send icon (). The remediation task records that match your search criteria are displayed. After the search is completed, the search criteria are not saved.

4. For iOS devices, with the Search RTs screen displayed, choose one to continue.

Option	Description
Clear or modify search criteria prior to exe cuting a search	To clear all criteria and return to the landing screen, tap the close icon (X). Any entered search criteria are not saved. Alternatively, to edit a field: **a.** With the Search RTs screen displayed, tap a field with search criteria to expand it. **b.** Tap an item on the list to deselect it, or tap **Clear All**. To clear a value for the Assign ment group and Assigned to fields, for no entry, select **None**. **c.** Tap **Done** to save the changes and return to the Search RTs screen.
Submit a search	With the Search RTs screen displayed with your entered search criteria, tap **Search**. The RT records that match your search crite ria are displayed. After the search is complet ed, the search criteria are not saved.

5. **Optional:** If your search returns multiple records, you can Filter records with the Vulnerability Response Mobile app to refine the search results.

Filter records with the Vulnerability Response Mobile app

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

Before you begin

Role required: Remediation owner (sn_vul.remediation_owner)

About this task

Time to complete this task: 5 minutes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon ().
2. With the Filters screen displayed, tap a field to expand it.
   A common field to enter search criteria for remediation task records is the State field.
3. From the options that are displayed, tap the check box or tap an item for your filter.
   For many of the filters, you can select more than one option.
4. Tap the Back icon () or **DONE** to save your changes to a field.
   The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap **RESET** to remove any filters and restore the default setting.
5. **Optional:** Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.
6. Tap the intersection icon () to create AND conditions.
7. Alternatively, tap the intersection icon () to create OR conditions.
8. After you have added all the criteria you want, with the Filters screen displayed, tap **DONE**.
   On the screen, only the records that match your filter criteria are displayed.

Related topics

Search for remediation tasks with the Vulnerability Response Mobile app

Vulnerability Response Orchestration

With Vulnerability Response Orchestration workflows and activities you can interact with and retrieve data from Windows or UNIX-based systems and environments using workflow orchestration. By enriching data, you can shorten the remediation life cycle.

For more information on editing workflows or creating custom workflows, see Exploring flows.

Scan vulnerability workflow

The **Vulnerability Response** > **Scan Vulnerability** workflow rescans a remediation task.

Before you begin

Role required: none

About this task

This workflow is triggered by **Rescan vulnerable group** during a **Close/Ignore** action.

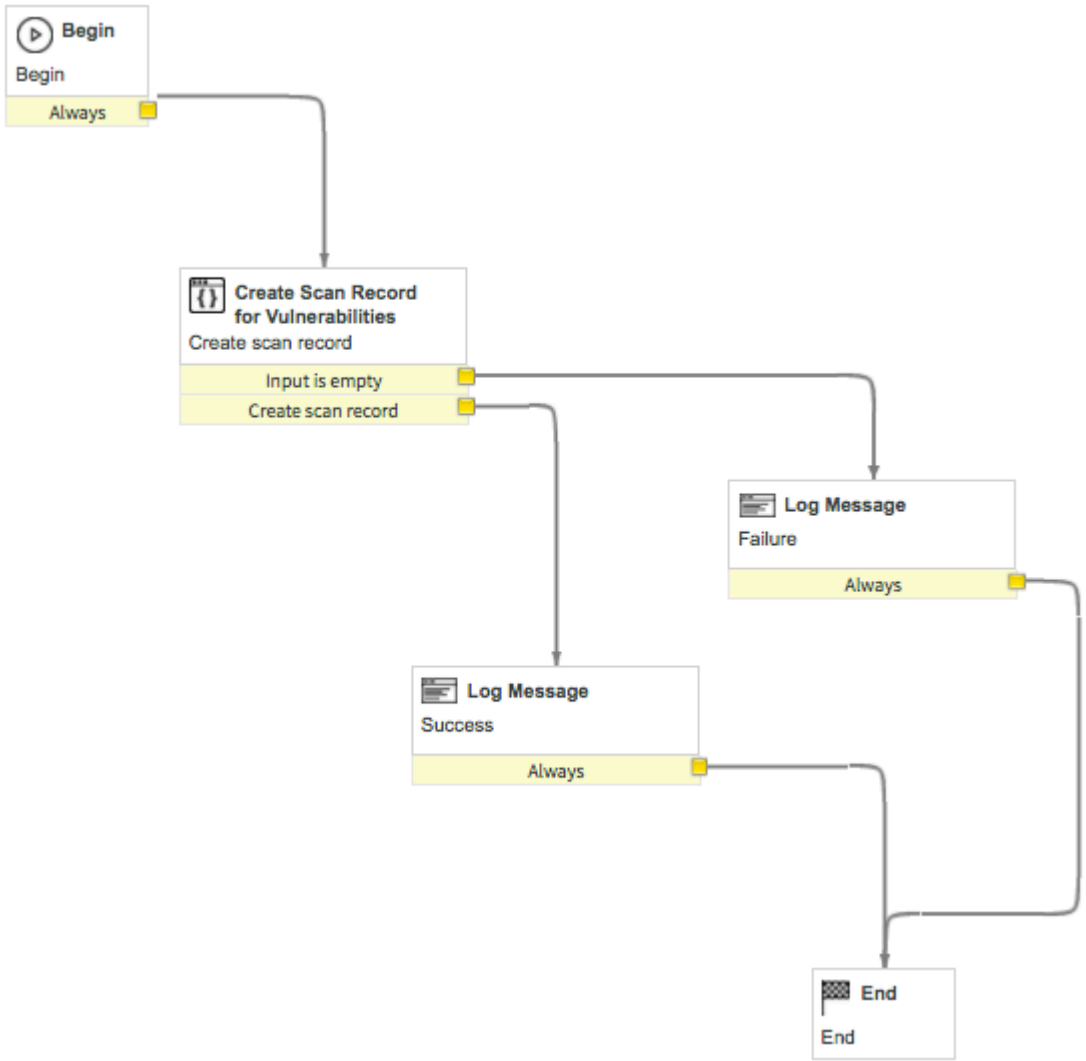
Workflow process activities include:

Variables for Create Scan Record for Vulnerabilities activity

Log Message

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scan Vulnerability workflow



Procedure

1. Navigate to **All** > **Vulnerability Response** > **Remediation Tasks**.
2. Open a task record (VUL).
3. Click **Close**.
4. Choose **Closed** for the **Desired State**.
5. Choose **Fixed** for the **Substate**.
6. Choose **Wait for confirmation from the next scan** for **Close now?**
   For the remediation task and vulnerable items, the **State** changes to **Pending Confirmation**, the **Substate** changes to **Fixed**, and a rescan runs.

Scan vulnerability item workflow

The**Vulnerable Response** > **Scan Vulnerability Item** workflow rescans a vulnerable item.

Before you begin

Role required: none

About this task

This workflow is triggered by **Rescan vulnerability**, during a **Close/Ignore** action.

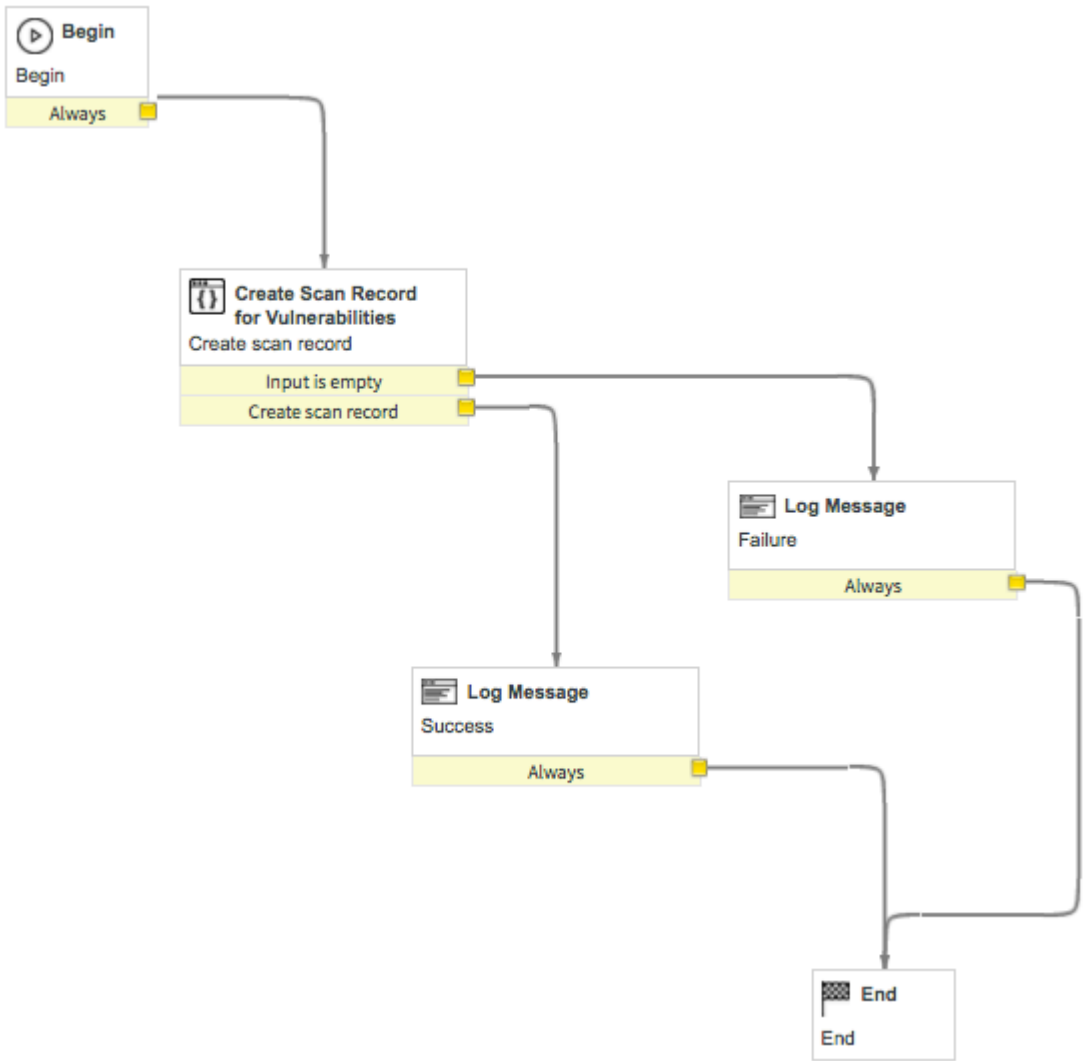
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Workflow process activities include:

Variables for Create Scan Record for Vulnerabilities activity

Log Message

Scan Vulnerability workflow



Procedure

1. Navigate to **Vulnerability** > **Vulnerabilities** > **Vulnerable Items**.
2. Open a vulnerability item.
3. Click **Close/Ignore**.
4. Choose **Closed**for the **Desired State**.
5. Choose **Fixed** for the **Substate**.
   The **State** of the group changes to **Pending Confirmation**, the **Substate** changes to **Fixed**, and a rescan runs.

Variables for Create Scan Record for Vulnerabilities activity

Vulnerability scans for single or multiple vulnerable items can be run using the **Create Scan Record for Vulnerabilities** workflow activity included in the base system. When the input is passed to the activity, it creates a scan record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
taskids [string]	A string of comma-separated sysIds that define the expected inputs. This field is mandatory.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
scanResult [Boolean]	Returns True if the input is not empty. A scan record is created for the taskIds.

Application Vulnerability Response

The Application Vulnerability Response (AVR) feature of the ServiceNow® Vulnerability Response application imports application vulnerable items (AVITs) and, according to rules, allows you to remediate application vulnerabilities. Vulnerability Response is available by separate subscription.

Starting with AVR v19.0, some key table and column names have been updated. As a result, you will see references to both the older and newer names in the documentation. For the complete list of updated terms, see Application Vulnerability Response product view.

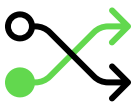
Starting with v19.0 of Vulnerability Response, You can ingest Software Composition Analysis (SCA) and Software Bill of Materials (SBOM) vulnerability data to help you identify weaknesses in your software applications. For more information, see Exploring Application Vulnerability Response and Veracode Vulnerability Integration.

Application Vulnerability Response

Explore	Configure	Integrate
		
Learn about Application Vulnerability Response concepts and features.	Configure Application Vulnerability Response.	Extend Application Vulnerability Response by integrating with other applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerability Response (continued)

Use the Vulnerability Response Workspaces  Learn how to monitor, manage, and remediate AVITs in the Vulnerability Manager, IT Remediation, and Vulnerability Assessment Workspaces.	**Remediate**  Learn how to remediate application vulnerabilities.	**Analytics & Reporting**  View Application Vulnerability Response analytics
Reference  Get details about Application Vulnerability Response components like fields, tables and properties.	**Upgrade Application Vulnerability Response to USEM**  Upgrade Application Vulnerability Response applications to Unified Security Exposure Management.	

Troubleshoot and get help

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring Application Vulnerability Response

Application vulnerabilities are vulnerabilities on your custom software applications that are scanned throughout the application's development life cycle.

Overview of Application Vulnerability Response and available versions

Application Vulnerability Response (AVR) is the part of the Vulnerability Response application that processes application vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions

Release version	Release Notes
Vulnerability Response v25.0, v24.0, v23.0	Application Vulnerability Response release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

How it works

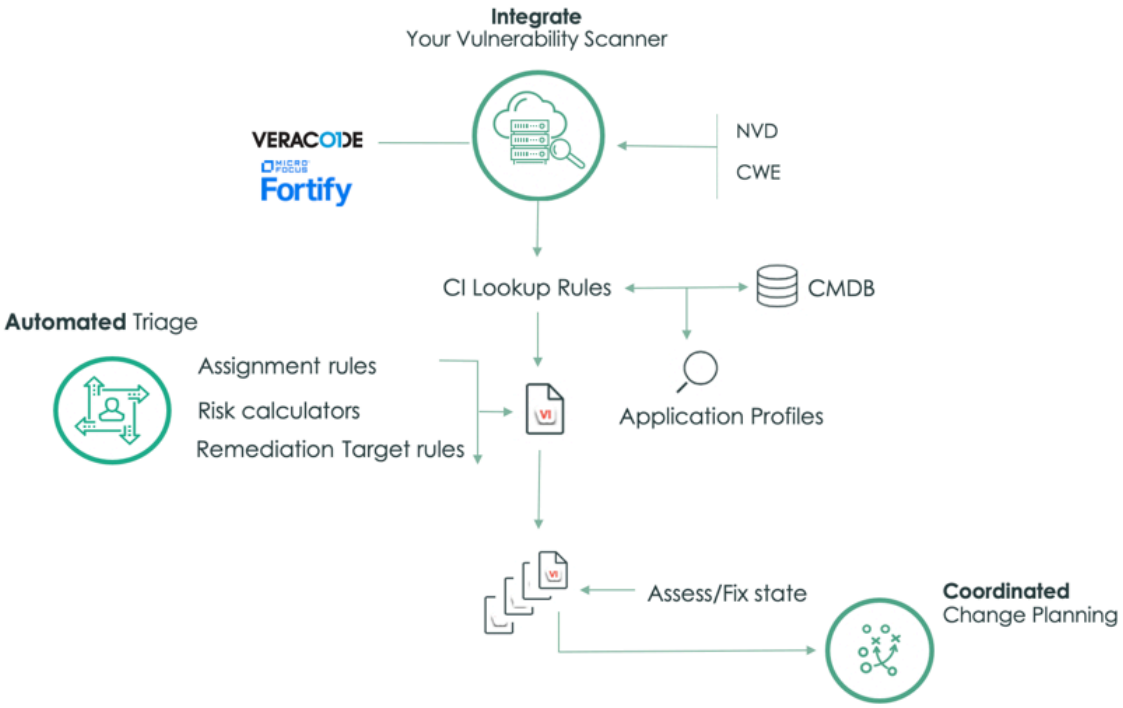
Vulnerability data is imported from internal and external sources, such as the Common Weakness Enumeration (CWE) or third-party integrations. After data is imported, it is compared to application data in your Configuration Management Database (CMDB) and processed in the Application Vulnerability Response application. If a match exists between imported application vulnerability data and data in your CMDB, an application vulnerable item (AVIT) is created.

The Application Vulnerability Response includes the following key features:

- Integrate with supported third-party scanners to import vulnerability data.
- Compare application vulnerability-related data and determine if application vulnerabilities are found in an application.
- Prioritize, remediate, and manage application vulnerable items (AVIT)s. Each application vulnerability represents a vulnerability entry in the CWE or third-party libraries.
- Starting with version 18.0 of Vulnerability Response, you can monitor and remediate AVITs in the Vulnerability Manager Workspace and IT Remediation Workspace respectively. For more information, see Vulnerability Manager Workspace and IT Remediation Workspace.
- Correlate Application Vulnerability Response data using calculators and libraries to help you perform the following tasks.
  - Create application vulnerable items automatically using **CI Lookup Rules**. During import, third-party vulnerabilities are associated to a CWE to create an AVIT.
  - Create assignment rules to automate application vulnerable item assignments.
  - Use calculator groups to determine business impact, specify varying conditions using filters, apply simple calculations, or use a script.
  - Create remediation target rules that define the expected time frame for remediating application vulnerable items so you can monitor upcoming remediation activities.
- Relate a single third-party vulnerability to multiple CWE entries and find the primary CWE for a vulnerability to help you determine risk. For more information on the **Primary CWE**, see Application Vulnerability fields.
- Use CWE records that are downloaded from the CWE database or imported from third-party integrations for reference to help you decide if you must escalate a vulnerability. Each CWE record also includes an associated knowledge article that describes the weakness.

Use Application Vulnerability Response to follow the flow of information, from integration through investigation, and then on to resolution.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Types of imported vulnerability data

Application Vulnerability Response supports the following types of imported application vulnerability data.

Note: Prior to v19.0, SAST, SCA, IAST, and penetration testing data was not ingested and may account for differences between what is shown within Veracode, Fortify, and Invicti and what appears in Application Vulnerability Response.

Dynamic Application Security Testing (DAST)

DAST scans find vulnerabilities application by sending input to your applications and monitoring its responses while they are running. This approach might imitate an outside attack. During dynamic scanning, a running service (URL) is scanned for vulnerabilities. Vulnerability results include a URL location of a discovered vulnerability.

Static Application Security Testing (SAST)

SAST scans review the source code of applications at rest and help you find vulnerabilities in the way you've written your code. The SAST scan takes place on non-compiled source code and so it exists independently of any application service. Returned results include a file and line number location of a discovered vulnerability.

Interactive Application Security Testing (IAST)

IAST scans detect software vulnerabilities by interacting with the program while it is running. Human observation, automated tests, and sensors are used in combination to interact with the application to locate vulnerabilities.

Software Composition Analysis (SCA)

Starting with v19.0 of Vulnerability Response, you can ingest Software Composition Analysis (SCA) vulnerabilities. SCA vulnerability data to helps you identify weaknesses in the open source software being used in your software applications.

Penetration testing

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You configure penetration test assessment requests in Application Vulnerability Response to help you understand where your application weaknesses are and what you can do to fix them.

Software Bill of Materials

Upload Software Bill of Materials (SBOM) data to identify vulnerabilities in your open source components. See Exploring Software Bill of Materials for more information.

Use cases

Some of the following DAST use cases are supported:

- Relate each vulnerability from scan results to some kind of cmdb_ci (child class).
- Relate DAST scan results to an existing application when there is a record in the CMDB from Discovery or a third-party integration.
- Relate DAST scan result to a newly inserted scanned application when a new Application has not previously been identified and/or stored in the CMDB.
- Store DAST scan results for a CMDB when you manage your applications in a product other than ServiceNow®.
- Store DAST scan results for a CMDB if you have previously customized for some other purpose.
- Create an application for Source code repository manually.

Some of the supported SAST use cases are supported:

- Relate each vulnerability from scan results to some kind of cmdb_ci (child class).
- Create a CI for Source code repository manually.
- Store SAST scan results that are without a related Application Service.

Third-party integrations

The third-party integrations supported by Application Vulnerability Response are available as a separate applications in the ServiceNow Store. See Integrating Application Vulnerability Response with other applications for more information.

Key features

- A shared API imports DAST, SAST, IAST, and SCA data and manual pen testing results. See Penetration testing.
- A separate API is used to import SBOM data. For more information, see Exploring Application Vulnerability Response and Veracode Vulnerability Integration.

CI lookup rules

Automatically search application data for matches in the Configuration Management Database (CMDB).

Assignment rules

Automatically assign application vulnerabilities based on user groups, user group fields, and scripts.

Risk Calculators

Automatically prioritize and rate the impact of AVITs using calculators, based on any criteria, by using condition filters.

Severity mapping

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Automatically calculate initial values for fields on application vulnerable items. Vulnerability entries have both source severity and normalized severity (based on severity mapping). Severity is tied to the Common Weakness Enumeration (CWE).

Remediation target rules

Define the expected time frame for remediating an application vulnerable item.

Reporting

Quickly gain insight into your security posture, remediation trends and top 10 Applications or Business Units with the most critical AVITs.

The common point for both types of scans is the application release. An application release, which defines a **Name** string, is the tie-in point to group scanned vulnerability results on the scanner side. This way AVR knows which application release the results belong to when importing scan results through the integration.

A Configuration Item [cmdb_ci] child table, Scanned Applications [sn_vul_app_scanned_application], was created in the Vulnerability Response application and scope. This table stores the Application Release abstraction and provides service graphing though its CMDB relationships. They can be viewed from the **All** > **Application Vulnerability Response** > **Administration** > **Applications** module. The list view for Scanned Applications contains the **Department** and **Support Group** added during setup.

Application Vulnerable Items (AVITs)

For application vulnerabilities, AVR relates a vulnerability to an application to create the application vulnerable item (AVIT) record. Because of the multiple definitions of what constitutes an application in the CMDB, Application Vulnerability Response limits applications to scanned applications. Scanned applications are the applications scanned in your environment identified by AVR as **Name** and **ID**. AVITs are based on the latest scan summary until confirmed **Fixed** by the scanner. If an AVIT is no longer found, it remains tied to the scan summary where it was last seen.

Application vulnerable items can be viewed from the **All** > **Application Vulnerability Response** > **Vulnerabilities** > **Vulnerable Items** module.

If an application is removed from the CMDB, any associated AVITs are closed.

For information on AVIT form fields, see Application Vulnerable Item fields.

User groups and roles in Application Vulnerability Response

Often a team works together to create, manage, and oversee the management of application vulnerabilities. There are strategic roles, as well as operational roles, among the team members. In most organizations, you may participate in more than one role and often share roles with others. Application Vulnerability Response uses three user groups containing granular roles: App-Sec Manager, Application Security Champion, and Developer. See Application Vulnerability Response user groups and roles for more information on these groups and roles.

Application Vulnerability Response states

Application Vulnerability Response offers a state model for the status of your application vulnerable items (AVITs) and helps you to determine when and how to remediate your AVITs.

An application vulnerable item has several possible states, see Application Vulnerable Item (AVI) states for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response applications and CSDM tables

The Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications manage (contribute data to) CSDM tables. These applications also use data from CSDM tables that other applications generate. Several ServiceNow products, therefore, benefit from and add value to these Security Operations applications. See Vulnerability Response applications and CSDM tables for more information.

Configuring Application Vulnerability Response

Before you run Application Vulnerability Response in your ServiceNow AI Platform instance, you must configure it.

Configure Application Vulnerability Response

Do the following setup steps prior to configuration so that you can ensure that your configuration is complete.

Before you begin

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that it's activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application isn't installed and activated, see Install Vulnerability Response.
Verify that the Performance Analytics for Vulnerability Response is installed and activated to see Application Vulnerability Response reports.	To verify that it's activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application isn't installed and activated, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.
Verify that the Veracode Vulnerability Integration is installed, activated, and configured. (Do not run the integrations at this point.)	To verify that it's activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application isn't installed and activated, see Install the ServiceNow Vulnerability Response Integration with Veracode.
Verify that the CWE 2000 integration is running in Vulnerability Response.	To verify the integration, see Verify that the scheduled job for updating NVD records is running.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
[Optional] Verify that the NVD integration is running in Vulnerability Response.	To verify, see Verify that the scheduled job for updating CWE records is running.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the user with the admin role installs the application and assigns users to the following user groups: App-Sec Manager, Security Champion, and Developer. For information on Group roles, see Application Vulnerability Response user groups and roles. • The App-Sec Manager group oversees configuration and verifies expected results. **Note:** Application Vulnerability Response configuration isn't available from the Setup Assistant feature in Vulnerability Response.

Role required: App-Sec Manager user group

Procedure

1. Navigate to **Security Operations** > **CMDB** > **Lookup Rules**.
   See Create a CI lookup rule to create or modify CI Lookup Rules for your environment.
2. Navigate to **Application Vulnerability Response** > **Administration**.
3. Select **Assignment Rules**.
   See Create or edit Application Vulnerability Response assignment rules to create or modify application assignment rules for your environment.
4. Select **Vulnerability Calculators**.
   See Calculate risk in Application Vulnerability Response automatically to create or modify application vulnerability calculators for your environment.
5. Select **Remediation Target Rules**.
   See Create or edit application remediation target rules to create or modify application remediation targets for your environment.
6. Select **Normalized Severity Maps**.
   See Map the severity of an application vulnerable item automatically to create or modify severity maps for your environment.
7. Navigate to either **Veracode Vulnerability Integration** > **Integrations** or **Fortify Vulnerability Integration** > **Integrations**.
8. Open the Veracode Application List Integration or the Fortify On Demand Application List Integration.
9. If it has not already run, select **Execute Now**.

Note: The other Veracode or Fortify integrations are inactive by default.

For integration run statuses, see View the Veracode Application Vulnerability Integration import run status or View the Fortify Vulnerability Integration import run status.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. After the Veracode or Fortify on Demand Application List Integration has completed its run, navigate to **Application Vulnerability Response** > **Administration** > **Applications**.
11. For each application, enter a value for **Support Group** (used by assignment rules) and for **Department** (used in reporting).
    To update multiple entries, see Edit multiple records in a list using the list editor to complete the task in bulk.

    Note: To see the auto-updated **Business Unit**, refresh the page. For information on Scanned Application form fields, see Scanned application fields.

12. Return to the Integrations list, and activate the other Veracode or Fortify integrations.
    See Activate Application Vulnerability Response Integrations to set your delta data integration imports.

    The Veracode and Fortify integrations are chained and will run consecutively when activated.

13. **Optional:** Navigate to **Application Vulnerability Response** > **Administration** > **Assignment Rules**.

    a. **Optional:** If you chose **Configuration Item: Support group** for **User group field** when creating or editing your assignment rules earlier, the values you added to the Scanned Applications list view are available to use now.
    Your assignment rules are edited.

    b. Select **Update**.

    c. From the Vulnerability Assignment Rules list view, select **Apply Changes** to reapply the assignment rules to your AVIs.

Result
Your Application Vulnerability Response configuration is now complete.

What to do next
Navigate to **Application Vulnerability Response** > **Overview** and see Application Vulnerability Management [PA] dashboard for information on your overall security posture.

Verify that the scheduled job for updating CWE records is running

Use Common Weakness Enumeration (CWE) records downloaded from the CWE database for reference when deciding whether a vulnerability must be escalated. Update common weakness records from the Common Weakness Enumeration database on a regularly scheduled basis. You can also update the default script or write your own scripts, as needed.

Before you begin
Role required: App-Sec Manager group
Each CWE record also includes an associated knowledge article that describes the weakness.

Procedure
1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Integrations**.
2. Select the **CWE Comprehensive 2000 Integration** scheduled job.
3. Verify that the **Active** check box is selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The settings in this form are shared by Vulnerability Response and Application Vulnerability Response. Modifying the integration settings requires coordination with and expertise in Vulnerability Response and ServiceNow.

4. If the box is selected, you are done.

Note: If the box is not selected, this integration may need to be configured within Vulnerability Response. See Importing data with the NVD and CWE integrations and managing third-party libraries for more information before selecting it.

As needed, see View vulnerability libraries to see the imported entries.

The **Primary CWE** field contains the CWE entry. If there is more than one CWE is associated with a vulnerability, see Application Vulnerability fields for information on how the primary CWE is determined.

Verify that the scheduled job for updating NVD records is running

Identify the repositories that you want updated regularly. You can execute a scheduled job to update National Vulnerability Database (NVD) records on a nightly or weekly basis. If it is not already running, you can enable the job

Before you begin

Roles required: App-Sec Manager group

The NVD integration runs as a scheduled job daily on Mondays at 00:00:00, by default.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Integrations**.
2. Select the **NIST National Vulnerability Database** scheduled job.
3. Verify that the **Active** check box is selected.

Note: The settings in this form are shared by Vulnerability Response and Application Vulnerability Response. Modifying the integration settings requires coordination with and expertise in Vulnerability Response and ServiceNow.

4. If the box is selected, you are done.

Note: If the box is not selected, this integration may need to be configured within Vulnerability Response. See Importing data with the NVD and CWE integrations and managing third-party libraries for more information before selecting it.

As needed, see View vulnerability libraries to see the imported entries.

Activate Application Vulnerability Response Integrations

Enable Application Vulnerability Response integrations to perform regular updates.

Before you begin

Role required: App-Sec Manager

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Integrations**.
2. Select an integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the **Active** check box.
4. Select **Update**.
5. Repeat as needed for each integration.
   After the initial run, the integrations are chained to do delta imports for subsequent runs.

Define Application Vulnerability Response email notifications

Set up email notifications to share useful information about important updates and activities such as approval and rejection of false-positive requests. Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Email Templates**.
2. Select **New**.

   For detailed instructions for creating email notifications, see Create an email notification.

Result
Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for the users with the role sn_vul.app_sec_manager.
- Links open in the IT Remediation Workspace for the users with roles, sn_vul.app_security_champion, or sn_vul.app_developer.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Create or edit remediation target notifications in Application Vulnerability Response

Vulnerability administrators can edit the remediation target notification or add new ones, specifying when to send the notification, who receives the notification, and what content is in the notification.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Notifications**.
2. Select the remediation target notification record or select **New**.
3. Fill in the fields on the form, as appropriate.
   For more information on the form fields, see Create an email notification.
4. Select **Preview Notification** to view the message.

Result
Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Links open in the Vulnerability Manager Workspace for users with the role, sn_vul.app_sec_manager.
- Links open in the IT Remediation Workspace for the users with roles, sn_vul.app_security_champion, or sn_vul.app_developer.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Exception Management in Application Vulnerability Response

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to an application vulnerable item (AVI) that cannot be remediated according to the policy.

Some vulnerabilities might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the vulnerability.

Note:

Starting from v21.0 of Application Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the application vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the application vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Life cycle of an exception

Definition of an exception

An exception is a request to defer the remediation of an AVI for a specified period. For example, as a developer, you can request an exception if a patch is not available for a machine.

Requesting an exception

As the developer, you can ask for an exemption for an AVI using the exception management process. After the application security analyst approves this request, the AVI moves to **Deferred** state.

Exception rules

Starting with v20, you can create exception rules to automatically defer existing and new application vulnerable items (AVI)s for a specific period if they match the conditions of the rule. Using exception rules to automatically defer AVIs minimizes the risk of missing service level agreements. The rules can help you manage multiple items, because you are eliminating manual intervention. See Create an Exception rule.

Requesting an extension for an exception rule

Starting with v20, you can submit a request for an extension to the **Deferred until** date of an exception rule. You might request an extension to a rule if you find that a large number of records created by the rule are not being resolved by its **Deferred until** date, the date when the remediation task stops accepting new AVIs. The extension updates the exception rule so it automatically extends the deferral date on your existing rule. You can enter dates up to one year from the current date, and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

you must include a reason for the extension. An extension request requires two-level approval from separate approval groups.

Approving an exception request

AVIs that can't be remediated immediately are reviewed by application security analysts, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level flow. If only the first-level approver is present, the exception can be requested and approved. However, if there's no first-level approver, an exception can't be requested. See Add an exception approver for Application Vulnerability Response for more information.

Note:

After an exception request for an AVI is approved, you can perform the following actions:

- Reopen
- Get more details

Tracking an exception request

After raising the exception, you can track its status by using the **State Change Approvals** tab of the AVI.

Expiry of an exception request and requesting an extension to an exception rule

When an exception request for a particular AVI expires, the impacted AVI reverts to its **Open** state.

However, starting with v20, you can submit a request to extend the **Deferred until** date on the exception rule.

Configure Exception Management for Application Vulnerability Response

Limit the duration of an exception requested and add a questionnaire to the exception or false positive request using the module. By default, an exception is requested using the ServiceNow® Application Vulnerability Response module. You can also request an exception using the GRC: Policy and Compliance Management integration.

Before you begin

Role required: sn_vul.app_manage_exception_configuration

About this task

If Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

If you add a questionnaire, it’s sent to the person raising the exception or the false positive request. You can either use the default questionnaire or create one based on your requirements.

It’s useful for the exception approver to understand the reason for requesting the exception.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Exception Management**.
2. On the Exception Management Configuration form, select how you want to manage an exception by selecting an option from the Manage exceptions using list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with Vulnerability Response version 17.1, you can select either Vulnerability Response or GRC: Policy and Compliance Management. You must activate the GRC plugin to use GRC: Policy and Compliance Management to request an exception. Changing the configuration doesn't impact the existing data.

3. Fill the fields on the form based on what option that you selected.
   - If you selected the Vulnerability Response option, then fill in the fields on the form.

Settings for VR Exception Management form

Field	Description
Duration	Period for which an exception can be requested.
Unit	Unit of time for the specified period.
Enable questionnaire to request exception	Option to add a questionnaire to the exception request being raised.
Questionnaire to request exception	Option to display the questionnaire selected by you to request an exception. The Exception Questionnaire is displayed by default.
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Questionnaire to mark false positive	Option to display the questionnaire selected by you to mark as a false positive. The questionnaire for false positive request is displayed by default.

   - If you selected the GRC: Policy and Compliance Management option, then fill in the fields on the form.

Settings for VR Exception Management form

Field	Description
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Questionnaire to mark false positive	Option to display the questionnaire selected by you to mark as false positive. The questionnaire for false positive request is displayed by default.

4. Select **Save**.

Configure approval rules for Exception Management

Starting with Application Vulnerability Response v15.0, use the flow designer to approve exception requests for exception management, exception rules, and false positive management. If you are deploying Application Vulnerability Response (AVR) for the first time, the flow designer is enabled by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
If you are an existing VR user, the default option is workflow.
If you have deployed Application Vulnerability Response v15.0 or later, the value of the system property *sn_vul.flow_designer_activation* is set to true. This means that the flow designer is enabled by default.

If you are already using Application Vulnerability Response prior to v15.0, the value of this system property is set to false. You can activate the flow designer by changing the value to true.

Note: You cannot revert to using the workflow after activating the flow designer. For a detailed comparison between the workflow and flow designer, see Exception management workflow versus flow designer.

To use the flow designer, create rules using the Approval Rules module. Using this module, you can configure approval rules for each of the following exception management workflows.

- Exception request for remediation tasks
- Exception request for application vulnerable items
- Exception rule
- False positive for remediation tasks
- False positive for application vulnerable items

Note: You can also define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow.

Procedure
1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Approval Rules**.
2. On the Approval Rules page, select the group for which you want to set the approval rule.
3. On the form, fill in the fields.

Approval Rule form

Field	Description
Name	Approval configuration name.
Table	Table on which the rule is applied.
Application	Default value is Vulnerability Response.
Rule type	Specifies the rule type. For example, exception management, false positive or exception rule.
Active	Enabled by default, signifying that the approval rule is in use.
Description	Short description of the approval rules.
Approval expiry (days)	Date until when the approver can approve the request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Starting from v21.0 of Application Vulnerability Response	
Notify approver (days) Starting from v21.0 of Application Vulnerability Response	Date after which the approver is notified to take action.

4. Select **Update**.
   In the Approval Configurations tab, there are two levels of approvers set up by default. You can select a rule to define the conditions based on different use cases within a rule.

   Note: In each configuration page, you can create multiple approval levels.

Example:
Based on different use cases, you can define different approval processes for the same vulnerabilities found on different configuration items.

Deferring remediation in Application Vulnerability Response

Starting with v20.0, you can defer remediation with the **Awaiting Implementation** state that is available for application vulnerable items (AVI)s and remediation tasks as they move through their life cycles. You can only transition records to this state manually by selecting **Awaiting Implementation** from AVI and remediation task records in the **Under Investigation** state.

Use case

As a remediation specialist, you can move a record into **Awaiting Implementation** to let your team know that your research and work on a task is complete. You might choose this update if you find that a fix is ready for implementation but isn't available. An example of an unavailable fix is a software patch. If the maintenance window for a patch isn't available when you finish your research, you can move the task to **Awaiting Implementation** until the patch can be deployed.

Required fields

There are two required, editable fields on the AVI and remediation task records that are in the Awaiting Implementation state:

Remediation commitment date

The planned remediation date.

Remediation plan

The description of the remediation plan for remediation. This text is displayed in the Notes on the record.

Fields and system properties

There are two system properties that are set to `true` by default for the modal that appears when you transition a record to **Awaiting Implementation**. If left in their default settings:

sn_vul.remediation_fields

Sets **Remediation commitment date** and **Remediation plan** as mandatory fields. If set to `false`, these fields are optional.

sn_vul.awaiting_implementation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Displays the modal with the **Remediation commitment date**, **Remediation plan** fields after you select **Awaiting Implementation** on a record. If set to `false`, you can change the state of an AVI to Awaiting implementation without a prompt for entering a commitment date or a plan.

Missed Remediation Commitment Date Module

View any AVIs that have missed their Remediation commitment dates in the **Missed Remediation Commitment Date** module. Navigate **Application Vulnerability Response** > **Vulnerable items** > **Missed Remediation Commitment Date** to view the list.

State roll down from remediation tasks to AVIs

The UI action button to transition a record into **Awaiting Implementation** is only visible on application vulnerable item and remediation task records in the **Under Investigation** state. For state roll down, on the modal that appears when you select **Awaiting Implementation** on a remediation task, there's an option to **Override existing AVIs**.

Option	Description
Select **Override existing AVIs**.	Select this option to override the Remediation commitment dates and Remediation plans any existing AVIs in the task already in the **Awaiting Implementation** state. If selected, this feature rolls down the date and plan data on the remediation task to the AVIs.
Leave **Override existing AVIs** deactivated.	Leave the option deactivated to keep the date and plan values intact for any existing AVIs on the task already in the **Awaiting Implementation** state. If deactivated, AVIs already in **Awaiting Implementation** preserve their existing date and plan data and are not impacted by state roll down.

Roll down examples

Say you want to transition a remediation task from **Open** to **Awaiting Implementation** so that you can update the task's commitment date and plan information for a software patch maintenance window. Assume that there is an AVI in this task in the **Awaiting Implementation** state, and you want to update its commitment date and plan information to match the remediation task.

To overwrite the AVIs date and plan data so it matches the remediation task, select the check box to **Override existing AVIs** when prompted. The AVI's date and plan values become the plan and date values that you enter for the task in the prompt when you select **Awaiting Implementation**.

If you don't select the override option in this case, and there is an AVI in **Awaiting Implementation**, the original date and plan data on the AVI remains intact. The plan and date values that you enter for the task in the prompt when you select **Awaiting Implementation** aren't used on any AVIs already in the **Awaiting Implementation** state in the task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If an AVI on a task is in **Resolved** or **Closed-fixed** and you transition the task to **Awaiting Implementation**, selecting **Override existing AVIs** doesn't change the AVIs from **Closed-fixed** and **Resolved** to **Awaiting Implementation** due to a higher state precedence.

If override is not selected while moving the task to **Awaiting Implementation** and there's an AVI already in **Awaiting Implementation** and you move the task back to **Open** or **Under Investigation**, the AVI remains in **Awaiting Implementation**.

Add an exception approver for Application Vulnerability Response

Add users to the approver groups so that you can request an exception.

Before you begin

Role required: sn_vul.app_exception_approver

About this task

An exception request for an application vulnerable item is approved using the default two-level approval flow. The request can be approved by two levels of approvers. Adding users to the first-level group is mandatory. If there are no users in the second level, the request is approved after the first-level approval.

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. In the Name column, search for **Exception**, and click **Application Exception Approver - Level 1**.

   Note: Starting from Application Vulnerability Response v12.8.1, you can use the system properties provided in the base system for exception approvals via workflow in the System Properties [sys_properties] table. So, when an exception or false positive request is raised via workflow, it's sent for approval to the group IDs defined in the system property. Navigate to **All** > **System Properties** and select *sn_vul.app_exception_approver_L1*, *sn_vul.app_exception_approver_L2*, or *sn_vul.app_false_positive_approver_group* to change the property value.

3. On the Group Application Exception Approver - Level 1 form, click the Group Members related list.
4. Click **New** to create a list.
5. On the form, fill in the fields.

User form

Field	Description
User ID	Unique identifier for the user.
First name	User's first name.
Last name	User's last name.
Title	User's job title. Enter a title or job description, or select one from the list.
Department	User's department.
Password	Password assigned to the user. This password can be permanent or temporary.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Password needs reset	Option to enable the user to reset the password to ensure security.
Locked out	Option to lock the user out of the instance and terminate all the user's active sessions. The system prevents users with the admin role from locking themselves out.
Active	Option to make this user active. Only you can see an inactive user in these areas: ○ Lists of users ○ Selection list on reference fields (magnifying glass icon) ○ Auto-complete list that appears when you type into a reference field
Web service access only	Option to designate this user as a non-interactive user.
Internal Integration User	Option to designate this user as an internal integration user.
Email	User's email address.
Language	User's preferred language.
Calendar integration	Calendar used to manage the work schedule. For example, Outlook.
Time zone	Time zone for this user's location.
Date format	User's preferred format for dates.
Business phone	User's business phone.
Mobile phone	User's mobile phone.
Photo	Photo that you can upload by clicking on **Click to add...**.

6. Click **Submit**.
7. **Optional:** Repeat steps 1–5 to create an Application Exception Approver - Level 2. The approver must navigate to **Application Vulnerability Response** > **My Approvals** and approve requests.

Requesting and approving an exception in Application Vulnerability Response

You can request to defer the remediation of an application vulnerable item and a remediation task for a specified period.

For example, as a developer, you can request an exception if a patch is not available for a machine. Approvers who have access can approve requests from other users.

You can also create exception rules and request an exception extension for an exception rule. By default, two-levels of approval is required for deferrals, exception rules, and exception extension requests.

To request or approve an exception, see:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Request an exception for an application vulnerable item
- Request an exception for application vulnerabilities using GRC: Policy and Compliance Management
- Approve exception rules and exception rule extension requests in Application Vulnerability Response
- Request an extension for an exception rule in Application Vulnerability Response

Note:

Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested.

Starting from v21.0 of Application Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the application vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the application vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Request an exception for an application vulnerable item

Request an exception for an application vulnerable item that cannot be remediated immediately. For example, as a developer, you can request an exception if a patch is not available for a machine.

Before you begin

Role required: Developer Group

Procedure

1. Navigate to **Application Vulnerability Response** > **Application Vulnerable Items** > **All** and select the item that you want to request an exception for.
   The selected item must be in Open or Under Investigation state.

   Note:

   Starting from v21.0 of Application Vulnerability Response, the previous state of an application vulnerable item is stored in the **backup_state** field.

2. On the Application Vulnerable Item form, click **Request Exception**.

   Note: Depending on whether Vulnerability Response is selected or GRC: Policy and Compliance Management in the **Application Vulnerability Response** > **Exception Management** screen, the Request Exception form changes. If GRC: Policy and Compliance Management, see Request an exception for application vulnerabilities using GRC: Policy and Compliance Management

3. If Vulnerability Response is selected in the Exception Management screen, fill in the fields in the Request Exception form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the duration selected in the **All** > **Application Vulnerability Response** > **Administration** > **Exception Management** screen. When the exception request expires, the group reverts to its **Open** state. **Note:** Starting with version 18.0 of Application Vulnerability Response (AVR), a deferred application vulnerable item can be closed and reopened by a scanner. If the item reopens before the exception window expires, the state of the AVIT reverts to deferred state honouring the active exception window. To enable this functionality, set the value of the system property sn_vul.auto_defer_avit_in_active_exception_window to true. Also, the deferred Until date persists even after the AVIT gets closed or the exception expires. The role required is sn_vul.app_manage_exception_configuration for both read and write.
Reason	Select the **Reason**. Choices are: ○ Risk Accepted ○ Awaiting Maintenance Window ○ Fix Unavailable ○ Mitigating Control in Place ○ Other To see how to add new reason choices, refer Define policy reason mapping.
Additional information	Details that are related to the reason why this request is being made. This required field is to be updated by the remediation owner.

4. Click **Request Approval** to submit the exception request.
   The state of the application vulnerability item changes to In Review. Use the **State Change Approval** tab to track the status of the exception request.

Request an exception for application vulnerabilities using GRC: Policy and Compliance Management

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Application Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Role required: sn_vul.remediation_owner

You can also request exceptions in the classic UI:

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Application Vulnerable Items** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.
2. On the selected form, click **Request Exception**.
3. If GRC: Policy and Compliance Management is selected in the Exception Management screen, fill in the fields in the Request Exception form.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you are requesting an exception for.
Control objective	Control objectives that are associated with the policy you selected. If a policy is not selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date cannot be in the past.
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid cannot exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This mandatory field must be filled in by the remediation owner.

   a. Click **Request Approval** to submit the exception request.
      The state of the vulnerable items changes to In Review and a policy exception is created.
      Use the **State Change Approval** tab to track the status of the exception request.

   b. Click the Policy Exceptions related list to view the policy exception.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Click the policy exception number.

d. In the **Approver** field, select the name of the approver.

e. Click the Source tab and select a control objective from the **Control objective** field.

f. Click the Risk assessment tab and select the risk rating from the **Risk rating** field.

g. Save the form.

h. Click Impacted Controls tab and click Add to add the controls.

i. Save the form.

Note: You can raise a compliance review by clicking **Request compliance review**.

j. The approval form is sent to the approver.

k. As an approver, you can either approve the request by clicking **Approve** or request additional approval by clicking **Request Additional Approval**.
The record state changes to Deferred. The reason stated is the one you selected when raising the exception request. The Deferral tab provides additional notes on the record.

Note: If the request gets rejected, the record moves to its previous state.

4. Click **Submit**.
For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

Request an exception for an application remediation task

Request an exception to defer a application remediation task for a specified period if it can't be resolved immediately.

Before you begin

You can request exceptions from the Vulnerability Response Workspaces. See Request an exception in the IT Remediation Workspace.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

Roles required: sn_vul.remediation_owner, sn_vul.app_security_champion or sn_vul_container.remediation_owner.

You can also request exceptions for application remediation tasks in the classic environment.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Remediation tasks** > **All**.
2. Select the group that you want to request an exception for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected task must be in the Open, Under Investigation, or Awaiting Implementation state.

3. On the application remediation task record, select **Request Exception**.
4. On the form, fill in the fields.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the exception duration that is defined in the configuration.
Reason	Justification for requesting an exception.
Additional information	Details that are related to the reason why this request is being made. This field is to be updated by the remediation owner.

5. Click **Request Approval**.

Approve exception rules and exception rule extension requests in Application Vulnerability Response

Approve exception requests for application vulnerable items that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

Before you begin

Role required: sn_vul.app_exception_approver

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Define policy reason mapping

You can define the reason choices to be available to any user who requests an exception.

Before you begin

You must have the GRC: Policy and Compliance Management application installed. This application is available from the ServiceNow® Store with a separate subscription.

For details on system requirements and family compatibility, view the application listing on the ServiceNow Store website.

Role required: sn_vul.compliance.manager and sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Integration Registry**.

   Note: You can either select a reason from the reason choices available in the Reason Choices table or add a new reason.

2. Click the integration registry for your application, for example, **Application Vulnerability Response**, **Vulnerability Response**, and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To add an existing reason choice, perform the following steps:
   a. In the Reason Choices list, click **New**.
   b. Click the magnifying glass icon to select a reason.
4. To add new reason choices to the Reason Choices table, perform the following steps:
   a. In the Reason Choices list, click **New**.
   b. Click the magnifying glass icon.
   c. Click **New**.
   d. On the form, fill in the fields.

Reason Choice List form

Field	Description
Label	Unique label for this choice.
Value	Unique value for this choice. This value is mapped in the Policy Exception Reason Mappings table for the respective applications. To navigate to this table, enter sn_vul_policy_reason_mapping.LIST in the filter navigator.
Order	Order for this choice. Reasons are ordered based on this number.
Default	Option to indicate that this reason choice will be available whenever an on demand policy exception is requested. If the integration registry doesn't contain any application-specific choices, then all reason choices that have the **Default** field selected will be available.
Active	Option to display the choice in the list of reason choices.

5. Click **Submit**.

Request an extension for an exception rule in Application Vulnerability Response

Request an extension for a deferred exception rule before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Roles required: App-Sec Manager sn_vul.app_sec_manager, Security Champion sn_vul.app_security_champion.

About this task

On an extension rule record, you can request an extension for the **Deferred Until** date only if the rule is in the **Approved** state. You might request this extension to a rule if you find a large number of records created by the rule are not being resolved by its **Deferred until** date, the date when the remediation task stops accepting new AVIs. The extension updates the exception rule so it automatically extends the deferral date on your existing rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Exception Rules**.
2. Select an approved exception rule.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the exception rule must be extended.
Reason	Enter the reason for deferring the exception rule. Choices include: ○ Risk accepted ○ Awaiting maintenance window ○ Fix unavailable ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the Deferred until, Reason and Additional information fields get updated on the exception rule and the associated remediation tasks and application vulnerable items. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred exception rule is extended again, the extend deferral count increases in the back end.

Request an extension for a deferred remediation task in Application Vulnerability Response

Request an extension for a deferred remediation task (VUL) before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Remediation Tasks**.
2. Open a deferred remediation task.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date when the Defer state expires and the remediation task is reactivated.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the changes on the remediation task are rolled down to the application vulnerable items as well, which are part of the remediation task. However, the application vulnerable items should be in the deferred state and their current until data precedes the updated until date. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred remediation task is extended again, the extend deferral count increases in the backend.

Request an extension for a deferred application vulnerable item in Application Vulnerability Response

Request an extension for a deferred application vulnerable item before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Vulnerable Items**.
2. Open a deferred application vulnerable item.
3. Select **Request Extension**.

   Note: The Request Extension button is visible only when the state of the application vulnerable item is Deferred.

4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the deferred application vulnerable item must be extended for remediation.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   An email is triggered on submission of the request and subsequent action by the approver.

   Note:
   - The request goes through two levels of approval.
   - If a deferred exception rule is extended again, the extend deferral count increases in the backend.

6. After the request is approved, the Until, Reason, and Deferral notes are updated.

Create, delete, and cancel an exception rule for Application Vulnerability Response

Create a rule to request an exception automatically for application vulnerable items (AVI)s that meet specific conditions.

Before you begin

As an example, you might create a rule with a condition that is based on a specific known or critical vulnerability that you know you cannot fix immediately. With this rule, you can defer new and existing AVIs automatically if they match the approved rule condition.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The exception rule is applied from the **Valid from** until the **Valid to** date that you enter on the rule record.
- The remediation task (AVUL) is created after the rule is approved for matching AVIs in the **Deferred** state.
- The grouping method for this AVUL is known as Exception Rules.
- You can't close, reopen, or delete this AVUL. New and reopened AVIs are deferred and added to this AVUL from the **Valid from** date until the group expires on the **Valid to** date.

Note:

Email notifications are sent at every stage of the exception rule workflow. These emails provide the status and other details of a request. For example, when an exception rule is requested, the requester receives an email that confirms that the request is submitted.

If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

Roles required: App SEC Manger sn_vul.app_sec_manager and Security Champion sn_vul.app_security_champion.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Exception Rules**.
2. On the Exception Rule new record page, select **New**.
3. Fill in the fields.

Field	Description
Name	Name of the exception rule.
State	Read-only: Draft
Valid from	Date from which this rule is active to defer AVIs.
Execution order	Unique order for each exception rule. A lower value precedes a higher one.
Valid to	Date on which the remediation task stops accepting new AVIs.
Deferred until	Date until the remediation tasks and AVIs are deferred. On this date, the AVULs are closed and all the AVIs move out of the tasks and are reopened. Group rules are reapplied to these AVIs.
Reason	Reason to create this exception rule.
Assignment group	Group the remediation task is assigned to for tracking the deferred AVIs.
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Condition	Filter conditions to specify which AVIs match this rule.
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run. If you leave this option deactivated, your rule runs daily by the scheduled job *Associate existing AVIs with Auto Exception Rule* starting with new data. If you enable the Execute on existing data option, a scheduled job runs one time on the existing data on the **Valid from** date.

4. Add the assignment group when you are creating the rule.
5. Choose one.

Option	Description
Save the rule	Save your changes and the rule is displayed on the Exception rule list [sn_vul_auto_exception_rule]. Until you submit the exception rule for approval, it remains in the **Draft** state.
Submit the rule	If you submit the rule, the status of the request changes to **In review**. An exception rule approval requires two levels of approval, one from Application Exception Approver - Level 1, and another from Application Exception Approver Level -2.

After the rule is approved, it moves to the **Approved** state. Your rule evaluates AVIs with the *Associate existing AVIs with Auto Exception Rule scheduled* job. If you selected **Execute on existing data**, it evaluates existing AVIs. A remediation task is automatically created for the rule, and any matching AVIs that meet its conditions are associated with the task.

The scheduled job runs the exception rule once on existing data. The rule does not run again on existing data even if no AVIs are found. It only evaluates new data because the existing AVIs that matched the rule have already been deferred.

6. To delete a rule, select **Delete** on the exception rule record.
   The following message appears: `If you delete the rule, the associated remediation task will be deleted and the related vulnerable items will be reopened. The remediation task rules will then be applied to the individual AVIs and the exception rule is deleted.`
7. Select**Keep rule** to stop or **Delete rule** to continue.
8. To deactivate a rule but keep it on the Exception rules list, select **Cancel**.
   The following message appears: `If you cancel this rule, the associated remediation task will be deleted and the related vulnerable`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
items will be reopened. The remediation task rules will then
be applied to the individual vulnerable items and the exception
rule will be moved to the draft state.
```

9. Select **Keep rule** to stop or **Cancel** to move the rule to **Draft** and deactivate it.

Application Vulnerability Response remediation tasks and task rules overview

Configure remediation tasks (AVULs) to help analysts and remediation specialists organize application vulnerable items (AVI) and analyze them in bulk. The criteria by which remediation tasks are formed is configured so that AVIs are automatically assigned into remediation tasks. Using remediation tasks, you can monitor progress and drive the remediation process more efficiently.

Tracking deferral counts for application vulnerable items and remediation tasks

Track the number of times a vulnerable item, application vulnerable item, container vulnerable item, or remediation task is deferred. The *`set deferral counts`* scheduled job runs daily to post counts for the records that are deferred more than once in the Deferral count column. Records are displayed in the Multiple deferrals modules for VR, AVR, and CVR.

Understanding remediation task rules

Remediation task rules enable you to define how application vulnerable items are automatically grouped and assigned. A default rule **Vulnerability** is included in the base system that gathers AVIs based on their vulnerabilities. However, you can group by any other set of values in columns accessible from the AVI. These values could include configuration item (CI), vulnerability entry, and the like.

There are task rules for Application Vulnerability Response that are included with the Vulnerability Response application that is available when you activate it.

You can create multiple conditions with the condition builder. In the Group by section, after you set a field pair, another row appears. You can have up to six **Group by** selections. You can automate group assignment as well. See Assign application vulnerable items in Application Vulnerability Response automatically and Filtering within Vulnerability Response for more information.

For example, you can group your application vulnerable items by the configuration item, or by the product model. You can have one task rule for low severity vulnerabilities or low risk CIs. You can have another task rule for critical servers, and vulnerabilities that expose the company to more risk. See Create, edit, and delete Application Vulnerability Response remediation task rules for more information about the options that you have available to you.

A different set of rules can be used for application vulnerable items that expose the company to more risk. The remediation task name is appended to the remediation task rule **Group by** values to make the short description of the new record.

When a new application vulnerable item is created, imported, or reopened after being closed, the rules are evaluated against it. An AVI is only evaluated once, automatically, unless it's reopened after being closed or the rules are reapplied manually.

The following process is used for each new or reopened AVI:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For each remediation task rule, the AVI is compared to the remediation task rule filter.
- For each rule where the remediation task rule condition matches, the rule pulls the data from the **Group by** selections on the AVI. It builds a group name and field. In this case, **High Risk: QID-32342:***Summary of QID-3242* (Name: vulnerability ID: vulnerability summary).

  Note: The short description field is limited to 160 characters. Longer vulnerability summaries are truncated.

  The rule checks to see if there's a matching **Open** remediation task that is assigned to the same assignment group as the AVI.
  - If the task is found, the AVI is added to the existing task in the **Open** state.
  - If no task in the **Open** state is found, the rule creates a **High Risk: QID-32342** task, assigns it to the same assignment group as the AVI, and places the AVI in the remediation task.

More than one remediation task rule can be defined to group different kinds of vulnerabilities. Since each vulnerability is compared with the remediation task rule conditions before putting it in a remediation task, too many rules might impact performance. Set up your task rules so the conditions help you avoid creating duplicate remediation tasks.

By default, remediation task rules use the assignment group set by the **Assignment Rules** on the AVI when grouping the items and assigns the remediation task to match the AVIs.

As part of the default task rule, the assignment of these remediation tasks is controlled by the rules in the **Assignment Rules** module. For more information on assignment rules, see Vulnerability Response assignment rules overview.

When a task rule is deleted from the form or list view, you have the option to delete all **Open** tasks created by that rule. Tasks not in the **Open** state are excluded.

Reapplying remediation task rules

When you want to change a remediation task rule, use the **Reapply** button on the remediation task rule page to rerun the changed rule on all active **Open** remediation tasks created by that rule. It deletes and recreates remediation tasks based on the changed rule automatically.

Reapply only checks existing remediation tasks.

After you select **Reapply**, the following message is displayed: `Reapplying this remediation task rule will delete and re-create the remediation tasks for this rule. Remediation tasks that are not in the Open state are not deleted.`

Creating remediation tasks and adding AVIs manually

You create an application remediation task (AVUL) from another application remediation task record and add application vulnerable items (AVITs) manually. See Create an application remediation task manually in Application Vulnerability Response for more information.

Remediation task rules and AVI creation and update

If a CI or product model from a scan is associated with a known vulnerability, an AVI is created. After it's created, the AVI is evaluated against the conditions of remediation task rules for a match. If there is a match to an existing remediation task, the AVI is added. If a matching remediation task is not found, one is created for the AVI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If any property that is captured in the remediation task filtering conditions is updated or changed on an AVI, the updated AVI is also evaluated against the remediation task rules for a match. If there's a match to an existing remediation task, the AVI is added. If a matching remediation task isn't found, one is created for the AVI.

State rollup and rolldown

If you update a remediation task to Open, or from Open to Under Investigation, the new state rolls down to all associated AVIs. State roll down occurs immediately after you change the state.

State rollup from AVIs to the remediation task only occurs if all the AVIs on the task are in **Deferred** or **Closed- fixed** states. Rollup is done with the *`Rollup application vulnerable item values to vulnerability and group`* scheduled job, which runs every 15 minutes. The state is not rolled up until the job runs. For a state to roll up to occur from the AVIs to the remediation task, the all the AVIs must be in the same state.

Create, edit, and delete Application Vulnerability Response remediation task rules

You can create rules to automatically group application vulnerable items (AVI) into remediation tasks (AVUL) based on filter conditions. These rules automatically group AVIs as they're imported or manually created.

Before you begin

If you create a new rule, it doesn't apply to existing data. After you submit it, it's run against new imports.

Role required: App-Sec Manager

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Remediation Task Rules**.
2. Open the rule or select **New**.
3. Fill in the fields on the form or edit them.

Remediation Task Rule

Field	Description
Name	Name of the task rule.
Active	Indicates whether the task is active.
Description	Description of the rule.
Case sensitive	Determines whether a condition is case sensitive or not. **Note:** The default value is case insensitive.
Condition	Optional filter conditions for the rule. By default, (**Case sensitive** check box not selected), the search text you enter in the condition builder on task rules records and forms isn't case-sensitive. You have the option to enable case-sensitive searches on task records and forms.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	An example condition is **Vulnerability** > **is** > **VULNENT123451** (a known imported vulnerability). Any AVIs that have this vulnerability match this condition.
Group by (up to six condition sets are available)	
Group application vulnerable items from	The table the rule uses to group AVIs. Select the elements from the tree: ○ Application Vulnerable Item [sn_vuln_vulnerable_item] ○ Application Vulnerable Item Configuration Item [cmdb_ci] ○ Application Vulnerable Item Application Vulnerability [sn_vul_third_party_entry] ○ Application Vulnerable Item Product Model **Note:** If you choose an extended table, the **Using field** is applied only for application vulnerable items that use that extended table.
Using field	Field on the table that the rule uses to group AVIs. Select conditions from the tree. **Note:** You can create group by conditions so that not all the AVIs that share data are assigned to the same remediation task. For example, if you select Assignment group and IP Address as the Using fields, and multiple AVIs match the initial filtering condition **Vulnerability**, these AVIs can be assigned to distinct assignment groups for remediation using the many options available in the Group by section. The Group by conditions give you the flexibility to create distinct remediation tasks that can be assigned to different group even if they share some data.
Assignment	
Assign remediation tasks by	When automatically assigning remediation tasks, the Assignment choice is used in addition to the **Group By** choices to group the vulnerable items. New tasks are created, as needed, so that each AVI is placed in a task with a matching assignment group set. To automate the assignment of tasks created based on this rule, choose one of the options available. ○ Group by field: If you selected any user group field from the **Using field** values in the **Group by**section, they appear in the drop-down menu. ○ User Group: Use the lookup list to select a static user group.

if you delete a rule from either the form or list view, you have the option to delete all **Open** remediation tasks created by that rule. Groups not in the **Open** state are excluded.

4. Select **Submit** for new rules.
   After you select **Submit**, your rule is displayed on the Remediation Task Rules list [sn_vul_grouping_rule]. The following situations initiate your rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- When new AVIs are created.
- When you select **Reapply**. You select **Reapply** to evaluate task rules on existing remediation tasks only.
- When AVIs are updated, either by you or by the system.

  If an AVI is updated, task rules are evaluated for matches to existing remediation tasks. Some common updates that initiate a rules check are:

  - When the State changes from Closed to Open, or from Closed to Under Investigation.
  - The configuration item (CI) is changed.
  - The vulnerability is changed.

The system checks all the task rules for matches to the updated AVI. If the conditions of a rule match the conditions of a remediation task, matching AVIs are assigned to it.

If no match is found, a new remediation task is created.

For more information about state roll up from AVIs to remediation tasks and state roll down from remediation tasks to AVIs, see Application Vulnerability Response remediation tasks and task rules overview.

For an example of a remediation task rule, see Application Vulnerability Response remediation task rule examples.

5. To delete a task rule, select the rule from the Remediation Task Rules list and select **Delete**. The following message is displayed: `The selected remediation task rule created n remediation tasks. Of the remediation tasks, n are in the Open state..`

Option	Description
Check box deactivated (default).	Only delete the rule. Tasks not in the **Open** state are excluded.
Check box selected.	Include the remediation tasks in the **Open** state when you delete the remediation task rule. Delete the rule and any remediation tasks in the **Open** state.

6. Choose one option and select **Delete**.

Create an application remediation task manually in Application Vulnerability Response

Create an application remediation task (AVUL) from another application remediation task record and add application vulnerable items (AVITs) manually.

Before you begin

Role required: sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Remediation Tasks** > **All**.
2. On the upper right of the page, select **New**.
3. On the Group Configuration tab, for Grouping method, select **Manual**.
4. Select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Locate your new task record (AVUL) on the Application Remediation Tasks [sn_vul_app_vulnerability] table.
   The record is created in the **Open** state.
6. Open the record and add new or existing application vulnerable items to this group using the Application vulnerable items related list (**Edit** or **Add**).
7. Select **Update** to save the record or other UI actions to transition the record into another state.

Create auto-close rules

Use auto-close rules to close older AVITs automatically based on the filter conditions that you set.

Before you begin

Role required: sn_vul.app_manage_auto_close_rules

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Auto-close rules**.
   The base system provides the following auto-close rules:

   Application Vulnerabilities last scanned Vulnerabilities not reported within the last 90 days are transitioned to **Stale** state.
2. Select **New** to create a new auto-close rule.
3. Fill in the fields on the form.

Field	Value
Name	Name of the auto-close rule.
Active	Option to activate the rule. If activated, it closes any detections automatically that match its filter criteria.
Execution order	Unique value for the execution of the auto-close rule. This value determines the order of execution. The default value is 100.
Integration type	Application Vulnerability Integration
Description	Description of the auto-close rule.
Condition	Filter conditions used to identify detections that should be closed.

4. Select **Submit**.

   The **Auto-close Rules Processor** scheduled job runs on a nightly basis. It identifies AVITs based on the specified conditions and transitions the matching ones to the **Stale** state. In cases where there are AVITs with both "Closed" and "Stale" statuses, the AVIT is closed with the sub-state set as **Fixed**.

Configure penetration testing

You can configure the sprint duration and estimated effort for penetration testing assessment types. This provides the scheduling functionality for application owners, helping them determine a tentative time frame for their penetration test assessment requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: Ethical Hacker

About this task
Configuring the penetration test assessment settings for the ethical hacking team also helps determine the group and point of contact that receives the penetration test assessment request.

Starting with v19.0 of Vulnerability Response, if you are using the Veracode Vulnerability Integration, the penetration assessment tests in the Veracode Vulnerability Integration are manual findings from Veracode. They are not linked to any penetration test assessment requests you configure in Application Vulnerability Response. For more information about penetration test assessments from Veracode, see the Veracode Vulnerability Integration.

Procedure
1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Penetration Testing Configuration**.
2. Use the first section to configure the assignment group.
3. On the form, fill in the fields.

Penetration Test Configuration form

Field	Description
Penetration testing team user group	Group to which the penetration test assessment request is assigned.
Default assignee for penetration testing assessment requests	Point of contact for the penetration test assessment request.

4. Select **Update**.
5. Use the second section to configure sprints.
   For details, see Configure sprints for penetration testing.
6. Use the third section to configure assessment types.
   For details, see Configure assessment types for penetration testing.

Configure sprints for penetration testing

Configure the sprint duration and capacity for the ethical hacking team so they can manage the sprint capacity for penetration test assessments.

Before you begin
Role required: Ethical Hacking

Procedure
1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Penetration Testing Configuration**.
2. Select the **Configure** option for Configure sprints.
3. On the form, fill in the fields.

Sprint Configuration form

Field	Description
Sprint duration (days)	Number of days in a sprint.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Start date	Start date for the sprint duration.
Number of sprints	Number of sprints that can be generated, based on the start and end dates for the sprint range.
End date	End date for the sprint duration.
Sprint capacity	
Sprint capacity (hrs)	Capacity of a sprint in hours.

4. Select **Generate Sprints**.
   To view the sprints created, select **View Sprints**.

   Note: After the sprints are generated and in progress, if you select **Generate Sprints** for the same duration, the current sprint is completed as usual. The remaining sprints are recalculated based on the updated sprint configuration.

Configure assessment types for penetration testing

Configure the estimated effort for each type of penetration testing assessment. This enables you to manage the capacity of each sprint, by estimating the effort required for each assessment type.

Before you begin

Role required: Ethical Hacking

About this task

Each sprint is assigned to a penetration testing request. Based on the estimated effort for the assessment type, the hours are adjusted to reflect the balance hours for the sprint.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Penetration Testing Configuration**.
2. Starting with v19.0 of Vulnerability Response, select **Configure** to display Assessment types, Application size and Estimated effort.
3. **Optional:** Select an Assessment type record to update the fields as required or create new records.

   (Optional) The Application size values provide you with more options to help estimate test time and effort more accurately. You can edit the hours for these records or select **New** to create your own combinations.

   You can modify Assessment type and Application size on values on existing penetration testing request records so that you can schedule tests to match sprint capacity. For example, if you fill out a test request, you might not see the number of sprints you configured, because some sprints are already taken for testing. If a sprint's estimated effort hours match the combination required for a test's type and size, they are not available for new requests.

   You can see the sprints that are assigned to test requests on records on the Penetration Testing Sprints list at **All** > **Application Vulnerability Response** > **Administration** > **Penetration Testing Configuration** > **Configure sprints**. See Configure sprints for penetration testing for more information on configuring sprints.

   The base values for Assessment type, Application size, and Estimated effort are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Penetration testing assessment type configuration form

Assessment type	Application size	Estimated effort (hrs)
Focused Test	Small	20
Focused Test	Medium	30
Focused Test	Large	40
Focused Test	Standard	40
Re-Test	Small	10
Re-Test	Medium	15
Re-Test	Large	20
Re-Test	Standard	20
Full Penetration Test	Small	60
Full Penetration Test	Medium	70
Full Penetration Test	Large	80
Full Penetration Test	Standard	80

4. Select Update to save your changes or Submit for a new record.
5. Prior to v19.0, select the **Configure** option for Configure assessment types.
6. Update the values for the assessment types as required.
   Base values are:

Penetration testing assessment type configuration form

Assessment type	Estimated effort (hrs)
Focused Test	40
Re-Test	20
Full Penetration Test	80

7. Save the changes.

Integrating Application Vulnerability Response with other applications

Vulnerability Response includes support for third-party integrations.

Third-party integrations

Application vulnerability integrations help enrich the application vulnerability data on your instance by retrieving data from external systems and vendors. See the following overview topics for more information about supported integrations:

- Fortify on Demand Vulnerability Integration
- GitHub Application Vulnerability Integration
- Invicti Vulnerability Integration
- Veracode Vulnerability Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Vulnerability Response Integration with Black Duck
- Manual ingestion of vulnerabilities for Application Vulnerability Response
- Atlassian Jira Integration

Important: In the Vulnerability Manager Workspace, you can create an agile issue manually using the list action and form action to track the remediation of AVITs and RTs.

Note:

Multi-source integrations are not supported in Application Vulnerability Response. Third-party integrations are treated separately. If more than one third-party integration application is in use in your environment, there is no application vulnerable item (AVI) deduplication across integrations.

Additional notes for integrations

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Application Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Vulnerability integrations for Application Vulnerability Response are configured to run on a scheduled basis. However, you can run them manually when needed.

Role required: sn_vul.app_read_integrations

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Integrations**.
2. Open the record for the integration that you want to run.
3. Click **Execute Now**.

Vulnerability Response Integration with Black Duck

The Vulnerability Response integration with Vulnerability Response Integration with Black Duck uses the data that is imported from the Black Duck Software Composition Analysis (SCA) tool to help you determine the impact and priority of the flaws in your code.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration overview

With the Vulnerability Response Integration with Black Duck, you can collect SCA and make that data available to the ServiceNow AI Platform. Starting with v22.0.5 of Vulnerability Response, you can import the SCA vulnerabilities data to your instance so that you can identify the vulnerabilities in your software applications. For more information, see Exploring Software Bill of Materials and Exploring supported applications for Software Bill of Materials.

A shared API ingests the SCA data.

Note: Each integration record has a configured run-as user. The default value for this user is VR System. Don't change this value.

Every day, scheduled jobs invoke the integrations automatically in the order that they're listed. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Available versions

Black Duck Integration available versions

Release version	Release notes
Vulnerability Response Integration with Black Duck 1.0.5	Application Vulnerability Response release notes

User group and roles

The Vulnerability Response Integration with Black Duck is installed by a user with the admin role and is configured by a member of the App-Sec Manager group. For more information, see the Application Vulnerability Response user groups and roles.

For integration run statuses, see View the Vulnerability Response Integration with Black Duck import run status

To view data in the third-party vulnerabilities, see View vulnerability libraries.

Prepare pre-integration tasks for Vulnerability Response Integration with Black Duck

Plan and execute the pre-integration tasks for the Vulnerability Response Integration with Black Duck so that your integration is successful. The Vulnerability Response Integration with Black Duck assumes that you're familiar with the Black Duck Software Composition Analysis (SCA) application and APIs.

Before you begin

Before you install and configure the Vulnerability Response Integration with Black Duck, you should run and install the Common Weakness Enumeration (CWE) integration, which is also used by Application Vulnerability Response. The CWE integration is installed with Vulnerability Response by default.

Note: Although the NIST Vulnerability Database (NVD) data isn't necessary to install the Black Duck Application Vulnerability Integration, it would be useful to have. For information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Each integration record has a configured run-as user. The default value for this user is VR.System. Don't change this value.

Role required: App-Sec Manager group

About this task

Note: Before running the integration, make any necessary configuration changes that are based on your requirements.

Validate your instance sizing by the number of application vulnerable items that you expect to import. An undersized instance can lead to long load times. If you don't know the size of your instance, contact Customer Service and Support.

The Vulnerability Response Integration with Black Duck requires an API URL and API token.

Procedure

Create the API token and key credentials.

a. Log in to the Black Duck platform.

b. Go to the user account menu and select **API Credentials**.

c. Select **Generate API Credentials**.

d. Record your credentials for later use.

Install the ServiceNow Vulnerability Response Integration with Black Duck

Before you run the integration on your instance, you must complete the installation and configuration steps so that the Black Duck Software Composition Analysis (SCA) tool properly integrates with Application Vulnerability Response.

Before you begin

Complete the following setup checklist before installation. You must do these setup tasks so that the Black Duck Software Composition Analysis (SCA) tool properly integrates with Application Vulnerability Response.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions that your organization has purchased. If the application isn't installed and activated, see Install Vulnerability Response.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks (continued)

Setup tasks	Description
	• If not already assigned, the user with the admin role installs the application and assigns users to the App-Sec Manager group. For information on group roles, see Application Vulnerability Response user groups and roles. • The App-Sec Manager group oversees the configuration and verifies the expected results.

Role required: admin

About this task

This SCA tool is available as a separate subscription.

Procedure

1. Log in to the instance that you want to install the Vulnerability Response Integration with Black Duck on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with the Black Duck application.
4. Select the application tile.
   The details about the application you're installing is displayed.

   Note: Consider reading the Other Requirements and Dependencies sections, as applicable.

5. Select **Request App** and enter your Now Support login credentials.
6. Select **Get**.
7. Enter the instance name and the reason for the instance, and select **Validate Instance**.
8. Select **Request**.
   You will receive an email with the detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and select **Install**.
    Your application is automatically installed on your instance.

What to do next

Configure the Vulnerability Response Integration with Black Duck for your environment. See Configure the Vulnerability Response Integration with Black Duck

Configure the Vulnerability Response Integration with Black Duck

Before you run the Vulnerability Response Integration with Black Duck on your instance, you must complete the installation and configuration steps so that the Black Duck Software Composition Analysis (SCA) tool properly integrates with the Application Vulnerability Response application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: App-Sec Manager user group

About this task
The Vulnerability Response Integration with Black Duck is available as a separate subscription.

Procedure
1. Navigate to **All** > **Blackduck Vulnerability Integration** > **Configuration**.
2. Select the Basic Authentication type.
   Basic Authentication requires a MID Server for instances that are on-premises. You can generate the API token that is required for basic authentication from your Black Duck account.
3. On the form, fill in the fields.
   Basic Authentication

Field	Description
API URL	Black Duck API URL for instances that are enterprise or on-premises. The on-premises instance is your Black Duck endpoint URL.
API Token	Token that you generated from your Black Duck console.
MID Server	MID Server that is required for instances that are on-premises for Basic Authentication.
Include SCA	Vulnerabilities from Software Composition Analysis (SCA) scans that are included by default. SCA scans identify the vulnerabilities in open-source components.
Select the option to manage False positives in ServiceNow	ServiceNow Option to Manage false positives. Leave this option activated if you want to triage the imported application vulnerable items (AVIs) with the **Source** states that are marked as **False Positive** or **Potential False Positive**. AVIs with these **Source** states that normally are mapped to a **Closed** state in your instance are mapped to **Open**. You can request a **False positive** from the AVI record. ○ Deactivate one or both options if you want to preserve the **Source** states that were imported from your scanner. ○ If deactivated, the **Request exception** and **False Positive** actions aren't visible on the AVIs.
Integration Instance	Instance that you're using to import the data.

4. Select **Save and Test credentials**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Run the **Black Duck Project List Integration** before you run other integrations.
   The other Black Duck integrations, such as the Black Duck Application List Integration and Black Duck Application Vulnerable Item Integration, depend on the current project and application data that you imported from the Project List Integration.

View the Vulnerability Response Integration with Black Duck import run status

Verify the success of your integration runs, locate any issues, and confirm your remediation decisions by viewing the Vulnerability Integration Runs related list.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **Blackduck Vulnerability Integration** > **Integrations**.
2. Select an integration.
3. Select the Vulnerability Integration Runs related list.
4. Verify that all imports have succeeded.
   Troubleshooting:

   The most common causes for a failed run include:

   - Network interruption.
   - An issue in the data transfer that results in corrupted data during a transform.

   If you encounter any of these conditions, select **Execute Now**, and rerun the integration.
5. View the imported repositories by navigating to the integrations list and selecting the Black Duck Integration record.
6. Select the Vulnerability Integration Runs related list and open a record.

Data transformation for the Vulnerability Response Integration with Black Duck

After you identify the data that you want to import, the data is retrieved from the Vulnerability Response Integration with Black Duck, processed through a set of data sources, and transformed in your instance.

Vulnerability Response Integration with Black Duck

The data from the API is first loaded into the Black Duck AppVul Item Import [sn_vul_blackduck_appvul_item_import] table, and the Black Duck AppVul Item Transform is used to transform the imported information.

To access this transform map, navigate to **System Import Sets** > **Transform Maps** and search for **Black Duck AppVul Item Transform**. The following table lists the transform map fields by integration.

Black Duck AppVul Item transform map fields

Source field	Target field	Description
app_id	source_app_id	Application ID.
issueid	source_avit_id	AVIT ID.
app_name	app_name	Application name.
version	app_version	Application version.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Black Duck AppVul Item transform map fields (continued)

Source field	Target field	Description
build_id	source_scan_id	Build ID of the application.
account_id	account_id	Account ID.
sandbox_id	sandbox_id	Sandbox ID.
last_update_time	last_scan_date	Last updated time.
app_name + last_scan_date	scan_summary_name	Scan summary.
life_cycle_stage	source_sdlc_status	Source SDLC status.
level	source_severity	Source severity.
category_name	category	Category.
source_severity	source_severity	Source severity.
category_id + " CWE-" + cweId	source_entry_id	Source entry ID.
source_vulnerability_summary	source_vulnerability_summary	Source vulnerability summary.
source_recommendation	source_recommendation	Source recommendation.
description	description	Description from the source.
description	source_vulnerability_explanation	Source vulnerability explanation.
mitigation_status_desc	source_mitigation_status	Source mitigation status.
remediation_status	source_remediation_status	Source remediation status.
line	line_number	Line on which the flaw is found.
module	application_module	Application module.
sourcefile	source_notes	Source notes.
affects_policy_compliance	complies_with_policy	Values can be Yes or No based on the source information being true or false.
Sourcefilepath + sourcefile	location	Location mapping a static flaw.
url	location	Location mapping for a dynamic flaw.
scope, type, exploitLevel	source_additional_info	Name value field populated with the values from the source for static flaws.

The following table lists the transform scripts that are run during the transformation process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Black Duck transform map script timing and purpose

Black Duck transform map script

When the script is run	Purpose
onStart (when an import set has created transformation).	Script that is used to process the record and updates the number of entities created, updated, or unchanged, and the ones that are imported as part of this integration. This script is for internal use and should not be modified or deleted.
onBefore (before an import set has completed transformation)	Script that is used to define the behavior for records that are invalid and must be ignored. Also, used to define the global object for record processing. This script is for internal use and shouldn't be modified or deleted.

Black Duck Integration state mapping

The following table shows the source states from the Black Duck Vulnerability Integration and their target states in your instance.

Black Duck source states and their corresponding ServiceNow AI Platform states

Black Duck source states	Description of source states	Target state in the ServiceNow AI Platform
New	Vulnerability affects this component version.	Open
Needs Review	Can't be determined if a vulnerability affects this component version.	Open
Remediation Required	Remediation is required for this version.	Open
Remediation Complete	Remediation for this vulnerability is complete.	Closed
Mitigated	Vulnerability has been mitigated.	Closed
Patched	Vulnerability has been patched.	Closed
Ignored	Vulnerability has been ignored.	Closed

Import the project information from the Black Duck integration instance

Import the project information from the Black Duck integration instance to make sure that the vulnerability integrations run sequentially. A successful integration helps you to identify and ingest the application vulnerable items (AVIs).

Before you begin

Role required: App-Sec Manager group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can import all the project information from Vulnerability Response Integration with Black Duck in the [sn_vul_blackduck_project] Black Duck projects table. All the required attributes, for example, Project GUID, which are required to query for different versions of the project, are captured in the [sn_vul_blackduck_project] Black Duck projects table.

Procedure

1. Navigate to **All** > **Blackduck Vulnerability Integration** > **Integrations**.
2. Select an integration.
   For example, you can select the **Black Duck Project List Integration.**
3. Select **Execute Now**.

   Note: Each Vulnerability Response Integration with Black Duck is intended to provide the most complete data retrieval. Running these integrations out of order could result in incomplete data and requires ServiceNow and Application Vulnerability Response expertise.

   After the import is complete, you can see the project details in the [sn_vul_blackduck_project] Black Duck projects table.
4. For integration run statuses, see View the Vulnerability Response Integration with Black Duck import run status.
5. **Optional:** If you want to modify other integration parameters, you must navigate to the integration instance.

Import Vulnerability Response Integration with Black Duck project versions to the Discovered Applications table

Import the Vulnerability Response integration with Black Duck project versions to the Discovered Applications [sn_vul_app_release] table so that the Black Duck Vulnerability integrations run sequentially. A successful integration helps you to identify and ingest the application vulnerable items (AVIs).

Before you begin

Role required: App-Sec Manager group

About this task

You can add and view all the different versions of the projects (see the details in the Black Duck projects table) that were imported from the Vulnerability Response Integration with Black Duck in the Discovered Applications [sn_vul_release] table.

Procedure

1. Navigate to **All** > **Blackduck Vulnerability Integration** > **Integrations** .
2. Select an integration.
   For example, you can select the **Black Duck Application List Integration**.
3. Select **Execute Now**.

   Note: Each project version of the integrations is intended to provide the most complete data retrieval. Running these integrations out of order could result in incomplete data and requires ServiceNow and Application Vulnerability Response expertise.

   After the import is complete, you can see the different versions of a project in the Discovered Applications [sn_vul_app_release] table. If you are using CI Lookup Rules, these discovered applications are linked to the configuration item [cmdb_ci] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. See the status of your integration runs.
   For more information, see View the Vulnerability Response Integration with Black Duck import run status.

Import the application vulnerable items from the Vulnerability Response Integration with Black Duck

Import the application vulnerable items (AVIs) from the Vulnerability Response integration with Black Duck so that the integration runs sequentially. A successful integration helps you to identify and ingest the AVIs.

Before you begin
Role required: App-Sec Manager group

About this task
You can view the scan results from the Vulnerability Response Integration with Black Duck, insert AVIs in your instance, and enrich your third-party vulnerability data. By default, if the scanner record is in the Closed state, AVIs aren't created. You can control existing AVIs by using the property sn_vul_create_closed.

Procedure
1. Navigate to **All** > **Black Duck Vulnerability Integration** > **Integrations**.
2. Select an integration.
   For example, you can select the **Black Duck Application Vulnerable Item Integration**.
3. Select **Execute Now**.

   Note: The Vulnerability Response Integration with Black Duck is intended to provide you with the most complete data retrieval. Running these integrations out of order could result in incomplete data and requires ServiceNow and Application Vulnerability Response expertise.

   After you import all the SCA vulnerabilities from the Vulnerability Response Integration with Black Duck, you can view the AVIs and the third-party vulnerability data.

   Note: This is a scheduled job. In case it is not scheduled, you will be required to trigger this manually by selecting "Execute Now".

Set the import times for the Vulnerability Response Integration with Black Duck

Set the start time for the Vulnerability Response Integration with Black Duck imports. You can set the integrations ahead of time so that you get better performance and faster import runs.

Before you begin
Role required: App-Sec Manager group

About this task
After the initial import, the Black Duck vulnerability integrations do a full import each time they run.

Procedure
1. Navigate to **All** > **Black Duck Vulnerability Integration** > **Integrations**.
2. Select an integration.
3. Set the new **Start time**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The time is calculated as hours in local time. The default time for the Black Duck Application List Integration imports is 00:00:00. The other integrations are **On Demand** and are chained, which means that they follow a sequence to run after the Black Duck Application List Integration. Changing the **Start time** requires advanced ServiceNow and Application Vulnerability Management expertise.

4. Select **Update**.
   The new time is used for the next scheduled import.

Include Closed Black Duck application vulnerable items

Include Closed application vulnerable items (AVIs) during the Black Duck vulnerable item integration imports because by default, they aren't created during the integration imports. If you want to create them, you must change the system property.

Before you begin

Make sure that the Vulnerability Response Integration with Black Duck is installed and running.

Role required: admin

Procedure

1. In the navigation filter, enter `sys_properties.list`.
2. In the **Name** field for the list, enter `sn_vul.create_closed`.
3. Double-click the **Value** field and set it to **True**
4. Save by selecting the green check mark icon .
   The records in the Closed state in the next Black Duck import are created as AVIs in Application Vulnerability Response.

Fortify on Demand Vulnerability Integration

The Fortify on Demand Vulnerability Integration uses data imported from the Fortify product to help you determine the impact and priority of flaws in your code.

Fortify Vulnerability Integration

The Fortify product collects scanner data and makes that data available to the ServiceNow AI Platform®. It easily integrates with the ServiceNow® Application Vulnerability Response feature of Vulnerability Response to map third-party vulnerabilities enriching the data in your instance.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Every day, scheduled jobs invoke the integrations automatically. Once all the integrations are activated, they are chained to run in sequence. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Available versions

Release version	Release Notes
Vulnerability Response integration with Fortify v2.4 Fortify v2.3	Application Vulnerability Response release notes For compatibility information, see

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Release version	Release Notes
Fortify v2.2 Fortify v2.1	KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Fortify Vulnerability Integration

To view the Fortify Vulnerability Integration, navigate to **Fortify Vulnerability Integration** > **Integrations**.

The following integrations are included in the base system. These integrations are not all active by default.

After the initial run, every day, scheduled jobs are chained to run the integrations automatically in order. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Fortify on Demand Vulnerability Integrations

Integration	Description
Fortify on Demand Application List Integration	Retrieves Fortify application scanner data (vulnerabilities, metadata) and enriches your third-party application data. This integration is set to run daily at 00:00:00. It is active by default.
Fortify on Demand Scan Summary Integration	Retrieves scan records from Fortify. This integration is chained to run following the Fortify on Demand Application List Integration when activated. It is inactive, by default.
Fortify on Demand Application Vulnerable Item Integration	Retrieves scan results from Fortify, inserts AVITs, and enriches your third-party vulnerability data. If the scanner record is in the **Closed** state, AVITs are not created. Existing AVITs are still updated. Starting with v2.3, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item integration. This integration is chained to run following the Fortify on Demand Scan Summary Integration when activated. It is inactive, by default.

For integration run statuses see, View the Fortify Vulnerability Integration import run status.

To view data in third-party vulnerabilities, see View vulnerability libraries.

Preparing for the Fortify on Demand Vulnerability Integration

A successful Fortify Vulnerability Integration requires planning and the execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Fortify Vulnerability Integration assumes that you are familiar with the Fortify product and API.

Before you begin

The Common Weakness Enumeration (CWE) integration is also used by Application Vulnerability Response and should be running prior to installing and configuring the Fortify Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: NIST Vulnerability Database (NVD) data is not necessary to install the Fortify Vulnerability Integration, however they provide enrichment and would be useful to have.

For information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Role required: App-Sec Manager

About this task

Note: Before running the integration, make any necessary configuration change based on your requirements.

Validate your instance sizing based on the number of application vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

The Fortify Vulnerability Integration requires an API Key, API Secret, and API root URL, available from your Fortify on Demand account.

Procedure

To create an API Secret Key:

a. Log in to your Fortify on Demand portal.

b. Navigate to **All** > **Administration** > **Setting** > **API**.

c. Add ServiceNow as an application.

d. Click **New Secret** to generate an API Secret.

e. Record your API Secret for later use.

Install the ServiceNow® Vulnerability Response Integration with Fortify on Demand

Before you run the integration on your instance, the installation and configuration steps must be completed so the Fortify product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
	If the application is not installed and activated see, Install Vulnerability Response.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns users to the App-Sec Manager group. For information on Group roles see, Application Vulnerability Response user groups and roles. • The App-Sec Manager group oversees configuration and verifies expected results.

Role required: App-Sec Manager

Procedure

1. Log in to the instance you want to install the Fortify Vulnerability Integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with Fortify application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
8. Click **Request**.
   You will receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.
    Your application is automatically installed on your instance.

What to do next

Configure the Fortify Vulnerability Integration for your environment. See Configure the Fortify on Demand Vulnerability Integration.

Configure the Fortify on Demand Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the Fortify product properly integrates with the Application Vulnerability Response feature of Vulnerability Response. This application is available as a separate subscription.

Before you begin

Roles required: App-Sec Manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.
Verify that the Vulnerability Response Integration with Fortify application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install the ServiceNow Vulnerability Response Integration with Fortify on Demand.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the app and assigns users to the App-Sec Manager group. • The App-Sec Manager oversees configuration and verifies expected results.
For the Fortify Vulnerability Integration, have your **API id** and **API key** ready.	Contact Fortify to obtain the **API id** and **API key**.

Procedure

1. Log in to the instance you want to install the Fortify application vulnerability integrations on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Vulnerability Response integration with Fortify application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
8. Click **Request**.
   You will receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.
    Your application is automatically installed on your instance.
11. Once the installation completes, navigate to **Fortify Vulnerability Integration** > **FoD Configuration**.
12. On the form, fill in the fields.

Fortify on Demand configuration form

Field	Description
API root URL	User's Fortify instance URL.
API key	Unique identifier sent to the Fortify API.
API secret	Client secret provided by Fortify.
Include DAST	Option to include vulnerabilities from DAST scans. DAST scans identify vulnerabilities in the behavior of your overall application.
Include SAST	Option to include vulnerabilities from SAST scans. SAST scans identify vulnerabilities in the code.
Triaging exceptions and false positives in ServiceNow (starting with v20.0 of Vulnerability Response)	Select options to manage Exception management and False positive for AVIs with ServiceNow workflows automatically upon import. These options are activated by default. For an example use case, see Managing state mapping for deferrals and false positives in Application Vulnerability Response. **Manage exceptions in ServiceNow** Leave this option activated if you want to triage imported AVIs marked for the **Deferred** state. AVIs with **Source** states that normally are mapped to a **Deferred** state in your instance are instead mapped to **Open**. You **Request an exception** from the AVI record. **Manage false positives in ServiceNow**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Leave this option activated if you want to triage imported AVIs with **Source** states marked as **False Positive** or **Potential False Positive**. AVIs with these **Source** states that normally are mapped to a **Closed** state in your instance are mapped to **Open**. You request a **False positive** from the AVI record. ○ Deactivate one or both check boxes if you want to preserve the **Source** states imported from your scanner. ○ These AVIs are mapped to the Target states and Target reason states as they are imported but are not triaged by the exception and false positive workflows. The **Request exception** and **False Positive** actions are not visible on AVIs.
Triaging in ServiceNow (prior to v20.0 of Vulnerability Response)	Manage your application vulnerability triaging in ServiceNow instance: ○ Select the check box to triage the AVIs within ServiceNow. If this option is selected, AVIs are imported in Open state. You can then request an exception or mark the AVI as a false positive. ○ To retain the source state, that is, the state imported from the scanner, ensure that the check box is not selected. **Note:** The **Mark as False Positive** and **Request Exception** options are available only for AVIs being triaged within ServiceNow.

13. Select **Save and Test Credentials**.

What to do next

If your environment requires domain-separated imports, see Create domain-separated imports for an integration.

On initial installation, see Configure Application Vulnerability Response for further instructions.

After initial installation, for modifications refer to Fortify on Demand Vulnerability modification and activities.

View the Fortify Vulnerability Integration import run status

Use the **Vulnerability Integration Runs** related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

To view the Fortify import run status:

- The Vulnerability Response and Fortify Vulnerability Integration applications must be installed and configured.
- The Fortify Vulnerability Integration imports must be scheduled and running.

Role required: App-Sec Manager

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Application Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Fortify Vulnerability Integration** > **Integrations**.
2. Select an integration.
3. Click the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.
5. Starting with v2.3, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item Integrations.

Fortify on Demand Vulnerability modification and activities

Configure optional modifications specifically for the Fortify Vulnerability Integration.

Note: Changing other Fortify Vulnerability Integration settings, other than the ones listed here, requires advanced ServiceNow and Application Vulnerability Response expertise and is beyond the scope of the product documentation.

Perform a manual Fortify application vulnerability import

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily scheduled job.

Before you begin

Role required: App-Sec Manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Fortify Vulnerability Integration** > **Integrations**.
2. Choose an integration, for example, the Fortify Application List Integration.
3. Select **Execute Now**.

> **Note:** For complete data retrieval, run the Fortify application vulnerability integrations in sequence.

Import data using the Fortify on Demand Vulnerability Integration

Import data from the Fortify scanner, to map Application Vulnerable Items (AVIs), thereby enriching the data in your instance.

Before you begin

Role required: App-Sec Manager

About this task

After the initial import, Fortify vulnerability integrations do a delta import each time they run, retrieving the latest data. See Perform a manual Fortify application vulnerability import for more information on full imports.

Procedure

1. Navigate to **All** > **Fortify Vulnerability Integration** > **Integrations**.
2. Choose an integration.
3. On the form, fill in the fields.

Field	Description
Name	Name of the integration run.
Active	Option to activate an integration.
Run	Frequency of the integration run.
Time	
Application	Application containing this record.
Source integration	Source Integration for this integration.
Source instance	Source instance for this integration.
Next integration	Next-in-sequence integration, to run after the current integration run.
Start time	Start date and time of the last successful integration run. The time is calculated as Hours in local time. The default time for the initial run is 00:00:00.
Integration Details	
Integration script	Script include that extends the *`VulnerabilityIntegrationBase`* to be executed when the integration runs. This script defines how to retrieve data from a third-party system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Integration factory script	Script that defines how to construct the script include selected for the Integration script.
Report processor strategy	Strategy you want to use to handle the data returned by the integration script when the integration runs.

4. Select **Execute Now** to run the integration.

Include Closed Fortify on Demand application vulnerable items

By default, **Closed** application vulnerable items (AVITs) are not created during Fortify Vulnerable Item integration imports. If you want to create them, you must change a system property.

Before you begin

The Fortify Vulnerability Integration must be installed and running.

Role required: App-Sec Manager

Procedure

1. In the left navigation **Filter navigator** text box, type `sys_properties.list`.
2. In the **Name** search box for the list, enter `sn_vul.create_closed`.
3. Double-click on the **Value** field and set to **True**
4. Click the green check mark icon to save.
   Records in the **Closed** state in the next Fortify import are created as AVITs in Application Vulnerability Response.

GitHub Application Vulnerability Integration

The GitHub Application Vulnerability Integration imports Static application security testing (SAST) and Software Composition Analysis (SCA) data to help you view vulnerability alerts in the repositories in your GitHub environment.

GitHub Application Vulnerability Integration

The GitHub Application Vulnerability Integration collects scanner data and makes that data available to the ServiceNow AI Platform®. It easily integrates with the ServiceNow® Application Vulnerability Response feature of Vulnerability Response to map third-party vulnerabilities and GitHub alerts in your instance.

The GitHub environment supports multiple organizations. These organizations, both on-premise and Enterprise, might contain various departments, such as Engineering, Quality, Documentation, and so on. Each organization, in turn, can support multiple repositories. After you import your application data with the GitHub Repos Integration, you can import vulnerability and alert data from these repositories. Imported data is processed like an application in the Application Vulnerability Response application. When scanners detect vulnerabilities and generate alerts for the repositories, vulnerabilities are created in Application Vulnerability Response.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions

Release version	Release notes
GitHub Application Vulnerability Integration v1.2, v1.1, 1.0	Application Vulnerability Response release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

GitHub integrations

Integration	Description
GitHub Repos Integration	Starting with v1.1, import all the application data for your GitHub on-premise and Cloud (Enterprise) accounts. The integration imports applications from the Repositories you have configured for an Organization (on-premise) or from your Enterprise (Cloud) environment. Run this integration before running the other GitHub integrations, because they depend on the current application data imported from the Repos Integration.
GitHub CodeScan Integration	Retrieves Code scanning vulnerability alerts from GitHub repositories for security vulnerabilities and coding errors. Imported data is mapped to SAST results in your instance.
GitHub Dependabot Integration	Retrieves Dependabot alerts for dependencies with known vulnerabilities from repositories. Imported data is mapped to SCA results in your instance.
GitHub Secret Scanning	Retrieves secrets from your organizations code along with the application security testing results. The data is mapped to SCA results in your instance. The system maps secrets to AVIT with scan type Secret and maps generic secrets to AVIT with scan type Generic Secret.
GitHub Secret Scanning Location	Retrieves the location and line numbers for the scanned secrets in your organizations code to help your developers remediate.

Uploading SBOM files to the ServiceNow AI Platform® from your GitHub repositories

Determine if SBOM files generated in your CI/CD (continuous integration and continuous delivery/deployment) pipelines have been successfully queued in your ServiceNow AI Platform® instance.

- Protect your environments from potentially harmful components during software development cycles with GitHub Actions that you initiate from your GitHub environment.
- Obtain any required GitHub Actions for SBOM upload in the GitHub Marketplace.

The SBOM applications are required to upload SBOM files. See Exploring Software Bill of Materials for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing imported data

Imported application data from the GitHub Repos Integration is displayed on the Discovered Applications [sn_vul_app_release] table. Run this integration first.

The Repos Integration imports tags and topics you have configured for a repository in your GitHub account from the Settings menu. Any Custom properties are located on the menu under your Repository. Values you set for the properties are imported as key-value pairs. For more information on where to view this information in your instance, see View the GitHub Application Vulnerability Integration import run status and imported repository data.

Imported data (findings) from the GitHub Dependabot Integration is displayed on the following tables.

- Discovered Applications [sn_vul_app_release].
- Application Vulnerability Scan Summaries [sn_vul_app_vul_scan_summary].
- Application Vulnerable Items [sn_vul_app_vulnerable_item].
- Packages [sn_vul_app_package].

Imported data from the GitHub CodeScan Integration is displayed on the following tables.

- Discovered Applications [sn_vul_app_release].
- Application Vulnerability Scan Summaries [sn_vul_app_vul_scan_summary].
- Application Vulnerability Entries [sn_vul_app_vul_entry].
- Application Vulnerable Items [sn_vul_app_vulnerable_item].

Preparing for the GitHub Application Vulnerability Integration

Prepare for the integration by performing these tasks. The GitHub Application Vulnerability Integration assumes that you are familiar with the GitHub product and API.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Roles required:

- admin to download, install, and activate applications and assign roles.
- GitHub administrator to obtain credentials and generate tokens in the GitHub console.
- admin to set up connections and alias records in your instance.

Setup tasks

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks (continued)

Setup tasks	Description
Verify that the GitHub Application Vulnerability Integration is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install the ServiceNow GitHub Application Vulnerability Integration.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the app and assigns users to the App-Sec Manager user group. • The App-Sec Manager oversees configuration and verifies expected results. • sn_vul_github_config_integration is inherited by the App-Sec Manager user group. This role contains the connection_admin and oauth_admin roles.
Obtain your GitHub credential and account information.	Account information is required on records you create for authentication. See Creating OAuth 2.0 credentials for GitHub Apps - JWT for the GitHub Application Vulnerability Integration for more information about details your need and setting up the required records for OAuth authentication.
Verify you are importing Common Weakness Enumeration (CWE) data.	The Common Weakness Enumeration (CWE) integration is also used by Application Vulnerability Response and should be running prior to installing and configuring the GitHub Vulnerability Integration. It is installed with Vulnerability Response, by default. **Note:** NIST Vulnerability Database (NVD) data is not necessary to install the GitHub Vulnerability Integration, however it provides enrichment and would be useful to have. For information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Creating OAuth 2.0 credentials for GitHub Apps - JWT for the GitHub Application Vulnerability Integration

Perform the following steps to integrate your GitHub Apps using the JWT bearer token for the GitHub Application Vulnerability Integration.

Roles required:

- sn_vul.app_sec_manager and admin for records in your ServiceNow AI Platform.
- No instance role required for tasks in your GitHub account.

.

Create and configure the GitHub app for the GitHub Application Vulnerability Integration

Create a custom GitHub App from your GitHub account to activate OAuth 2.0 authentication with your GitHub Application Vulnerability Integration in your instance.

Before you begin

Role required: No instance role required

About this task

Complete these steps from your GitHub account. See Building GitHub Apps on the GitHub Developer site for instructions on creating and configuring custom applications.

Procedure

1. From your GitHub account, create your GitHub App by navigating to **Developer Settings** > **GitHub Apps**.
2. In the **Homepage URL** field, enter `https://<instance-name>.service-now.com`.
3. In the **User authorization callback URL** field, enter `https://<instance-name>.service-now.com/oauth_redirect.do`.
4. In the **Identifying and authorizing users** section, deselect the **Expire user authorization tokens** field.
5. In the **Webhook** section, select the **Active** field.
6. In the **Webhook URL** field, enter `https://instance-name>.service-now.com/`.
7. Leave the remaining fields empty (default).
8. In the **Repository permissions** section, configure the following settings.

Code scanning	Read-only
Contents	Read-only
Custom properties	Read-only
Dependabot alerts	Read-only
Metadata	Read-only
Secret scanning alerts	Read-only

Note: If you are already using a GitHub App and you update any of the permissions, you must review and accept those permissions for your GitHub App. You can navigate to your app, and select **Configure > Review request > Accept new permissions**.

9. Leave the remaining permissions as `No access` (default).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. In the **Subscribe to events** section, select the **Deployment protection rule** option.
11. Right-click in the header to save the changes.
12. Install the newly created GitHub App on the accounts of your choice.
    a. From the GitHub Apps settings page, select your app.
    b. In the left sidebar, select **Install App**.
    c. Select **Install** next to the organization or personal account containing the correct repository.
    d. Install the app on all repositories or select repositories.
    For more information, see Installing GitHub Apps.
13. After installation, select the settings (gear icon) for your App and write down or note the following information.

    These details are required when you create the application registry in your ServiceNow AI Platform instance.

    - App ID
    - Client ID
    - Client secret.
    - Note the token in the URL. This is the token ID you enter in the Token URL in your instance.
14. Scroll down the page and generate a new private key and save it to your machine.

Generate the JKS certificate for the GitHub Application Vulnerability Integration

Generate a JKS certificate for the JWT authentication for the GitHub Application Vulnerability Integration.

Before you begin

You need to note the password that you use to generate the .jks file (KeyStore password).

Role required: sn_vul.app_sec_manager

Procedure

1. Create a CA signed certificate using the GitHub App private key:

```
openssl req -new -x509 -key <file-name>.pem -out
 <certificate-name>.pem -days 1095
```

2. Enter the required details.
3. Create the PKCS 12 file using the GitHub App private key and CA signed certificate:

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey
 <file-name>.pem -certfile <certificate-name>.pem -out
 <PKCS-12-file-name>.p12
```

4. Provide the export password.
5. Create the JKS file:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
keytool -importkeystore -srckeystore
 <PKCS-12-file-name>.p12 -srcstoretype pkcs12 -destkeystore
 <JKS-certificate-filename>.jks -deststoretype JKS
```

6. Provide the destination and source keystore passwords.

Attach the GitHub Java Key Store certificate to your instance for the GitHub Application Vulnerability Integration

Activate the JWT Bearer Grant token authentication by attaching the valid GitHub Java KeyStore (JKS) certificate to your instance.

Before you begin

A valid Java KeyStore certificate.

Role required: sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **System Definition** > **Certificates**.
2. Select **New**.
3. On the form, fill in the fields.

X.509 Certificate form fields

Field	Description
Name	Name to uniquely identify the record. For example, `My GitHub App Certificate for AVR`.
Notify on expiration	Option to specify the users to be notified when the certificate expires.
Warn in days to expire	Number of days to send a notification before the certificate expires.
Active	Option to enable the certificate.
Type	Option to select the type of the certificate. Select **Java Key Store**.
Expires in days	Number of days until the certificate expires.
Key store password	Password associated with the certificate (hint: the destination KeyStore password previously created).
Short description	Summary about the certificate.

4. Select the attachments icon and attach a JKS certificate.
5. Select **Validate Stores/Certificates**.
   A Valid key_store message is displayed for valid certificate files.

Create a JWT signing key for the GitHub JKS certificate for the GitHub Application Vulnerability Integration

Create a JSON Web Token (JWT) signing key to assign to your GitHub Java KeyStore certificate.

Before you begin

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- admin
- sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **System OAuth** > **JWT Keys**.
2. Select **New**.
3. On the form, fill in the fields.

JWT Keys form fields

Field	Description
Name	Name to uniquely identify the JWT signing key. For example, `My GitHub App JWT Key for AVR`.
Signing Keystore	Select the Valid JKS certificate you attached in the previous task.
Key Id	Leave this field blank.
Signing Algorithm	Leave this value as RSA 256.
Signing Key Password	Password associated with the signing key. This is the password you used to generate the JKS file.
Active	Option to enable the key.

4. Right-click anywhere in the gray header of the page and select **Save**.

Create a JWT provider for your GitHub signing key for the GitHub Application Vulnerability Integration

Add a JSON Web Token (JWT) provider to your ServiceNow instance for GitHub.

Before you begin

Roles required:

- admin
- sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **System OAuth** > **JWT Providers**.
2. Select **New**.
3. On the form, fill in the fields.

JWT Provider form fields

Field	Description
Name	Name to uniquely identify the JWT provider. For example, `My GitHub App JWT Provider for AVR`.
Expiry Interval (sec)	Number in seconds to set the lifespan of JWT provider tokens. You can leave this setting in its default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Signing Configuration	Select the JWT key you created in the previous steps.

4. Right-click the form header, and select **Save**.
5. E nter your GitHub App **App ID** for the value of the **iss** claim, in the Standard Claims related list. This is the App ID from the GitHub App in your GitHub console that you created in the previous steps.
6. Leave **aud** and **sub** values blank (default).
7. Right-click the form header, and select **Save**.

Register GitHub as an OAuth Provider (JWT) for the GitHub Application Vulnerability Integration

Use the information generated during GitHub App account configuration to register GitHub as an OAuth provider and allow the instance to request OAuth 2.0 tokens.

Before you begin

Roles required:

- admin
- sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **System OAuth** > **Application Registry**.
2. Select **New**.
   The **What kind of OAuth application?** message is displayed.
3. Select **Connect to a third party OAuth Provider**.
4. On the form, fill in the fields.

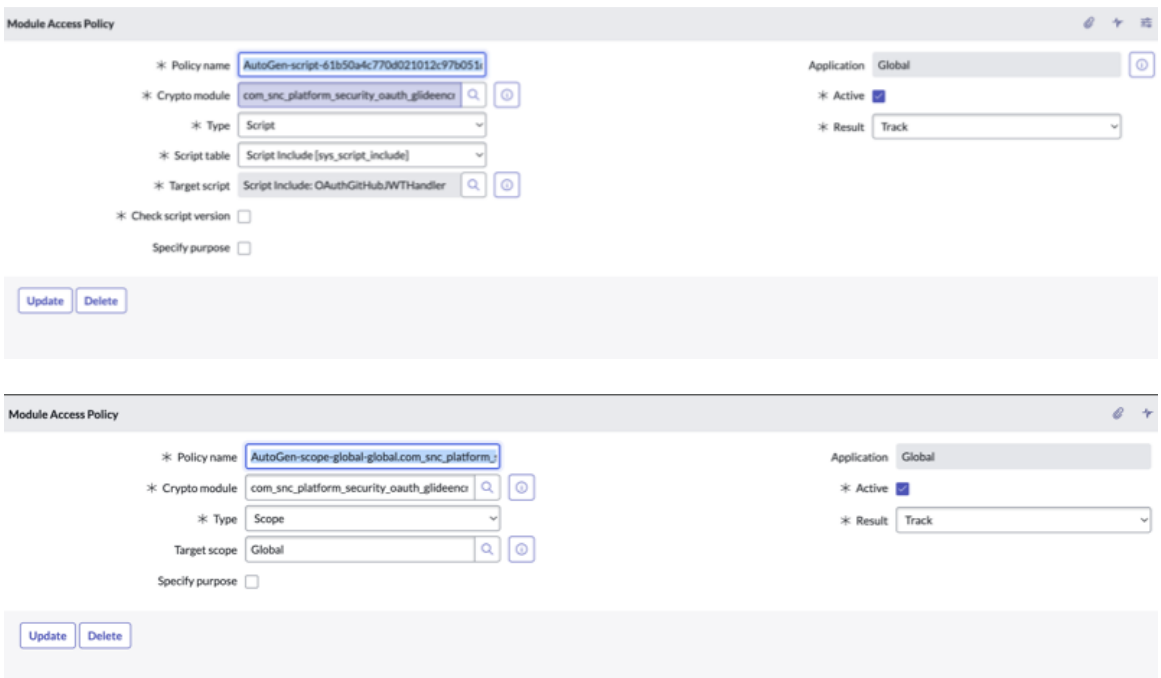
Application Registry form fields

Field	Description
Name	Name to uniquely identify the record. For example, enter `My GitHub App Provider for AVR`.
Client ID	Client ID of your GitHub App. The Client ID is from the GitHub application in your GitHub console that you created in the previous steps. This ID available in the **About** section of your GitHub App configuration in GitHub.
Accessible	Leave this setting in its current value.
Client Secret	Client Secret of your GitHub App. The Client secret is from the GitHub application in your GitHub console that you created in the previous steps. This ID available in the **About** section of your GitHub App configuration in GitHub.
Active	Option to enable the key. Leave this selected.
Authorization URL	This URL is generated automatically.
Token URL	The location of the token endpoint that the instance uses to retrieve and refresh tokens. Enter the Token from the URL in your GitHub App. This is the token displayed in the URL after your app is installed in GitHub. From the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Install App section in your GitHub App configuration in GitHub, select the gear. The token is displayed in the webpage URL. ○ For Cloud: https://api.github.com/app/installations/49374672/access_tokens. Installation ID: 9374672. ○ For on-premise: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3.
OAuth API script	Option that enables you to reference an amended OAuthUtil script include. Select **OAuthGitHubJWTHandler**.
Default Grant type	Type of grant associated with application registry. Select **JWT Bearer**.

5. Leave the rest of the form fields as default.
6. Right-click the form header, and select **Save**.
7. Scroll to the **OAuth Entity Profiles** related list, select it, and open the default profile that was created on the list.
8. Populate the **JWT Provider** field with the JWT provider previously created and save the form.
9. Return to the application registry file and save it.
10. Navigate to **Key Management** > **Module Access Policies** > **All**.
11. Select the policy that has `com_snc_platform_security_oauth_glideencrypter` as the **Crypto module** field value and the Script Include: `OAuthGitHubJWTHandler`.



12. Verify the **Result** field is set to `Track` and save your changes.

Create Credentials and Connections for the GitHub Application Vulnerability Integration

Create a credential record to the GitHub App provider previously created to authorize actions.

Before you begin

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- admin
- sn_vul.app_sec_manager

Procedure

1. Navigate to **Credentials and Connections** > **Credentials**.
2. Select **New**.
3. Select **OAuth 2.0 Credentials**.
4. Select **New** and fill in the fields.

Field	Description
Name	Unique name for the record.
Applies to	Select All MidServer or a specific MidServer.
OAuth Entity Profile	Select the search icon and locate the entity profile you created in the preceding steps.
Other fields	Leave these fields in their defaults.

5. Right-click anywhere in the header of the page and select **Save**.
   The Credentials list is displayed.
6. Open the record you just created and select the **Get OAuth Token** related link.
   A message is displayed that the OAuth token was imported successfully.
7. Navigate to **Credentials and Connections** > **Connections & Credential Aliases**.
8. Select **New** and fill in the fields.

Field	Description
Name	Name for the record.
Application	Read-only.
Parent Alias (optional)	Select the search icon and choose one from the list.
Type	Connection and Credential.
Connection type	HTTP.
Support Multiple Active Connections (optional)	Deactivated.
Default Retry Policy	Default HTTP Retry Policy
Configuration Template	Leave empty.

9. Select **Submit**.
   The Connections and Credential Aliases list is displayed.
10. Open your record and on the Connections related list tab select **New** and fill in the fields on the HTTP Connection record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name for the record.
Active	Activated.
Credential	Select the Credential record you created in the preceding steps.
Connection alias	Your record is displayed.
URL builder	Deactivated.
Connection URL	This is the base URL: https://api.github.com for Enterprise. The on-premise is your GitHub endpoint URL.
Use MID Server (optional)	MID Server is required for on-premise. It is optional for Enterprise.
Connection timeout	Enter a value.

11. Select **Submit**.
    The Connections and Credential Aliases list is displayed. You are now ready to complete the steps to Configure the GitHub Application Vulnerability Integration. In the Connection field, you enter the credentials that you created in the preceding steps.

Install the ServiceNow® GitHub Application Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the GitHub Application Vulnerability Integration properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Role required: admin

Procedure

1. Log in to the instance you want to install the GitHub Application Vulnerability Integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for GitHub Application Vulnerability Integration application.
4. Select the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Select **Request App** and enter your Now Support login credentials.
6. Select **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and select **Validate Instance**.
8. Select **Request**.
   You receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Locate the application, select it, and select **Install**.
    Your application is automatically installed on your instance.

Configure the GitHub Application Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the GitHub product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Roles required:

- App-Sec Manager user group
- sn_vul.app_sec_manager required for OAuth set up

Procedure

1. Navigate to **All** > **Github Vulnerability Integration** > **Configuration**.
2. Choose **Basic Authentication** or **OAuth** for Authentication type.
   - Basic authentication requires a MID Server for on-premise instances. Generate the API token required for Basic authentication from your GitHub account.
   - OAuth requires the OAuth App, credential, and connection setup described in Creating OAuth 2.0 credentials for GitHub Apps - JWT for the GitHub Application Vulnerability Integration.
3. Fill in the fields based on the type you choose.
   Basic Authentication

Field	Description
API URL	The appropriate GitHub API URL for Enterprise or on-premise. The default URL is https://api.github.com. On-premise is your GitHub endpoint URL.
API Token	Token you generated from your GitHub console.
API Type	Choose one: **Organization** Choose this option if you want to import data for a specific organization by name. The GitHub environment supports multiple organizations. Each organization can support multiple repositories. If you enter an organization, only data from that organization is imported. **Enterprise** The Enterprise environment supports multiple organizations. Choose this option if you want to import vulnerability data from

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	all the organizations in your Enterprise (Cloud) environment.
Organisation Name	Name of your GitHub Repository. Only data from the organization you enter is imported.
MID Server	For on-premise instances for Basic Authentication, a MID Server is required.
Select options to manage Exception management and False positives.	Select options to manage Exception management and False positive for applications vulnerable items (AVIs) with ServiceNow workflows automatically upon import. **Manage exceptions in ServiceNow** Leave this option activated if you want to triage imported AVIs marked for the **Deferred** state. AVIs with **Source** states that normally are mapped to a **Deferred** state in your instance are instead mapped to **Open**. You **Request an exception** from the AVI record. **Manage false positives in ServiceNow** Leave this option activated if you want to triage imported AVIs with **Source** states marked as **False Positive** or **Potential False Positive**. AVIs with these **Source** states that normally are mapped to a **Closed** state in your instance are mapped to **Open**. You request a **False positive** from the AVI record. ○ Deactivate one or both check boxes if you want to preserve the **Source** states imported from your scanner. ○ If deactivated, the **Request exception** and **False Positive** actions are not visible on AVIs.
Integration Instance	Instance into which you are importing data.

OAuth

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
API URL	The appropriate GitHub API URL for Enterprise or on-premise. The default URL is https://api.github.com. On-premise is your GitHub endpoint URL.
Connection	The connection you created described in Creating OAuth 2.0 credentials for GitHub Apps - JWT for the GitHub Application Vulnerability Integration.
API Type	Choose one: **Organization** Choose this option if you want to import data for a specific organization by name. The GitHub environment supports multiple organizations. Each organization can support multiple repositories. If you enter an organization, only data from that organization is imported. **Enterprise** The Enterprise environment supports multiple organizations. Choose this option if you want to import vulnerability data from all the organizations in your Enterprise (Cloud) environment. **Note:** GitHub Apps do not support Enterprise-level APIs.
Organisation Name	Organization name for your GitHub repositories. Only data from the repositories in the organization you enter is imported.
Select options to manage Exception management and False positives.	Select options to manage Exception management and False positive for applications vulnerable items (AVIs) with ServiceNow workflows automatically upon import. **Manage exceptions in ServiceNow** Leave this option activated if you want to triage imported AVIs marked for the **Deferred** state. AVIs with **Source** states that normally are mapped to a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Deferred state in your instance are instead mapped to **Open**. You **Request an exception** from the AVI record. **Manage false positives in ServiceNow** Leave this option activated if you want to triage imported AVIs with **Source** states marked as **False Positive** or **Potential False Positive**. AVIs with these **Source** states that normally are mapped to a **Closed** state in your instance are mapped to **Open**. You request a **False positive** from the AVI record. ○ Deactivate one or both check boxes if you want to preserve the **Source** states imported from your scanner. ○ If deactivated, the **Request exception** and **False Positive** actions are not visible on AVIs.

4. Select **Save and Test credentials**.
5. Run the GitHub Repos Integration before running the other integrations.
   The other GitHub integrations depend on current application data imported from the Repos Integration. Data from the Repos Integration is stored in the Discovered Applications [sn_vul_app_release] table. See View the GitHub Application Vulnerability Integration import run status and imported repository data for more information.

View the GitHub Application Vulnerability Integration import run status and imported repository data

Use the **Vulnerability Integration Runs** related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin

Role required: sn_vul.app_sec_manager

Procedure

1. Navigate to **All** > **GitHub Vulnerability Integration** > **Integrations**.
2. Select an integration.
3. Select the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.

Trouble?

The most common causes for a failed run include:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Network interruption.
- An issue in the data transfer resulting in corrupted data during the transform.

If you encounter any of these conditions, select **Execute Now**, and rerun the integration.

5. To view imported repositories, navigate back to the integrations list and select the GitHub Repos Integration record.
6. Select the **Vulnerability Integration Runs** related list and open a record.
   The number of repositories you imported with an integration run is displayed in the Imported items column.

   Any tags and topics you have configured for a repository in your GitHub account from the Settings menu are imported. Any imported Custom properties are located on the menu under your Repository.

   Tags, topics, and custom properties are imported into your instance only if they are configured in your GitHub account.

   If imported, this GitHub information is displayed in your instance on the Source additional info column on the Discovered Applications [sn_vul_app_release] table and the Source additional info. section on a discovered application record. Custom properties are displayed as key-value pairs, and tags and topics are displayed in arrays.

View GitHub Application Vulnerability Integration import sets

View details for import information for the GitHub Application Vulnerability Integration.

Before you begin

Role required: sn_vul.app_sec_manager

Procedure

1. Navigate to the **GitHub Vulnerability Integration** > **Import Set Tables**.
2. Select a record for an integration.
3. Select a Related link to view the following information:
   - Import sets
   - Transform Maps
   - Transform History

Invicti Vulnerability Integration

The Invicti Vulnerability Integration uses application data imported from the Invicti product to help you determine the impact and priority of flaws in your code.

Invicti Vulnerability Integration

The Invicti Vulnerability Integration collects scanner data and makes that data available to the ServiceNow AI Platform®. It easily integrates with the ServiceNow® Application Vulnerability Response feature of Vulnerability Response to map imported third-party application vulnerability information into your instance.

The integration imports the following types of scanned data.

- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)

For more information about DAST and IAST, see Exploring Application Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions

Release version	Release notes
Invicti Vulnerability Integration v1.1 Invicti Vulnerability Integration 1.0	Application Vulnerability Response release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Integrations

The following integrations are included in the base system. The integrations are chained so that after one integration successfully completes, the next integration is initiated. The integrations run in the order listed in the following table.

After the initial run, every day, scheduled jobs are chained to run these integrations automatically in order. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Invicti application vulnerability integrations

Integration	Description
Invicti Application List Application	Imports applications scanned by Invicti into the Discovered Applications [sn_vul_app_release] table or the Scanned Application [sn_vul_app_scanned_application] table based on how the *sn_vul.use_product_model* system property is set for the CI lookup rule records. • If the product model property is set to true, an application is inserted in the Discovered Application release table. • If the product model property is set to false, an application is inserted in the Scanned Application table. You can choose to activate lookup rules with configuration items (CIs) as the lookup targets by modifying the system property. If you modify it, you should also activate CI Lookup rules to match the lookup target. For more information, see: • Configure the Invicti Vulnerability Integration • Create a CI lookup rule • Reapplying CI Lookup rules in Application Vulnerability Response
Invicti Scan List Integration	This integration is initiated after the Application List Integration is successfully

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Invicti application vulnerability integrations (continued)

Integration	Description
	completed. This integration imports data about the date and time a scan was run.
Invicti Application Vulnerable Item Integration	This integration is initiated after the Scan List Integration is successfully completed. Starting with v1.1, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item integration. Each vulnerability in Invicti has a type, for example,**DirectoryListing**. This type is mapped as a unique ID in your instance and displayed as part of the value in the Vulnerability field on the application vulnerable item (AVI) record: **Invicti-DirectoryListing**. For more information about mapping, see Invicti Vulnerability Integration state mapping.

The upper limit for items per page for all three integrations is 200.

Prepare for the Invicti Vulnerability Integration

A successful integration requires planning and the execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Invicti Vulnerability Integration assumes that you are familiar with the Invicti product and API.

The Common Weakness Enumeration (CWE) integration is also used by Application Vulnerability Response and should be running prior to installing and configuring the Invicti Vulnerability Integration.

Note: NIST Vulnerability Database (NVD) data is not necessary to install the integration, however it provides vulnerability enrichment and is useful.

For information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Note: Before running the integration, make any necessary configuration change based on your requirements.

Validate your instance sizing based on the number of application vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support. The admin role is required to install and configure applications on your ServiceNow AI Platform instance.

Obtain your API credentials and API token on your Invicti console. Review the information available on the Invicti product website at API Overview.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install the ServiceNow® Vulnerability Response Integration with Invicti

Before you run the integration on your instance, the installation and configuration steps must be completed so the Invicti Vulnerability Integration application properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Role required: admin

Procedure

1. Log in to the instance you want to install the Invicti Vulnerability Integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for the Invicti Vulnerability Integration application.
4. Select the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Select **Request App** and enter your Now Support login credentials.
6. Select **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and select **Validate Instance**.
8. Select **Request**.
   You receive an email with detailed installation instructions.
9. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
10. Locate the application, select it, and select **Install** to activate it.
    Your application is automatically installed on your instance.

Configure the Invicti Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the Invicti Vulnerability Integration properly works with the Application Vulnerability Response feature of Vulnerability Response.

Before you begin

Roles required:

- admin to install and activate applications
- App-Sec Manager user group to configure the integration

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	If the application is not installed and activated see, Install Vulnerability Response.
Verify that the Invicti Vulnerability Integration is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install the ServiceNow Vulnerability Response Integration with Invicti.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the app and assigns users to the App-Sec Manager group. • The App-Sec Manager oversees configuration and verifies expected results.
For the Inviciti Vulnerability Integration, have your **User ID** and **API token** ready.	Contact your Invicti administrator to obtain the **User ID** and **API token** if you don't know them. For more information, see the Invicti product website at API Overview.

Procedure

1. Navigate to **All** > **Invicti** > **Invicti Configuration**.
2. Fill out the fields.

Field	Description
API URL	User's Invicti's instance URL. This is the information you obtained from Prepare for the Invicti Vulnerability Integration.
User ID	Unique user ID.
API token	API token you generated from your Invicti console. This is the information you obtained from Prepare for the Invicti Vulnerability Integration.
Choose the scan type. You must select at least one.	
Import DAST	Option to include vulnerabilities from DAST scans. DAST scans find vulnerabilities for an application dynamically while it is running. This approach might imitate an outside attack.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Import IAST	Option to include vulnerabilities from IAST scans. IAST scans detect software vulnerabilities by interacting with the program while it is running. Human observation, automated tests, and sensors are used in combination to interact with the application to locate vulnerabilities.
Date format	Parameter that converts the start time to the format supported by the Invicti API used by the Invicti Application Vulnerable Item Integration. This parameter should match the format you've defined or selected in your Invicti account, for example, **dd/MM/yyyy**. Verify the date and time formats in your Invicti console match those you enter for the Date format in your ServiceNow AI Platform instance. To change this format in your Invicti console: **a.** Log in at Invicti Sign In. **b.** Select **User name** in the top right. **c.** Navigate to **User settings** > **Date and time format**. **Note:** Failed imports might occur if you enter an invalid date format in your ServiceNow AI Platform instance. If you enter a valid format in your instance that differs from the date format in your Invicti console, Invicti will return an empty payload.
Manage exceptions in ServiceNow	Choose one: **Activated (selected)** Application vulnerable items (AVIT) from Invicti with states such as **Present** and **AcceptedRisk** that might be deferred in your instance are instead mapped to **Open** automatically. **Deactivated (not selected)** Source states for Application vulnerable items (AVITs) imported from Invicti are preserved. You must manage exceptions for these AVITs (defer them) from AVIT records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For more information about Invicti source states and target fields, see Invicti Vulnerability Integration state mapping.
Manage false positives in ServiceNow	Choose one: **Activated (selected)** AVITs with states from Invicti such as **Present** and **False Positive** that might transition to **Closed** in your instance are instead mapped to **Open** automatically. **Deactivated (not selected)** AVIT states imported from Invicti are preserved. You must manage false positives or potential false positives for these AVITs from AVIT records.

3. Select **Save and Test Credentials**.
4. **Optional:** Modify your lookup rules so they are based on configuration items.

   (Optional) By default, the **sn_vul.use_product_model** system property is activated (set to `true`) for your Lookup rules listed on the [sn_sec_cmn_ci_lookup_rule] table based on the product model. When this rule is activated:

   - This rule identifies matches between imported data and the data in your Configuration Management Database (CMDB) based on the product model.
   - Records are created or updated on the Discovered Applications [sn_vul_app_release] table.
   - When you create or edit your lookup rules for Invicti, **Product Model** is displayed in the **Lookup target** field on the rule form.

   To modify your rules so they are based on configuration items, you must manually deactivate (set to `false`) the **sn_vul.use_product_model** system property.

   a. Navigate to **All** > **System Properties** and locate the **sn_vul.use_product_model** record and set the Value to `false`.

   b. Select **Update**.

   c. Navigate to **All** > **Security Operations** > **CMDB** > **Lookup Rules**.

   d. Locate the Application name and Source Application ID rules that have the Lookup target as **Configuration item**.

   e. Select the Active check box for these rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

f. Select **Update**.
When you create or edit your lookup rules for Invicti, note that **Configuration item** is displayed in the **Lookup target** field on the rule form. Records are created or updated on the Scanned Applications [sn_vul_app_scanned_application] table.

Viewing the Invicti Vulnerability Integration import run status and records

Use the **Vulnerability Integration Runs** related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Viewing import status, import sets, and records

To view the status of your imports, as a user in the App-Sec Manager user group, navigate to **All** > **Invicti Vulnerability Integration** > **Integrations** and select an integration record. Select the **Vulnerability Integration Runs** related list.

Starting with v1.1, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item integration.

To view the import sets, navigate to **All** > **Invicti Vulnerability Integration** > **Integrations** > **Import Set Tables** and select an integration.

The Application List Integration creates or updates records based on the Lookup Target:

- Product model: Discovered Applications [sn_vul_app_release] table
- Configuration item: Scanned Applications [sn_vul_app_scanned_application] table

The Scan List integration creates or updates records in the Scanned Applications [sn_vul_app_vul_scan_summary] table.

The Application Vulnerable Item Integration creates or updates records in the Application Vulnerable Items [sn_vul_app_vulnerable_item] and CWEs [sn_vul_cwe] table.

Note: Each vulnerability in Invicti has a 'type', for example, ProductDirectoryListing. This type is imported mapped as a unique ID into your instance and displayed as part of the value in the Vulnerability field on the application vulnerable item (AVIT) record. In this example the value is `Invicti-ProductDirectoryListing`, and this value is also displayed as the unique ID on the Application Vulnerability Entry record. Invicti AVITs support multiple Common Weakness Enumeration (CWE) entries, so CWEs are not used as unique IDs. CWEs are also displayed on the AVIT record.

For Invicti AVITs, if there are duplicate types in Invicti for a vulnerability, the word 'custom' is inserted in the value, for example, `Invicti-custom-ProductDirectoryListing`. If you create a Custom type for vulnerabilities, the vulnerability ID might be `Invicti-Custom-<title of vulnerability>`.

New fields: For `scan type=Invicti`, the Affected parameters, and Custom fields might include data that can help you understand the vulnerability and help you remediate it. If there is no data, these fields are not displayed on the AVIT.

Invicti Vulnerability Integration state mapping

The following source states from the Invicti Vulnerability Integration and their target states in your instance are listed in the following table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Invicti source states and their corresponding ServiceNow AI Platform states

Invicti source states	Description of source states	Target state in the ServiceNow AI Platform
Present	The Issue is identified.	Open
Present, AcceptedRisk, Revived	The Issue has been considered and is marked as a low risk vulnerability.	Deferred
Present, False Positive	The Issue has been considered and is marked as not a genuine vulnerability.	Closed
FixedUnconfirmed, Fixed Unconfirmed	The Issue has been fixed but not confirmed by Invicti Enterprise.	Resolved
Fixed (Confirmed), FixedConfirmed, FixedConfirmed, AcceptedRisk, FixedConfirmed, False Positive	The Issue has been fixed and confirmed by Invicti Enterprise and no further action is required.	Closed
Fixed (Can't Retest)	The Issue has been identified but Invicti cannot retest to confirm whether the Issue has been fixed or not.	Resolved
Revived	The issue was fixed in previous scans but has been found again.	Open
Deferred, Ignored	The Issue was ignored by the user. In Invicti Enterprise, to ignore an issue, a user updates its status to “accepted risk”.	Risk Accepted

Application release mapping

Source Field	Target field on ServiceNow AI Platform
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date
Name	app_name
RootUrl	Source_additional_info
Description	description
Tags	Tags

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability mapping

Source Field	Target field on ServiceNow AI Platform
Type	Category name
Vulnerability detail	Summary
Impact	Threat
Source references	Web references
Source recommendation	Solution
Type	source_entry_id/ID
Severity	source_severity
Classification["Cwe"]	CWE list
CvssVectorString	CVVS v3 fields

Scan summary mapping

Source field	Target Field
Source	Source
TotalVulnerabilityCount	Detected_flaw_count
Initiated date	Dynamic scan date
id	source_scan_id

Application vulnerable item (AVIT) mapping

Source Field	Target field on ServiceNow AI Platform
Type	Scan type
Website ID	Source app ID
ID	Source AVIT ID
Last seen date	Last found
First seen date	First found
Last updated date	Last scan date
parameters	Affected parameter
URL	Affected URL
Severity	Source severity
Url	Source link
Vulnerability detail	Source vulnerability summary
External references	Source references
Remedy + Remedy references	Source recommendation
State	Source remediation status

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Impact	Source vulnerability explanation

Veracode Vulnerability Integration

The Vulnerability Response Integration with Veracode application uses data imported from the Veracode product to help you determine the impact and priority of flaws in your code.

Veracode Vulnerability Integration

The Veracode product collects Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and manual scanner data and makes that data available to the ServiceNow AI Platform®. It easily integrates with the Application Vulnerability Response feature of Vulnerability Response to map third-party vulnerabilities enriching the data in your instance.

Starting with v19.0 of Vulnerability Response, you can import Software Composition Analysis (SCA) vulnerabilities and Software Bill of Materials (SBOM) vulnerability data to help you identify weaknesses in your software applications. For more information, see Exploring Software Bill of Materials.

A shared API ingests DAST, SAST, SCA data and manual penetration testing results.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Every day, scheduled jobs invoke the integrations automatically in the order they are listed. You can also execute individual scheduled jobs manually. Scheduled jobs simplify the vulnerability remediation life cycle by keeping the instance synchronized with other vulnerability management systems.

Get more details from Veracode

Starting with v4.2, select **Get More Details** on application vulnerable items (AVITs) that have Veracode as the Source on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table or from the list views in the Vulnerability Response Workspaces to view the following Veracode data.

- HTTP Source request and Source response details for Dynamic Application Security Testing (DAST) scans are displayed on the HTTP Request/Response related list.
- Solution recommendations from Veracode are displayed on the Findings related list.
- HTTP Source request, Source response, and recommendations are displayed on the Details tab In the Vulnerability Response Vulnerability Response workspaces.
- The Description column is supported on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table.
- To support deleted applications Veracode Link Projects and Veracode SBOM Integrations for these two integrations, you can choose to skip 403 and 404 errors and retry 50x errors. The following parameters are included in a retry mechanism in a script include: VeracodeLinkProjectsIntegration and VeracodeSBOMIntegration
  - HTTP_CODES_TO_SOFT_RETRY: [500, 501, 502, 503, 504, 429]
  - HTTP_CODES_TO_SKIP_RETRY: [404, 403]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions

Release version	Release Notes
Veracode v4.3 Veracode v4.2 Veracode v4.1	Application Vulnerability Response release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

User group and roles

The Veracode Vulnerability Integration is installed by a system administrator [admin] and configured by a member of the App-Sec Manager group. See Application Vulnerability Response user groups and roles for more information.

Veracode Vulnerability Integration

To view the Veracode vulnerability integrations, navigate to **All** > **Veracode Vulnerability Integration** > **Integrations**.

The following integrations are included in the base system.

Veracode Vulnerability Integration

Integration	Description
Veracode Application List Integration (JSON)	This integration is inactive by default. Retrieves Veracode application scanner data (vulnerabilities, metadata) and enriches your application data. Retrieves scan records from Veracode via a JSON-based API.
Veracode Application List Integration (XML)	This integration is inactive by default. The XML-based version of this integration has been deactivated (deprecated). Retrieves Veracode application scanner data (vulnerabilities, metadata) and enriches your application data. This integration is set to run daily at 00:00:00. **Note:** A JSON-based API from Veracode is used to retrieve the list of applications. This API imports the 'last policy compliance check date' for these applications, signifying when these applications were last scanned by Veracode.
Veracode Scan Report Integration	This integration uses the reporting API to import scan information. It solves the existing problem of Veracode Scan Summary Integration failing intermittently and backdating integration taking longer than expected to complete. The existing Veracode Scan Summary Integration is deprecated.
Veracode Scan Summary	This integration is inactive by default. Retrieves scan records from Veracode via a JSON-based API. This integration replaces the XML-based API integration. It is chained and follows the Veracode Application List Integration when activated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Veracode Vulnerability Integration (continued)

Integration	Description
Integration (JSON)	
Veracode Scan Summary (XML)	This integration is inactive by default. The XML-based version of this integration has been deactivated (deprecated). Retrieves scan records from Veracode. This integration is chained and follows the Veracode Application List Integration when activated. **Note:** Automatically follows the Veracode Application List integration when it is activated. With the 'Last policy compliance check date' for the applications from Veracode, this integration retrieves data only for the applications that were scanned after the 'delta_start_time' of this integration.
Veracode Application Vulnerable Item JSON Integration	Starting with v4.2, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item integrations. This integration is inactive by default. Retrieves scan results with more vulnerability data than the XML-based integration from Veracode. It inserts AVIs and enriches your third-party vulnerability data.
Veracode Application Vulnerable Item Integration (XML)	Starting with v4.2, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item integrations. This integration is inactive by default. Retrieves scan results from Veracode, inserts Application Vulnerable Items (AVITs) and enriches your third-party vulnerability data. By default, if the scanner record is in the **Closed** state, AVITs are not created. Existing AVITs are still updated. This integration is chained and follows the Veracode Scan Summary integration when activated. The XML-based API is deprecated for the Veracode Scan Summary JSON integration. **Note:** Automatically follows the Veracode Scan Summary integration. With the 'Last policy compliance check date' for the applications from Veracode, this integration retrieves data only for the applications that were scanned after the 'delta_start_time' of this integration.
Veracode Categories Integration	This integration is inactive by default. Retrieves enhanced Categories data from Veracode.
Veracode CWE Integration	This integration is activated by default. Retrieves Veracode - specific Common Weakness Enumeration (CWE) data for threat information and remediation recommendations. These data are populated and updated on Application Vulnerability Entry records. This CWE integration operates independently from the scheduled job for the CWE Comprehensive 2000 Integration you activate for the Vulnerability Response application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Veracode Vulnerability Integration (continued)

Integration	Description
	Your data is not duplicated if you have the Veracode CWE Integration and the CWE Comprehensive 2000 Integration activated.
Beginning with v4.1:Veracode Link projects Integration	This integration is activated by default. Retrieves all associated projects for each application from Veracode. Applications can have multiple projects in the Veracode application. Imported data from this integration is displayed on the following records: • **Last SCA Scan Date**, **App Creation Date**, and **App Update Date** are listed on records in **Discovered Applications**. • On Application Vulnerability Scan Summary records and application vulnerable items (AVITs), the **Source SDLC status** (Software Development Life Cycle) is displayed. • **Source exploitability** is displayed on application vulnerable item (AVI) records.
Veracode Software Bill of Materials (SBOM) Integration	Version 4.3 of the Veracode Vulnerability Integration includes the following enhancements with Veracode SBOM files: • If you have installed SBOM Response, you have the option to include vulnerabilities found by Veracode for the SBOM files you upload. • Veracode is mapped to the **Source** field for records in the Bill of Materials [sn_sbom_doc] table for the Veracode SBOM files. This integration is activated by default. Beginning with v4.2, imports Software Bill of Materials files in CycloneDX and SPDX formats generated by Veracode and queues them for parsing in your instance. You must have the Software Bill of Materials applications installed to import this data and view it.
Veracode DevOps Integration	This integration is inactive by default. The integration is viewable on the Application Vulnerability Integrations list in Application Vulnerability Response. If you have a DevOps Change Velocity license, this feature is structured so that DevOps users do not need a SecOps license to view summary details for third-party vulnerability scans. There is no impact or change to Application Vulnerability Response.

For integration run statuses see, View the Veracode Application Vulnerability Integration import run status.

To view data in third-party vulnerabilities, see View vulnerability libraries.

Preparing for the Veracode Vulnerability Integration

A successful Veracode Vulnerability Integration requires planning and the execution of pre-integration tasks. Prepare for the integration by performing these tasks. The Veracode Vulnerability Integration assumes that you are familiar with the Veracode product and API.

Before you begin

The Common Weakness Enumeration (CWE) integration is also used by Application Vulnerability Response and should be running prior to installing and configuring the Veracode Vulnerability Integration. It is installed with Vulnerability Response, by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: NIST Vulnerability Database (NVD) data is not necessary to install the Veracode Application Vulnerability Integration, however they provide enrichment and would be useful to have. For information on NVD, see Importing data with the NVD and CWE integrations and managing third-party libraries.

There is a configured run-as user for each integration record. The default value for this user is **VR.System**. Do not change this value.

Role required: App-Sec Manager group

About this task

Note: Before running the integration, make any necessary configuration changes based on your requirements.

Validate your instance sizing based on the number of application vulnerable items you expect to import. An undersized instance can lead to long load times. If you do not know the size of your instance, contact Customer Service and Support.

The Veracode Vulnerability Integration requires an API id and API key.

Procedure

To create the API ID and key credentials:

a. Log in to the Veracode Platform.

b. Go to the user account menu and select **API Credentials**.

c. Click **Generate API Credentials**.

d. Record your credentials for later use.

Install the ServiceNow® Vulnerability Response Integration with Veracode

Before you run the integration on your instance, the installation and configuration steps must be completed so the Veracode product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns users to the App-Sec Manager group. For information on Group roles see, Application Vulnerability Response user groups and roles. • The App-Sec Manager group oversees configuration and verifies expected results.

Role required: admin

Procedure

1. Log in to the instance you want to install the Veracode Vulnerability Integration on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with Veracode application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

   Note: Consider reading the **Other Requirements** and **Dependencies** sections, as applicable.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Enter the **Instance Name** and **Reason for the Instance**, and click **Validate Instance**.
8. Click **Request**.
   You will receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.
    Your application is automatically installed on your instance.

What to do next

Configure the Veracode Vulnerability Integration for your environment. See Configure the Veracode Vulnerability Integration.

Configure the Veracode Vulnerability Integration

Before you run the integration on your instance, the installation and configuration steps must be completed so the Veracode product properly integrates with Application Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the Vulnerability Response application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.
Verify that the Vulnerability Response Integration with Veracode application is installed and activated.	To verify that this application is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install the ServiceNow Vulnerability Response Integration with Veracode.
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the app and assigns users to the App-Sec Manager user group. • The App-Sec Manager oversees configuration and verifies expected results.
For the Veracode Application Vulnerability integration, have your **API id** and **API key** ready.	Contact Veracode to obtain the**API id** and **API key**. See Preparing for the Veracode Vulnerability Integration. Starting with version 4.0, if you are using the Veracode Vulnerability Integration, the penetration assessment tests in the Veracode Vulnerability Integration are manual findings from Veracode. These findings are not linked to any penetration test assessment requests you configure in Application Vulnerability Response. For more information about penetration test requests in Application Vulnerability Response, see Configure penetration testing.

Role required: App-Sec Manager user group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Veracode Vulnerability Integration** > **Configuration**.
2. Fill in the **API ID** and **API Key** fields.
3. Choose your testing results.

Option	Description
Version 4.0:	**a.** Select **DAST** or **SAST** data types to include in the import. **Note:** You can choose one or the other, or both, but you must select at least one. **b.** Select **SCA** to import Software Composition Analysis (SCA) vulnerabilities. **c.** Select **Include Manual** to import manual penetration testing results from Veracode. AVITs are created for these results.
Version 3.0	Select **DAST** or **SAST** data types to include in the import. **Note:** You can choose one or the oth er, or both, but you must select at least one.
Version 1.0:	Dynamic Application Security testing results are selected, by default.
Update SCA findings from	'Default' is the set value until you change it. You must select the Include SCA findings check box and choose one from the list: ○ Agent – the agent scan results make the fi nal updates to SCA findings ○ Upload – the upload scan results make the final updates to SCA findings ○ Default – the last scan processed, either the agent or upload scan, makes the final updates to SCA findings **Note:** If you do not select the Include SCA findings check box on the configu ration page, the scan you selected from the list is not used, and the last scan that is processed makes the final up dates.

4. Add the Veracode **Severity** level to filter your imported data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This value is imported from Veracode. You can add multiple values to the field. If populated, the import only gathers data that matches the Severity levels you've added.

5. Save and validate your choices.

Option	Description
Version 3.0:	Click **Save and Test Credentials**. **Note:** Configuration is successfully completed unless an error message is displayed. If an error message is dis played during the configuration, reenter your data.
Version 1.0:	Click **Save**. Verify successful configuration by clicking **Test Credentials**. **Note:** Configuration is successfully completed unless an error message is displayed. If an error message is dis played during the configuration, reenter your data.

6. Select how you want to manage exceptions and false positives for AVITs upon import. Options to manage AVITs upon import with the ServiceNow Exception management and False positive workflows are activated by default. The workflows are triggered based on how the **Source** states on the AVITs are mapped in your instance. For an example use case, see Managing state mapping for deferrals and false positives in Application Vulnerability Response.

Activated	**Manage exceptions in ServiceNow** Leave this option activated if you want to triage imported AVITs marked for the **Deferred** state. AVITs with **Source** states that normally are mapped to a **De ferred** state in your instance are instead mapped to **Open**. You **Request an exception** from the AVI record. **Manage false positives in ServiceNow** Leave this option activated if you want to triage imported AVITs with **Source** states marked as **False Positive** or **Potential False Positive**. AVITs with these **Source** states that normally are mapped to a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	Closed state in your instance are mapped to **Open**. You request a **False positive** from the AVIT record.
Deactivated	Deactivate one or both check boxes if you want to preserve the **Source** states imported from your scanner. These AVITs are mapped to the **Target** and **Target reason** states as they are imported but are not triaged by the exception and false positive workflows. The **Request exception** and **False Positive** actions are not visible on AVITs.

7. Starting with v4.3, choose or verify settings for the following parameters.

Parameter	Description
API region	Select a region from the list.
API timeout	The default is 30K. You might prefer to leave this field in its default setting.
Include SBOM vulnerabilities	Select to include any vulnerabilities that are ingested by the Veracode integrations in the Veracode SBOM files you upload. Leave the field cleared so Veracode vulner abilities are not parsed on Veracode SBOM files.

8. Select **Save and Test Credentials**.

What to do next

If your environment requires domain-separated imports, see Create domain-separated imports for an integration.

On initial installation, refer to Configure Application Vulnerability Response for further instructions.

After initial installation, for modifications refer to Veracode Vulnerability Integration modifications and activities.

View the Veracode Application Vulnerability Integration import run status

Use the **Vulnerability Integration Runs** related list to verify the success of your integration runs, locate any issues, and inform your remediation decisions.

Before you begin

To view the Veracode Vulnerability Integration import run status:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Application Vulnerability Response and the Veracode Vulnerability Integration must be installed and configured.
- The Veracode Vulnerability Integration imports must be scheduled and running.

Role required: App-Sec Manager group

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Application Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.
- *sn_vul_veracode.app_mark_unseen_apps_inactive*: When this property is set to `true` (activated), the successful import of the Application List Integration marks any unseen applications in the Platform as inactive (active flag `false`).

Procedure

1. Navigate to **All** > **Veracode Vulnerability Integration** > **Integrations**.
2. Select an integration.
3. Click the **Vulnerability Integration Runs** related list.
4. Verify that all imports have succeeded.

   Trouble?

   The most common causes for a failed run include:

   - Network interruption.
   - An issue in the data transfer resulting in corrupted data during the transform.

   If you encounter any of these conditions, click **Execute Now**, and rerun the integration.
5. Starting with v4.2, view details such as total processing times, average times for pre- and post-integration run processes, and reports on the integration run records for the Application Vulnerable Item Integrations.
   For more information about viewing additional details imported by Veracode, see Get more details in Veracode Vulnerability Integration.

View Veracode scan summaries

View details for scan summary information for the Veracode Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: App-Sec Manager group

Procedure

1. Navigate to the Application Vulnerability Scan Summaries [sn_vul_app_vul_scan_summary_list] table.
2. Select a record for a Veracode scan.
3. Starting with v19.0 of Vulnerability Response and v4.0 of the Veracode Vulnerability Integration, use the personalize list icon (gear icon) to display the following columns.
   - Static scan size
   - Third party library count
   - Third party vulnerable library count
   - Third party flaw count by severity
   - Third party library issue count
   - Third party license issue count
   - Mixed Flaw count
   - Mitigated Flaw count
   - Unmitigated Flaw count
   - Static flaw count by severity
   - New flaw count by severity
   - unmitigated flaw count by severity
   - Total flaw count by severity
   - Last SCA scan rating
   - Last SCA scan date
   - Scan published date
   - Tags

Data transformation for the Veracode Vulnerability Integration

After you identify the data that you want to import, the data is retrieved from the Veracode application, processed through a set of data sources, and transformed in your instance.

Veracode Application Vulnerable Item Integration

The data from the API is first loaded into the Veracode AppVul Item Import [sn_vul_veracode_appvul_item_import] table, and the Veracode AppVul Item Transform is used to transform the imported information.

To access this transform map, navigate to *System Import Sets > Transform Maps* and search for Veracode AppVul Item Transform. The following table lists the transform map fields by integration.

Veracode AppVul Item transform map fields

Source field	Target field	Description
app_id	source_app_id	Application ID.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Veracode AppVul Item transform map fields (continued)

Source field	Target field	Description
issueid	source_avit_id	AVIT ID.
app_name	app_name	Application name.
version	app_version	Application version.
build_id	source_scan_id	Build ID of the application.
account_id	account_id	Account ID.
sandbox_id	sandbox_id	Sandbox ID.
last_update_time	last_scan_date	Last updated time.
app_name + last_scan_date	scan_summary_name	Scan summary.
life_cycle_stage	source_sdlc_status	Source SDLC status.
level	source_severity	Source severity.
category_name	category	Category.
source_severity	source_severity	Source severity.
category_id + " CWE-" + cweId	source_entry_id	Source entry ID.
source_vulnerability_summary	source_vulnerability_summary	Source vulnerability summary.
source_recommendation	source_recommendation	Source recommendation.
description	description	Description from the source.
description	source_vulnerability_explanation	Source vulnerability explanation.
mitigation_status_desc	source_mitigation_status	Source mitigation status.
remediation_status	source_remediation_status	Source remediation status.
line	line_number	Line on which the flaw is found.
module	application_module	Application module.
sourcefile	source_notes	Source notes.
affects_policy_compliance	complies_with_policy	Values can be Yes or No based on the source information being true or false.
Sourcefilepath + sourcefile	location	Location mapping in case of a *`static`* flaw.
url	location	Location mapping in case of a *`dynamic`* flaw.
scope, type, exploitLevel	source_additional_info	Name value field populated with the values from source in case of static flaws.

The following transform scripts are run during the transformation process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Veracode transform map script timing and purpose

When the script is run	Purpose
onComplete (when an import set has completed transformation)	Script that is used to process the data source and update the count of AVITs created, updated or unchanged, and the ones imported as part of this integration from Veracode. This script is for internal use and should not be modified or deleted.

Veracode Vulnerability Integration modifications and activities

Configure optional modifications specifically for the Veracode Vulnerability Integration.

Viewing additional data imported by the Veracode Vulnerability Integration

Note: Changing other Veracode Vulnerability Integration settings, other than the ones listed here, requires advanced ServiceNow and Application Vulnerability Response expertise and is beyond the scope of the product documentation.

Get more details from Veracode

Starting with v4.2, select **Get More Details** on application vulnerable items (AVITs) that have Veracode as the Source on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table or from the list views in the Vulnerability Response Workspaces to view the following Veracode data.

- HTTP Source request and Source response details for Dynamic Application Security Testing (DAST) scans are displayed on the HTTP Request/Response related list.
- Solution recommendations from Veracode are displayed on the Findings related list.
- HTTP Source request, Source response, and recommendations are displayed on the Details tab In the Vulnerability Response Vulnerability Response workspaces.
- The Description column is supported on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table.

Modify Veracode integration instance parameters

After initial installation, you can modify parameters for the Veracode integrations in the Veracode Integration instance.

Before you begin

Role required: App-Sec Manager group

About this task

You can modify the parameters for an integration from its instance to determine what type of data you ingest. For some of these settings, you can also modify these parameters from the integration's configuration page.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Integrations**.
2. Select **Veracode Application Vulnerability** in the Source Instance column for the Veracode integration that you want to modify.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the **Integration Instance Parameters** tab and double-click a field in the Value column to modify the values.

   Starting with v19.0 of Vulnerability Response and v4.0 of the Veracode Vulnerability Integration, you can configure the following parameters for the Veracode integrations.

   import manual

   Enter `true` to import manual penetration testing results from Veracode. You can also modify this value from the integration configuration page.

   The penetration assessment tests in the Veracode Vulnerability Integration are manual findings from Veracode. These findings are not linked to any penetration test assessment requests you configure in Application Vulnerability Response. For more information about penetration test requests in Application Vulnerability Response, see Configure penetration testing.

   import_sca

   Enter `true` to import Software Composition Analysis (SCA) vulnerabilities. You can also modify this value from the integration configuration page.

   status

   Enter `Open` or `Closed` to import findings for the states you want. If you leave this field empty, the integration import findings for both Open and Closed states.

   policy_sandbox

   Enter a `policy` or `sandbox` to import records that correspond to a policy or to a sandbox. These records might be related to how applications are tested in your environment.

   policy_rule_passed

   Enter `true` or `false` to import records that have passed a policy rule. These records might be related to how applications are tested in your environment.

4. Select **Update** to save your changes.

Perform a manual Veracode application vulnerability import

If your initial import failed, or you do not want to wait for the scheduled initial import, you can perform a full data import independent of the daily scheduled job.

Before you begin

Role required: App-Sec Manager group

Procedure

1. Navigate to **All** > **Veracode Vulnerability Integration** > **Integrations**.
2. Choose and integration, for example, the Veracode Application List Integration.
3. Click **Execute Now**.

   Note: Each of the Veracode application vulnerability integrations are intended to provide the most complete data retrieval. Running them out of order requires ServiceNow and Application Vulnerability Response expertise and could result in incomplete data.

   Once the import is complete, scheduled imports resume.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. For integration run statuses see, View the Veracode Application Vulnerability Integration import run status.
5. If you want to modify other integration parameters, you must navigate to the integration instance.

Set Veracode Vulnerability Integration import times

For your convenience, you can reset the start time for the Veracode Vulnerability Integration.

Before you begin

Role required: App-Sec Manager group

About this task

After the initial import, the Veracode vulnerability integrations do a full import each time they runs. See Perform a manual Veracode application vulnerability import for more information on performing imports.

Procedure

1. Navigate to **All** > **Veracode Vulnerability Integration** > **Integrations**.
2. Choose an integration.
3. Set the new **Start time**.
   Time is calculated as Hours in local time. The default time for the Veracode Application List Integration imports is 00:00:00. The other integrations are **On Demand** and chained to run after the Veracode Application List Integration. Changing the **Start time** for either of these requires advanced ServiceNow and Application Vulnerability Management expertise.
4. Click **Update**.
   The new time is used for the next scheduled import.

Include Closed Veracode application vulnerable items

By default, **Closed** application vulnerable items (AVIs) are not created during Veracode Vulnerable Item integration imports. If you want to create them, you must change a system property.

Before you begin

The Veracode Vulnerability Integration must be installed and running.

Role required: admin

Procedure

1. In the left navigation **Filter navigator** text box, type `sys_properties.list`.
2. In the **Name** search box for the list, enter `sn_vul.create_closed`.
3. Double-click on the **Value** field and set to **True**
4. Click the green check mark icon to save.
   Records in the **Closed** state in the next Veracode import are created as AVIs in Application Vulnerability Response.

Manual ingestion of vulnerabilities for Application Vulnerability Response

Security professionals and application testers can create and manage the application penetration test findings within the Penetration Testing Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Penetration testing forms are available in the Penetration Testing Workspace to document the vulnerabilities identified in the core business applications.

The security professionals and application testers can manually import findings from external sources and platforms using the provided templates in Excel or CSV format. All the vulnerability findings are made available in the Penetration Testing Workspace.

To access and download the template for uploading to Penetration testing workspace, navigate to **All** > **Manual AVIT Ingestion** > **Upload File UI**.

A new penetration test form is created for every file upload for the respective application. All the vulnerability findings within that upload are associated to the same penetration test form. The Application Name must match with the records in of the tables:

- Application Table
- Business Application Table
- Scanned Application Table

The Application Name is a mandatory field present in the template for identifying the vulnerabilities present within an application, associated to a penetration test form. Any record missing the Application Name will not be processed and skipped during vulnerability creation.

Note: Mandatory fields in the template are necessary for processing the penetration test findings. It is necessary to ensure all the fields in the template are intact to prevent any issues during the processing of penetration test findings.

Mandatory fields required as part of template for penetration test finding creation

Column Name	Mandatory	Description	Available Options/ Max characters in strings
Risk rating	Mandatory	Severity of the application vulnerable item	Critical High Medium Low None (Default)
Requested by	Mandatory	Requested by	151
CWE category	Mandatory(Fill only one column)	CWE ID	255
Vulnerability ID	Mandatory(Fill only one column)	Vulnerability ID	255
Application	Mandatory	Application Name	255
Purpose of application	Mandatory	Purpose of application	4000
Types of sensitive data	Mandatory	List types of sensitive data accessible from applications	40

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mandatory fields required as part of template for penetration test finding creation (continued)

Column Name	Mandatory	Description	Available Options/ Max characters in strings
List of compliance programs	Mandatory	List of compliance programs	4000
Technology stack details	Mandatory	Technology stack details	4000
Application team	Mandatory	Application team Name; group responsible for developing and maintaining software applications	100
URLs to test	Mandatory	URLs to test	4000
Steps to reproduce	Mandatory	Steps to reproduce	1000
Technical details	Mandatory	Technical details	1000
Assigned to	Mandatory	Assigned to (individual responsible for conducting penetration tests and generating security findings)	151
Assignment group	Mandatory	Assignment group (group responsible for conducting penetration tests and generating security findings)	151

Upload application vulnerabilities using a template file

Use a template file to upload the application vulnerabilities. To access and download the template, navigate to **All** > **Manual AVIT Ingestion** > **Upload File UI**.

Before you begin

Role required: Ethical Hacker **sn_vul.app_pen_tester**

Procedure

1. Navigate to **All** > **Manual AVIT Ingestion** > **Upload File UI**.
2. Select the Excel or CSV links and download the template in the respective format.
3. In the template, enter the vulnerability data in the records.
   For instructions on how to populate the data in the template, see the “examples” sheet in the template.
4. Select Import File and upload the updated template.
5. Select Submit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Vulnerability Integration Push Queues page is displayed. You can track the status and view log notes related to the submissions.

Note: For any errors that occurs:

- An **error log file** is attached directly to the related **Push Queue** record.
- Additional **error details** can also be found within the **Log Notes** section of the same Push Queue record.
- This approach ensures that Ethical Hackers can easily monitor and troubleshoot their submissions without needing access to deeper system-level integration details.

Verify integration run

If the integration run is successful, review the count of individual detections and the penetration test findings created or updated.

Before you begin

Role required: Admin

Procedure

1. Navigate to **All** > **Manual AVIT Ingestion** > **Integrations**.
2. Select the name of the integration based on the file type uploaded.
3. Select the Vulnerability Integration Runs tab.
4. Select the integration run number.
5. Select the Items tab.
   Review the information in the Items tab.

Result

Items tab

Tab/Field	Description
Items tab	Displays the total number of AVITs that are imported.
New items	Displays the number of Application vulnerable items that are created from this integration run.
Imported items	Displays the sum of all the fields in this section.
Duplicate items	Displays duplicate items. This field is not populated anymore.
Unchanged items	Displays Application vulnerable items found during the integration run that exist in the database but were not updated, because none of the relevant field values had changed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: After confirming the successful integration run, track the submission status by navigating to the **Push Queue** record. The Push Queue record provides the following details:

- **Log Notes**: Consists of record processing information.
- **Error Files**: Consists of error details occurred during the push.

Verify upload status

Verify whether the vulnerability integration run was successful, partially successful, or a failure.

Before you begin

Role required: sn_vul.app_pen_tester

Procedure

1. **Access Upload History**: Navigate to **All** > **Manual AVIT Ingestion** > **Upload File History**.
2. **Review Upload status**: In the **Application Vulnerability Integration Push Queues** table, examine the Created column for the upload timestamp and the State column for the upload status.
3. **Optional: Verify Success**: In the Notes field, view the success massage to ensure all the records were processed successfully.
4. **Error Handling (Failed/Partial Success)**
   - For uploads with a "Failed" or "Partial Success" state, an error log file is generated.
   - Admin users can view this file to understand the reasons for upload failure.
   - Users with the app_pen_tester role can view the Push Queue records and their associated error details.
   - The error log file contains only the findings that failed processing, providing specific information for correction and re-ingestion.
5. **Re-ingestion Guidelines**:
   - Re-ingesting successfully processed findings will create duplicate records.
   - To avoid duplicates, only re-ingest findings listed in the error log file.

Tenable Web Application Scanning Vulnerability Response Integration

Import applications, findings and associated application vulnerabilities from the Tenable Web application and manage them in ServiceNow Vulnerability Response.

The Tenable Web Application Scanning (Tenable.was) integration enables ServiceNow® Vulnerability Response (VR) customers to automatically import **web applications** and **application vulnerabilities** discovered through Tenable's Dynamic Application Security Testing (DAST). This integration provides continuous visibility into web application exposure by synchronizing application metadata, vulnerability findings, and scan details from Tenable.was into dedicated ServiceNow tables.

The integration uses Tenable's export APIs to retrieve applications and findings in chunks, ensuring scalable data ingestion even in environments with large scan volumes. Imported data is transformed into Application Vulnerable Items (AVITs), Application Vulnerability Entries, and Scan Summaries using AVR processing frameworks and CI lookup rules.

You can control whether each integration uses CI Lookup or Product Model independently, instead of using one global setting for all integrations. The "Lookup strategy" field is added to each integration's configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This enables security teams to:

- Maintain a unified view of application security posture.
- Correlate Tenable WAS findings with CMDB applications.
- Prioritize remediation based on severity, CVSS, and risk indicators.
- Track dynamic scan data for each application.

Configure Tenable Web Application Scanning Vulnerability Response Integration using Setup Assistant

Establish authenticated communication between ServiceNow and Tenable.was using API keys so the platform can retrieve application and vulnerability data.

About this task

A configured Tenable.was Integration Instance in Setup Assistant.

API Access Key and Secret Key generated from Tenable.

Procedure

1. Navigate to **Setup Assistant** > **Scanner Integrations** > **Tenable.was**.
2. Fill in the following details: **Account Name**, **Instance URL**, **Access Key**, **Secret Token**.
3. Save the **Configuration**.
4. System validates the credentials by sending a GET /session request to Tenable.was.
5. On successful authentication, the returned session object confirms connectivity and permissions.

Import Applications Data from Tenable Web Application Scanning Vulnerability Response Integration

Import application assets from Tenable WAS Vulnerability Response Integration using the Assets Export APIs and create import queue entries for transformation.

Procedure

1. Navigate to **All** > **Tenable WAS Vulnerability Integration** > **Administration** > **Integrations**.
2. Select an integration.
   For example, Tenable.was Application List Integration.
3. Select Execute Now to start the import.
   After the import completes, view the imported applications in the Discovered Applications [sn_vul_app_release] table. The "Lookup strategy" field to each integration's configuration. You can choose between using the system-wide setting or forcing a specific lookup method per integration.
   - **Field Details:**
   - Table: Third Party Integration (sn_sec_int_integration)
   - New Field: Lookup strategy (lookup_strategy)
   - **Values:**
     - default - Use system-wide setting (backward compatible)
     - cmdb_ci - Always use CI Lookup/Scanned Application
     - cmdb_model - Always use Product Model

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Impact: existing integrations maintain their current behavior until you choose to configure them differently.

4. See the status of your integration runs.
5. For more information, see Understanding Tenable Vulnerability Response Integration.

Import Vulnerabilities Data from Tenable Web Application Scanning Vulnerability Response Integration

Import vulnerability findings and associated metadata using Tenable WAS Export Findings APIs.

Procedure

1. Navigate to **All** > **Tenable WAS Vulnerability Integration** > **Administration** > **Integrations**.
2. Select an integration.
   For example, Tenable.was Vulnerabilities Integration.
3. Select **Execute Now** to start the import of vulnerability findings.
   After the import completes, view the vulnerability data in the Application Vulnerability Entries, Scan Summaries, and Application Vulnerable Items (AVITs) tables.
4. View the status of your integration runs to verify if all finding chunks were processed successfully.
   For more information, see Understanding the Tenable WAS Vulnerability Response Integration.

Remediating Application Vulnerability Response vulnerabilities

Monitoring remediation is a process that begins with reviewing status and ends with closing application vulnerable items (AVITs). Application Vulnerability Response offers tools and procedures to make that process more productive and efficient.

Application Vulnerability Response remediation process

Application vulnerable item remediation is done manually.

An overview of the process:

- Log in to your Application Vulnerability Response instance.
- Validate that your rules (CI Lookup, Assignment) for application vulnerable items are working as expected. For information on revising CI Lookup Rules, see Identify applications in Application Vulnerability Response automatically. For information on Assignment rules, see Assign application vulnerable items in Application Vulnerability Response automatically.
- Validate that your remediation targets are correct. See Automate remediation target tracking in Application Vulnerability Response for information on how remediation target rules work and how to revise them. View the remediation target status of an application vulnerable item.

  Note: Remediation target rules belong to AVITs. These rules are run when the AVIT is imported.

- Review the dashboards or reports. For example, view dashboards that show AVITs aging by states.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

When the Performance Analytics for Vulnerability Response application (com.snc.vulnerability.analytics) is activated, users with certain roles can view data of interest to the members of the App-Sec Manager and Security Champion groups.

For App-Sec Managers, Performance Analytics for Vulnerability Response contains the Application Vulnerability Response Overview, which can help you monitor areas of concern. See Analytics and Reporting Solutions for Application Vulnerability Response and Application Vulnerability Management [PA] dashboard.

Starting with version 13.0 of the Vulnerability Response application: For Security Champions, Performance Analytics for Vulnerability Response contains the My Application Vulnerabilities dashboard, which can help you monitor your areas of concern. See My Application Vulnerabilities dashboard.

Starting with version 13.0 of the Vulnerability Response application: To limit the amount of data gathered for reports or related lists, see Define service classifications for Vulnerability Response reporting and related lists.

- Review the state of AVITs, in order of priority, searching for what has changed.
- Revise the risk for the AVITs, as needed. See Create an application vulnerability calculator for more information.
- Reassign the AVIT to an assignment group for remediation, if needed.
- Rescans are triggered automatically by the third-party import schedule.
- After rescan, if the state is **Fixed**, AVITs are automatically closed during import.
- After the scan, if the state is not **Fixed**, the AVIT is reopened.

Get more details from Veracode

Select **Get More Details** on application vulnerable items (AVITs) that have Veracode as the Source on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table or from the list views in the Vulnerability Response Workspaces to view the following Veracode data.

- HTTP Source request and Source response details for Dynamic Application Security Testing (DAST) scans are displayed on the HTTP Request/Response related list.
- Solution recommendations from Veracode are displayed on the Findings related list.
- HTTP Source request, Source response, and recommendations are displayed on the Details tab In the Vulnerability Response Vulnerability Response workspaces.
- The Description column is supported on the Application Vulnerable Item [sn_vul_app_vulnerable_item] table.

View vulnerability libraries

You can view vulnerability data imported from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), or third-parties to decide whether to escalate a vulnerability group.

Before you begin
Role required: App-Sec Manager group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

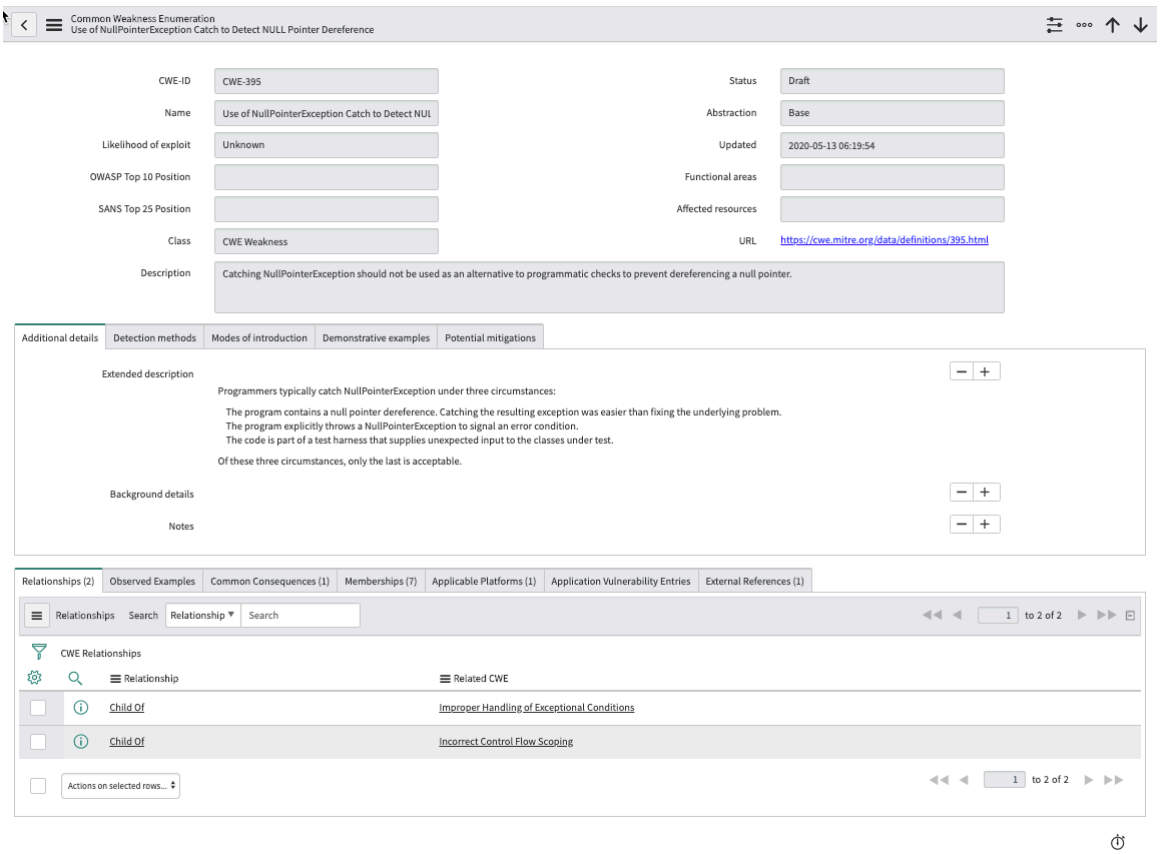
Procedure

1. Navigate to **All** > **Application Vulnerability Response** > for **Libraries**.

   The following libraries are available:

Libraries	Description
NVD	List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics including exploits.
CWE	List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. You cannot escalate a vulnerability from the Common Weakness Enumerations screen, it is for reference only.
Third-party	List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, CWEs, and CVEs.

2. Choose a library to view vulnerabilities.



For information on specific fields, see Application Vulnerability fields.

Application Vulnerability fields

Vulnerabilities are created automatically when records are downloaded from the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) or third-party integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

NVD and CWE are stored under **Libraries** in Vulnerability Response or under **Vulnerabilities** in Application Vulnerability Response.

CWE vulnerability entry fields

The fields in this table are read-only.

Field	Description
CWE-ID	Identifier for this vulnerability entry. This identifier is used for both Categories and Weaknesses, and is unique between the two datasets.
Name	Descriptive name assigned to this CWE-ID.
Likelihood of exploit	How likely the weakness is to be exploited, on a qualitative scale. One of: • Low • Medium • High
OWASP Top 10 Position	This vulnerability's numerical position in the OWASP top 10 list.
SANS To 25 Position	This vulnerability's numerical position in the SAN top 25 list.
Class	Type of weakness
Status	One of: • Incomplete • Draft • Stable • Deprecated • Obsolete • Unstable
Abstraction	One of: • Variant • Class • Base • Compound
Updated	Last time the record was updated in the instance.
Functional areas	List of functional areas affected. For example, **File Processing**. Only populated for 24/862 weaknesses.
Affected Resources	List of affected resources. For example, **File** or **Directory**. Only populated for 51/863 weaknesses.
URL	Knowledge base article associated with this vulnerability.
Description	Description of the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Integration run	The integration run this CWE was imported in.
Sections	
Additional details	Software concept descriptions that further explain the weakness. Includes: • Extended description • Background details • Notes
Detection methods	Details on how you might detect this weakness in an application.
Modes of introduction	The phases in which the weakness is introduced, for example, **Implementation**, **Architecture and Design**, and so on.
Demonstrative examples	Code examples of the weakness with accompanying descriptions.
Potential mitigations	Details on how to prevent the weakness, including which phase of the application life cycle it occurs in, and the effectiveness of the mitigation.
Related Lists	
Relationships	CWEs associated to this vulnerability. Lists relationships between this CWE and others. Can include parent/child, follows/precedes, requiredby/requires (for composite weaknesses), CanAlsoBe, PeerOf, MemberOf .
Observed Examples	Some CVEs that are representative of this weakness.
Common Consequences	Consequences of a successful exploit, in terms of scope and impact. For example: Scope: Confidentiality Impact: Read Application Data
Memberships	CWE memberships with this vulnerability.
Applicable Platforms	Platforms associated with this vulnerability.
Application Vulnerability Entries	Other application vulnerability entries associated with one.
External References	Information about the vulnerability from external sources.

Application vulnerability entry fields

The fields in this table are read-only.

Field	Description
ID	Identifier for this vulnerability entry.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source	Origin of the vulnerability — whether a scanner or physical test.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Map the severity of an application vulnerable item automatically.
Version 13.0: Primary CWE Version 12.1: CWE entry	Reference to the Common Weakness Enumeration element that this vulnerability best fits into. If there is more than one CWE associated to the vulnerability, the primary CWE is determined as follows: • Is the CWE mapped to the OWASP Top 10. If so, use this CWE. If not, continue. • Is the CWE mapped to the SANs Top 25? If so, use this CWE. If not, continue. • Does the CWE have the highest severity? If so use this CWE. If not, continue. • Select the latest of all the CWEs. The latest CWE is the one with the latest **Updated** field value in the CWE record.
Category name	Classification provided by the third-party integration. Aids in assignment.
Vulnerability Details	
Threat	Description of the threat from this vulnerability.
Mitigation description	Description of the steps that could be taken to mitigate the vulnerability.
Related List	
Version 13.0: CWEs	List of the CWEs associated with this vulnerability. Non-applicable for the Veracode Vulnerability Integration.

NVD entry fields

The imported fields in this table are read-only.

Note:

NVD data is not used in Application Vulnerability Response and entries represent Vulnerability Response data only.

CWEs, which are used in Application Vulnerability Response, can point to NVD entries, as examples of a weakness, and are provided here for informational purposes only.

Field	Description
ID	Identifier for this vulnerability entry.
Risk rating	(Hidden when no Vulnerability Response vulnerable items (VIs) are associated with the vulnerability)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Quantified **Risk Score** separating VIs into Critical, High, Medium, Low, and None.
Risk score	(Hidden when no VIs are associated with the vulnerability) Calculated amount of risk the vulnerable item poses to your environment.
Severity	Normalized degree of severity of this vulnerability in Vulnerability Response. Severity maps are provided for NVD and with ServiceNow third-party integrations. Application Vulnerability Response **Severity** is derived from imported **Source severity** and not NVD. For information on Application Vulnerability Response severity mapping, see Map the severity of an application vulnerable item automatically.
Exploit exists	Yes, if at least one exploit is associated with this vulnerability.
Exploit skill level	Lowest skill level required to exploit this vulnerability.
Exploit attack vector	Most vulnerable attack vector of the exploits for this vulnerability.
Active VIs	(Hidden when no VIs are associated with the vulnerability) Number of vulnerable items associated with this vulnerability, not in the Closed state. If there are no active AVIs for this vulnerability, **Risk Rating** and **Risk Score** are not displayed.
CWE entry	Reference to the Common Weakness Enumeration element that this vulnerability best fits into according to the NVD.
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Summary	Description of the vulnerability.
Vulnerability Details	
CVSS v2	Imported CVSS v2 data
CVSS v3	Imported CVSS v3 data, not available prior to 2015.
Preferred solution	(Hidden when no VIs are associated with the vulnerability) Solution of the highest-supersedence in the chain, derived from the solutions referenced in the vulnerability. If more than one highest-supersedence exists in the chain, no value is set. Any value set manually can be overwritten on subsequent imports. Setting this value manually should be done on the vulnerable item.
Remediation Status (Hidden when no VIs are associated with the vulnerability)	
Excludes Deferred	
Vulnerable items	Number of active application vulnerable items with this vulnerability. This count excludes deferred vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Total VIs	Total number of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability. This count excludes deferred vulnerable items.
Includes Deferred	
Vulnerable items	Number of active vulnerable items with this vulnerability.
Total VIs	Total number of vulnerable items with this vulnerability.
%VIs remediated	Percent complete for remediation of vulnerable items with this vulnerability.
Related Links	
Prior to v13.0: Force software vulnerability import **Note:** Removed in v13.0	(Deprecated) Re-calculates product mapping with ITSM Software Asset Management based on information from NVD. Updates the Vulnerable Software library.
Update status	Displays date and time of the last update. Updates the following: • Vulnerability group state • Risk score and rating • Metrics such as Active VIs, Total VIs from the Remediation Status section
Related Lists	
Vulnerable Items	(Hidden when no VIs are associated with the vulnerability) Vulnerable items associated with this vulnerability.
Vulnerability References	Information about the vulnerability from external sources, cited by NVD.
Exploits	Exploits associated with this vulnerability.
Solutions	(Hidden when no VIs are associated with the vulnerability) All Vulnerability Solution Management integration solutions associated with this vulnerability.
Version 13.0: Weaknesses	Imported CWE Weakness data associated to a Common Vulnerabilities and Exposures (CVE).
Version 13.0: Vulnerable Software	(Hidden when no VIs are associated with the vulnerability)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Imported Common Platform Enumeration (CPE) data associated with the vulnerability.

Identify applications in Application Vulnerability Response automatically

When data is imported from a third-party integration, Application Vulnerability Response automatically uses application data to search for matches in the Configuration Management Database (CMDB). It does this using **CI Lookup Rules**. These rules identify applications for the application vulnerable item (AVI) record to aid in remediation.

As applications are imported, a lookup is performed on the Scanned Application [sn_vul_app_scanned _application] table using source_app_id and app_name to find matches to applications from prior imports. When an application ID match is found, its values are used in the **Application** and **App release** fields in the application vulnerable item record.

If a match is not found, or the application ID field is empty, the rules use the other application information to attempt to correctly identify the application. If a match is still not found, a placeholder scanned application record is created with only **Application name** and **Application ID** fields.

The **Source Application Id** and **Application Name** lookup rules are shipped with the Veracode Vulnerability Integration, by default.

Note: Default CI lookup rules for Application Vulnerability Response are available only for the Veracode Vulnerability Integration.

When attempting a match, the lookup rules are evaluated by lowest **Order** value first. They stop when a rule returns a single CI as a match.

Note: If a rule is created in such a way that it returns more than one CI, only the first match is used.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the **CI matching rule** field for Scanned Applications. Click the Update Personalized List gear icon at the top of the Scanned Application list view to add it to the view.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

CI lookup rules can be domain separated and are source-specific. If supported, each source could have multiple deployments. For example, the Veracode Vulnerability Integration, can have multiple deployments of the Veracode Vulnerability Integration. Each deployment has its own set of CI Lookup Rules.

Note: CI lookup rules are shared by all deployments of the vulnerability integration. If a rule is deleted or modified, the deletion or changes affect all deployments of the vulnerability integration.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined **CI Lookup Rules**. See Prevent duplicate or orphaned records after running Application Vulnerability Response CI lookup rules for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Configuration Management and the CMDB

Create a CI lookup rule

The **CI Lookup Rules** module contains rules that define what fields have matching data in the Configuration Management Database (CMDB). These rules are used to identify applications and application releases and add them to the application vulnerable item (AVI) record to aid in remediation.

Before you begin

Role required: App-Sec Manager group

About this task

Creating CI lookup rules requires advanced ServiceNow and Application Vulnerability Management expertise. Rather than modifying one of the existing lookup rules, consider copying it and modifying the copy. When you are satisfied that the new rule does what you want, deactivate the original.

Note: Rules, once removed, cannot be recovered. Rather than removing existing rules, deactivate them when creating new ones.

Procedure

1. Navigate to **All** > **Security Operations** > **CMDB** > **CI Lookup Rules**.
2. Click **New**.
3. On the form, fill in the fields.

CI lookup rule form

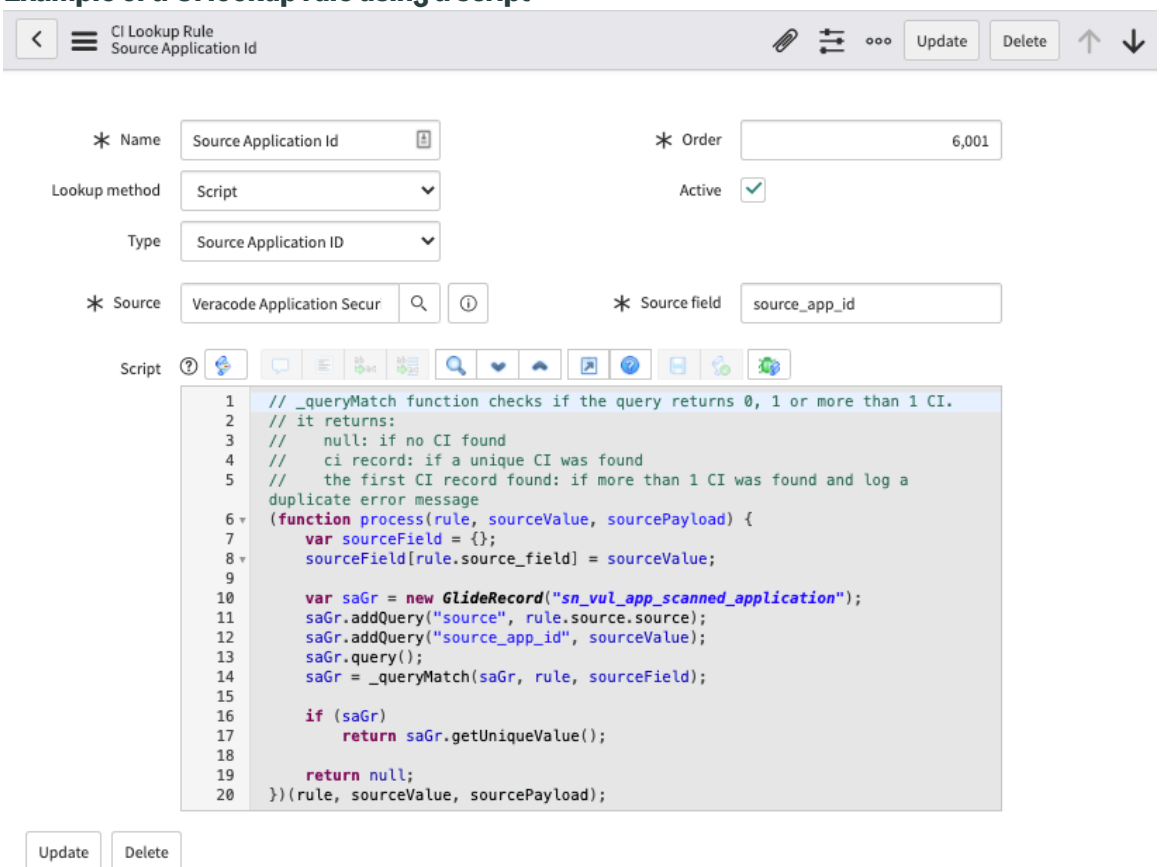
Field	Description
Name	Name of the rule.
Lookup method	Method used for matching. Choices are: ○ **Script**: Pre-built or custom script. ○ **Field matching**: Search on table or field in the CMDB.
Type	Type used with the Script **Lookup method**.
Order	Order of precedence for the rule. Matches with the lowest order are evaluated first.
Active	Check box for whether the rule is active or disabled.
Source	Source used as input to this rule. Once chosen, Condition filters appear.
Source field	Source field used as input to this rule. Fields must be a string or number.
Description	Text describing the rule.
V19.0: Lookup target	Lookup approach you want to follow. Select from: ○ Configuration item ○ Product model
Script	Editable sample script, based on the **Type**, is shown. Implement the custom script following the comments included in the template of the default function.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The process function has three parameters: *rule*, *sourceValue*, and *sourcePayload*
Search on CI table	Table to search within the CMDB. Used with field matching **Lookup Method**.
V19.0: Search on product table	If you choose the Product model **Lookup target**, the default value is Application Model.
Search on CI field	Field that contains information that can be used to locate a CI. Used with the field matching **Lookup method**. This field may be on the CI record, or on a related record, such as a network adapter.
V19.0: Search on product model field	If you choose the Product model **Lookup target**, the default value is Name.

4. Click **Submit**.

Example of a CI lookup rule using a script



Related topics

Application Vulnerable Item fields

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reapplying CI Lookup rules in Application Vulnerability Response

You can reapply your configuration item (CI) lookup rules to update existing CIs (scanned applications and product models) on discovered application records.

Reapplying a lookup rule

You can "Reapply Lookup Rules" for selected or filtered items in the discovered applications table.

If no filter is applied, the reapply option is disabled. After reapplying, users can receive a background job URL or an error message if the integration is running.

To reapply the rules to existing discovered applications, navigate to **All** > **Security Operations** > **CMDB** > **Lookup Rules**.

Note: Starting with v25.0.3 of Application Vulnerability Response, a new auto-close rule 'CI Decommissioned' is introduced to close the vulnerable items and detections related to decommissioned CIs.

Setting the lookup target

By default, the *sn_vul.use_product_model* system property is activated (set to **true**). Depending on how the system property is set on the CI lookup rule records, discovered application records are updated in the following manner:

- If the Value field is set to **true**, product model is the lookup target for CI Lookup rules and discovered applications are updated with the product models.
- If the Value field is set to **false**, Configuration item (scanned apps) is the lookup target and discovered applications are updated with the Configuration items (scanned applications).

To modify the *sn_vul.use_product_model* system property so configuration items are used as the target:

1. As a user with the sn_vul.app_sec_manager role, navigate to **All** > **System Properties** > **All**
2. Locate *sn_vul.use_product_model*.
3. Open the record.
4. Set the Type field to **false**.
5. Select **Update**.

If you reset this system property, you must modify your rules so the lookup targets match the system property setting. For example, if you reset the system property so you are using the configuration item as your target, locate the rules that have the Lookup target as Configuration item.

1. Select the Active check box for these rules and select **Update**.
2. Locate the rules that use Product model as the target and deactivate them by deselecting the Active check box and selecting **Update**.

If you are creating a new lookup rule, you set the Lookup target for the rule on the rule form. See Create a CI lookup rule for more information.

Prevent duplicate or orphaned records after running Application Vulnerability Response CI lookup rules

Take steps to prevent duplicate or orphan records resulting from matching (configuration items (CIs) within the CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Importing vulnerability data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. Thorough testing and debugging of processing scripts in the rules helps alleviate the potential of issues later in the process.

Preventing duplicate or orphaned records

- Use small subsets of data that are specific to the CI lookup rule being tested.
  - Set all **CI Lookup Rules**, other than the one being tested, to **Inactive**.
  - Analyze the imported applications and configuration items (CIs) to ensure that you are observing the expected behavior and matching is occurring properly.
- Review CI states such as **Retired**.
- Remove Test Data. Once you begin to observe the correct or expected behavior in CI matching, start over. This can be done by:
  - Deleting the data used for testing: (see the **Deleting data from tables** section)
    - Scanned applications
    - Application Vulnerable Items (AVIs)
  - Manually rerun the integrations.

.

Deleting data from tables

Sometimes you have imported data and realize something is wrong. If this happens in a development or performance environment, you could reclone from a better environment but, that isn't always an option.

Note: Performing these actions requires advanced ServiceNow expertise.

There are four options for deleting data from tables:

- Using **Delete All Records** on **Table Configuration**.
- Configure the **Table Cleaner** by navigating to **Auto Flushes** (sys_auto_flush.list) and creating a new **Auto-flush** record.
- Truncate the gs.truncateTable using a background script.

  Note: Never use *`truncateTable`* in a production environment. Consult your Support representative before executing large deletions in production or shared environments.

- Create a request in HI to have the data deleted.

Assign application vulnerable items in Application Vulnerability Response automatically

Automatically assign application vulnerabilities based on application tags, or any of the assignment groups in the Configuration Item [cmdb_ci] or platform assignment groups, to reduce the mean time to assignment.

Assigning application vulnerable items automatically

There are three different ways to assign AVIs using **Assign using**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The assignment recommendation feature in Vulnerability Response is not available for Application Vulnerability Response.

- User Group: This option allows you to select any of the existing ServiceNow AI Platform® user groups.
- User Group Field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default, you see the following three group fields in the list menu under **User group field**.
  - None: Indicates no default value for this mandatory field
  - Configuration Item: Approval Group
  - Configuration Item: Assignment Group
  - Configuration Item: Support Group
- Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow expertise.

Run high priority rules (items that need special handling, where risk is critical, or an AVI should be handled by regulatory compliance) first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign AVIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.

Assignment rule evaluation process

When a new AVI is created, imported, or reopened after being closed, the assignment rules are evaluated against it. An AVI is only evaluated once, unless it is reopened after being closed. You can manually reapply rules after changes.

The following process is used for each new, updated, or reopened AVI:

- For each vulnerability assignment rule, the AVI is compared to the assignment filter, lowest order rule first.
- Where the condition matches, the AVI is assigned an assignment group. The lookup stops.
- Where the conditions do not find a match among all the other rules, the AVI is assigned to the default assignment group, if a default rule exists.

Note: If there is no default rule, then the AVI remains unassigned.

Assignment type, whether **Manual** or **Rule** and **Assignment rule** is available from the Form Layout slushbucket on the application vulnerable item (AVI) form. Any AVI that was originally assigned by a rule but later manually reassigned contains a reference to the original rule. Use **Assignment rule** and **Assignment type** information to identify cases where the assignment rules did not find a correct match for the intended recipient. Or which rules had the most reassignments.

Note: The assignment rules do not reevaluate manually created assignments.

Reapplying assignment rules

When you change an assignment rule, use the **Apply Changes** button on the Assignment Rules list view to rerun all the changed rules on all active Open AVIs (except those that were manually assigned).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If the *Reapply all vulnerability assignment rules* scheduled job has not run before the first time you use **Apply Changes**, then it runs all the assignment rules on all Open AVIs except those AVIs that were manually assigned. After that, all subsequent uses of **Apply Changes** rerun only the changed rules and any dependent rules. Changes to one rule may result in an AVI matching a different unmodified rule.

The scheduled job [*Reapply all assignment rules*] is inactive, by default. When activated, it applies all the rules to all open AVIs except those manually assigned. It can run **Daily**, **Weekly**, **Monthly**, **Periodically**, **Once**, or **On Demand**. Depending on how many active AVIs you have in your environment, remember to set the **Run** field appropriately following the initial run to prevent performance impacts.

Create or edit Application Vulnerability Response assignment rules

You can create rules to automatically assign application vulnerable items (AVIs) based on filter conditions. These rules assign AVIs as they are imported or manually created.

Before you begin

Role required: App-Sec Manager group

About this task

With assignment rules, you define the condition of assignment and the order of execution. Once an AVI matches a rule condition, the assignment lookup stops. See Filtering within Application Vulnerability Management for more information.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Assignment Rules**.
2. Click **New**.
3. If **New**, fill in the fields on the form, as appropriate.

Application Vulnerability Assignment Rule

Field	Description
Name	Name of the group rule.
Active	Indicates whether the assignment rule is active.
Execution order	Order in which the rules are evaluated. High priority rules, items that need special handling, where risk is critical, or an AVI should be handled by regulatory compliance, to be run first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign AVIs to the group that will figure out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.
Description	Description of the assignment rule.
Condition	
Condition fields	Conditions that must be met.
New Criteria	Adds more condition filter fields to choose from.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Assign using	To automate the assignment of groups created based on this rule, choose one of the options available. ○ User group: Select a user group from the lookup table. ○ User group field: Select a user group field from the list menu. ○ Script: Create or edit a script. **Note:** Creating or edit a script requires ServiceNow expertise.

4. Click **Submit**.
   New or updated rules are evaluated on the next import.

Removing assignments from Application Vulnerability Response vulnerable items and remediation tasks

You can clear the **Assigned to** and **Assignment group** fields on Application Vulnerability Response vulnerable items directly from the application vulnerable item and remediation task records that you determine might be incorrectly assigned to you or your groups.

Overview for the workflow

If you determine that Application Vulnerability Response vulnerable items (AVITs) and remediation tasks (AVULs) aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups, you can remove yourself or your groups from the **Assigned to** and **Assignment group** fields on AVIT and AVUL records.

The unassign workflow is supported in the classic and workspace views for AVITs and AVULs.

You have the option to send requests to clear the assignment fields for approval. See Approve or reject an unassign request in Vulnerability Response for more information.

- The **Unassign** button is displayed on AVIT and AVUL records in any state other than the Closed or Resolved.
- After the request to clear the fields is approved, all the **Assigned to** and **Assignment group** fields on the AVITs that are associated with an AVUL that have the same assignment group are also unassigned. If any application vulnerable item has a different assignment group than its associated remediation task, it is not unassigned. In most cases these application vulnerable items have been manually assigned. See Removing assignments from vulnerable items and remediation tasks for more information.
- Any records that you update with either the UI action or manually are displayed on the Unassigned module for Application Vulnerability Response.
- You can clear the assignment fields for multiple AVITs on a list. After you select the AVITs and select **Bulk Edit**, on the dialog that is displayed, select the **Unassign** check box.

See Remove assignments from vulnerable items and remediation tasks for more information about the steps for how to clear the assignment fields.

System properties and approval notifications

If a remediation owner selects **Unassign** on a record, by default, the sn_vul.unassign_vr.approval_required system property triggers the approval flow and creates a state change approval record in the Review state, and the request is routed for approval. The request is displayed on the My Approvals list for users with the sn_vul_.unassign_approver.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: As a vulnerability administrator [sn_vul.vulnerability_admin], you can set the *sn_vul.unassign_vr.approval_required* system property to **false** to disable the approval process.

Additionally, you can change the value in the *sn_vul.default_assignment_group* system property so if the assignment fields are cleared, a specific group is assigned. For example, if a user clicks **Unassign** on a record and you want to redirect it to a specific group for review, you can add the system ID for the group of your choice in the value field of the system property.

Note: If you change this value, notifications for all the VITs, AVITs, and CVITs that are unassigned are sent to the group you specify.

See Removing assignments from vulnerable items and remediation tasks for more information about changing the system properties.

Calculate risk in Application Vulnerability Response automatically

Application vulnerability calculators automate calculating initial risk values for the fields on application vulnerable items (AVIs). Risk calculations offer insight into prioritizing remediation. The condition for each calculator is evaluated in order, and the first matching calculator is used.

Application Vulnerability Calculators

The Application Vulnerability Response base system includes two vulnerability calculators that set the base **Risk Score** on the application vulnerable item.

- **Basic Risk Calculator**
- **Advanced Risk Calculator**

Application vulnerability calculators can be built to prioritize and rate the impact of AVIs based on any criteria by using condition filters. Whether it's the business impact of the vulnerability, the class of the configuration item (CI), or the age of the AVI, you can create additional vulnerability calculators to set other fields on AVIs. Or you can customize the existing vulnerability calculators. A calculator can be written to reflect any set of priorities. See Filtering within Application Vulnerability Management for more information.

AVIs contain the **Risk Score** value derived from the risk calculators.

Note: An AVI displays **Source Severity** but not normalized severity. Normalized severity is used by the calculators to get the **Risk Score** value but isn't shown on AVIs.

Each calculator contains a list of calculator rules, with a condition determining when to apply it. When the calculator is run, the condition for each calculator rule is evaluated in order, and the first matching calculator rule is used.

All enabled vulnerability calculators set the selected fields each time that an AVI is created, when an associated CI or vulnerability changes.

The **Basic Risk** calculator calculates **Risk Score** for AVIs using the normalized vulnerability severity.

Note: Only one calculator per target field (**Risk Score**) can be active at a time.

The **Basic Risk** is enabled by default. The **Advanced Risk Calculator** is inactive by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application vulnerability calculator rules

The base system **Basic Risk Calculator** calculator contains calculator rules that assign each level of severity (None to Critical) a value (0-100) for **Risk Score** based on severity. **Unknown Severity** is automatically assigned a risk score of 100. These values can be adjusted and, like **Advanced Risk Calculator**, new calculator rules or new risk rules can be created.

Note: Starting with v23.0 of Application Vulnerability Response, whenever the risk score is updated on an AVIT, the **Notes** section is updated with the following details:

- Calculator group name
- Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, select any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If **Template** is selected, the risk score is updated according to the specified condition in the rule. If **Script** is selected, you can either add or update the existing script. The system property *sn_sec_cmn.risk_score_changes_add_worknotes* helps populate the Work notes section. Starting with v25.0.3 of Application Vulnerability Response, the system property *sn_sec_cmn.risk_score_changes_add_worknotes* is inactive by default. If you enable it, only then you can see all the changes related to the risk score of an application vulnerable item in the Work notes section. Additionally, the work notes are updated only if there's a change in the risk score.

The base system **Advanced Risk Calculator** calculator contains a specialized vulnerability calculator rule called **Default Risk Rule**. It calculates **Risk Score** based on multiple values:

- Vulnerability severity
- OWASP top 10
- SANS top 25

You can customize the criteria for the default risk rule. For more information, see Define fields and weights for the risk rule.

You can adjust the values to use in the **Default Risk Rule** and how much weight to give each of these values. Weights are used to adjust how much each element counts when setting the **Risk Score**.

Each rule has an **Order** setting however, the first one to match the conditions updates the **Risk score** field in the AVI. Non-scripted calculator rules typically create less of a performance impact than scripted calculator rules.

Vulnerability Risk Score Weights

All vulnerabilities are assigned a risk score and rating based on factors such as severity, criticality, exploit information, and so on. The business rule *Update Risk Rating from Risk Score* on the vulnerable item table is responsible for calculating the risk rating. Whenever the risk score changes, the risk rating is calculated and populated on the vulnerable items. Prior to version 17.1 of the Vulnerability Response (VR) application, the following risk ratings were provided as part of script include `VulnerabilityUtils`, which were hard-coded.

Value (Risk Rating)	Weight (Risk Score)
1	90–100
2	70–89

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Value (Risk Rating)	Weight (Risk Score)
3	40–69
4	1–39
5	0

Starting with the 18.0 version of Vulnerability Response,

- The risk rating types are shipped in the base table as avr_risk_rating. These types are passed as part of the business rule on each table where the risk rating is calculated.
- The script is modified so that you can query the entries in the Risk Score Weights table values for risk rating calculation.
- Add additional entries for an existing type or create a new type. When you create a new type, ensure that you add the labels for the new risk rating, and also modify the related scripts and business rules. You must also add a new style for the new risk score.
- Modify the script to query the records in the base table.

You can access the Risk Score Weights table by entering sn_sec_cmn_risk_score_weight (for versions below 30.0) or sn_sec_calculator_risk_score_weight (for versions 30.0 and above) in the filter navigator.

In addition, the risk score is automatically recalculated in the following scenarios:

- When a configuration item (CI) changes from non-internet facing to internet facing.
- When the associated Common Vulnerabilities and Exposures (CVEs) or third-party entries (TPEs) on the vulnerability items (VIs) are linked to a CVE Known Exploit Vulnerability (KEV).

Define fields and weights for the risk rule

Customize the parameters and weights for the risk rule so that you can generate risk scores that use the vulnerability and asset data that are unique to your organization. By selecting the fields that are included in the risk rule, you can define an effective risk scoring framework.

Before you begin

Role required: sn_vul.app_manage_risk_score_configuration

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Vulnerability Calculators**.
2. On the Vulnerability Calculators page, click **Advanced Risk Calculator**.
3. Navigate to **Vulnerability Calculator page** > **Vulnerability Calculator Rules tab** > **Default Risk Rule**.
4. **Optional:** In the Risk Calculator Criteria section of the Vulnerability Risk Rule page, set the weight for each criterion according to its importance in the overall risk score calculation.
5. To deactivate the rule, you must clear the **Active** check box.
6. To add risk rule fields to the Risk Calculator Criteria, click **Add criteria**.
7. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk rule field form

Field	Description
Choose reference table	Table that you use to define the risk score weightage. You can select one of these options: ○ **Application Vulnerable Item**: Add fields that are directly dot-walkable from the vulnerable item (VI). ○ **Application Vulnerable Item - Configuration Item**: Add dot-walkable fields that are part of the base table extensions, such as the Hardware table. These fields are not part of the base table (cmdb_ci). ○ **Application Vulnerable Item - Vulnerability**: Add dot-walkable fields that are part of the tables that extend the base table, for example, Third-party Entry. These fields are not part of the Vulnerability Entry base table. ○ **Application Vulnerable Item Reference Table**: Add fields that are a part of the Related tables (m2m) or tables that have a reference to the vulnerable item. These fields are not directly dot-walkable from the VI. ○ **Configuration Item Reference Table**: Add fields that are a part of the Related tables (m2m) of cmdb_ci or tables that have a reference to cmdb_ci. These fields are not directly dot-walkable from the VI. ○ **Vulnerability Reference Table**: Add fields that are a part of the Related tables (m2m) of sn_vul_entry or tables that have a reference to sn_vul_entry. These fields are not directly dot-walkable from the VI. ○ **Custom Conditions**: Use this option to assign weights to the rule by evaluating the condition. For example, the Internet-facing filter determines if a configuration item (CI) is external or internal.
Table	Field that appears only when one of the following options is selected from the Choose reference table: ○ **Application Vulnerable Item -> Configuration Item** ○ **Application Vulnerable Item -> Vulnerability**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Application Vulnerable Item Reference Table** ○ **Configuration Item Reference Table** ○ **Vulnerability Reference Table**
Field	Field to be used for risk score calculation for this rule.
Aggregation	Field that appears only when a reference table is selected from the Choose reference table. Select the minimum or maximum value to be considered for calculations when Field is selected from the Related tables (m2m).
Weight	Weightage of this field within the risk rule. The value must be an integer from 0 through 100.
Define Value Weightage	Component to assign weights to each field value. For numeric fields, field values can be defined as a range (for example, 1–5). The weights must be integer between 0–100. **Note:** This field does not appear if the Custom Conditions option is selected from the Choose reference table.
Condition table	Field that appears only when Custom conditions is selected from the Choose reference table. Select a condition from the list.
Field name	Field that appears only when Custom conditions is selected from the Choose reference table. Enter a name for the risk criteria.
Condition	Field that appears only when Custom conditions is selected from the Choose reference table. Preview the items in this table that match the defined conditions.

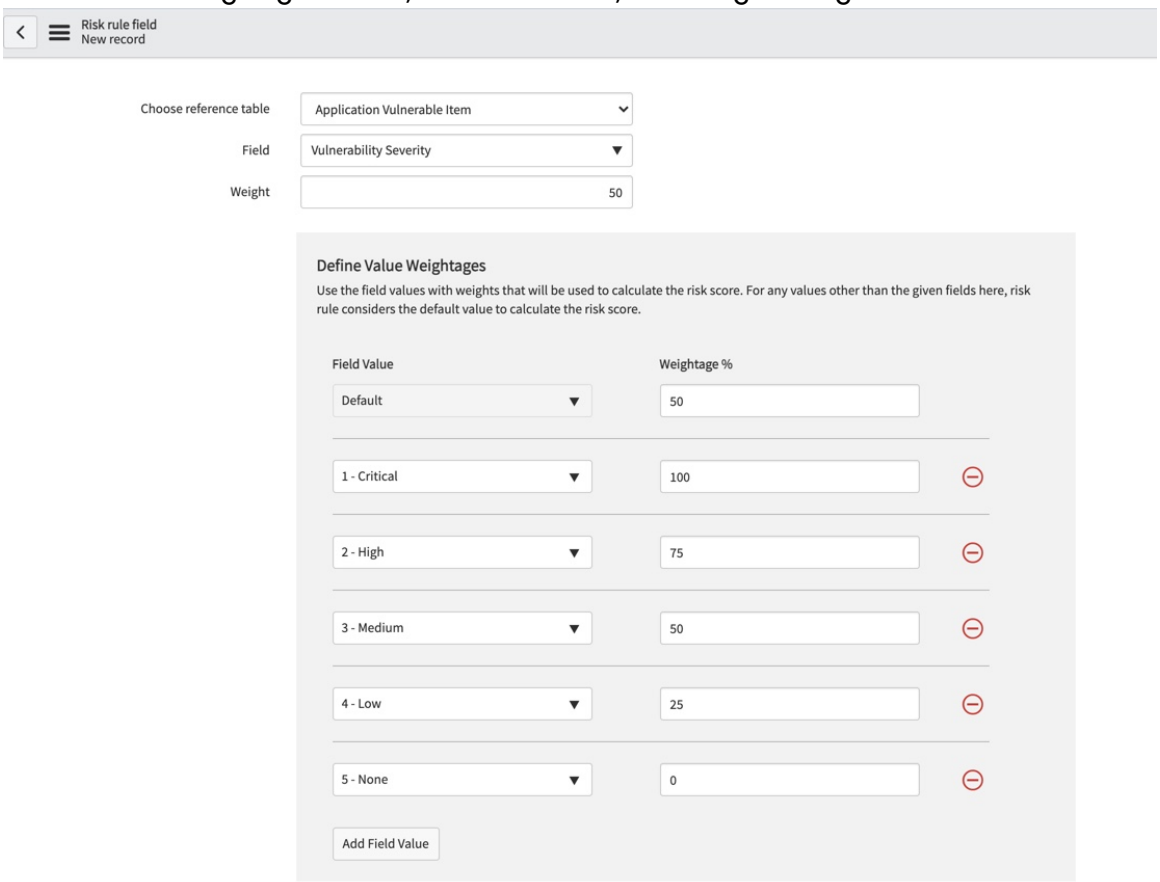
8. Click **Submit**.
9. In the Rule page, activate and reapply the rule to reevaluate the risk score on the active vulnerable items.

Example:
Add source severity as a criterion for a risk rule.

Use case: Third-party vendors, like Qualys and Tenable, provide their own scores. These scores are populated in the **Source Severity** field on the sn_vul_entry table. Use this field for risk score calculations. To use this score to compute the risk score, do the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to the Risk rule page.
2. To deactivate the rule, clear the **Active** check box.
3. To add risk rule fields to the Risk Calculator Criteria, click **Add criteria**.
4. From the Choose reference table list, select **Application Vulnerable item**.
5. From the Field list, select **Vulnerability.Severity**.
6. In the **Weight** field, enter the relative importance of this field within the risk rule. The value must be an integer from 0 through 100.
7. In the Define Value Weightage section, add field values, and assign a weight to



them. Submit Cancel

8. Click **Submit**.

Related topics

Vulnerability Response calculators and vulnerability calculator rules

Create an application vulnerability calculator

An application vulnerability calculator is a pre-defined formula to calculate a target field when certain criteria are met. Calculators, which calculate the application vulnerable item (AVI) **Risk Score**, can contain **Risk Rules**. Risk calculations offer insight in prioritizing remediation.

Before you begin

Role required: App-Sec Manager group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You may notice performance degradation when running application vulnerability calculators that contain scripts.

Order your rules to run the simplest rules first. Only run scripts on the items that cannot be handled with a condition and template value or a risk rule.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Vulnerability Calculators**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Vulnerability calculator form

Field	Description
Name	The name of the application vulnerability calculator.
Table	Auto-filled with the name of the AVI table.
Application	Auto-filled with Vulnerability Response.
Target field	Field to calculate.
Description	Text description of the calculator.
Active	Turn the calculator on or off.

4. Right-click in the header to **Save**.
   The **Vulnerability Calculator Rules** section appears.
5. Create a rule for the calculator by clicking **New**.

Note: For the **New Risk Rules** form (only available when the **Target field** is **Risk Score**) see step 10.

6. Fill in the fields, as appropriate.

Vulnerability Calculator Rule form

Field	Description
Name	Name of the calculator rule.
Order	The order in which to run the vulnerability calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Calculator	Auto-filled with the calculator parent.
Active	By default the **Active** check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.
Advanced view	When selected, scripted conditions and scripted values can be selected from **Condition type** and **Value type**.

7. Fill in the fields in the **When this condition is met** tab, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When this condition is met tab

Field	Description
Condition type	Available when you select the **Advanced view**. Choices include: ○ Filter: Uses filter conditions. ○ Filter group: See create and define filter groups to define the calculator criteria. ○ Script: Script condition used to determine when to apply this calculator. **Note:** Before you write scripts for determining when to apply the calculators, return to the **Application Vulnerability Calculators** list. Explore the vulnerability calculator records shipped with the base system.
Condition	Defines basic filter conditions for determining whether to use the calculator or not. Selecting either the **Filter group** or **Script** condition types, hides this field.

8. Click the **Set these values** tab and fill in the fields on the form, as appropriate.

Set these fields tab

Field	Description
Value type	Available when you select the **Advanced view**. Choices include: ○ Template: Define the values to set on each field. ○ Script: Used to set the values on each field.
Script values	Available if you selected the **Script** value type. Defines what values to apply the calculations to.
Template	Select the fields and values you want to use for the calculator. Selecting either the **Script** value type, hides this field.

9. When you have completed all entries, click **Submit**.

Note: When you edit an existing calculator, and you want to update all existing scores, you can use the **Reapply Calculator** button. It runs through all active AVIs, and if that calculator would be used to set its value, recalculates the value for those AVIs. Since reapplying a calculator can take a long time, a scheduled job handles it.

10. For the **New Risk Rules** form, fill in the fields as appropriate.

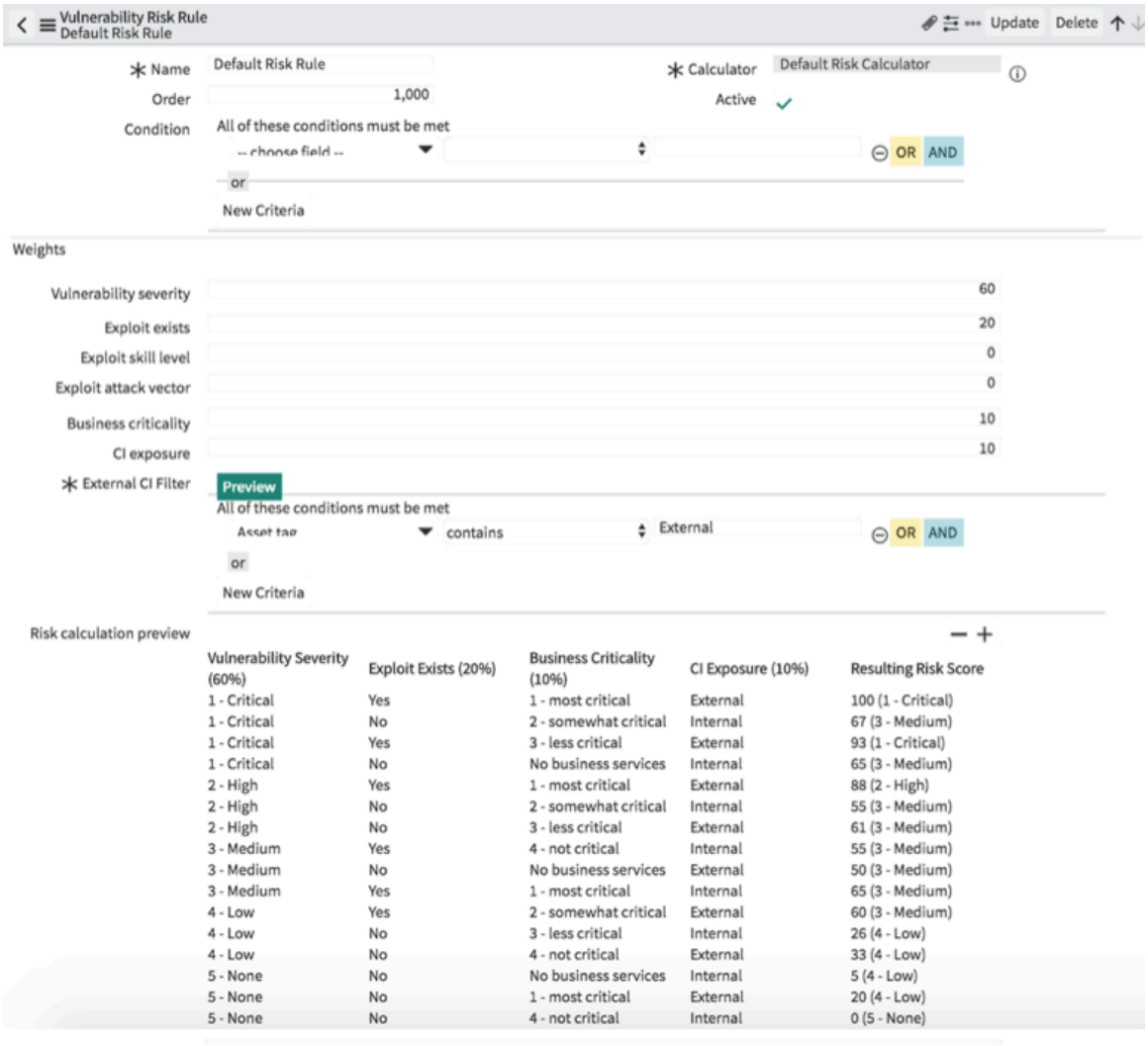
Set each weight according to the percentage of the result that should come from that value. For any data that your scanner does not provide, or for data that should not be part of the risk score, set the weight to zero.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As you update the weights, scenarios display the weights remaining, as well as anticipated **Risk Score** results.

Field	Description
Name	Name of the calculator rule.
Order	The order in which to run the calculator. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Calculator	Auto-filled with the calculator parent.
Active	By default the **Active** check box is selected, which means the calculator rule is active. If you clear this check box, this rule does not apply to new vulnerable items created in the system.
Condition	Defines basic filter conditions for determining whether to use the calculator. Selecting either the **Filter group** or **Script** condition types, hides this field.
Weights	
Vulnerability Severity	Percentage of the result that comes from severity.
OWASP top 10	Percentage of the result that comes from the vulnerability's presence in the OWASP top 10 list. If this information is not present in your vulnerabilities, set the weight to zero.
SANS top 25	Percentage of the result that comes from the vulnerability's presence in the SANS top 25 list. If this information is not present in your vulnerabilities, set the weight to zero.
Running total	Auto-computed percentage totals. When this value reaches 100, the Scenario preview shows sample risk scores in different scenarios.
Sample scenarios	When all weights total 100%, risk score scenarios display, providing a preview of the risk score in some of the possible scenarios.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



11. Click **Submit**.

Map the severity of an application vulnerable item automatically

Application Vulnerability Response severity mapping transforms third-party source severity fields to recognizable fields within Vulnerability Response.

Before you begin

Role required: App-Sec Manager group

About this task

Application Vulnerability Response third-party integrations such as the Veracode Vulnerability Integration provide severity mappings on installation. These maps can be adjusted by changing the fields in existing maps.

Creating or editing a severity map is intended only for customized or non-standard third-party mappings in your environment and requires Application Vulnerability Response and ServiceNow expertise.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Normalized Severity Mapping**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field mapping

Field	Description
Source	The name of the source for the severity mapping.
Source value	The source severity value.
Target value	The target severity value. Choices are: ○ 1- Critical ○ 2 - High ○ 3 - Medium ○ 4 - Low ○ 5 - None

4. Repeat Step 3 for each source severity level.
5. Click **Submit**.

Filtering within Application Vulnerability Management

Calculators, and Assignment Rules use conditions during import, created using the **condition builder**. Changes to their criteria can affect performance since each record is evaluated using these filters.

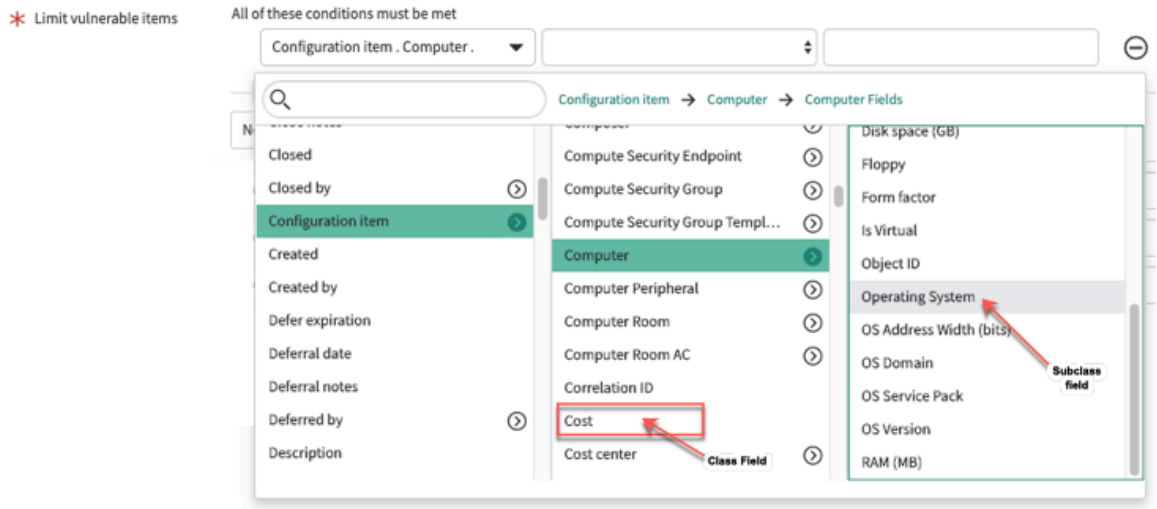
The rules and calculators shipped with the base system are optimized for performance. Editing or creating rules or calculators takes care and may require both ServiceNow and Application Vulnerability Response expertise. That said, some guidance is available.

Avoid filtering based on subclass fields

Some tables support extension. An example of that is the CMDB CI [cmdb_ci] table. Tables like cmdb_ci_hardware and cmdb_ci_computer extend this table. If you filter based on a field that is not on the parent table, that filter can be expensive to construct and evaluate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Condition filter drop-down menu



For example, filtering on **Configuration Item** > **Cost** would not adversely affect performance because **Cost** is a class field, and not a subclass field, of **Configuration Item**.



Configuration Item > **Computer**, however, is a subclass requiring a dot-walk to another field, in this case, **Operating System**. This process can take many milliseconds which add up quickly, when millions of vulnerable items are being imported, and affect performance.



Note: Using the [contains] condition is like a wild-card search and can cause performance impact. Using [is], wherever possible, is more efficient.

Automate remediation target tracking in Application Vulnerability Response

Application Remediation Target Rules define the expected timeframe for remediating application vulnerable items (AVIs), providing a timeframe for remediating the vulnerability itself. For example, if an application vulnerable item contains a critical risk rating then the vulnerability on that item needs to be fixed within 15 days.

App-Sec Managers can create application remediation target rules by defining:

- The remediation target.
- The reminder target.

App-Sec Managers can see the remediation target date in the AVI form and list views, however dates are not updated for AVIs in the **Deferred**, **Resolved**, or **Closed** state.

The **Remediation target date** is color-coded coded on the AVI list view as dots, as follows:

- AVIs that have not reached their notification date are shown in green.
- AVIs approaching the remediation target date are shown in orange.
- AVIs past the remediation target date are shown in red.

Default rules

Application Vulnerability Response ships with three default rules which are inactive by default:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Critical Risk Rating Rule: A remediation target with a **1-Critical** risk rating, a remediation target of 15 days, and a reminder of **7** days before the target date.
- Medium-High Risk Rating rule: A remediation target with either a **2-High** or **3-Medium** risk rating a remediation target of 30 days, and a reminder of **7** days before the target date.
- Less Critical Risk Rating rule: A remediation target with a **4-Low** risk rating a remediation target of 45 days, and a reminder of **7** days before the target date.

Remediation target rules can be deactivated or deleted

When a rule is deactivated, the current remediation target dates for the AVIs it was applied to, are cleared. If an AVI satisfies any active rule that rule is applied, otherwise the AVI has no rule or target date, and its status is **No Target**.

When rules are deleted, the **Remediation target** date and related fields on closed AVIs are preserved. The **Remediation target** date and related fields on non-closed AVIs are cleared and any dependent rules are reapplied.

Remediation rule scenario

When multiple remediation target rules are applied to the same AVI, the most restrictive rule is applied.

For example, if an AVI meets the condition for two application remediation target rules:

Scenario: AVI last opened on 03/01/2018 at 10:00:00.

- Application remediation target rule 1: Last opened on 03/07/2018; remediation target is 15 days since it was last opened; calculated remediation target date is 03/16/2018 10:00:00.
- Application remediation target rule 2: Last opened on 03/10/2018; remediation target is 10 days since it was last opened; calculated remediation target date is 03/11/2018 10:00:00.

In this scenario, the Application remediation target rule 2 applies to the AVI since it has the more restrictive date. 10 days since the AVI was first identified versus 15 days.

Note: Application remediation targets are calculated from the **Last Opened** date plus the number of days (measured as 24-hour increments). You can add this field to the AVI form from the Form Layout slushbucket. It is the date the AVI was most recently opened in your instance.

Starting from V17.1, remediation targets are calculated from the **Target from (date)**. The default value remains **Last Opened date**.

Note: Once the application remediation target rule is defined, remediation target dates are calculated by the *`Evaluate remediation targets`* scheduled job or the **Apply Changes** button on the Remediation Target Rules list view.

About the Evaluate remediation targets scheduled job

`Evaluate remediation targets` runs once at 4:00:00 daily.

`Evaluate remediation targets` iterates through all active vulnerability rules, starting with those rules with the earliest remediation target date. It looks at all AVIs that:

- Are not in a **Closed**, **Deferred**, or **Resolved** state.
- Have no remediation target date.
- Have a remediation target date that is later than the date in the application remediation target rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Evaluate remediation targets adds a remediation target date, if one does not exist, or if this rule contains an earlier date than the one in the record, it updates the existing target date. Finally, it updates the **Remediation target date** and **Remediation status** fields in the AVI form. For inactive rules, **Evaluate remediation targets** clears the remediation fields on the AVI.

Reapplying remediation target rules

When you change a remediation target rule, use the **Apply Changes** button on the Remediation Target Rules list page to rerun all the changed rules on all active Open AVIs except those in the **Closed**, **Deferred** or **Resolved** state.

Note:

If the scheduled job, *Evaluate remediation targets* is running, you cannot initiate a reapply process. However, if a reapply process is already running, and the scheduled job is triggered, they run in parallel.

The reapply processes in Vulnerability Response and Application Vulnerability Response are independent and can run in parallel.

Create or edit application remediation target rules

Drive the remediation of high-risk vulnerabilities in a timely manner by setting up a remediation target rule at the application vulnerable item (AVI) level.

Before you begin

Role required: App-Sec Manager group

Note: The base system ships with three remediation target rules.

- Critical Risk Rating Rule
- Less Critical Risk Rating Rule
- Medium-High RIsk Rating Rule

These rules are inactive by default. If you choose to edit one, rather than create a new one, remember to check the**Active** box before saving.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Administration** > **Remediation Target Rules**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	Name of the rule.
Target (days)	Specify the number of days within which the AVIs should be remediated, since last opened.
V17.1: Target from (date)	Date from when the target SLAs are computed. You can specify only the date or the date and time type fields. Default value is Last opened date. To customize the values for this field, see KB1642413.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	By default the **Active** check box is selected, which means the remediation target rule is active. If this check box is cleared, this rule does not apply to new AVIs created in the system.
Notify (days before due)	Number of days prior to the targeted remediation time for a reminder to be set. The notification date calculated using this value is used to show the remediation status and color coding. If the date is before the notification date, the remediation status is "In flight." If it is past the notification date and before the remediation target date, the status is shown as approaching target. **Note:** If this field is set to 0, only a **Target Missed** notification is set.
Rule applies to	Using the condition filter, select the criteria for applying the rule to the AVIs. To prevent performance impact, test your conditions at full production scale. Testing enables you to determine how long the **Evaluate remediation targets** job takes to execute, given the conditions and the size of your Configuration Management Database (CMDB).
Update history	
Activities	Unused for initial creation of a rule. Subsequently, system work notes are logged here.

4. Click **Submit**.
   This rule goes into effect during the next run of the scheduled job, *`Evaluate remediation targets`*. The same is true when an existing rule is updated or when using the **Apply Changes** button on the Remediation Target Rules list view. The same is true when an existing rule is updated. For more information on the scheduled job and **Apply Changes** see, Automate remediation target tracking in Application Vulnerability Response.

View the remediation target status of an application vulnerable item

When an application vulnerable item (AVI) has nearly reached (or passed) its remediation target date, as defined by a remediation target rule, the AVI record is updated with a status. This information can help you proactively monitor upcoming remediation activities.

Before you begin

Role required: App-Sec Manager group

About this task

The **Evaluate remediation targets** scheduled job runs once per day to compare the current date against the vulnerable item remediation date specified in the associated remediation target rule. When the current date falls within the number of days before the remediation is past due, a remediation status is added to the vulnerable item record.

Procedure

Navigate to **All** > **Application Vulnerability Response** > **Vulnerable Items**.
If the remediation date for the AVI is within range of the conditions set in the remediation target rule, check the Remediation Target Status columns, visible on the Vulnerable Items list view. If the remediation target date has passed for an AVI, an annotation appears on the AVI form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: To view the number of AVIs that are **Approaching Target**, **In-flight**and**Past Target**, see Application Vulnerability Management [PA] dashboard.

Related topics

Create or edit application remediation target rules

Close a remediation task

If you determine that the issue associated with an application remediation task can be immediately closed without further analysis, you can use the **Close** feature. Starting with v23.0 of Vulnerability Response, the **Close** button has been removed for an application remediation task.

Before you begin
Role required: admin

About this task
In the Vulnerability Response Workspaces, a remediation task transitions through the same states as a remediation task prior did in previous versions of Vulnerability Response. When all the vulnerable items (VITs) in a remediation task are closed, the remediation task transitions to the Inactive state.

Important: You can manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move remediation tasks from the `Closed` or `Deferred` states.

Procedure

1. Open the record that you want to request a review for.
2. Select the **Close** button.
3. Fill in the fields on the form, as appropriate.

Field	Description
State	Select the state as Closed.
Reason	Enter the reason for closing the issue.
Additional information	Enter any other relevant information.

4. Select **Submit**.
   The remediation task is marked **Closed**.

Change Management for Application Vulnerability Response

Create change requests from remediation tasks in the Application Vulnerability Response application to expedite your investigation for application vulnerabilities (AVIT)s that require manual intervention.

Create change requests with prepopulated information for scanned applications that are classified as configuration items (CI)s to help you expedite your investigation for application vulnerabilities (AVITs) that require manual intervention.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The change request workflow in Application Vulnerability Response is similar to the workflow supported in Vulnerability Response.
- For more information about the Vulnerability Response change request workflow, see Change management for Vulnerability Response.

Create a change request for Application Remediation task

As a App-sec Manager or Security Champion, you can create change requests from remediation tasks in the Application Vulnerability Response application.

Before you begin

Roles required:

From Vulnerability Manager Manager Workspace: sn_vul.app_sec_manager.

From ITRem Owner workspace: sn_vul.app_sec_champion or sn_vul.app_developer, and itil role.

About this task

To create a change request from the classic environment, follow the steps listed below.

You can create, approve, implement, review, and close change requests directly from a remediation task. You can create three types of change requests with pre-populated information from a remediation task:

- Standard. A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.
- Normal. Normal change requests follow a prescriptive process that requires two levels of approval before being implemented, reviewed, and closed.
- Emergency. A change to resolve a major incident.

Note: Change requests are supported for Application Vulnerability Response only if the discovered application is associated with a configuration item (CI), which occurs only when you set 'Product model' to 'False' in the Use Product Model [sn_vul.use_product_model] system property.

Procedure

1. To create a complete change request from an existing remediation task record, navigate to **All** > **Application Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**.
   The list of remediation tasks assigned to your assignment group is displayed.
2. **Optional:** Navigate to **All** > **Application Vulnerability Response** > **Remediation Overview** to view the Remediation Overview dashboard and locate a VUL assigned to you or your assignment group.
3. Alternatively, in the Number column, click a remediation task to open the record and view the details.
   The record is displayed.
4. With the APP-VUL record displayed that you want to create the change request for, in the upper right of the record, click **Create Change**.
   The Create change request form is displayed.
5. Fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. From the choice list of the Applies to field, choose one to continue.

Option	Description
All active application vulnerable items in this group	If selected, all active application vulnerable items from this remediation task with a state other than Closed are added automatically to the change request after you click **Create Change**.
All application vulnerable items in this group matching a set of conditions	If selected, the Condition builder is displayed as shown in the second figure below. Enter filter criteria to identify the vulnerable items that you want for the new change request. An example of a filter might include only vulnerable items that match specific search criteria: **State is Open** and **Risk score greater than 75**. After you enter your conditions, a message is displayed with the number of AVITs that match your criteria (10). A link (**Preview matching items**) to preview the matching items is displayed. If no items match your filter conditions, a message is displayed below the Condition builder that instructs you to adjust your filter. After you click **Create Change**, all application vulnerable items that match this condition filter are moved a new remediation task. This change request is associated with the new remediation task.

Create change request form for application vulnerable items in a task that match a set of conditions

b. Optional: If displayed on the form, click the **Preview matching items** link for a list of the AVITs that match your filter criteria.
The Remediation Task List preview is displayed. You can select items on this preview list and perform UI actions on them, however, these actions are also performed on the APP-VUL. For example, if you delete a VI from the preview list, that AVIT is also deleted from the APP-VUL.

c. After you complete your preview, close the browser window to return the change request form.

d. For the Add CIs to CR check box, choose one to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Add CIs to CR check box selected	Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this remediation task are added to this change request. The APP-VUL automatically moves to the `Awaiting Implementation` state.
Add CIs to CR check box cleared	Clear the check box if you do not want the CIs from the active application vulnerable items from this remediation task added to the new change request. When disabled, the state of the change request is not synched to the APP-VUL, and the APP-VUL remains in its current state.

e. From the choice list for the Change type field, choose one to continue.

Change type	Description
Emergency	A change to resolve a major incident.
Normal	A change type that is used to implement any change to a service that is not a standard or emergency change.
Standard	A pre-authorized, low-risk change request that is frequently implemented. Approved standard change requests can be predefined in a catalog of templates to make accessing and requesting a standard change more efficient. If selected, two fields are displayed. Select one from each choice list to fill in these fields: ▪ Change category: Select a category for the change from your existing catalog, for example, `Hardware`, `Server Standard Changes`, `Software`. In this example, `Patching Standard Changes` is selected. ▪ Change template: Select one available template for change requests with pre-defined supporting tasks from your catalog. In this example, the `Microsoft Monthly Patching Cycle` template is selected. For more information on ITSM change request categories, templates, and change types, see Change types.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The feature automatically reads the types of change requests that you set up in your catalog in ITSM Change Management. For example, if you change the name for your Standard change requests in ITSM from `Standard` to `Pre-approved`, your new name is automatically displayed in the Change type choice list on the Create change request from as shown in the following figure.

The fields in the Change Request Preview section of the form are pre-populated with information from the APP-VUL. If required, these field values can be edited. For example, review the values in the fields in the following figure:

Planned end date

This date (`2019-10-10`) is the same value that is displayed in the Remediation target date field of the APP-VUL. This value is derived from the earliest remediation target date from the application vulnerable items that belong to the APP-VUL. If you are creating a change request for a critical issue that requires an earlier remediation date, you may prefer to edit this value and the value in the Priority field.

Justification

This field displays the number of CIs that are added to the CHG. If you want to add additional information, you may prefer to edit this text. For example, you may prefer to add a note in this field about the filter you used to create the new APP-VUL, for example, `Risk score greater than 75`. This text can help you locate your new change request and remediation task.

Implementation plan

This field displays the preferred solution for the vulnerability.

Assignment group and Assigned to

Edit these fields to change the assignment group or reassign this change request to a user in one of your assignment groups.

6. Continue to preview and edit the fields as required.
7. To save your changes and remain on this page, in the gray banner at the top of the form, right-click and select **Insert and Stay**.
8. After you complete your edits, choose one to continue.

Option	Description
Create Change	Your change request is created and the new change request is displayed in the New state. At the top, messages are displayed that indi cate the change request is successfully creat ed with the number of application vulnerable items that were added. If state synchronization is enabled and the VUL is not already in `Under Investiga tion`, the VUL is automatically moved to `Un der Investigation` and a work note is posted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Cancel	The change request is not created and the APP-VUL is displayed.

Note:

For a remediation task in the `Open` state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the task after you click **Create Change**. In addition, the Add CIs to CR check box must be selected. At the top of the VUL, a blue confirmation message is displayed that indicates this assignment.

What to do next

Monitor the change request and the change tasks to verify that they are completed and the change request is implemented. After this CHG is implemented and moved to the `Review` state, if state synchronization is enabled, the APP-VUL automatically moves to `Resolved`.

Associate a remediation task to an existing change request

As a Appsec Manager or Security Champion, avoid creating duplicate change requests (CHG) as you work to resolve your remediation tasks by associating a remediation task (APP-VUL) to a change request that is already available in your instance.

Before you begin

Roles required:

From Vulnerability Manager Manager Workspace: sn_vul.app_sec_manager.

From ITRem Owner workspace: sn_vul.app_sec_champion or sn_vul.app_developer, and itil role.

About this task

As a remediation owner, you can associate remediation tasks that are assigned to you or your assignment group to existing change requests directly from the remediation task records. The following image illustrates the basic flow for associating a change request to an existing APP-VUL (VG).

Note: You can associate an existing change request to a APP-VUL in any state (Open, Under Investigation, Awaiting Implementation, Closed, and Deferred). When you associate a change request to an existing VUL, only the active VIs are added to the change request.

Before you begin, to avoid creating duplicate change requests, you might prefer to view any existing change requests already associated with a APP-VUL. To easily track the number of change requests that are related to a specific APP-VUL, refer to the CR count column on the Remediation Tasks list. If not displayed, click the settings icon () in the upper right. Move the CR count column from Available to Selected and click **OK**.

To automatically populate the new column, for customers with existing data in this table, run the scheduled job: `Populate new CR Count Column`.

Procedure

1. To associate a remediation task to an existing change request, navigate to **All** > **Application Vulnerability Response** > **Remediation Tasks**.
2. Locate the remediation task you are working with.
3. **Optional:** Navigate to **All** > **Application Vulnerability Response** > **Remediation Overview** to view the Remediation Overview dashboard and locate a APP-VUL assigned to you or your assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the Number column, click a APP-VUL record to open it.
   The APP-VUL record is displayed.
5. With the open record displayed, if not already displayed, scroll to the Change Requests related list and select it.
   Any change requests associated with the APP-VUL are displayed along with the **Add** button. In the following figure, there are no change requests already associated with this APP-VUL.
6. To associate the APP-VUL with an existing CHG, click **Add**.
   The Add Existing Change Request to Remediation Task form is displayed.
7. In the form, click the search icon.
   A list view of existing change requests is displayed in a new window as shown in the following figure.
8. Select an item from the displayed list, or, alternatively, click the filter () and enter conditions to limit your search results.
9. For the Add CIs to CR check box, choose one to continue.

   Note: This check box is displayed only for existing change requests in the New state.

Option	Description
Add CIs to CR check box selected	Default is selected. If the check box is selected, any configuration items (CI) that belong to active vulnerable items in this remediation task are added to this change request. When selected, the state of the change request is synched to the APP-VUL. For more information, see State synchronization between change requests and remediation tasks.
Add CIs to CR check box cleared	Clear the check box if you do not want the CIs from the active vulnerable items from this remediation task added to the new change request. When disabled, the state of the change request is not synched to the APP-VUL, and the APP-VUL remains in its current state.

10. With the change request number you want displayed in the Search for Change Request field, click **Submit**.
    The APP-VUL is displayed. At the top of the record, the blue confirmation message is displayed indicating that the change request you selected is successfully associated to the APP-VUL.

    Note: For a APP-VUL in the Open state with the Assignment group and Assigned to fields unassigned (empty), the current logged-on user is automatically assigned to the APP-VUL after you click **Add**. In addition, the Add CIs to CR check box must be selected. At the top of the APP-VUL, a blue confirmation message is displayed that indicates that the current user is assigned.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Review the APP-VUL record. In the Change Request column on the Change Requests related list, click link for the new CHG to view CR record. On the open CHG record, you can monitor the state of the change request. The affected configuration items (CI)s and the remediation tasks are displayed on the Affected CIs and remediation tasks related lists.

Penetration testing

Penetration testing in Application Vulnerability Response enables application owners to assess the security posture of their application. It is the manual testing of an application by the ethical hacking team.

Roles required

Penetration testing requires the following roles:

App-Sec Manager: Contains security managers and application owners who manage the penetration testing assessment requests. It contains the following granular roles:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

Ethical Hacker: Contains members of the ethical hacking team who perform penetration testing of applications. It includes the following granular roles:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

For more information about these roles, see Application Vulnerability Response user groups and roles.

Starting with v19.0 of Vulnerability Response, if you are using the Veracode Vulnerability Integration, the penetration assessment tests in the Veracode Vulnerability Integration are manual findings from Veracode. They are not linked to any penetration test assessment requests you configure in Application Vulnerability Response. For more information about penetration test assessments from Veracode, see the Veracode Vulnerability Integration.

Life cycle of penetration testing

As an application owner, you can request the ethical hacking team for a penetration test assessment of your application. The ethical hacking team acts on this request and creates penetration test findings. These findings are manually-created Application Vulnerable Items (AVIs).

The penetration testing workflow covers the penetration testing life cycle from raising the testing request to resolving the findings of the ethical hacking team.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Requesting a penetration test assessment

Starting with v19.0, you can create new requests or copy existing requests at **All** > **Penetration Test Assessment Requests** > **All**.

Prior to v19.0, as the application owner, you can request a penetration test assessment for your application using the ITSM service catalog.

Reviewing the penetration test assessment request

The ethical hacking team reviews and assesses the application and the scope of the penetration test assessment request, and adds it to the existing backlog.

Preparing an environment

The ethical hacking team then sends a request to the application owner to provide an environment for them to start testing. Once the environment is ready, the application owner informs the ethical hacking team.

For more information about configuring test requests, see Configure penetration testing.

Testing and reporting the penetration test findings

The ethical hacking team tests the application and reports the findings to the application owner. The ethical hacking team also defines the Service Level Agreements (SLAs) for the penetration test findings using the remediation target date. These findings are the manually-created AVIs. The application owner in turn reviews the AVIs created by the ethical hacking team. They plan the fixes and assign them to the application team.

Note: Remediation target rules do not apply to the penetration test findings.

The ethical hacking team can create a library of Application Vulnerability Entries (AVEs) and reuse them while reporting the AVIs. They can also track the status of the penetration test findings.

Fixing and validating the penetration test findings

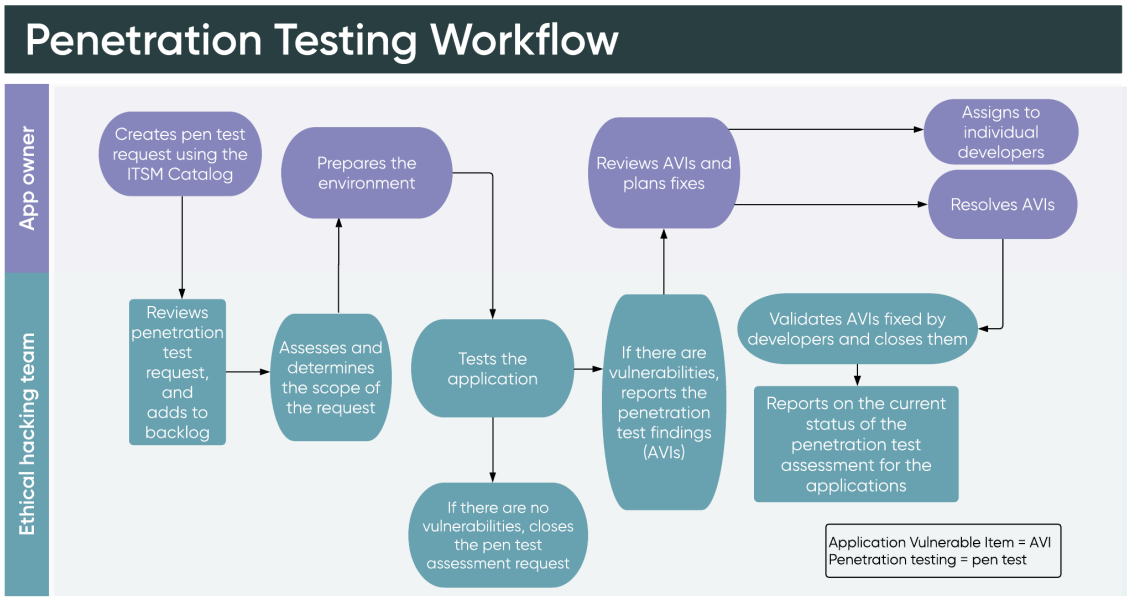
After the penetration test findings are fixed and resolved by the application team, the fixes are validated manually and closed by the ethical hacking team.

Application Vulnerability Management reports

Use the reports available on the Application Vulnerability Management PA dashboard to track the penetration test findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Penetration testing life cycle



Create a penetration test assessment request from existing requests (v19.0)

Starting with v19.0, you create penetration test assessment requests directly from the list of existing requests. You can also copy existing requests in the Closed state on this list to create requests.

Before you begin

Role required: App-Sec Manager

About this task

Starting with v19.0 of Vulnerability Response, if you are using the Veracode Vulnerability Integration, the penetration assessment tests in the Veracode Vulnerability Integration are manual findings from Veracode. They are not linked to any penetration test assessment requests you configure in Application Vulnerability Response. For more information about penetration test assessments from Veracode, see the Veracode Vulnerability Integration.

Procedure

1. Navigate to **All** > **Penetration Test Assessment Requests** > **All**.
2. **Optional:** Alternatively, you can create a request by replicating closed requests.
   All the values from the original request are preserved in the new form. Active application vulnerable items (AVIs) are automatically copied to the new request. Select **Copy And Create Request** from records in the Closed state.
3. Select New and fill out the fields.

Penetration Testing Assessment Request form

Field	Description
Number	Unique identifier generated for the penetration test assessment request.
State	Select a value based on the status of the request.
Requested by	Person requesting the assessment of the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Assignment group	Group selected to work on the penetration test findings. Can be manually added or edited by an App-Sec Manager. To configure groups, see Configure penetration testing.
Application	Select an application using the search option.
Assigned to	Individual from the selected assignment group that works on the penetration test findings. Can be manually added or edited by an App-Sec Manager.
Application type	Select an option from: ○ Web service (known as API prior to v16.1) ○ Web Application ○ Thick Client ○ Mobile (If you select **Mobile**, the Mobile tab is displayed at the bottom of the form with additional fields)
Sprint	Displays the sprints with bandwidth available to accommodate the assessment request based on the selected Assessment type field. See Configure sprints for penetration testing and Configure assessment types for penetration testing for more information about modifying sprint capacity and testing scope.
v19.0: Application size	Select the size of the application you want to test. ○ Small ○ Medium ○ Large ○ Standard (select this option if you are not sure of the size) See more Configure penetration testing more information about modifying sprint capacity and testing scope with application size and sprint capacity.
Created	Date and time the request was created.
Assessment type	Select the type of assessment from: ○ Full penetration Test ○ Focused Test ○ Re-test

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For more details about testing combinations and testing scope, see Configure assessment types for penetration testing.
Updated	Date and time the request was last updated.
Demo date	Date when this application can be demonstrated.
Product deployment planned on	Planned date to deploy this application in production.
Application version/release planned for deployment	Version of the application planned for production deployment.
v19.0: Application owned by third-party vendor or a joint venture tab If you select Yes for this field, the Vendor/ Joint Venture Information tab is displayed. Fill in the additional fields.	
Clause exists that enables us to perform pen testing?	The term 'Clause' might refer to standards for testing that include any agreements that exist between two or more parties you want to add. If you select **Yes**, add the clause.
The clause citing the permission to perform pen testing	
Full legal name and address of the vendor	
Intrusion detection system	
Technical contact from vendor	
Has the logged information been reviewed form malicious activity?	
Application hosted by another third-party vendor?	
Contact from vendor who will be signing off on the pen test	
Application Details tab	
Purpose of application	Description of the application's functionality.
Technology stack details	Complete technology stack from front end to back-end, databases, and other key technologies.
Is third-party application?	Confirms if this application is owned by a third-party vendor.
List types of sensitive data accessible from application	Types of sensitive data accessible from the application. For example, PII data, PHI data, and financial data such as credit card numbers.
Authentication type	Specifies if this application uses LDAP authentication, its own native authentication, or other forms of authentication.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Is application in scope for any compliance program?	Specifies if this application impacts any compliance programs such as PCI.
Application team contacts	Members of the application team to be contacted by the ethical hacking team for any questions.
List of compliance programs	
Related third-party interfaces or applications	
IP address	
Approximate number of users in production?	
Automated script exists?	
Production version of this app is external-facing?	
v 19.0: Business Impact	
Financial damage	Select one from the list.
Non-compliance	Select one from the list.
Reputation damage	Select one from the list.
Privacy violation	Select one from the list.
Testing details tab	
URLs to test	URLs that must be included in penetration testing.
URLs to exclude	URLs that must be excluded from penetration testing.
Was this application tested previously?	Specifies if this application has already been penetration tested.
Reason for retest	Reason for asking for a penetration test reassessment if the application was tested earlier.
When was the application tested?	Time frame when the application was penetration tested.
Test account details	Details of the test account that can be used by ethical hacking team for penetration testing.
Application roles	Roles supported by the application for its users.
Most used roles	Most commonly used roles in the application.
Additional Comments tab	
Work notes	

4. Select **Save** to save your edits or **Submit** to initiate the request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a penetration test assessment request (prior to v19.0)

Initiate a penetration test assessment request for your web applications or APIs. These requests are submitted to the ethical hacking team, who then proceed to test these applications and manually report the penetration test findings.

Before you begin

Role required: App-Sec Manager

About this task

The application owner raises a penetration test assessment request to manually scan their application or APIs. The ethical hacking team tests the application and manually creates penetration test findings. These findings are manually-created application vulnerable items (AVIs).

The default assignment group for the penetration test finding is the group configured in the 'Application team' field of the associated penetration test assessment request. The assignment type of the penetration test finding is Manual. The assignment rules cannot override the assignment of these penetration test findings.

Starting with v19.0, you can create penetration test assessment requests directly from the Penetration Test Assessment Requests [sn_vul_pen_test_assessment_request_list] table. See Create a penetration test assessment request from existing requests (v19.0) for more information.

Procedure

1. Prior to v19.0, navigate to **All** > **Self-Service** > **Service Catalog** > **Services** > **Penetration Testing Assessment Request**.
2. **Optional:** Alternatively, you can create a request by replicating closed requests.
   All the values from the original request are preserved. Active application vulnerable items (AVIs) are automatically copied to the new request.
3. On the form, fill in the fields.

Penetration Testing Assessment Request form

Field	Description
Number	Unique identifier generated for the penetration test assessment request.
Requested by	Person requesting the assessment of the application.
Parent assessment request	Original penetration testing assessment request used to create the child request. It is created using a closed assessment request. Visible only on the child assessment request form.
Application	Select an application using the search option.
Application type	Select an option from: ○ Web Service (known as API prior to v16.1) ○ Web Application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Thick Client ○ Mobile (If you select Mobile, the Mobile tab is displayed at the bottom of the form with additional fields)
v19.0: Application size	Select the size of the application you want to test. ○ Small ○ Medium ○ Large ○ Standard (select this option if you are not sure of the size)
Assessment type	Select the type of assessment from: ○ Full penetration Test ○ Focused Test ○ Re-test For details, see Configure assessment types for penetration testing.
Purpose of application	Description of the application's functionality.
Technology stack details	Complete technology stack from front-end to back-end, databases, and other key technologies.
Is third-party application?	Confirms if this application is owned by a third-party vendor.
List types of sensitive data accessible from application	Types of sensitive data accessible from the application. For example, PII data, PHI data, and financial data such as credit card numbers.
Authentication type	Specifies if this application uses LDAP authentication, its own native authentication, or other forms of authentication.
Is application in scope for any compliance program?	Specifies if this application impacts any compliance programs such as PCI.
Application team contacts	Members of the application team to be contacted by the ethical hacking team for any questions.
Demo date	Date when this application can be demonstrated.
Product deployment planned on	Planned date to deploy this application in production.
Application version/release planned for deployment	Version of the application planned for production deployment.
v19.0: Application owned by third-party vendor or a joint venture	If you select Yes for this field, the Vendor/Joint Venture Information tab is displayed with additional fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The term 'Clause' might refer to standards for testing that include any agreements that exist between two or more parties.
State	Select a value based on the status of the request.
Assignment group	Group selected to work on the penetration test findings. Can be manually added or edited by an App-Sec Manager.
Assigned to	Individual from the selected assignment group that works on the penetration test findings. Can be manually added or edited by an App-Sec Manager.
Sprint	Displays the sprints with bandwidth available to accommodate the assessment request based on the selected Assessment type field.
Created	Date and time the request was created.
Testing start date	Date and time when the testing begins.
Updated	Date and time the request was last updated.
Testing details	
URLs to test	URLs that must be included in penetration testing.
URLs to exclude	URLs that must be excluded from penetration testing.
Was this application tested previously?	Specifies if this application has already been penetration tested.
Reason for retest	Reason for asking for a penetration test reassessment if the application was tested earlier.
When was the application tested?	Timeframe when the application was penetration tested.
Test account details	Details of the test account that can be used by ethical hacking team for penetration testing.
Application roles	Roles supported by the application for its users.
Most used roles	Most commonly used roles in the application.

4. Select **Submit**.
   An email notification is sent to the ethical hacking team that the request has been created for the relevant application.

Replicate a penetration test request in closed state

Create a penetration test assessment request by replicating a request in Closed state. Active application vulnerable items (AVIs) are copied to the new request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: Application Team

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Penetration Test Assessment Requests** > **All**.
2. Select a request in Closed state.
3. Select **Copy and Create Request**.
   A new request is created and the active AVIs are copied to this request with updated data. To view the original state of the AVIs from the parent request, navigate to the **Penetration Test Findings Snapshot** tab.

Create penetration test findings based on assessment requests (prior to v19.0)

Create penetration test findings based on the penetration test assessment request. These findings are manually-created Application Vulnerability Items (AVIs).

Before you begin
Role required: Ethical Hacker

Procedure

1. Navigate to **All** > **Self-Service** > **Service Catalog** > **Services** > **Penetration Test Assessment Requests**.
2. To create an AVI for a penetration test assessment request, select the relevant request.
3. In the Application Vulnerable Items section, select **New**.
4. On the form, fill in the fields.

Application Vulnerable Item form (penetration test view)

Field	Description
Number	Automatically generated AVI identifier for this record.
Assessment request	Penetration test assessment request with which this AVI is associated.
Vulnerability	Vulnerability selected from the Vulnerability Entries table using the search option.
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see Calculate risk in Application Vulnerability Response automatically. Starting from V16.1, by default the value is the same as the severity of the vulnerability.
Impacts any compliance program?	Confirms whether there is an impact on any compliance program. Choices are Yes and No.
List of compliance programs impacted	This field is displayed when then value of the 'Impacts any compliance program' field is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	set to *Yes*. Lists the impacted compliance programs.
Planned release/fix version	Release by when the penetration test findings must be resolved.
State	Default value is **Open** when the AVI is created. See Application Vulnerable Item (AVI) states for more information on how states are mapped.
Assignment group	Group selected to work on this AVI. Can be manually added or edited by an App-Sec Manager.
Assigned to	Individual from the selected assignment group that works on this AVI. Can be manually added or edited by an App-Sec Manager.
Remediation target	Date by which the AVIs must be remediated, since first identified. This field only appears when applicable. For more information on remediation targets, see Automate remediation target tracking in Application Vulnerability Response.
Created	Timestamp when the application vulnerable item (AVI) was created.
Updated	Timestamp when the application vulnerable item (AVI) was updated.
Opened by	User who created this penetration test finding.
Security team contact	Point of contact in the ethical hacking team.
Short description	Brief explanation of the penetration test finding.
Details	
Technical details	Technical details of the penetration test finding.
Impact	Assessment of the impact of the penetration test finding.
Steps to reproduce	Document the steps to reproduce and review the penetration test finding.
Recommendation	Record the recommended actions in this field.
Notes	
Work notes	Add notes to communicate information about state transitions and other field updates.
V16.1: Affected URLs	Further information related to the affected URLs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
V16.1: Affected parameters	Further information related to the affected parameters.
V16.1: Affected functionalities	Further information related to the affected functionalities.

5. To save the form, select **Submit**.

Create an application vulnerability entry

Create an application vulnerability entry for the vulnerability specified for the penetration test finding. Application vulnerabilities are vulnerabilities on the custom software applications.

Before you begin

Role required: Ethical Hacker

About this task

Application Vulnerability Response relates a vulnerability to an application to create the penetration test finding. These findings are manually-created application vulnerable items (AVIs). You can reuse an existing entry or create one manually for each vulnerability during penetration testing.

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Libraries** > **Third-Party**.
2. On the Application Vulnerability Entries page, select **New**.
3. On the form, fill in the fields.

Application Vulnerability Entry form (Penetration test view)

Field	Description
ID	Identifier for this vulnerability entry.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see Map the severity of an application vulnerable item automatically.
Primary CVE	Reference to the Common Weakness Enumeration element that this vulnerability best fits into.
Category name	Classification provided by the third-party integration. Aids in assignment.
Vulnerability Details	
Attack vector	Most vulnerable attack vector for this vulnerability.
Attack complexity	Metric that describes the conditions beyond the attacker's control that must exist to exploit the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Scope	Metric to measure the ability of a software vulnerability to impact resources beyond its means.
Integrity	Metric to measure the impact to the integrity of a successfully exploited vulnerability.
CVSS Vector	Open framework to capture the characteristics and severity of software vulnerabilities.
Privileges required	Level of privileges an attacker must possess before successfully exploiting the vulnerability.
User interaction	Requirement for human interaction to successfully exploit a vulnerability.
Confidentiality	Impact to the confidentiality of the information resources due to a successfully exploited vulnerability. These resources are managed by a software component.
Availability	Impact to the availability of the impacted component resulting from a successfully exploited vulnerability.
CVSS Base Score	Numeric (0-10) representation of the severity of an application vulnerability entry.
Threat	Description of the threat from this vulnerability.
Mitigation description	Description of the steps to mitigate the vulnerability.

4. To save the form, select **Submit**.

Note: AVEs are created in the Application Vulnerability Entry (sn_vul_app_vul_entry) table. The Application Vulnerability Entry table is a child of the Vulnerability Entry (*sn_vul_entry*) table. Hence, the AVEs created are added to the Vulnerability Entry table as well.

Penetration testing workspace

Penetration testing workspace in Application Vulnerability Response helps customers request for penetration test assessment request and track it using the workflow. It enables application owners to assess the security posture of their application. It is the manual testing of an application by the ethical hacking team.

Roles required

Penetration testing requires the following roles:

sn_vul.app_pen_tester: Represents a pen tester who is responsible to create pen test findings as part of the application penetration testing.

sn_vul.app_pen_test_requester: select record for action: sn_vul.app_pen_test_requester.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lifecycle of Penetration Testing

As an application owner, you can request the ethical hacking team for a penetration test assessment of your application. The ethical hacking team acts on this request and creates penetration test findings. These findings are manually created Application Vulnerable Items (AVIs).

The penetration testing workflow covers the penetration testing life cycle from raising the testing request to resolving the findings of the ethical hacking team.

Create a new penetration testing assessment request

Initiate a penetration test assessment request for your web applications, mobile applications, or APIs. These requests are submitted to the ethical hacking team, who then proceed to test these applications and manually report the penetration test findings.

Before you begin

Role required: App-Sec Manager

Procedure

1. Navigate to **Penetration Testing Workspace**.
2. On the **Penetration Testing Assessment Request** form, fill in the fields.
3. Select **Submit**.
   An email notification is sent to the ethical hacking team that the request has been created for the relevant application.
4. Once the form is submitted, the ethical hacking team can **Start Scoping**.
5. Post scoping, the application owner prepares the test environment and the ethical hacking team can **Start testing**.
6. In case you must verify the details in the request from, you can mark the testing phase on hold by selecting the **Put on hold** button.
7. Once the testing is complete, you can view the AVITs under the Penetration Testing Test findings tab.

> **Note:** You can duplicate a request from an existing request. Once duplicated, the AVITs attached to the parent request are moved (not copied) to the duplicated request.

Create penetration test findings based on an assessment questionnaire

Create penetration test findings aligning testing with recognized standards of MASVS questionnaire into the penetration testing workflow. These findings are manually created Application Vulnerability Items (AVIs).

Before you begin

Role required: App-sec Manager

Procedure

1. Navigate to **Penetration Test Findings** tab.
2. Select the published questionnaire based on your application.
3. Review tests and mark the testing phase as completed.
4. Post completion of the above step, close the request.

> **Note:** The preceding steps can be performed by a member of the Ethical hacking team.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Publish the assessment questionnaire

For testing a mobile application, there are certain standards developed by the OAS community to help testers identify the bugs in their products. Navigate to the assessment workspace to create the questionnaire of your choice. Publish them to be able to view in the assessment request form.

Before you begin

Role required: sn_vul.app_pen_test_requester

Roles required for Penetration testing Requester and Tester:

sn_vul.app_manage_pen_test_request:

contains: sn_smart_asmt.assessment_reader sn_smart_asmt:assessment_admin sn_smart_asmt.actor.

sn_vul.app_pen_tester

contains: sn_smart_asmt.assessment_reader sn_smart_asmt:actor.

Note: As part of the Smart Assessment Engine feature, we have added the above roles. These roles are essential for the Penetration testing requester and tester to be able to view and submit the questionnaires.

Procedure

1. Navigate to **Assessment workspace**.
2. There are guidelines inside each questionnaire, review the questionnaires, if necessary change to meet your organization's testing needs following which you can finish the testing. The questionnaire by default follows the MASVS standards. For more info visit:
3. Publish the questionnaires and select the published questionnaire from the list under the testing details section of the Penetration Testing assessment request form.

   Note: Publish the questionnaire to be able to view it on the Penetration Testing request assessment request form.

4. The persona performing testing can then mark the tests as pass or fail or not applicable under the assessment tab of the Penetration Testing request form.

Use an assessment questionnaire

Post creation of the assessment questionnaire, you can use these questionnaires for testing purpose.

Before you begin

Role required: sn_vul.app_pen_tester

Procedure

1. Navigate to **Penetration testing request** form.
2. Follow the guidelines mentioned on the form.
3. Select a **Penetration testing request**.
4. Navigate to the **Assessment tab**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Open the tab, respond to the questionnaire and **Submit**.

> **Note:** The persona assigned to the Penetration testing request can submit it.

Penetration Testing Dashboard

Get an overview of your penetration test requests and manual findings on your personal Penetration Test Dashboard. You can view the progress of your team with in the Penetration Test Workspace.
The dashboard provides you with an overview of penetration test findings, view, and prioritize tests that need your attention, track test findings, and view assignments.

The Pen-test Manager / Ethical Hacking Team lead can identify and analyze the key metrics such as monitoring the penetration test requests, and view the overall progress of their team in the penetration test workspace. The Pen-test Manager / Ethical Hacking Team lead can also view the following insights:

- Overview of manual findings categorized by state and assessment type to inform strategic decision-making.
- Distribution of assigned Penetration tests across individuals for better capacity planning
- Prioritize overdue findings based on their progress to enhance resolution efficiency.
- Understand the landscape of pen-test findings based on critically distribution.

Penetration Dashboard components

Analyze your team's progress and data visually and drive business outcomes with the help of the components on your personal dashboard.

Important Items indicators

View the unassigned emergency release, tests past overview date, unassigned tests and any critical validation pending.

- **Unassigned emergency release**: Indicates the total count of unassigned penetration test requests for the 'emergency release' assessment type.
- **Tests Overdue**: Indicates the total count of tests past due date.
- **Unassigned tests**: Indicates the total count of unassigned tests to the team.
- **Critical Validation Pending**: Indicates the total count of AVITs for all the requests in the "Validation Pending" state.

> **Note:** Select each tile to view the list of items and perform the required tasks.

Penetration Test Requests

View the test requests by state, tests overdue, and tests by release approvals.

- **Test requests by state**: Indicates the number of test requests in these different states of the Penetration Testing cycle. You can view and navigate to the list of test requests in different states by clicking on each colored tile. You can also view the state of these tests for the following six months by selecting the month from the filter drop-down on the top-right section of the tab. Following are the different test request states:
  - Open: Number of test requests open.
  - Scoping in progress:
  - Scoping completed:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Environment preparation:
- Environment ready for testing:
- Testing in progress:
- Full penetration test:
- Bug bounty programs: Incentives ethical hackers with rewards to find and report security vulnerabilities.
- Focused test:
- Executive interest: Report on senior management's engagement and support for critical projects within the organization.
- One-off reviews: Assess specific projects outside regular development and release cycles to evaluate performance and implement improvements.
- Emergency release: Supports emergency releases that are required for rapid software updates to address critical issues like security vulnerabilities.

- **Tests overdue:**: Indicates the test pending from a certain time period. You can select the timeline for which you want to view the due tests, the drop-down options are: **Due Yesterday**,**Due this week**,**Due last week**,**Due last month**, and **Due before last month**.
- **Tests by release approvals**: Indicates approval states for completed tests ready for release. Also, verifies that all necessary checks are completed before deploying new software. You can also view the state of these tests for the following six months by selecting the month from the filter drop-down on the top-right section of the tab.

Findings

Indicates the number of open penetration test findings (AVITs) reported along with the number of AVITs pending validation. You can view and navigate to the list of findings in different states by selecting each colored tile. The following data you can view under this section:

- **Open findings (AVITs) by risk rating**
- **Validation pending for findings (AVITs)**

Team Overview

Indicates the tests assigned to team members for the following six months period. Following are the different states:

- **Scoping in progress**
- **Open**
- **Scoping completed**
- **Environment ready for testing**
- **Testing in progress**
- **Environment preparation**

Understanding compensating controls for risk reduction in Application Vulnerability Response

Compensating controls are the measures taken to reduce the risk posed by vulnerabilities that can't be patched immediately. They can be used to mitigate the likelihood or impact of a successful exploit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The compensating controls feature is available for host & application vulnerabilities only.

Applying compensating controls can help in reducing the risk of a vulnerability.

The following table shows the use cases for compensating controls:

Use cases for compensating controls

Use case	Compensating control
A vulnerability in a web server that enables attackers to execute arbitrary code.	Implement a Web application firewall (WAF) to block malicious requests to the web server.
A vulnerability in an operating system that enables attackers to escalate privileges to root.	Implement an application control to restrict the execution of applications on the host system.
A vulnerability in a database server that enables attackers to access sensitive data.	Implement network segmentation to isolate the database server from other hosts and critical systems.

For more information on compensating controls, see Understanding compensating controls for risk change

Platform Analytics Solutions for Application Vulnerability Response

Platform Analytics Solutions contain prepackaged Platform Analytics content for use with other ServiceNow AI Platform products. This Platform Analytics Solution presents important metrics for analyzing your Application Vulnerability Management process.

Overview

The Performance Analytics for Vulnerability Response content pack is available on the ServiceNow® Store as a separate subscription. The application is not automatically installed with the Vulnerability Response application. The Application Vulnerability Response content pack is a part of the Performance Analytics for Vulnerability Response content pack.

For more information about setting up, installing, and configuring your Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

Key terms

Performance analytics (PA)

Solution that creates management dashboards, reports on KPIs and metrics, and answers key business questions to help increase quality and reduce costs.

Application Vulnerable item (AVI)

An application vulnerability reported by a third-party vulnerability scanner that is present on a configuration item (CI).

PA indicator

Defines a performance measurement taken at regular intervals of an activity, or organizational behavior, for example, Top 10 Applications with the Most Critical Application Vulnerable Items.

PA indicator source

Data sets that filter records from one table or database view, for example, AVI Active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The the My Application Vulnerabilities dashboard tracks the volume, performance, and progress of application vulnerabilities from initial analysis/detection to containment, or remediation.
- View remediation target attainment rates and efficiently determine which application vulnerable items (AVIs) present the most risk to your organization.

Required roles

The following roles and tasks are associated with this Solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Analytics and Reporting Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the indicators, breakdowns, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.

The following dashboards provide a graphical view into AVI activity to help determine remediation plans and status progress. You can focus on the KPIs associated with critical affected applications and high-visibility vulnerabilities.

- The Application Vulnerability Management (PA) dashboard communicates KPIs for vulnerability risk and prevalence, affected applications, remediation trends, and remediation progress. The default for trends is three months but can be changed to 7 day, one month, 3 months, 6 months, YTD, 1 year, or All.
- The the My Application Vulnerabilities dashboard tracks the volume, performance, and progress of application vulnerabilities from initial analysis/detection to containment, or remediation.

> **Note:** The My Application Vulnerabilities dashboard is a subset of the Overview dashboard and only available when a member of the Security Champion user group logs into an instance. For more information on the My Application Vulnerabilities dashboard, see My Application Vulnerabilities dashboard.

Application Vulnerability Management (PA) dashboard

Track the volume, performance and progress of application vulnerabilities from initial analysis and detection to containment or remediation.

Use cases

User	Dashboard use
Vulnerability managers	With the Application Vulnerability Management dashboard, vulnerability management can determine which application vulnerable items (AVIs) present the most risk to their organizations. These dashboards provide a graphical view into AVI activity to help them determine remediation plans and status progress. Focus on the KPIs associated with critical affected applications and high-visibility vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required ServiceNow AI Platform roles, setup, and the dashboard tabs

The Application Vulnerability Management (PA) dashboard is included as a part of the Performance Analytics for Vulnerability Response content pack. The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application. It is available on the ServiceNow® Store as a separate subscription.

For more information about setting up, installing, and configuring your Performance Analytics for Vulnerability Response application, see Install and configure the Performance Analytics for Vulnerability Response [PA] application.

To view the dashboard, as a user assigned to Security Champion, App-Sec Manager, or Developer user groups, navigate to **Application Vulnerability Response** > **Overview**.

Note: The My Application Vulnerabilities dashboard is a subset of the Overview dashboard and only available when a member of the Security Champion user group logs into an instance. For information on the My Application Vulnerabilities dashboard, see My Application Vulnerabilities dashboard.

Starting with version 19.0 of Application Vulnerability Response, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the**Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

The Overview dashboard communicates KPIs for vulnerability risk and prevalence, affected applications, remediation trends, and remediation progress. The default for trends is three months but can be changed to 7 day, one month, 3 months, 6 months, YTD, 1 year, or All.

Breakdown the data in the Application Vulnerability Management dashboard by **Scan Type**, **Application** or **Business unit**. Each of these choices has an additional filter, **Select elements**, to refine your selections. Starting from Application Vulnerability Response v15.0, business and CI applications have been added to the choices for the **Application** filter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

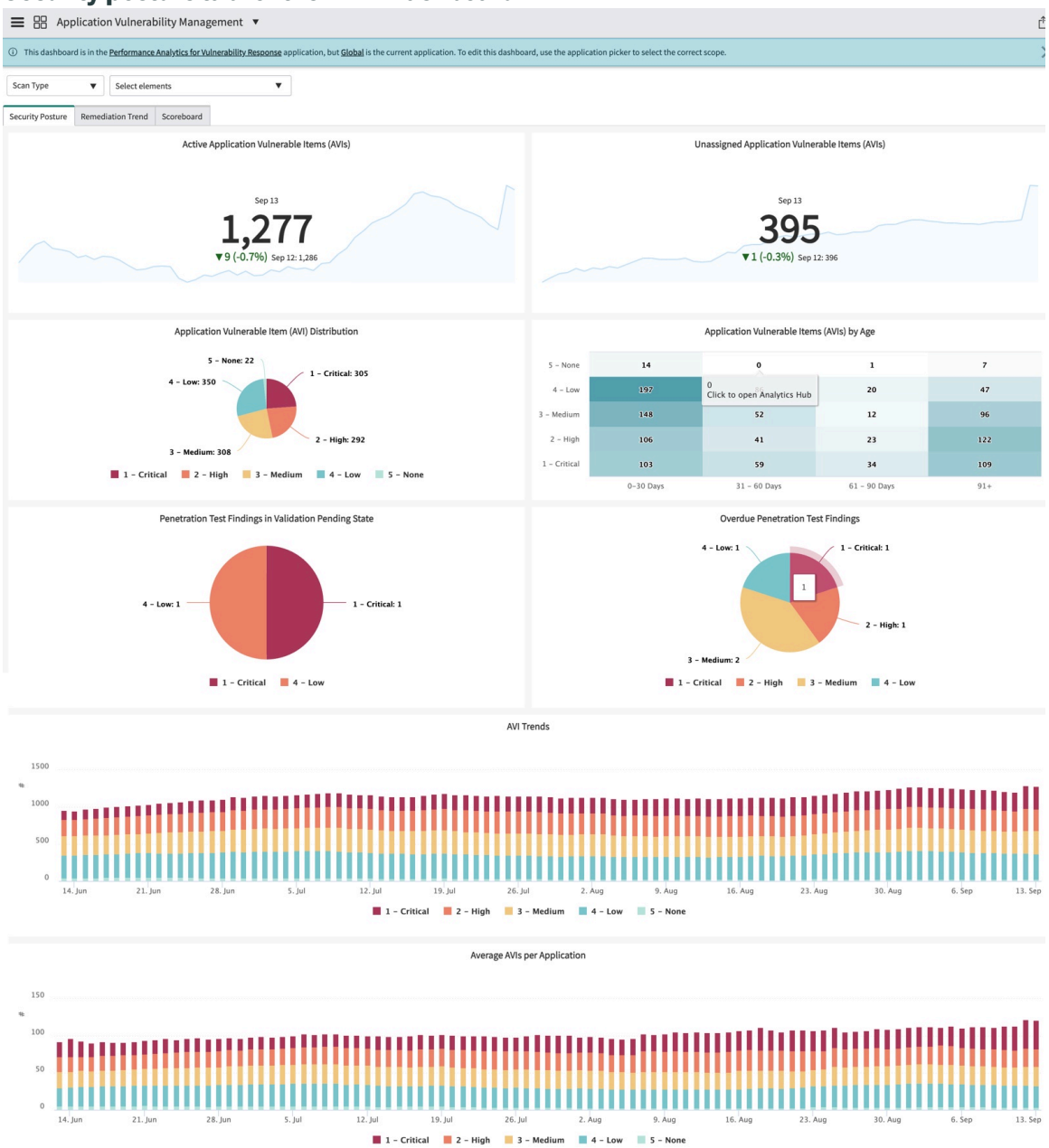
Security Posture tab

The Security Posture tab helps you understand your security posture and the progress of your remediation actions.

Starting from Application Vulnerability Response v15.0, you can view the penetration test findings reports. Penetration test findings are Application Vulnerable Items (AVIs) that are manually created based on the penetration test assessment requests.

Note: The Scan Type for these widgets is Manual.

Security posture tab for the AVM Dashboard



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

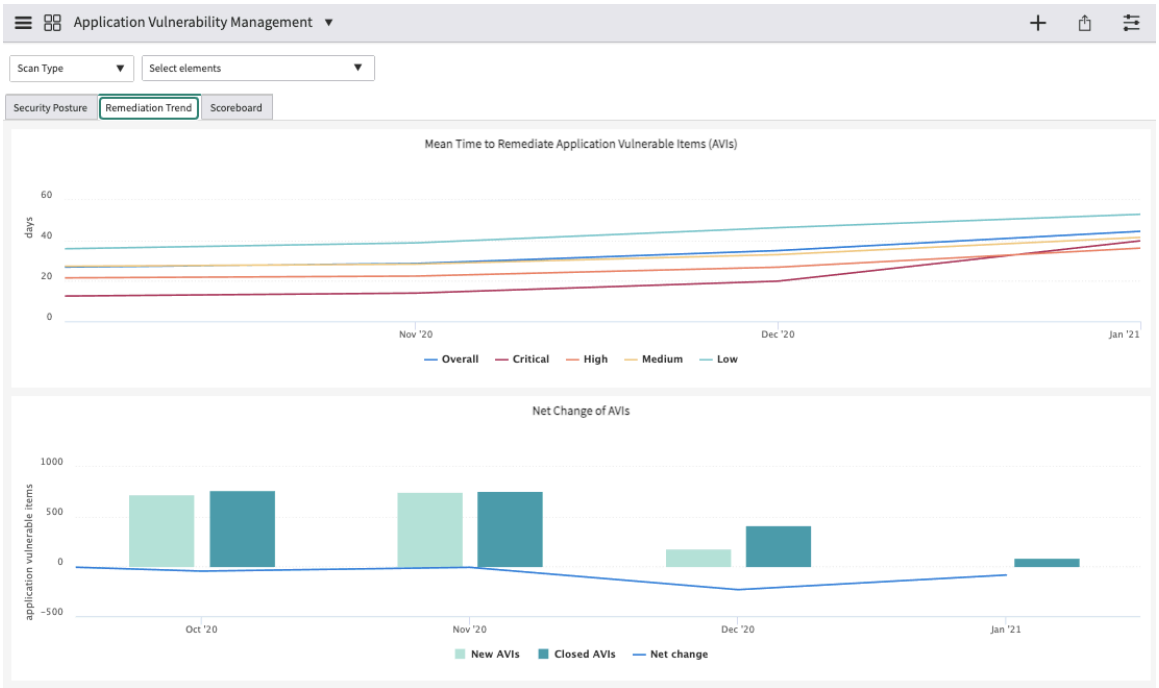
Exceptions tab

This dashboard helps you understand where your organization is taking risk due to potentially excessive deferrals and reconsider remediation options.

You can view Deferred Application Vulnerable items by Reason, Expiring Deferral Requests for AVIs, Exceptions for Critical Application Vulnerable Items by Assignment Group, AVI Exception Requests by Requester.

Remediation Trend tab

The Remediation Trend tab helps you understand the progress of your remediation actions.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

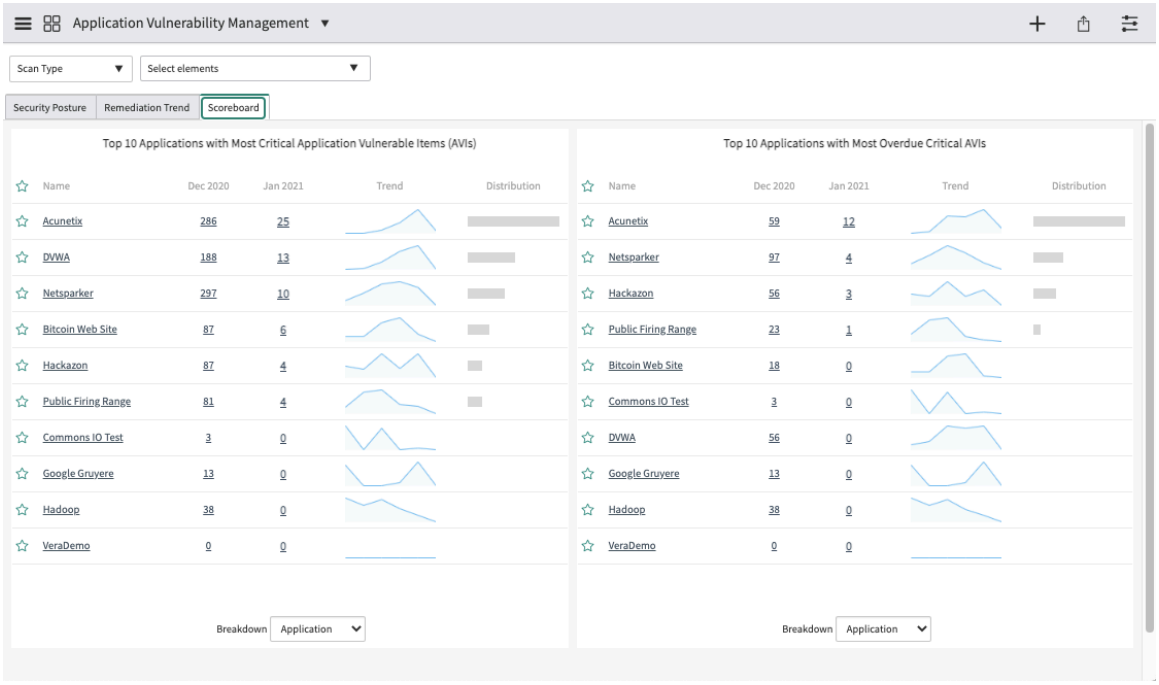
Scoreboard tab

The Scoreboard tab helps you understand the progress of your remediation actions, and which AVIs need the most assistance with their completion.

Scan Type elements:

- Dynamic: Use only metrics from dynamic data import
- Static: Use only metrics from static data import

You can choose either or both.



Indicators

Mean time to remediate Low AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 4 - Low]] / [[Closed Application Vulnerable Items > Risk Rating = 4 - Low]]`. Goal is to minimize.

Application Releases

It is the count distinct on applications from AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Application Vulnerable Items

It is the count on app vul items AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Average AVIs per application

`[Active Application Vulnerable Items]] / [[Application Releases]]`. Goal is to minimize.

Unassigned VIs

It is the count on indicator source AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Mean time to remediate AVIs

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

`[[Summed Duration of Closed Application Vulnerable Items]] / [[Closed Application Vulnerable Items]]`. Goal is to minimize.

Mean time to remediate High AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 2 - High]] / [[Closed Application Vulnerable Items > Risk Rating = 2 - High]]`. Goal is to minimize.

Closed Application Vulnerable Items

It is the count on indicator source AVI.Closed, which is using the table: sn_vul_app_vulnerable_item. Goal is to maximize.

Mean time to remediate Critical AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 1 - Critical]] / [[Closed Application Vulnerable Items > Risk Rating = 1 - Critical]]`. Goal is to minimize.

New Application Vulnerable Items

It is the count on indicator source AVI.New, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Mean time to remediate Medium AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 3 - Medium]] / [[Closed Application Vulnerable Items > Risk Rating = 3 - Medium]]`. Goal is to minimize.

Net change in VIs

`[[New Application Vulnerable Items]] - [[Closed Application Vulnerable Items]]`. Goal is to minimize.

Summed Duration of Closed Application Vulnerable Items

It is the count on indicator source AVI.Closed, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Critical Overdue Application Vulnerable Items

It is the count on data source AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Critical Application Vulnerable Items

It is the count on indicator source Applications with active AVIs, which is using the table: sn_vul_analytics_app_ci_dept_bu. Goal is to minimize.

Breakdowns

- Age
- Age Closed
- Application
- Business Unit
- Risk Rating
- Scan Type

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data visualizations

Security Posture

Name	Type	Description
V15.0: Penetration Test Findings in Validation Pending State	Pie Chart 	Penetration test findings in Resolved state, but with validation pending, grouped by risk rating.
V15.0: Overdue Penetration Test Findings	Pie Chart 	Critical penetration test findings that have missed their remediation target date, grouped by risk rating.
Active Application Vulnerable Items (AVIs)	Single Score 	Number of active (non-closed) application vulnerable items (AVIs).
Unassigned Application Vulnerable Items (AVIs)	Single Score 	Number of active application vulnerable items (AVIs) without an assignment group.
Application Vulnerable Item (AVI) Distribution	Pie Chart 	Distribution of all active application vulnerable items (AVIs) grouped by risk rating.
Application Vulnerable Items (AVIs) by Age	Heatmap 	Number of active application vulnerable items (AVIs) grouped by risk rating and age (in days).
AVI trends	Trend 	Trend of active application vulnerable items (AVIs) grouped by risk rating.
Average AVIs per application	Trend 	Trend of average application vulnerable items (AVIs) per application, grouped by risk rating.

Remediation Trend

Name	Type	Description
Mean time to Remediate Application Vulnerable Items (AVIs)	Line	Trend of the average remediation time for application vulnerable items (AVIs) by risk rating.
Net change of AVIs	Trend 	Trend of new application vulnerable items (AVIs) detected vs closed by month.

Scoreboard

Name	Type	Description
Top 10 Applications with Most Critical Application Vulnerable Items (AVIs)	Score card and Distribution Bar 	Applications with most number of critical application vulnerable items (AVIs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scoreboard (continued)

Name	Type	Description
Top 10 Applications with Most Overdue Critical Application Vulnerable Items (AVIs)	Score card and Distribution Bar 	Applications with the most number of active application vulnerable items (AVIs) that are past their remediation target dates.

My Application Vulnerabilities dashboard

This dashboard presents important metrics for analyzing your Application Vulnerability Management process, such as viewing remediation target attainment rates.

Required ServiceNow AI Platform roles and viewing the dashboard

Note:

- This dashboard is part of the Application Vulnerability Response content pack. The Application Vulnerability Response content pack is part of the Performance Analytics for Vulnerability Response content pack.
- The Performance Analytics for Vulnerability Response content pack is available on the ServiceNow® Store as a separate subscription.
- The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application.

The My Application Vulnerabilities dashboard is available only when a member of the Security Champion user group logs into an instance. For information on the Overview dashboard, see Application Vulnerability Management [PA] dashboard.

To view the dashboard, navigate to **Application Vulnerability Response** > **My Application Vulnerabilities**.

Starting with version 19.0 of Application Vulnerability Response, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the**Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

View reports that show trending data over time. View trends of important metrics on a regular schedule to analyze your overall business processes and identify areas of improvement.

The My Applications Vulnerabilities dashboard is included with the Performance Analytics for Vulnerability Response content pack. The Performance Analytics for Vulnerability Response content pack is not automatically installed with the Vulnerability Response application. It is available on the ServiceNow® Store as a separate subscription.

Use cases

User	Dashboard use
IT specialists, remediation owners, or analysts who remediate vulnerabilities assigned to them or to a group they belong to.	A Security Champion uses the My Application Vulnerabilities dashboard to track the volume,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User	Dashboard use
	performance, and progress of remediation for application vulnerabilities. Efficiently determine which application vulnerable items (AVIs) present the most risk to your organization. These dashboards provide a graphical view into AVI activity to help determine remediation plans and status progress. You can focus on the KPIs associated with critical affected applications and high-visibility vulnerabilities. Quickly gain insight into your vulnerability exposure and security posture. Track from initial analysis and detection to containment, or remediation.

My Application Vulnerabilities [PA] dashboard tabs

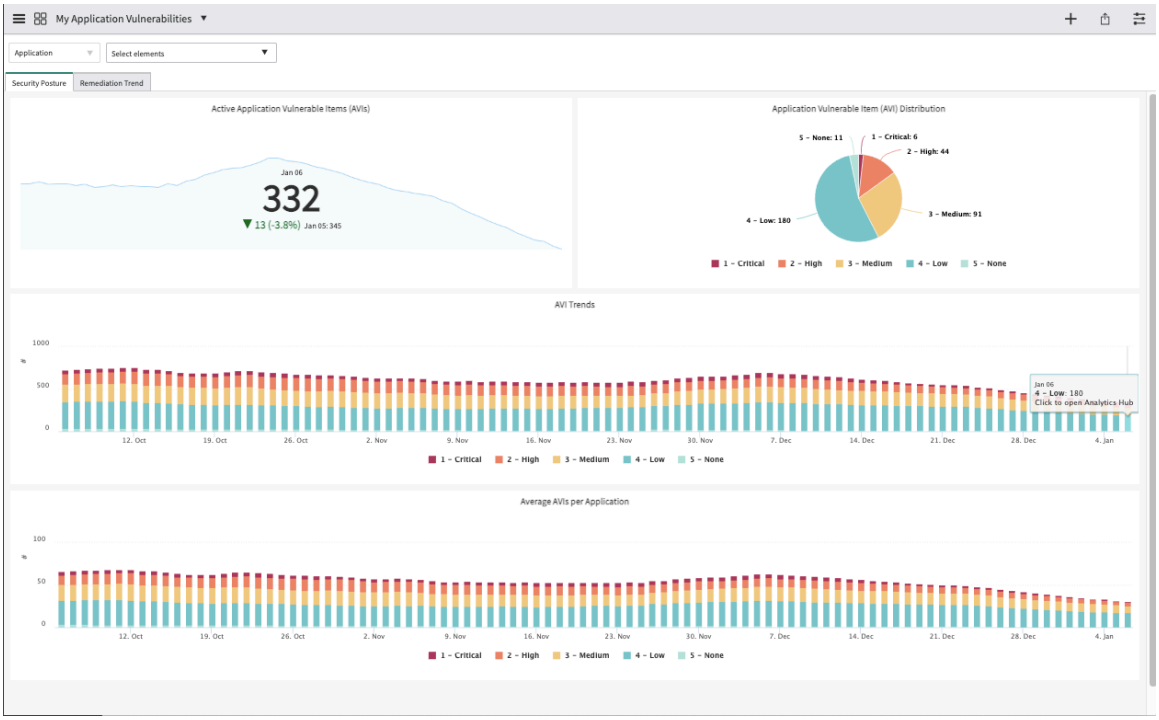
The My Application Vulnerabilities dashboard communicates KPIs for vulnerability risk and prevalence, affected applications, remediation trends, and remediation progress. The default for trends is three months but can be changed to 7 day, one month, 3 months, 6 months, YTD, 1 year, or All.

Data is broken down in the dashboard by **Application**. Use the **Select elements** list to refine your selections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

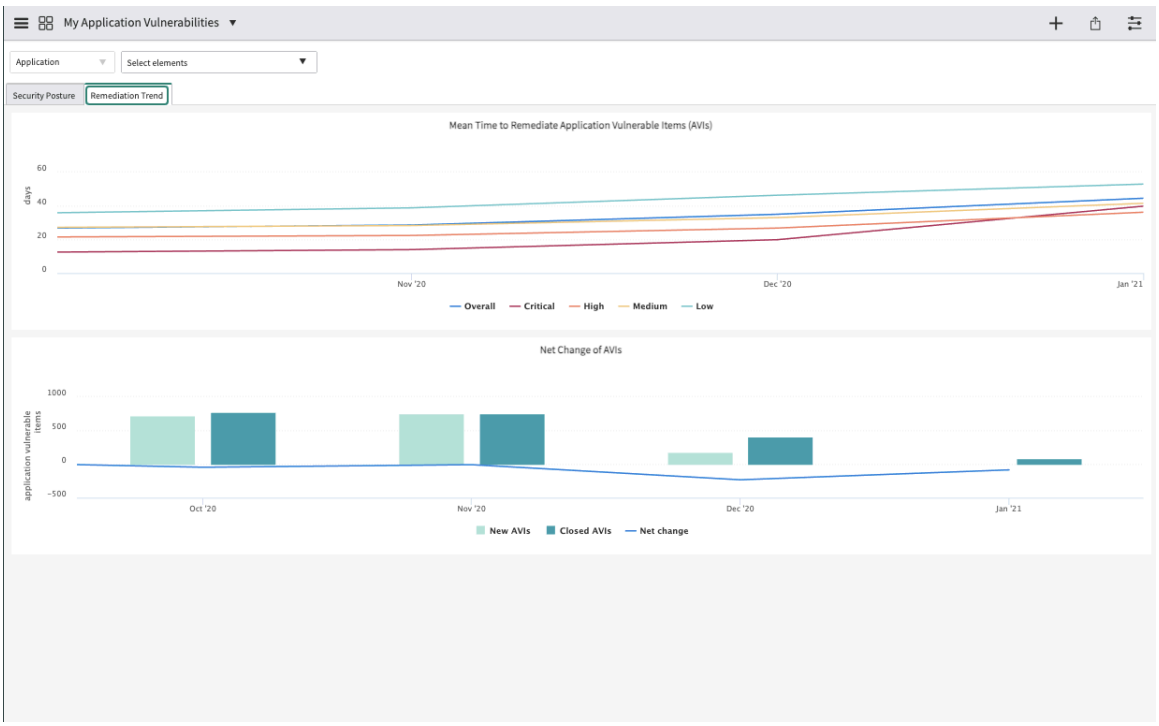
Security Posture tab

The Security Posture tab helps you understand your security posture and the progress of your remediation actions. Breakdown the data in the Application Vulnerability Management dashboard by **Scan Type, Application** or **Business unit**. Each of these choices has an additional filter, **Select elements**, to refine your selections.



Remediation Trend tab

The Remediation Trend tab helps you understand the progress of your remediation actions.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Indicators

Mean time to remediate Low AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 4 - Low]] / [[Closed Application Vulnerable Items > Risk Rating = 4 - Low]]`. Goal is to minimize.

Application Releases

It is the count distinct on applications from AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Application Vulnerable Items

It is the count on app vul items AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Average AVIs per application

`[Active Application Vulnerable Items]] / [[Application Releases]]`. Goal is to minimize.

Unassigned VIs

It is the count on indicator source AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Mean time to remediate AVIs

`[[Summed Duration of Closed Application Vulnerable Items]] / [[Closed Application Vulnerable Items]]`. Goal is to minimize.

Mean time to remediate High AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 2 - High]] / [[Closed Application Vulnerable Items > Risk Rating = 2 - High]]`. Goal is to minimize.

Closed Application Vulnerable Items

It is the count on indicator source AVI.Closed, which is using the table: sn_vul_app_vulnerable_item. Goal is to maximize.

Mean time to remediate Critical AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 1 - Critical]] / [[Closed Application Vulnerable Items > Risk Rating = 1 - Critical]]`. Goal is to minimize.

New Application Vulnerable Items

It is the count on indicator source AVI.New, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Mean time to remediate Medium AVIs

`[[Summed Duration of Closed Application Vulnerable Items > Risk Rating = 3 - Medium]] / [[Closed Application Vulnerable Items > Risk Rating = 3 - Medium]]`. Goal is to minimize.

Net change in VIs

`[[New Application Vulnerable Items]] - [[Closed Application Vulnerable Items]]`. Goal is to minimize.

Summed Duration of Closed Application Vulnerable Items

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

It is the count on indicator source AVI.Closed, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Critical Overdue Application Vulnerable Items

It is the count on data source AVI.Active, which is using the table: sn_vul_app_vulnerable_item. Goal is to minimize.

Critical Application Vulnerable Items

It is the count on indicator source Applications with active AVIs, which is using the table: sn_vul_analytics_app_ci_dept_bu. Goal is to minimize.

Breakdowns

- Age
- Age Closed
- Application
- Business Unit
- Risk Rating
- Scan Type

Data visualizations

Security Posture

Name	Type	Description
Active Application Vulnerable Items (AVIs)	Single Score	Number of active (non-closed) application vulnerable items (AVIs).
Application Vulnerable Item (AVI) Distribution	Pie Chart	Distribution of all active application vulnerable items (AVIs) grouped by risk rating.
AVI trends	Trend	Trend of active application vulnerable items (AVIs) grouped by risk rating.
Average AVIs per application	Trend	Trend of average application vulnerable items (AVIs) per application, grouped by risk rating.

Remediation Trend

Name	Type	Description
Mean time to Remediate Application Vulnerable Items (AVIs)	Line	Trend of the average remediation time for application vulnerable items (AVIs) by risk rating.
Net change of AVIs	Trend	Trend of new application vulnerable items (AVIs) detected vs closed by month.

Aggregated reports framework for Application Vulnerability Response

Using the aggregated reports framework, you can create reports for the data that involves complex and long-running on-the-fly queries for better performance.

The aggregated reports framework improves the performance by:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- using lesser resources and rendering reports faster,
- aggregating the data and reusing aggregations and breakdowns (Group By) and
- reducing the queries to the database

When you have more than one million application vulnerable items (AVITs), use the aggregated reports framework alongside the standard reports.

Required roles

The following roles and tasks are associated with this solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Platform Analytics Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the aggregations, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.
- Admin (sn_vul_cmn.admin): Create aggregations.
- VR write(sn_vul_cmn.write): Edit the data in the Aggregations and Aggregated Results.
- VR read (sn_vul_cmn.read): Review the data in the Aggregations and Aggregated Results.
- Vulnerability analyst (sn_vul.vulnerability_analyst): Review Aggregated Results.

Related topics

Configure an aggregation for source data

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Create a report using an aggregation

Application Vulnerability Response references

Reference topics containing information about tables, roles, and properties installed with the Application Vulnerability Response application.

For details, see:

- Application Vulnerability Response user groups and roles
- Components installed with Application Vulnerability Response
- Application Vulnerable Item (AVI) states
- Scanned application fields
- Application Vulnerable Item fields
- Application Vulnerability fields
- Penetration testing states

Application Vulnerability Response user groups and roles

Before you can successfully remediate vulnerabilities with Application Vulnerability Response (AVR), you must assign users to user groups.

Roles define what you and your groups can see and do in Application Vulnerability Response, Performance Analytics for Vulnerability Response, and third-party integrations with Application Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User groups

Following are the default user groups supporting Application Vulnerability Response:

- App-Sec Manager: Contains security managers. Starting from Application Vulnerability Response v15.0, it will also contain application owners who manage the penetration test assessment requests.
- Security Champion: Contains liaisons between the development group and security managers.
- Developer: Contains individual contributors.
- V15.0: Ethical Hacker: Contains members of the ethical hacking team who perform penetration testing of applications.

The system admin [admin] role is required to assign users to the Application Vulnerability Response default user groups, using the User Administration module,

Note:

Assigning AVR users to the Application Vulnerability Response user groups for Application Vulnerability Response is not available in the Vulnerability Response Setup Assistant feature. Only Vulnerability Response roles are assigned there.

The following table lists the available Application Vulnerability Response user groups and the roles associated with them. Use this table to determine which users should be assigned which groups.

User Group	Roles in this group
Security Champion Members of this group can: • Read and write application vulnerable items (AVIs) assigned to you. • Assign an AVI, that is assigned to you, to another individual or group.	• cmdb_read • canvas_user • sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul_cmn.smart_assessment_actor (If the sn_smart_assessment_designer is installed) • sn_vul.app_pen_test_requester • sn_vul.app_edit_effort • sn_sec_cmn.read • sn_sec_cmn.read_approval_rules • sn_vul.app_pa_sc_view
App-Sec Manager Members of this group can: • Read, write, delete, and all operations on application remediation task rules. • Read and write all AVIs.	• sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User Group	Roles in this group
• Configure AVR by create and manage rules, calculators, and severity maps. • Configure integrations. • Delete AVIs. • Assign AVI to individuals or groups. • Manage applications. • Allows access to the Application module. • Schedule, configure, execute integration. • Read and execute integrations. • View AVR Performance Analytics dashboards and reports. • V15.0: Manage penetration test assessment requests.	• sn_vul.app_configure_integrations **Note:** By default, this role contains granular roles for third-party integration configuration. To define or edit an App-Sec Manager user group by single or specific integrations, see Vulnerability Response personas and granular roles. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Version 13.0: sn_vul.app_manage_app_sc • Version 12.0 only: sn_vul.app_read_application_release [Removed in v12.1. Do not use] • sn_sec_int.admin • Version 13.0: pa_power_user • pa_viewer **Note:** Starting with Vulnerability Response v13.0, pa_viewer is included in pa_power_user and no longer needed by itself. • V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
Developer Members of this group can: • Read and write AVR records assigned to you. • Assign an AVI, that is assigned to you, to another individual or group.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0: Ethical Hacker Members of this group can:	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User Group	Roles in this group
• Configure default assignment group and assignee for penetration test assessment requests. • Manage penetration test findings. • Manage penetration test assessment requests. • View application vulnerable items. • Update assignment for application vulnerable items.	• V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits • V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

Assign users to user groups in Application Vulnerability Response

Assign users to groups using the User Administration module in your instance.

Before you begin

Role required: admin

Procedure

To assign or remove a user from a group:

a. Navigate to **Administration** > **Groups**.

b. Locate and open the appropriate group, for example, **App-Sec Manager**.
The group record is displayed.

c. Select the **Group Members** tab.
The current members of the group are displayed.

d. Click **Edit**.
The Edit members form is displayed.

e. From **Collection** list, select users to add to or remove from the group.

f. Once all users have been added to the **Group Members List** or removed, click **Save**.
You are returned to the **Group Members** tab.

g. Click **Update** to save your changes and return to the Groups list.

Related topics

Components installed with Application Vulnerability Response

Components installed with Application Vulnerability Response

Several types of components are installed with activation of the Application Vulnerability Response feature, including tables, user roles, and scheduled jobs.

Starting with v24.0.6 of Application Vulnerability Response, the most frequently used system properties are now accessible within the Application Vulnerability Response application. To view these system properties, navigate to **All**Application Vulnerability Response**Properties**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Roles installed

Granular roles in Application Vulnerability Response are assigned to specific User Groups, by default.

Note: Using granular roles outside these user groups requires coding and advanced Application Vulnerability Response or ServiceNow expertise.

Role title [name]	Description	Contains roles
V20.0: sn_vul.app_manage_auto_exception_rule	Create, update, delete, and cancel (deactivate) exception rules.	sn_vul.app_read_auto_exce
sn_vul.app_manage_group_rules	Read, write, delete, and all operations on application remediation task rules.	• sn_vul.app_read_all • sn_vul.app_read_group_r
V20.0: sn_vul.app_exception_approver	Approves exception rules and exception rule extension requests. Starting from v20.0, the granular role, sn_vul.app_read_all, has been removed for this role so that you can access the application vulnerable items and remediation tasks assigned to you and your group instead of all the application vulnerable items and remediation tasks.	• sn_vul.app_read_auto_ex • sn_vul.view_manager_wor
sn_vul.app_false_positive_approver	Approves or rejects false positive requests.	sn_vul.view_manager_works
sn_vul.app_read_assigned	View application vulnerable items (AVIs) assigned to you in both the Classic UI and IT Remediation Workspace. **Important:** Starting with v24.0 of Vulnerability Response, the sn_vul.app_read_assigned role has the privilege to access the IT Remediation Workspace.	sn_vul.view_rem_workspace
sn_vul.app_read_all	View all AVIs and related information in both the Classic	sn_vul.view_manager_works

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	UI and Vulnerability Manager Workspace. **Important:** Starting with v24.0 of Vulnerability Response, the sn_vul.app_read_all role has the privilege to access the Vulnerability Manager Workspace.	
sn_vul.app_write_assigned	Update AVIs assigned to you.	
sn_vul.app_write_all	Update all AVIs and related information.	
sn_vul.app_update_assignment_group	Update AVI Assignment group.	**Note:** When used outs of the default user grou requires sn_vul.app_wri sn_vul.app_write_assign
sn_vul.app_update_assigned_to	Update AVI assignee.	**Note:** When used outs of the default user grou requires sn_vul.app_wri sn_vul.app_write_assign
sn_vul.app_configure_integrations	Configure third-party integrations.	sn_vul.app_read_all sn_vul.app_read_integration sn_sec_int.admin sn_vul_veracode.configure_ sn_vul.configure_nvd_admi **Note:** To define or edi Sec Manager user grou single or specific integra Vulnerability Response granular roles.
sn_vul.app_read_integrations	View all third-party integrations.	
sn_vul_veracode.configure_integration	Define, update, and delete Veracode integrations.	
sn_vul.app_manage_assignment_rules	Define, update, and delete AVI assignment rules.	sn_vul.app_read_all sn_vul.app_read_assignmer
sn_vul.app_read_assignment_rules	View assignment rules.	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
sn_vul.app_manage_remediation_target_rules	Define, update, and delete AVI remediation target rules.	sn_vul.app_read_all sn_vul.app_read_remediatio
sn_vul.app_manage_risk_score_configurations	Define, update, and delete AVR calculators and risk rules.	sn_vul.app_read_all sn_vul.app_read_risk_score sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	View AVR calculators and risk rules.	
sn_vul.app_manage_applications	View, update, and delete application records.	
sn_vul.app_manage_app_sc	Gives a Security Champion the ability to add or remove themselves from the Scanned Application related list.	
sn_vul.app_pa_sc_view	Provides relevant view to the specific Security Champion.	
sn_vul.app_manage_app_vul_permissions	[internal] Used by sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Update mapping to normalized severity.	sn_vul.app_read_normalize
sn_vul.app_read_normalized_severity [Removed in v12.1. Don't use.]	View normalized severity records.	
sn_vul.app_read_application_release	View application release records.	
sn_sec_int.admin	Provides access to integrations.	
pa_power_user	Provides access to reports	pa_viewer
sn_vul.app_sec_manager	Prioritizes and manages application vulnerable items.	
sn_vul.app_developer	Developer responsible for fixing the application vulnerabilities.	
sn_vul.app_create_watch_topic	Create Watch Topics for application vulnerabilities.	
sn_vul.app_read_watch_topic	Read Watch Topics for application vulnerabilities.	
sn_vul.app_edit_watch_topic	Edit Watch Topics for application vulnerabilities.	
sn_vul_blackduck.configure_integration	Configure third-party integrations.	sn_vul_blackduck.configure

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled jobs installed

For Vulnerability Response shared scheduled jobs see, Components installed with Vulnerability Response.

Scheduled job	Description
Associate existing AVIs with Auto Exception Rule	Evaluates application vulnerable items for matches to exception rules.
Populate Entry and CVE M2M	Makes existing records consistent with multiple CWE records. Run once after upgrade to populate then disable.
Resync primary CWE	For customized primary CWE calculations. Run once after upgrade to resync then disable.
Rollup application vulnerable item values to vulnerability and group	Calculates vulnerabilities and group roll ups for application vulnerable items. **Note:** Starting with v23.0 of Application Vulnerability Response, the scheduled job is enhanced to create background jobs with multithreading capabilities. This upgrade involves segmenting the job into several smaller child jobs, which are executed either in parallel or concurrently. This modification enables processing of multiple records simultaneously, thus significantly speeding up the overall task.
Black Duck Project List Integration	Pulls and ingests data into the Black Duck projects table.
Black Duck Application List Integration	Imports applications into discovered applications table for all the project versions available with Black Duck Integration in projects table.
Black Duck Application Vulnerable Item Integration	Ingests vulnerable items into ServiceNow application based on the vulnerabilities detected by scanners for every discovered application in the system.

Tables installed

Table	Description
Application Release [sn_vul_app_release]	Contains application version information.
Version 13.0:	Contains the Application Vulnerability Response Security Champion group records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Application Security Champions [sn_vul_app_m2m_app_sc]	
Application Vulnerability Entry [sn_vul_app_vul_entry]	Contains application vulnerability entries.
Application Vulnerability Integration [sn_vul_app_integration]	Contains Application Vulnerability Response integration records.
Application Vulnerability Scan Location [sn_vul_app_vul_scan_location]	Contains third-party scan location information.
Application Vulnerability Scan Summary [sn_vul_app_vul_scan_summary]	Contains third-party scan summary information.
Application Vulnerable Item [sn_vul_app_vulnerable_item]	Contains AVI records. Starting with v19.0, the following columns are added for Software Bill of Materials: • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Scanned Application [sn_vul_app_scanned_application]	Contains application information.
State Map [sn_vul_app_state_map]	Contains state mapping from third-party integrations to application vulnerable item (AVI) states.
Vulnerability CWEs [sn_vul_m2m_entry_cwe]	Links CVE data to application vulnerable entries.
Application Remediation Task Manifest sn_vul_app_rt_manifest	Any updates on remediation task are done by using this manifest table by scheduled jobs.
Application Remediation Task	Contains application remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
sn_vul_app_vulnerability	
Application Remediation Task Item sn_vul_app_m2m_vul_group_item	M2M table between AVI and application remediation tasks.
Version 21.0: Application Vulnerable Items sn_vul_app_vulnerable_item	Contains AVI records.
Version 21.0: Package [sn_vul_app_package]	Contains application package details.
Version 21.0: Licenses sn_vul_app_license	Contains application licenses.
Version 21.0: Application Remediation Tasks sn_vul_app_vulnerability	Contains application remediation tasks.
sn_vul_blackduck_config	Contains Black Duck integration configuration details.
sn_vul_blackduck_project	Contains details of the projects coming from Black Duck.
sn_vul_blackduck_project_import	Import set table for the Black Duck project ingestion.
sn_vul_blackduck_app_import	Import set table for the Black Duck application ingestion.
sn_vul_blackduck_avit_import	Import set table for the Black Duck AVIT ingestion.

Application Vulnerable Item (AVI) states

Application Vulnerability Response offers a state model for the status of your application vulnerable items (AVIs), at any given time. Knowing how each state relates to and affects each other helps you to determine when and how to remediate your AVIs.

Application Vulnerable Item states

Understanding how states work helps with creating or editing application vulnerable item (AVI) rules. AVIs have several possible states that are mapped from imported Remediation status from the third-party integration. In an AVI, the **State** field is read-only.

Application Vulnerability Response state flow diagram

State	Description
Open	State upon creation. From this state you can: **V16: Get More Details**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerability Response state flow diagram (continued)

State	Description
	Get the following information about an AVI imported from Fortify: • Vulnerability summary • Vulnerability explanation • Recommendation • References • Request • Response **V16: Mark as false positive** Mark an item as false positive if the scanner reports that a vulnerability exists in the system, but in reality there is no vulnerability. **V16: Request exception** Request an exception, a reopen (Until) date, a reason, and optionally, provide addition information. Defers the remediation of the item until the date till which an exception is requested. **V15: Close** Select the Closed state, a reason from the Close Vulnerable Item dialog box, and provide addition information. Closes the AVI. **V15: Resolve** Mark an open AVI as Resolved to move it to a resolved state. You must add resolution notes in the Resolve Application Vulnerable Item dialog box.
Deferred	**V15:** This is triggered by the **Request Exception** option. As part of the approval workflow, the Deferred state is In Review and cannot be closed until approved. From this state you can: **V16: Get More Details** Get the following information about an AVI imported from Fortify:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerability Response state flow diagram (continued)

State	Description
	• Vulnerability summary • Vulnerability explanation • Recommendation • References • Request • Response **Reopen** Transitions a closed or resolved AVI back to an Open state. **Close** Select the Closed state, a reason, and provide addition information. Closes the AVI.
Under Investigation	Select this option from the **State** list. From this state you can: **V20.0** Manually transition a remediation task or AVI record to **Awaiting Implementation**. **V16: Get More Details** Get the following information about an AVI imported from Fortify: • Vulnerability summary • Vulnerability explanation • Recommendation • References • Request • Response **V16: Mark as false positive** Mark an item as false positive if the scanner reports that a vulnerability exists in the system, but in reality there is no vulnerability. **V16: Request exception** Request an exception, a reopen (Until) date, a reason, and optionally, provide addition information. Defers the remediation of the item until the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerability Response state flow diagram (continued)

State	Description
	date till which an exception is requested. **V15: Close** Select the Closed state, a reason from the Close Vulnerable Item dialog box, and provide addition information. Closes the AVI. **V15: Resolve** Mark an open AVI as Resolved to move it to a resolved state. You must add resolution notes in the Resolve Application Vulnerable Item dialog box.
Awaiting Implementation	You can only transition records to this state manually by selecting Awaiting Implementation from AVI and remediation task records in the Under Investigation state. From this state you can: **Open** Transitions AVI back to an Open state. **Under Investigation** Get more information for resolution. Transitions to Under Investigation. **Resolve** Mark an open AVI as Resolved to move it to a resolved state. You must add resolution notes in the Resolve Application Vulnerable Item dialog box. **Close** Select the Closed state, a reason from the Close Vulnerable Item dialog box, and provide addition information. Closes the AVI. In this state, Transition a record into Awaiting Implementation when your research and work on a task is complete and although a fix is ready for implementation, it is not yet available. Set the **Remediation Commitment date** and **Remediation plan** fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerability Response state flow diagram (continued)

State	Description
	After implementation, you resolve or close the records.
Resolved	Triggered from the Resolve button. From this state you can: **V16: Get More Details** Get the following information about an AVI imported from Fortify: • Vulnerability summary • Vulnerability explanation • Recommendation • References • Request • Response **Reopen** Transitions back to an **Open** state. **Close** Select the **Closed** state, a reason, and provide addition information. Closes the group. Notes and Resolution information appear under the **Notes** tab.
Closed	Triggered from the Close button. From this state you can: Reopen: Transitions back to an Open state.

Note: Refer to the Integrating Application Vulnerability Response with other applications for understanding different integrations that sourced the AVI.

Application Remediation Task states

From the creation to closure of an Application Remediation Task, the Application Remediation Task transitions through various states during the entire remediation process.

The state precedence is as follows:

Closed > **Deferred** > **Resolved** > **In Review** > **Awaiting Implementation** > **Under Investigation** > **Open**

The state transition happens as you perform various actions such as Defer, Open, Close, etc.

The actions you can perform on an Application Remediation Task at a specific state is similar to that of a Host Remediation Task. Hence, for more information, see the Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

remediation task states and State roll-up and roll-down scenarios in the Vulnerability Response documentation.

Note: Starting with v23.0 of Vulnerability Response, the **Close** button has been removed to ensure that the closure of the Remediation task is driven by the scanner.

Application Vulnerability Response remediation task rule examples

A example of a remediation task rule example using the condition builder.

A remediation task rule using vulnerability, product model, IP address, and assignment group

1. In the condition builder on a new record, set the condition as **Vulnerability** > **is** and enter a known vulnerability.

   Vulnerabilities are imported from the Nation Vulnerability Database (NVD) and Common Weakness Enumeration (CWE) integrations as described in Configure Application Vulnerability Response.

2. In the Group by section, select **Application Vulnerable item** for the **Group application vulnerable items from** field.
3. In the Using field, select **Assignment group**.

   Use Assignment rules to automatically set the **Assignment group** field for use in your remediation task rule. You can use a rule provided with the application or set up your own assignment rules. See Assign application vulnerable items in Application Vulnerability Response automatically for more information.

4. Select another condition, for example, Application Vulnerable item configuration item in the **Group application vulnerable item from** field, and IP address or product model in the **Using** field.
5. In the Assignment section, for Assign remediation task field by field, select **Group by field**.
6. In the Group by field, select **Assignment group**.

   As described in this section, this selection assigns vulnerable items to various groups based on the conditions you set in the group by section. Although the AVIs share the vulnerability, they're assigned to different groups based on the CI product model or by IP address.

7. Select **Submit** to save your rule.

Scanned application fields

Applications are stored during import under **Administration** > **Discovered Applications** in Application Vulnerability Response.

Scanned Application fields

The imported fields in this table are read-only unless otherwise specified. **Department** and **Support Group** entries can be manually added or edited by an App-Sec Manager.

Field	Description
Name	Imported name of the application.
Version	Imported version of the application, where applicable.
Operational status	Imported operational status of the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Department	Imported department to which the application belongs. If empty, it can be added manually.
Business unit	Imported business unit to which the department belongs. When the **Department** field is filled, this field is automatically filled with the Business unit to which the department belongs. Otherwise, it is left empty and read-only.
Support group	Imported support group to which the application belongs. If empty, it can be added manually.
Description	Imported description of the application.
Last policy compliance check date	Date when the application was last scanned by Veracode for policy compliance. It is used in the chained integrations of Application List integration, where support is available for delta ingestion for applications, by comparing this date to the delta start time of the respective integrations. **Note:** Data is retrieved for applications are pulled from Veracode, whose 'Last policy compliance check date' value is greater than or equal to the 'Start time' (delta_start_time) of the chained integrations.
Related List (visible only to an App-Sec Manager or Security Champion)	
Security champion	Lists the applications associated with a security champion. App-Sec Managers can add or remove members from the list.

Application Vulnerable Item fields

Application vulnerable items (AVITs) are automatically created during third-part vulnerability integration imports.

Application vulnerable item fields

Except for the **Assignment group**, **Assigned to** fields and **Notes**, all other fields in the AVI are read-only.

Field	Description
Number	Automatically generated AVI identifier for this record.
Scan type	Type of scanner that found this AVI. Choices are: • Dynamic • Static • SCA
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see, Calculate risk in Application Vulnerability Response automatically.
Risk score	Calculated amount of risk the AVI poses to your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For more information, see Calculate risk in Application Vulnerability Response automatically.
Remediation commitment date	The date AVITs should be remediated after it is moved into **Under Investigation**. This field only appears if the AVIT is in **Under Investigation**.
Remediation target	Date by which the AVITs should be remediated, since first identified. Only appears when applicable. For more information on remediation targets, see Automate remediation target tracking in Application Vulnerability Response.
Remediation status	Status of the remediation for the AVIT. It is determined by the AVIT with the nearest due date, when applicable. States include: • In-flight • Approaching Target • Past Target
Category Name	Name of the category of the vulnerability.
Vulnerability	ID of the vulnerability associated with this application vulnerable item.
Application release	Version of the application.
Application module	Affected application in DAST scan. Hidden for SAST scans.
Location Version 14.0: SAST	DAST: URL location of the vulnerability within the application. SAST: File path and line number of the vulnerability within the application.
State	This field defaults to **Open** when created. See Application Vulnerable Item (AVI) states for more information on how states are mapped.
Reason	[Only visible when the AIV is in the **Closed** state.] Explanation of the State.
Assignment group	Group selected to work on this AVIT. Can be manually added or edited by an App-Sec Manager.
Assigned to	Individual from the selected assignment group that works on this AVI. Can be manually added or edited by an App-Sec Manager
First found	Date the third-party source first found the application vulnerable item.
Last found	Date the third-party source last found the application vulnerable item.
Closed	[Only visible when the AVIT is in the **Closed** state.] Date the AVI was closed.
Closed by	[Only visible when the AVIT is in the **Closed** state.] Entity that closed the AVIT.
Summary	Imported description of the vulnerability.
Findings	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Read-only data imported from third-party integration.	
Source AVIT ID	Imported identifier for the source AVIT.
Source severity	Imported severity from the source application.
Source target fix date	Imported date by which the source expects the AVIT to be remediated.
Source mitigation status	Imported mitigation status from the source application.
Source remediation status	Imported remediation status from the source application.
Source finding status	[Only visible when populated] Imported issue status from the source application.
SDLC status	Imported Software Development Life Cycle status.
Complies with Policy	Imported compliance status. If not status is provided, this field is set to **Not Applicable**.
Source link	URL to the source AVIT.
Source notes	Imported notes from the source.
Vulnerability summary	Imported summary from the source.
Vulnerability explanation	Imported explanation from the source.
Recommendation	Imported recommendation from the source.
References	Imported references from the source.
HTTP Request/Response (only visible for DAST scans)	
Source request	HTTP request
Source response	HTTP response
Notes	
Remediation Plan	Details for how the AVITs will be remediated. The plan should be implemented by the **Remediation commitment date**. This field only appears if the AVIT is in **Under Investigation**.
Additional comments/Work notes	Any relevant information. Select the text box for Work notes to add information. Starting with Vulnerability Response v20.0, you can add work notes in the Notes section for a deferred application vulnerable item.

Age calculations for an AVIT:

- The Age column in the AVIT list displays the duration (format: Days HH:MM:SS) for which an AVIT is active. The Age value is zero for a closed AVIT.
- The Age closed column in the AVIT list displays the duration (format: Days HH:MM:SS) for which an AVI is active before it is closed. For a AVITs, other than in the Closed state, the Age closed value is zero.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Penetration testing states

Application owners can request penetration test assessment for their applications, and monitor the progress of the ethical hacking team until the request is resolved.

The penetration test assessment request passes through the following transition states until it is resolved.

Stages of the penetration test assessment request

Field	Description
Penetration testing states	
Open	State when the assessment request is created by the application owner.
Scoping	Ethical hacking team assesses the request and the scope of the application.
Environment Preparation	Application owner creates an environment with roles and other information and provides it to the ethical hacking team for testing.
Testing	Ethical hacking team manually tests the application to identify the penetration test findings.
V16.1: Testing In Progress	Ethical hacking team indicates that testing is currently in progress. If this state is selected, the **Testing On Hold** option becomes available on the form.
V16.1: Testing On Hold	This field is displayed only when the Testing In Progress state is selected. Ethical hacking team controls the service level agreements (SLAs) of the penetration test assessment requests by selecting this state, if required. This ensures accurate SLAs are reported.
V16.1: Testing In Review	Ethical hacking team indicates that testing is complete, and is being reviewed by a subject matter expert.
Closed	The ethical hacking team closes the penetration test assessment requests after the penetration test findings are reported. **Note:** Starting from V16.1, you can use the **Copy and Create Request** option on the form to replicate the request in Closed state and create a new request. For details, see Replicate a penetration test request in closed state.
V16.1: Cancelled	Application owner cancels the penetration test assessment request.
V16.1: Draft	Application owner creates a request and saves it as a draft before submitting the request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Stages of the penetration test assessment request (continued)

Field	Description
Application Vulnerable Item states	
Open	When the ethical hacking team identifies and creates the penetration test findings, their status is Open.
Resolved	When the application team resolves the penetration test findings, their status is moved to Resolved. **Note:** If the penetration test finding has been resolved but is yet to be validated by the ethical hacking team, the substate is *Validation Pending*.
Closed	Ethical hacking team validates that the penetration test findings have been resolved and moves the status to Closed.

Managing state mapping for deferrals and false positives in Application Vulnerability Response

You can manage how the **Source** states on application vulnerable items (AVIs) imported by the Veracode Vulnerability Integration and Fortify Vulnerability Integration are mapped in your instance after import.

Starting with v20.0 of Vulnerability Response, you have more options for triaging your imported AVIs with ServiceNow workflows.

When you Configure the Fortify on Demand Vulnerability Integration or the Configure the Veracode Vulnerability Integration, the integration configuration pages provide you with two options to help you manage exceptions and false positives in your instance.

- Manage exceptions in ServiceNow
- Manage false positives in ServiceNow

Role required: App-Sec Manager.

Use case for Exception management

AVIs are imported from these integrations with **Source** states. Upon import, these state are mapped to **Target** and **Target reason** states in your instance, because in some cases there are no exact matches between the source states of your scanner and the states used by your instance.

For example, source states such as **Will Not Fix**, **Remediation Deferred**, **Risk Accepted**, and **Risk Mitigated** from the Fortify on Demand Vulnerability Integration are mapped to the **Deferred** state with a substate of **Risk Accepted** or **Mitigating Control in Place** in your instance.

You have the following options on the configuration pages for these integrations:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Check box selected	Description
Manage exceptions in ServiceNow	Y (by default)	If you leave this option selected, you must request exceptions from AVI records. Imported AVIs marked for the **Deferred** state are triaged with the ServiceNow Exception Management workflow. AVIs with **Source** states that normally are mapped to a **Deferred** state are mapped to the **Target triage state** in the **Open** state.
	N	If you deactivate the check box, you preserve the **Source** states imported from your scanner. These AVIs are mapped to the **Target state** as **Deferred**, and to a **Target reason** state in your instance. They are not triaged by the exception workflow, because they are not mapped to the **Target triage** state and **Target triage reason** states. The **Request Exception** UI action is not available on the AVI record, because the record already in the **Deferred** Target state.

Use case for False positive

For false positives from the Veracode Vulnerability Integration as an aexample, source states such as **False Positive** or **Potential False Positive** are mapped to the **Closed Target state** with a substate of **False Positive**.

Option	Check box selected	Description
Manage false positives in ServiceNow	Y (by default)	If you leave this option selected, you must request a **False Positive** from AVI records. Imported AVIs marked for the **False Positive** or **Potential**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Check box selected	Description
		False Positive states are triaged with the ServiceNow Exception Management workflow. AVIs with **Source** states that normally are mapped to a **Closed Target state** are mapped to a **Target triage** state in **Open**. The **False Positive** UI action is available on the AVI record.
	N	If you deactivate the check box, you preserve the **Source** states imported from your scanner. These AVIs are mapped to the **Target state** as **Closed** and a **Target reason** state in **False Positive** in your instance. They are not triaged by the false positive workflow. The **False Positive** UI action is not available on the AVI record, because the record is already in the **Closed** Target state.

Application Vulnerability Response references

The following terms are used in Application Vulnerability Response.

Application Vulnerable items (AVIs)

Pairings of vulnerability entries and potentially vulnerable applications in your company environment.

Assignment Rules

Rules used to assign AVIs based on your defined criteria.

Common Platform Enumeration (CPE)

A NIST NVD structured naming scheme for information technology systems, software, and packages.

Common Vulnerabilities and Exposures (CVE)

Dictionary of publicly known information-security vulnerabilities and exposures.

Common Weakness Enumeration (CWE)

List of community-developed software weakness types.

Integrations

Scheduled jobs that pull report data from CWE or a third-party system, such as Veracode, to retrieve vulnerability data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If the NIST National Vulnerability Database integration in Vulnerability Response is activated and configured, CVE enrichment is available for CWEs but not required. For information on the NIST National Vulnerability Database integration, see Importing data with the NVD and CWE integrations and managing third-party libraries.

National Vulnerability Database (NVD)

U.S. Government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

Remediation Target Rules

Rules used to assign AVIs target dates for remediation based on your defined criteria.

Vulnerability Calculators

Calculators used to prioritize and categorize application vulnerabilities based on your defined criteria.

Exception rule example for Application Vulnerability Response

An example rule based on a known vulnerability for an exception rule.

Field	Description
Name	A unique name to help you identify its purpose and locate the rule easily, for example, `Veracode-1 cwe-22 exception`.
State	Read-only: Draft
Valid from	Date this rule is active to defer AVIs.
Execution order	Unique order for each exception rule. A lower value precedes a higher one.
Valid to	Date on which the remediation task stops accepting new VIs.
Deferred until	Date until when the remediation tasks and AVIs are deferred. On this date, the AVUL is closed, all the AVIs move out of the task and are reopened. Group rules are reapplied to these AVIs.
Reason	Reason to create this exception rule. Select one from the list, for example, **Fix Unavailable**.
Assignment group	Group assigned for tracking the deferred VIs, for example, APP Sec Manager.
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task. In this example, `Defer AVIs with the vulnerability – Veracode-1-22.`
Condition	Filter conditions to specify which AVIs match this rule. For this example, `Vulnerability is Veracode-1-22`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run. If you leave this option deactivated, your rule runs daily by the scheduled job *Associate existing AVIs with Auto Exception Rule* starting with new data. If you enable the Execute on existing data option, a scheduled job runs one time on the existing data on the **Valid from** date.

Application Vulnerability Response product view

The Application Vulnerability Response (AVR) product ingests the weaknesses and vulnerabilities detected by your application security testing tools and provides a single pane of glass to understand the security posture of all the applications in your environment.

AVR enables you to reduce the risks with the remediation workflows. The objective of this product view is to help you understand how AVR key entities work with the core CSDM framework.

Updated terminology

Starting with AVR v19.0, the following key table and column names have been updated. As a result, you will see references to both the older and newer names in the documentation.

Updated list of terms, table, and field names for AVR

Prior to AVR v19.0	Starting from AVR v19.0
CI lookup rules	Lookup rules
CI lookup rule form	Lookup rule form
CI matching rule	Matching rule
Search on table	Search on CI table
Search on field	Search on CI field
Application release	Discovered applications
Application release table	Discovered applications table
Business criticality	Source business criticality

Prerequisites

Install the latest versions of the following applications:

- Security Support Common
- Vulnerability Response
- Security Integration Framework

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Support Orchestration
- Scanner integrations such as Veracode and Fortify

AVR and CSDM 4.0

Prior to AVR v19.0, when application vulnerabilities were ingested, the application for which the vulnerabilities were ingested were looked up using the CI lookup rules, against the Scanned Applications (sn_vul_app_scanned_application). If the application name record was not there, an entry would be made.

Starting from AVR v19.0, to align with the CSDM 4.0 framework, the Product Model tables are used instead of the Scanned Applications table. If the application has the version, the lookup is against the Software Model table. If there is no version, the lookup is against the Application Model table. Both Application Model and Software Model are child tables of the Product Model table, that is the foundation table in CMDB. The following screenshot explains the Product Model.

System property

To use the CSDM 4.0 product model-based lookup process, set the system property *`sn_vul.use_product_model`* to *`true`*.

System property considerations

System property name	System property value	Lookup target value	Considerations
sn_vul.use_product_model	true	Select the value **Product model**	New users should select the value **Product model** to use the CSDM 4.0 framework's Product model lookup rules.
	false	Select the value **Configuration item**	Existing users can continue using the CI lookup process and the existing **CI lookup rules**.

Note: To set the lookup target value, navigate to the **Lookup Rule** page > **[AVR integration lookup rule]** > **Lookup target** field.

Lookup rules in AVR

In the CSDM 4.0 framework, product model-based lookup rules are used instead of CI lookup rules to create entries into the respective product model classes. Similarly for scripts, you can define the lookup rules within the framework of the CSDM 4.0 model.

Starting from AVR v19.0, while creating a lookup rule, you must define whether you want to use the configuration item or product model approach using the **Lookup target** field. For more information, see Create a CI lookup rule.

Discovered applications

Navigate to **All** > **Discovered Applications**. The Discovered Applications table displays the applications ingested from the scanners. If the system property

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

sn_vul.use_product_model is set to *true*, you can see the corresponding product models for the applications.

AVR considerations

Presence of duplicate CI or product model records

Verify that the system property *sn_vul.use_product_model* has been correctly configured for the lookup process. Ensure that you select either **Configuration item** or **Product model** as the Lookup target while configuring the Lookup rule form.

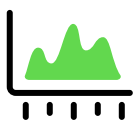
Container Vulnerability Response

The ServiceNow® Container Vulnerability Response application imports container vulnerable items (CVITs) and according to the rules enables you to remediate container vulnerabilities. Vulnerability data is pulled from internal and external sources, such as the National Vulnerability Database (NVD) or third-party integrations.

Request apps on the Store

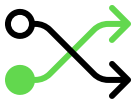
Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Container Vulnerability Response

Explore  Learn about Container Vulnerability Response concepts and features.	**Configure**  Configure Container Vulnerability Response.	**Integrate**  Extend Container Vulnerability Response by integrating with other applications.
Use the Vulnerability Response Workspaces  Learn how to monitor, manage and remediate CVITs in the Vulnerability Manager, IT Remediation, and Vulnerability Assessment Workspaces.	**Remediate**  Learn how to remediate container vulnerabilities.	**Analytics & Reporting**  View Container Vulnerability Response analytics

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Container Vulnerability Response (continued)

Reference	Upgrade Container Vulnerability Response to USEM	
 Get details about Container Vulnerability Response components like fields, tables and properties.	 Upgrade Container Vulnerability Response applications to Unified Security Exposure Management.	

Benefits

The Container Vulnerability Response application provides the following benefits:

- Integrates with third-party container security products, like Prisma Cloud Compute from Palo Alto Networks.
- Imports vulnerability data for the images that are deployed to runtime, and enriches the vulnerability data with runtime contextual information (hosts, Kubernetes clusters, services, and namespaces).
- Provides a list of the references created from vulnerabilities to the relevant Kubernetes entities in the Configuration Management Database (CMDB) using ServiceNow Kubernetes Discovery.
- Offers a comprehensive reporting dashboard, providing insights into the vulnerability and remediation trends.

Key features

The Container Vulnerability Response application manages vulnerabilities detected in the containers. It provides the following features:

- Point to source Docker Image from CVITs instead of running containers.
- Configure granularity of CVITs to track at image, Kubernetes cluster, namespace, or service level.
- Track new image versions to identify fixed vulnerabilities. Any vulnerabilities reported in older versions are automatically resolved in ServiceNow when new image versions are deployed at runtime.
- Track CVITs in Base images separately from Application images to enable independent remediation.
- Raise exception requests or false positive requests, which can be reviewed through a multi-level approver process.
- Define exception rules to defer CVITs automatically.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use cases

Containers are a great way of deploying and scaling applications on multiple environments with less overhead and increased portability. However, vulnerabilities in container images can pose risk to the underlying host and ultimately to the infrastructure where containers have been launched from these images. While there are many container security products that scan container images for vulnerabilities, there are a few considerations and problems associated with remediation of the vulnerabilities. Container Vulnerability Response can help solve various problems or use cases involved in remediating container image vulnerabilities. Explore ways to take advantage of the Container Vulnerability Response module:

Runtime context

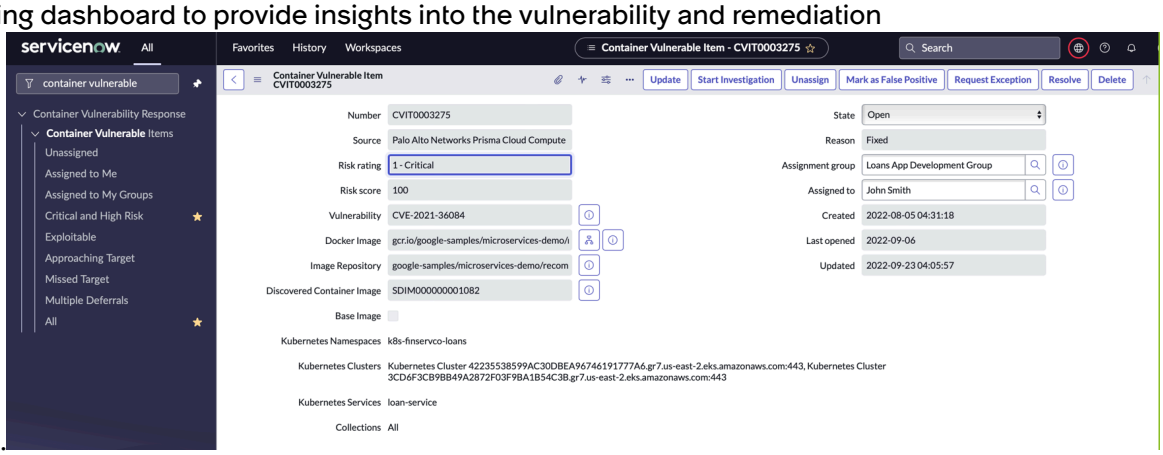
Vulnerabilities in container images can be discovered by scanning the image in the following stages of the application life cycle.

- Stage 1: When images are being built in the CI/CD pipeline.
- Stage 2: When images are published to the registry
- Stage 3: When images are deployed to runtime.

While it's important to identify vulnerabilities as early as possible in stage 1 and stage 2, performing a scan on those images that are deployed to a runtime environment is equally important. It offers the following benefits:

- Identifying any new common vulnerabilities and exposures (CVEs) that got published.
- Providing accurate visibility into the risk posture of applications deployed.
- Prioritizing of vulnerabilities that must be resolved. The runtime context in terms of the application services or business services impacted due to a vulnerability can help with prioritization.

Container Vulnerability Response integrates with container security products such as Prisma Cloud Compute from Palo Alto Networks to pull the vulnerability data for those images that are deployed to runtime and enriches the vulnerability data with the runtime contextual information such as hosts, Kubernetes clusters, services, and namespaces where these container images are deployed. Customers using the ServiceNow Kubernetes discovery can see the references created from vulnerabilities to the relevant Kubernetes entities in their Configuration Management Database (CMDB). In addition to enriching the metadata, ServiceNow also offers a comprehensive reporting dashboard to provide insights into the vulnerability and remediation trends.



Identify ownership

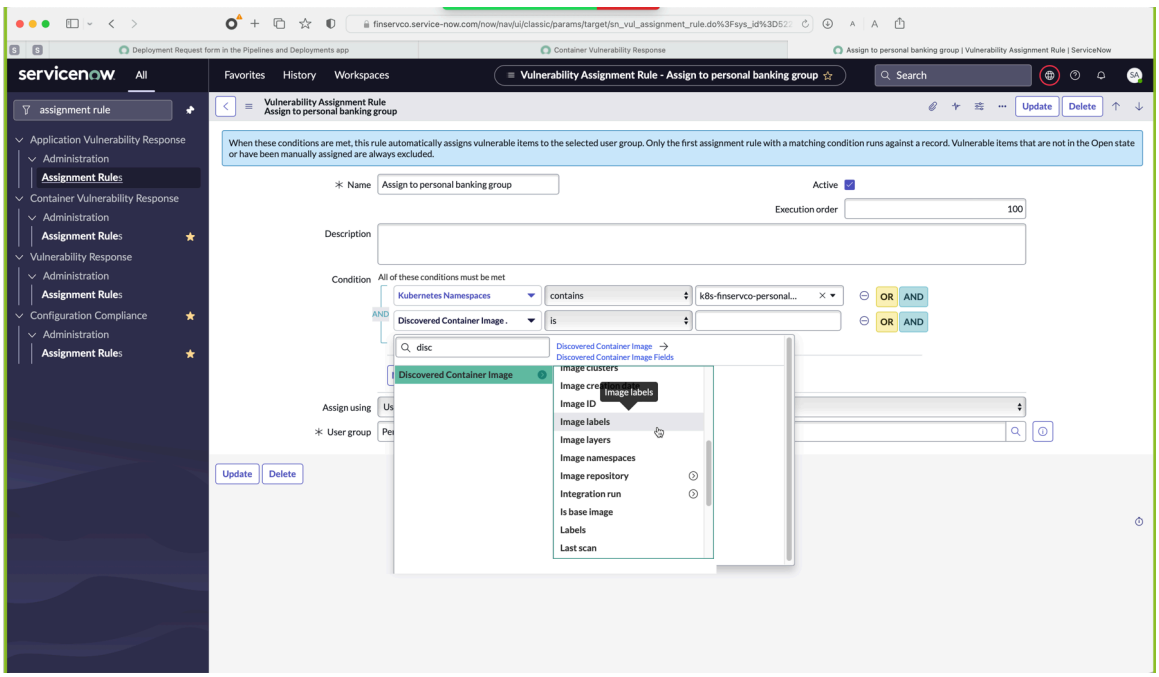
Pre-requisites

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Kubernetes metadata and references**: For Container Vulnerability Response to populate Kubernetes metadata (namespace, cluster, and so on) and references to Configuration Management Database (CMDB) entries, you must implement the Kubernetes discovery from Information Technology Operations Management (ITOM). Kubernetes discovery populates Docker Image, the running Docker Containers, Pods, Kubernetes Clusters, and so on, in the CMDB. Container Vulnerability Response identifies the Docker Image in CMDB based on image ID, and then identifies the related Kubernetes entities and populates the references to those entities from vulnerable items.
- **Cloud metadata and Docker Image labels**: Container Vulnerability Response also populates Docker Image labels, cloud account IDs, regions where an image is deployed. This data is maintained in "Discovered Container Image" record associated with the vulnerable item. There are no pre-requisites for this data to be populated. Container Vulnerability Response uses the data returned by container security products (for example, Palo Alto Prisma Cloud Compute) to populate these entries.

Ownership for patching a vulnerability in a container image can vary from organization to organization. This information may be captured in different places. A few organizations use Docker Image labels as a way of identifying the application teams who own a certain container image while other organizations may use the Kubernetes namespace or the cloud account where a container image is deployed to identify the right owner.

Container Vulnerability Response provides the necessary data model elements to be able to capture and use the Docker Image labels, Kubernetes cluster/service/namespace metadata, or the cloud account metadata (cloud account id, region, provider, and so on) in the 'Assignment rules' module and automatically assign vulnerabilities to the right application team based on the metadata of the image or the runtime environment.



Track vulnerabilities in the base images

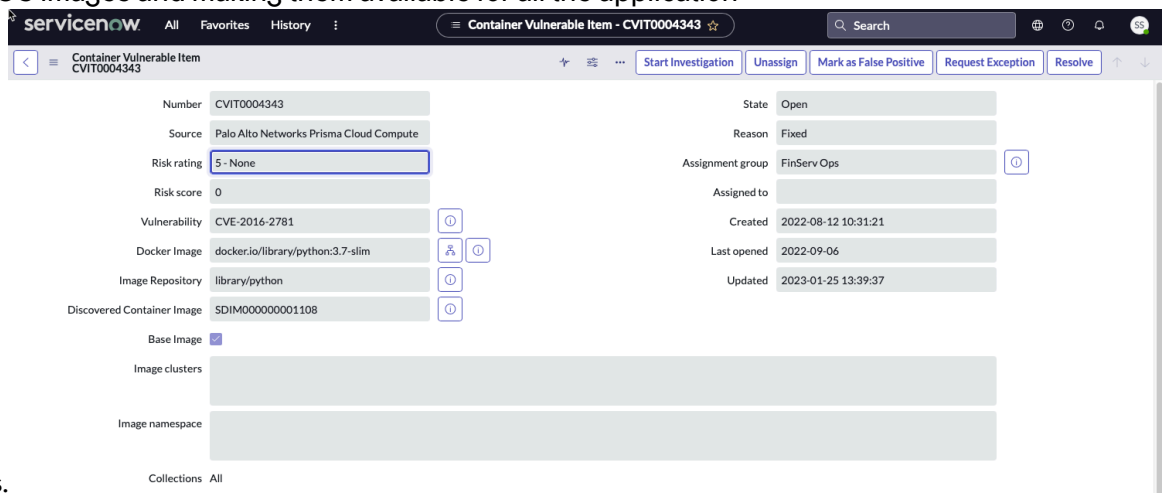
Pre-requisites

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For ‘Base Image’ property to be populated in Container Vulnerability Response, base images must be configured explicitly in the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute console. For more information on how to configure base images in Prisma Cloud, see https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/vulnerability_management/base_images.

Container Vulnerability Response enables for the creation of separate vulnerability records for a base layer so that they can be assigned to a different team.

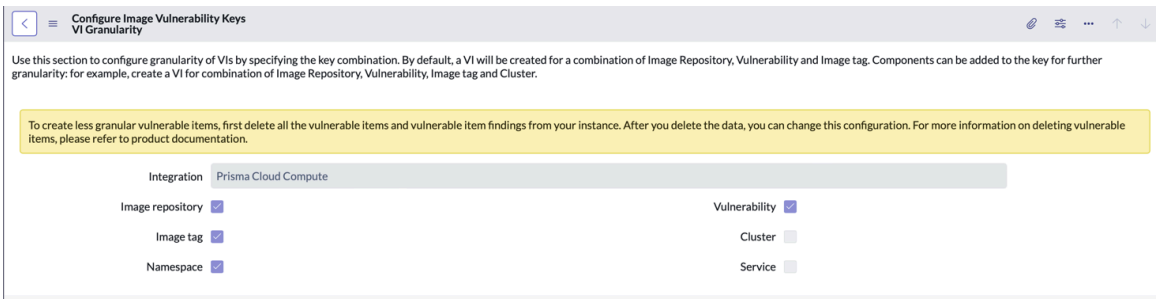
Track vulnerabilities identified in a base OS image such as Alpine from the vulnerabilities detected in other layers of the container image. Many organizations have dedicated teams who are responsible for patching base OS images and making them available for all the application teams.



Define granularity for vulnerable items

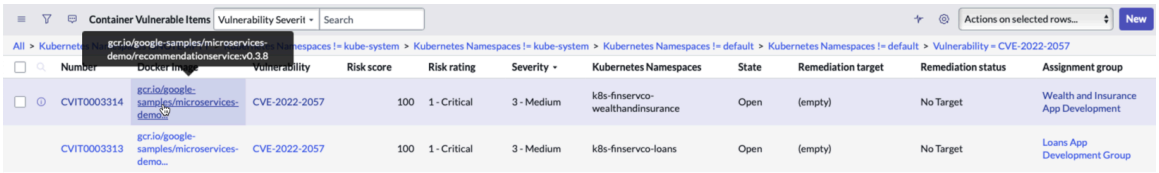
Pre-requisites

Configure the granularity of CVITs by navigating to **All** > **Container Vulnerability Response** > **Administration** > **Configure VI Granularity**.



By default, a vulnerable item is created for every unique combination of CVE and the Docker Image version (reference + tag). However, a few Docker Images may be deployed in more than one Kubernetes namespace and each namespace could be owned by different business units or teams. Each team may follow their own cadence for rolling out new versions of container images to fix vulnerabilities. To accommodate this scenario, Container Vulnerability Response enables you to define granularity for vulnerable items: Whether one vulnerable item should be created for each Kubernetes namespace/cluster/service even for every unique combination of Docker Image version and vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



In the example, you can see two vulnerable items created for the same Docker Image and CVE combination. One for the Kubernetes namespace ‘k8s-finservco-loans’ and the other one for ‘k8s-finservco-wealthandinsurance’.

Identify impacted services using tag-based service identification

Pre-requisites

- Identify various services in your application and define the tags/ key-value pairs that represent those services.
- Deploy Docker Images and Kubernetes pods with those tags or labels.
- Deploy ITOM Kubernetes Discovery Define 'Tag-based Services' with the right tags or labels.
- Deploy ITOM Kubernetes Discovery
- Define 'Tag-based Services' with the right tags or key-value pairs.
- Import vulnerability data into ServiceNow using Container Vulnerability Response

Risk calculation for vulnerable items can be done by looking at the CI (Docker Image) and the criticality of associated services in CMDB. However, to make it easier to identify impacted services, Container Vulnerability Response offers tag-based service identification.

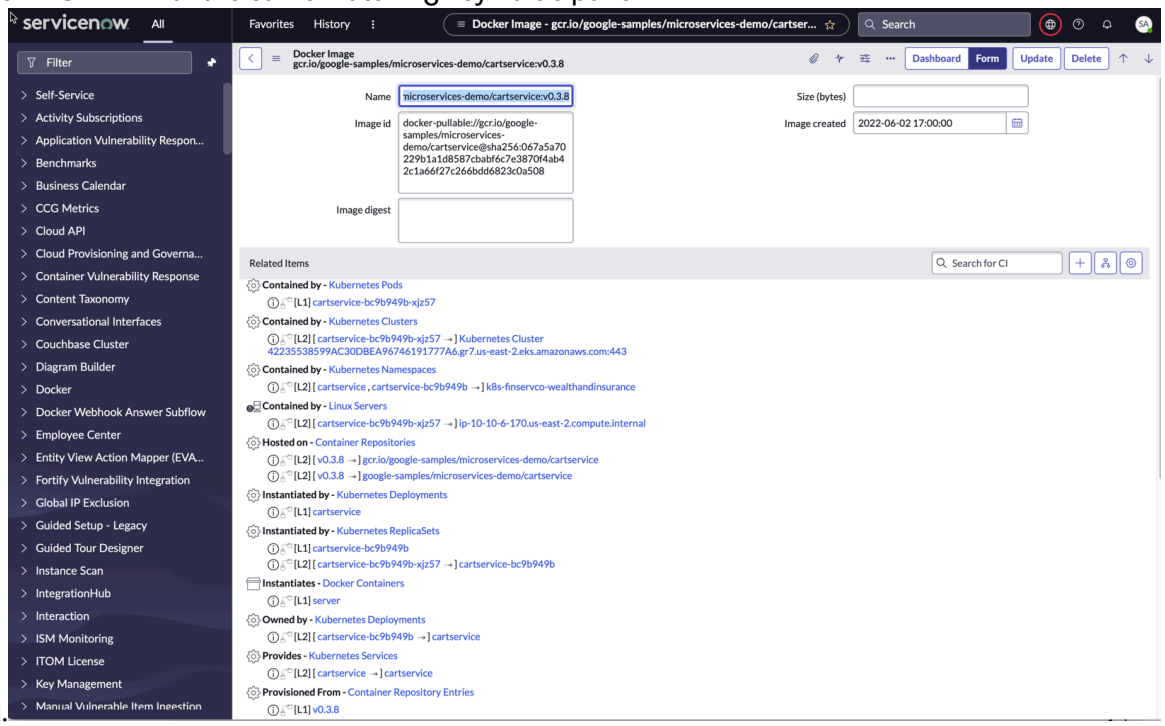
When Kubernetes pods or entities are published with key-values or labels matching the key-values defined in any ‘Tag-based Service’ in ServiceNow, Container Vulnerability Response automatically establishes the relationship between a Docker Image, and the impacted application service and uses the criticality of that application service in risk calculation.

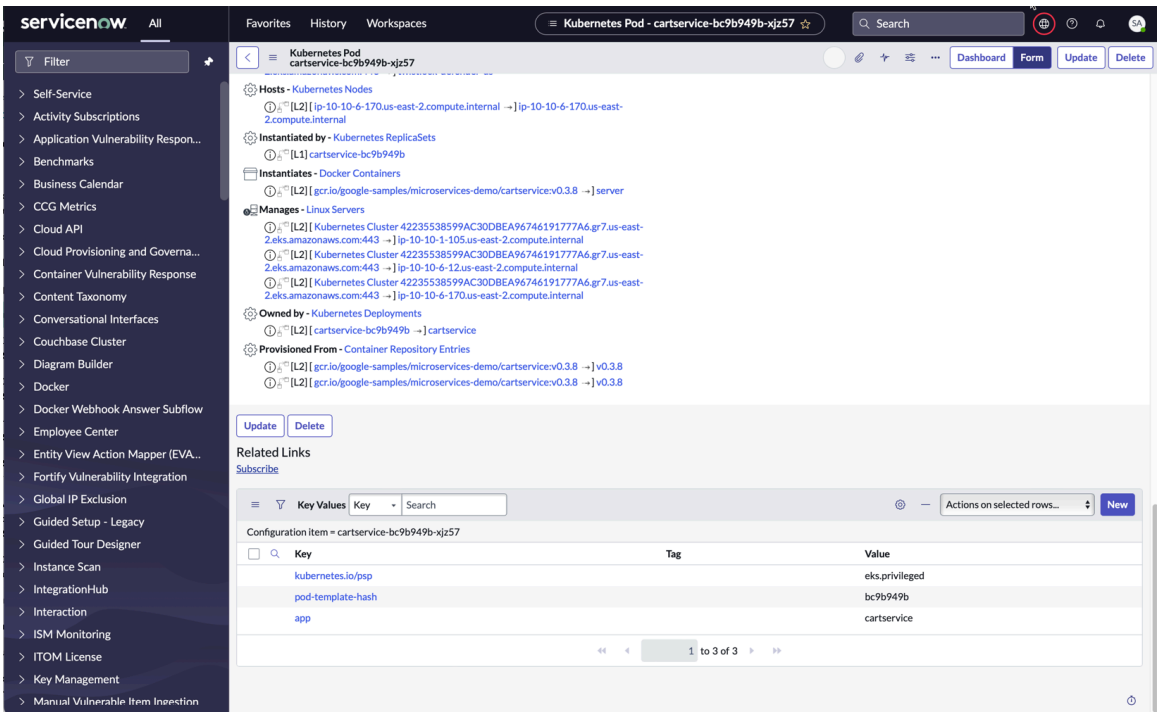
The flow is as follows:

1. Container Vulnerability Response imports vulnerability data from container security product.
2. For each container vulnerable item, Container Vulnerability Response populates the Docker Image from CMDB that has the vulnerability.
3. Container Vulnerability Response then looks at the Docker Image labels, or the labels/key-values published with Kubernetes pods where this image is deployed. This image is available in CMDB if you have the Kubernetes discovery running.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

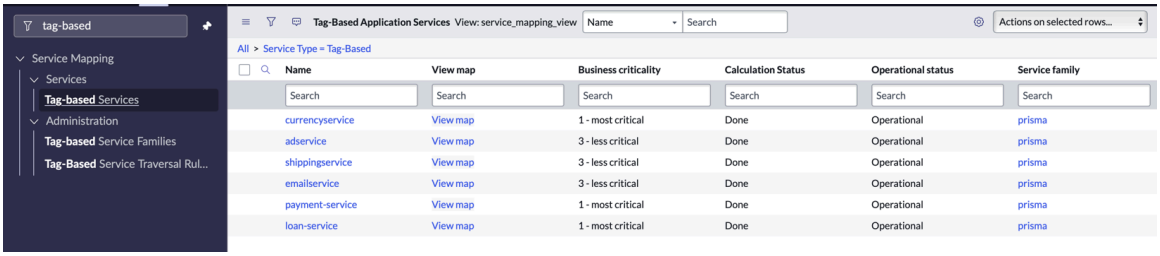
4. Container Vulnerability Response then searches for ‘Tag-based Services’ in CMDB with the same matching key-value pairs defined.

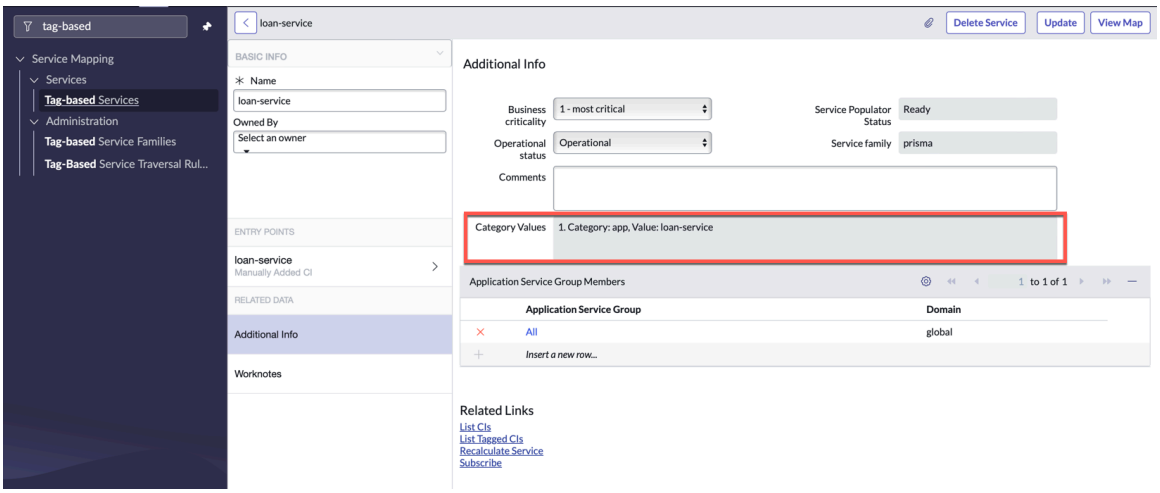




5. Container Vulnerability Response uses the ‘Business criticality’ of the matched ‘Tag-based Service’ (if any found) to calculate the risk of a container vulnerable item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

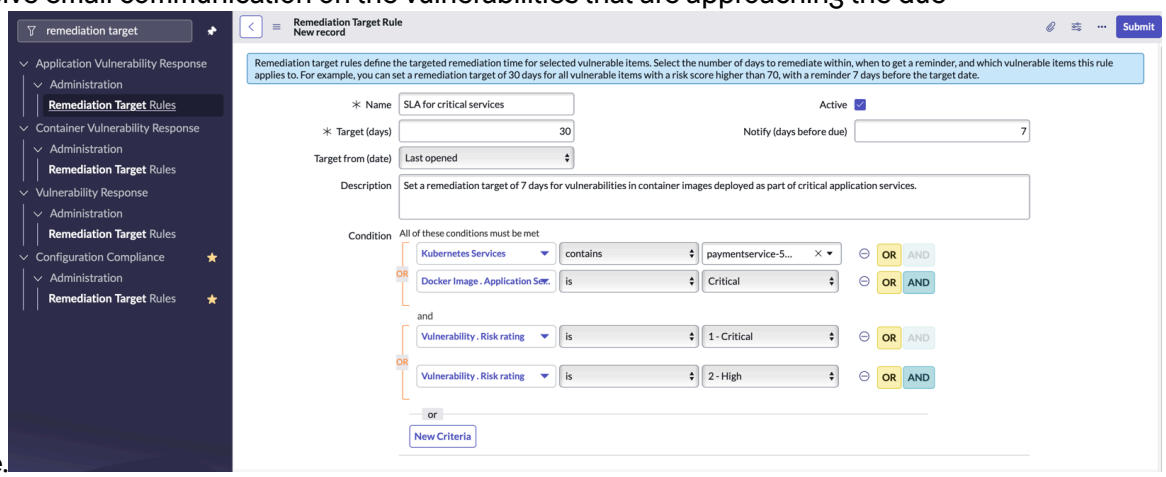




Tracking Vulnerabilities

Setting remediation targets

ServiceNow enables vulnerability managers to define 'Remediation target rules' to be able to define service level agreements (SLAs) for fixing vulnerabilities found in container images. Remediation target date can be defined based on a condition/ criterion on image metadata or vulnerability information. Remediation owners receive email communication on the vulnerabilities that are approaching the due date.



Identifying fixed vulnerabilities

Unlike host vulnerabilities that can be fixed by applying a patch on a host, container vulnerabilities can't be patched. New versions of container images must be created and deployed to replace the older versions. The new versions have a different identifier (image ID) compared to the previous versions that makes it challenging to keep track which vulnerabilities have been fixed already.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

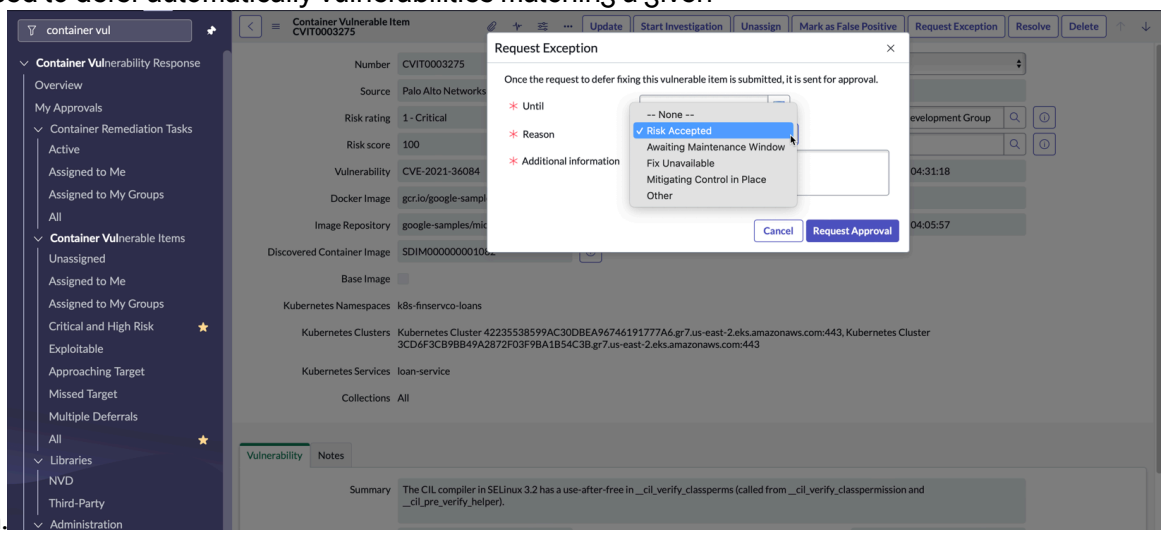
ServiceNow identifies vulnerabilities that were reported in the previous versions of the container images but resolved in the latest version of the image and automatically moves those vulnerabilities to ‘Closed/Fixed’ state so that security teams always have accurate visibility into the latest risk posture.

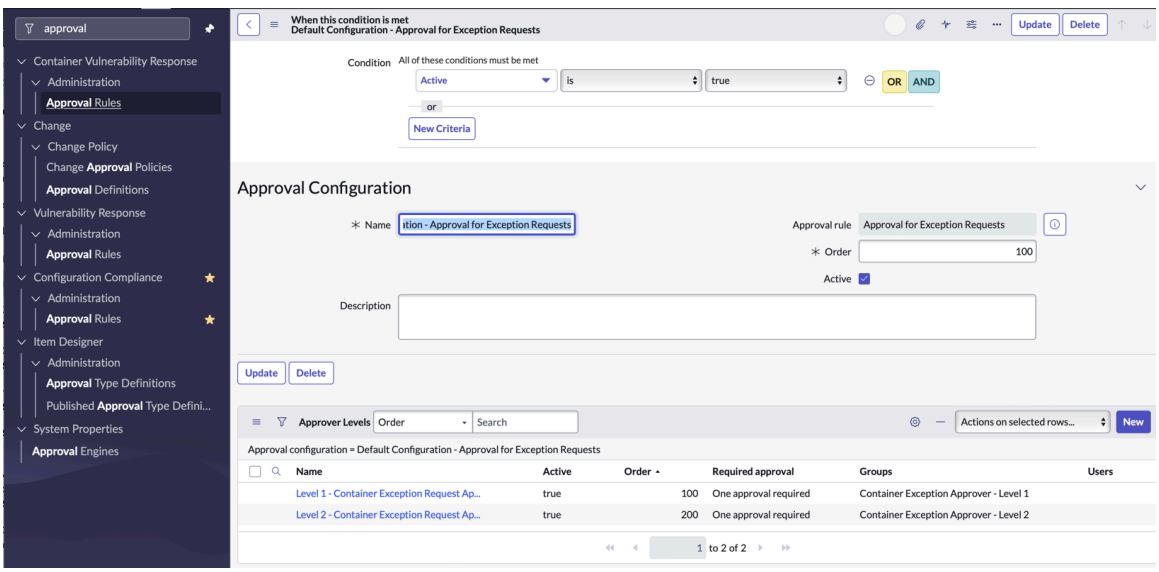
Manage exceptions

Application teams or remediation owners for the vulnerabilities might need the ability to request for an exception due to the following reasons.

- A mitigation control is already in place
- Risk accepted
- Awaiting maintenance window to push the fix.

ServiceNow enables security admins to define multiple levels of approvers for exception requests. You can also define auto exception rules that can be used to defer automatically vulnerabilities matching a given condition.





What's new

To learn more about what's new and what's changed in Xanadu, see the Xanadu release notes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

- For an overview about Security Operations in your ServiceNow AI Platform instance, see Understanding Security Operations.
- For information about all the Security Operations applications available for download from the ServiceNow Store, see Security Operations and the ServiceNow Store.

Exploring Container Vulnerability Response

The Container Vulnerability Response application imports container vulnerable items (CVITs). According to the rules, the feature enables you to remediate the container vulnerabilities. Container Vulnerability Response is available through a separate subscription.

Unlike traditional applications, containers package all the application source codes along with their dependencies into a binary file called a container image. The image is published to a registry to provide an option to run this image as an application or a container instance on any platform. The stages in a container pre-deployment life cycle are as follows:

1. Compose the container image: The container image is composed and pointed to a source code or a dependent library.
2. Build the container image
3. Publish the container image: The container image file is published to a registry. Each image has its own unique ID based on the contents of the image. These images are pulled from the registry into the run-time environment in post-deployment mode. The images then run as container instances on the host in the production environment.

Scanning container images

A container image can be scanned for vulnerabilities either before or after deployment. If container images are scanned during the pre-deployment phase, you may get many vulnerability alerts, which may not need your immediate attention. However, scanning for vulnerabilities during the post-deployment phase provides greater benefits, such as the following:

- Providing visibility on the risk associated with the deployed applications.
- Providing a focused view on only the images in the production environment.
- Identifying and prioritizing the vulnerabilities that must be acted on immediately.
- Grouping and assignment of vulnerabilities based on the metadata of the image. For example, an image repository, an image label, and other attributes related to the container image can be used for grouping and assignment rules.

Each container image has the following key components:

- Container or image repository: Represents the docker image with a given repository or name. It hosts all the versions of the image.
- Docker image: Represents a specific version of the build docker image.
- Docker container: Represents a running instance of the docker image. Each version has a unique ID and has multiple instances of the containers running in the production environment.

Container Vulnerability Response modules

The Container Vulnerability Response module provides details on the following:

Container Vulnerable Items

The container vulnerable items (CVITs) are grouped and listed based on assignment, criticality, exploitability, and remediation status.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Libraries

Get access to the National Vulnerability Database (NVD) and third-party libraries. While the NVD library provides information limited to vulnerability item ID, the third-party library provides most of the details on a vulnerability item. Information in the NVD screen is populated only when the NVD integration is triggered.

Administration

The Administration module provides information on the vulnerable items' assignment rules, remediation target rules, and container vulnerability integrations. In addition, you can also configure the duration after which a vulnerable item should be auto closed. You can use the Configure VI Granularity section to configure the granularity of CVITs by specifying the key combinations. By default, a CVIT is created for a combination of an image repository, an image tag, and a vulnerability. You can add additional components to the key for further granularity. For example, you can create a CVIT for a combination of image repository, image tag, vulnerability, and cluster.

Available versions

Release version	Release Notes
Container Vulnerability Response v2.12, v2.11, v2.10	

Container Vulnerability Response remediation task and container vulnerable item states

With the Container Vulnerability Response application, you can use the state model to see the status of a remediation task, at any given time. Knowing how each state relates to and affects each other helps you to determine when and how to remediate your container vulnerable items (CVITs).

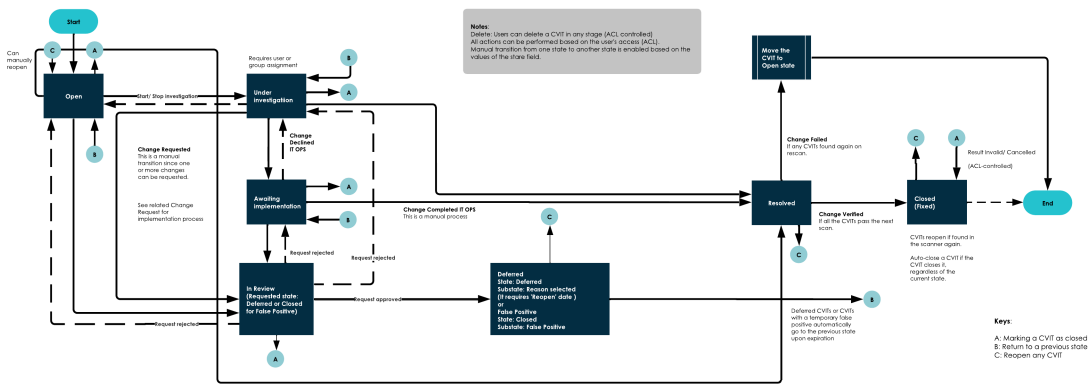
Remediation task states

Complex use cases can sometimes result in a container vulnerable item being in a different state than its remediation task. Understanding how states work helps to explain this behavior and can help with creating remediation tasks and creating or editing remediation task rules.

Remediation tasks have many possible states as shown in the following diagram.

Container Vulnerability Response state flow

Container Vulnerability Response state flow diagram that describes the remediation task states as follows: Open, Under Investigation, Awaiting Implementation, In Review, Deferred or False Positive, Resolved, and Closed.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- Container vulnerable items cannot be closed manually.
- Each task form contains **Follow** and **Update** buttons that are standard for ServiceNow tasks.

Remediation task and CVIT state transition and precedence order

Remediation tasks and vulnerable items states can affect each other. Most of the time, a remediation task state updates the vulnerable item state, with the highest precedence task state used to update the vulnerable items in the group.

From the creation to closure of a Container Remediation Task, it transitions through various states during the entire remediation process.

The state precedence is as follows:

Closed > **Deferred** > **Resolved** > **In Review** > **Awaiting Implementation** > **Under Investigation** > **Open**

The state transition happens as you perform various actions such as Defer, Open, Close, etc.

The actions you can perform on a Container Remediation Task at a specific state is similar to that of a Host Remediation Task. Hence, for more information, see the Vulnerability Response remediation task states and State roll-up and roll-down scenarios in the Vulnerability Response documentation.

Configuring Container Vulnerability Response

Before you run Container Vulnerability Response in your ServiceNow AI Platform instance, you must configure it.

Install Vulnerability Response and Configuration Compliance for Containers

Before you run the Vulnerability Response and Configuration Compliance for Containers application in your ServiceNow AI Platform instance, you must get entitlement and download the application from the ServiceNow Store. Install the application on your ServiceNow AI Platform instance, and complete a few installation steps in the Setup Assistant.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Setup tasks	Description
Verify that the application is installed and activated.	To verify that it is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. If the application is not installed and activated see, Install Vulnerability Response.

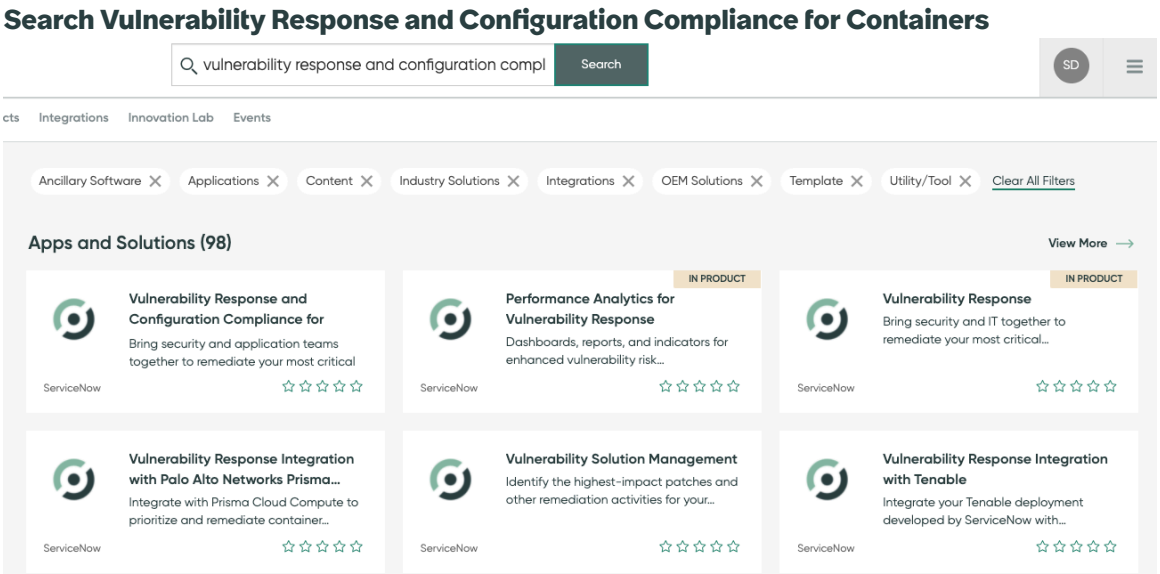
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
Verify that you have the required ServiceNow roles assigned for your instance.	The admin role is required for installation. If not already assigned, the System Administrator [admin] also assigns the Vulnerability Admin, sn_vul.vulnerability_admin or sn_vul.admin (deprecated)] role.

Role required: admin

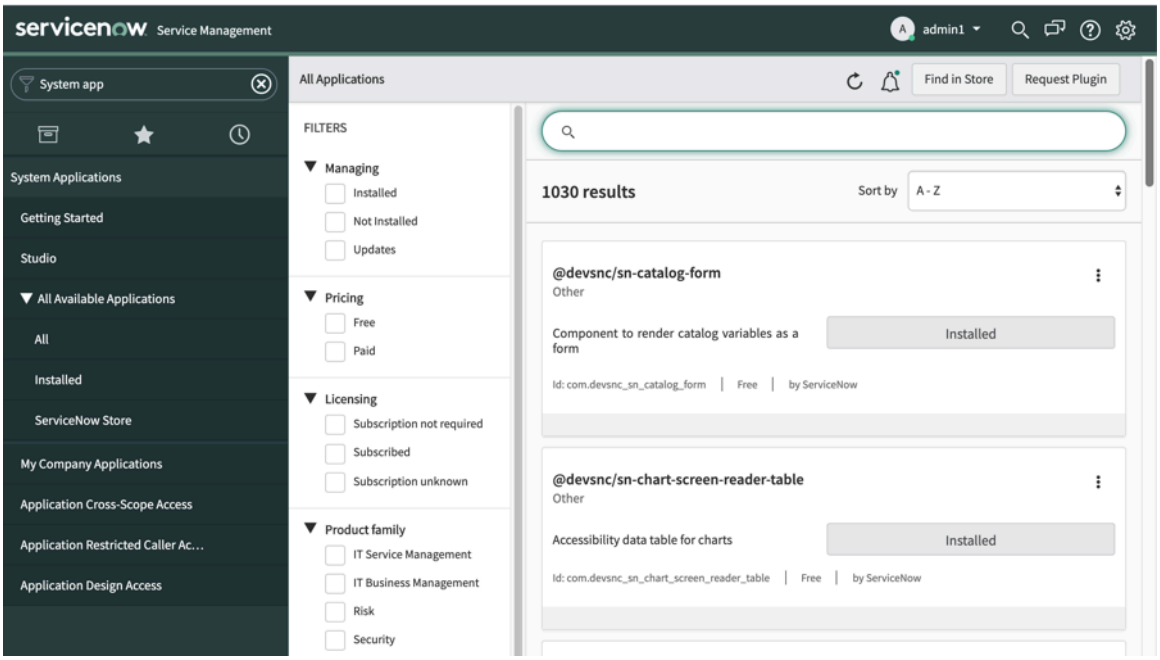
Procedure

1. To get entitlement and download the Vulnerability Response and Configuration Compliance for Containers application, navigate to the ServiceNow Store.
2. In the upper right of the page, click **Log In**.
3. In the search bar, type Vulnerability Response and Configuration Compliance for Containers.
4. Under Apps and Solutions, click the Vulnerability Response and Configuration Compliance for Containers tile.



5. Click **Request Install**.
6. Login to the ServiceNow AI Platform instance where you want to install the Vulnerability Response and Configuration Compliance for Containers application on.
7. Navigate to **System Applications** > **All Available Applications** > **All**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. From the applications listed, locate the Vulnerability Response and Configuration Compliance for Containers application, select a version from the list, and click **Install**.
   The Application installation dialog is displayed. Any dependencies that are installed are displayed.
9. Click **Close**.

Define Container Vulnerability Response email notifications

Set up email notifications to share useful information about important updates and activities such as approval and rejection of false-positive requests. Creating an email notification involves specifying when to send it, who receives it, and what it contains.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Email Templates**.
2. Select **New**.

   For detailed instructions for creating email notifications, see Create an email notification.

Result

Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for users with the roles, sn_vul_container.vulnerability_analyst, or sn_vul_container.vulnerability_admin.
- Links open in the IT Remediation Workspace for users with roles, sn_vul_container.remediation_owner.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create or edit remediation target notifications

Vulnerability administrators can edit the remediation target notification or add new ones, specifying when to send the notification, who receives the notification, and what content is in the notification.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Notifications**.
2. Select the remediation target notification record or select **New**.
3. Fill in the fields on the form, as appropriate.
   For more information on the form fields, see Create an email notification.
4. Select **Preview Notification** to view the message.

Result

Starting from v21.0 of Vulnerability Response, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for the users with the roles, sn_vul_container.vulnerability_analyst, or sn_vul_container.vulnerability_admin.
- Links open in the IT Remediation Workspace for the users with roles, sn_vul_container.remediation_owner.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Configure Exception Management for Container Vulnerability Response

Limit the duration of an exception requested and add a questionnaire to the exception or false positive request using the Container Vulnerability Response module. By default, an exception is requested using the ServiceNow® Container Vulnerability Response module. You can also request an exception using the GRC: Policy and Compliance Management integration.

Before you begin

Role required: sn_vul_container.manage_exception_configuration

About this task

If Container Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

If you add a questionnaire, it's sent to the person raising the exception or false positive request. You can either use the default questionnaire or create one based on your requirements. .

It's useful for the exception approver to understand the reason for requesting the exception.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Management**.
2. On the **Exception Management Configuration** form, select how you want to manage an exception by selecting an option from the **Manage exceptions using** list.
   You can select either Vulnerability Response or GRC: Policy and Compliance Management.
3. If you selected the Vulnerability Response option, enter the following information:

Vulnerability Response fields

Field	Description
Duration	Period for which an exception can be requested.
Unit	Unit of time for the specified period.
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Enable questionnaire to request exception	Option to add a questionnaire to the exception request being raised.
Questionnaire to request exception	Displays the questionnaire selected by you to request an exception. Exception Questionnaire is displayed by default.

Note: When you select GRC: Policy and Compliance Management, the Duration and Unit fields disappear as Governance, Risk, and Compliance handles that flow.

4. Select **Save**.

Configure approval rules for Exception Management

Starting with Vulnerability Response v15.0, use the flow designer to approve exception requests for exception management, exception rules, and false positive management. If you are deploying Vulnerability Response (VR) for the first time, the flow designer is enabled by default.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

To use the flow designer, create rules using the Approval Rules module. Using this module, you can configure approval rules for each of the following exception management workflows.

- Exception request for remediation tasks
- Exception request for container vulnerable items
- Exception rule
- False positive for remediation tasks
- False positive for container vulnerable items

You can also define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Approval Rules**.
2. On the Approval Rules page, select the group for which you want to set the approval rule.
3. On the form, fill in the fields.

Approval Rule form

Field	Description
Name	Approval configuration name.
Table	Table on which the rule is applied.
Application	Default value is Vulnerability Response.
Rule type	Specifies the rule type. For example, exception management, false positive or exception rule.
Active	Enabled by default, signifying that the approval rule is in use.
Description	Short description of the approval rules.
Approval expiry (days) Starting from v2.5 of Container Vulnerability Response	Date until when the approver can approve the request.
Notify approver (days) Starting from v2.5 of Container Vulnerability Response	Date after which the approver is notified to take action.

4. Select **Update**.
   In the Approval Configurations tab, there are two levels of approvers set up by default. You can select a rule to define the conditions based on different use cases within a rule. For more information, see Create configurations for an approval rule.

   Note: In each configuration page, you can create multiple approval levels. For more information, see Create approval levels for Exception Management.

Example:
Based on different use cases, you can define different approval processes for the same vulnerabilities found on different configuration items.

Quick start tests for Container Vulnerability Response

Validate that Container Vulnerability Response still works after you make any configuration change such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

The test execution property is disabled by default to prevent running tests on a production system. Run tests only on development, test, and other non-production instances. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production. See Run the Automated Test Framework (ATF) test suite for Vulnerability Response for more information about setting up and running the test suite for Container Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Container Vulnerability Response quick start tests require activating the Container Vulnerability Response application (sn_vul_container).

Container Vulnerability Response tests

Test	Description	Release version
CVR: Assignment Rules	Determine whether a sample set of assignment rules can successfully auto-assign container vulnerable items to an assignment group for remediation.	Vancouver
CVR: Exception Rule	Test exception rules.	Vancouver
CVR: Mark as False Positive Flow	Test whether the mark as false positive flow is working on the container vulnerable item.	Vancouver
CVR: Remediation Target Rules	Create a Remediation Target Rule.	Vancouver
CVR: Request Exception Flow	Test whether request exception flow is working as expected.	Vancouver
CVR: Vulnerability Calculators	Test the container vulnerability calculators.	Vancouver

Related topics

Quick start tests

Run the Automated Test Framework (ATF) test suite for Container Vulnerability Response

Run the Automated Test Framework (ATF) test suite after you install or upgrade the Container Vulnerability Response application.

Before you begin

Confirm a successful installation and that your instance works as designed.

The test execution property is disabled by default to prevent running tests on a production system. Run tests only on development, test, and other non-production instances. If demo data or demo accounts are created, all demo data should be removed prior to using the instance in non-production or production.

- To enable the test, follow these steps:
  1. Navigate to **All** > **Automated Test Framework (ATF)** > **Administration** > **Properties**.
  2. If not selected, select the **Enable test/test suite execution** check box.
  3. Click **Save**.
  4. If the scope is not set to **Container Vulnerability Response** in the header, or the scope is not displayed in the header, click the settings icon.
  5. In the System Settings window, click **Developer**.
  6. If not selected, click **Show application picker in header** and close the window.
  7. In the list that is displayed next to `System Administrator`, click **Container Vulnerability Response** for the field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: admin or atf_test_admin

Procedure

1. Navigate to **All** > **Automated Test Framework (ATF)** > **Tests**.
2. From the Package list, locate **Vulnerability Response and Configuration Compliance for Containers**.
3. Select a test to open the record.
4. In the open record, select the **Active** check box.
5. In the Test Steps related list, select true in the Active column.
6. Click **Update**.
7. Open the test again and click **Enable tests and test suite execution here**.
8. Enable Test/ Test Suite Properties and Test Debugging Properties.
9. Click **Save**.
10. If the **Run Test** button is not displayed, refresh your screen, open the record again and click **Run Test** to start the test.
    After a few moments, the Run Test dialog indicates a successful test. Click **Go to Result** for more information.

What to do next

Congratulations! You can continue with your configuration of Container Vulnerability Response.

For more information about automated tests for Container Vulnerability Response and automated tests, tests suites, and creating automated tests, see Automated Test Framework (ATF).

Integrating Container Vulnerability Response with other applications

Extend the capabilities of Container Vulnerability Response by integrating with other applications.

Container Vulnerability Response integrates with container security products to pull vulnerability data for those images which are deployed to runtime. It then enriches the vulnerability data with the runtime contextual information such as hosts, Kubernetes clusters, services, and namespaces where these container images are deployed. With ServiceNow's Kubernetes discovery, you can see the references created from vulnerabilities to the relevant Kubernetes entities in your Configuration Management Database (CMDB). In addition to enriching the metadata, ServiceNow also offers a comprehensive reporting dashboard to provide insights into the vulnerability and remediation trends.

Container Vulnerability Response provides integrations with the following applications:

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integration
- Understanding the Atlassian Jira integration with Vulnerability Response

> **Important:** In the Vulnerability Manager Workspace, you can create an agile issue manually using the list action and form action to track the remediation of CVITs and RTs.

Additional notes for integrations

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 2.1.2 of Container Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integration

The Prisma Cloud Compute integration enables you to scan container images to detect vulnerabilities.

Starting with version 23.0 of the Vulnerability Response, you can use the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in the Container Vulnerability Response application to import vulnerabilities on the running hosts. The Prisma Host APIs enable retrieval of comprehensive vulnerability information for a specific host and also provides a snapshot of the host vulnerabilities at a specific time. This API enables regular synchronization between Prisma and ServiceNow instance. As Prisma is offered both as software as a service (SaaS) and on-prem solution, using a MID Server is necessary to invoke Prisma APIs from the ServiceNow instance.

Starting with version 16.1 of the Vulnerability Response, you can use the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute in the Container Vulnerability Response application to import container image vulnerability data for deployed containers. You can then view reports on vulnerabilities and vulnerable items on the Vulnerability Response dashboards. These vulnerabilities can then be prioritized and remediated.

If the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server. For more information, see MID Server system requirements.

Viewing the integrations

You can view the integrations that are part of the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. To view the integrations, navigate to **All** > **Prisma Cloud Compute Integration** > **Integrations**.

The following integrations are available.

Run Sequence	Schedule	Integration	Description
1	Daily	Prisma Cloud Compute Base Images Integration	Retrieves the vulnerabilities for base images from the Prisma API and reports the base images vulnerabilities separately. It also creates image findings and vulnerable items, which point to the base images.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run Sequence	Schedule	Integration	Description
2	Daily	Prisma Cloud Compute Vulnerabilities Integration	Retrieves container vulnerabilities. Creates findings and container vulnerable items (CVITs) and discovered container images.
3	On Demand	Prisma Cloud Compute Container Counts Integration	Retrieves container counts for each non base image.
4	Daily	Prisma Cloud Compute Registry Integration	Retrieves static image findings obtained from the Prisma registry scan and ingests into Container Vulnerability Response.

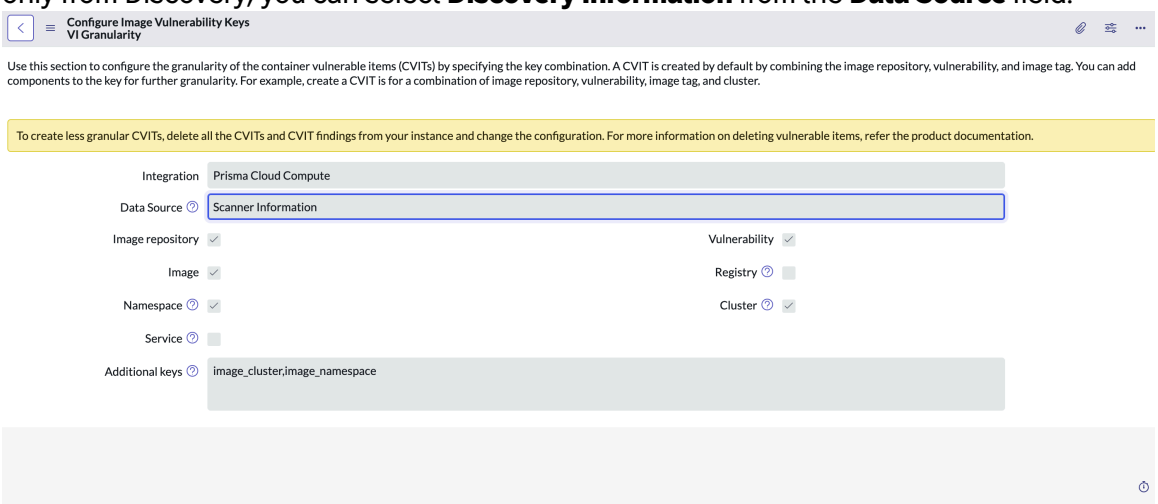
Base image configuration in Prisma

In the Prisma console, you can configure the registry and then configure the base images from those registries. If a vulnerability is present in the base image, then when you run the Prisma Cloud Compute Base Images Integration, the **Base image** check box is selected indicating the vulnerabilities are present in the base image.

Configure CVR-based VI granularity

To configure the granularity of CVITs, navigate to **All** > **Prisma Cloud Compute Integration** > **Configure CVR based VI Granularity** and specify the key combinations. By default, a CVIT is created for a combination of image repository, image, and vulnerability. You can add additional components to the key for further granularity. For example, you can create a CVIT for a combination of image repository, image, vulnerability, and cluster.

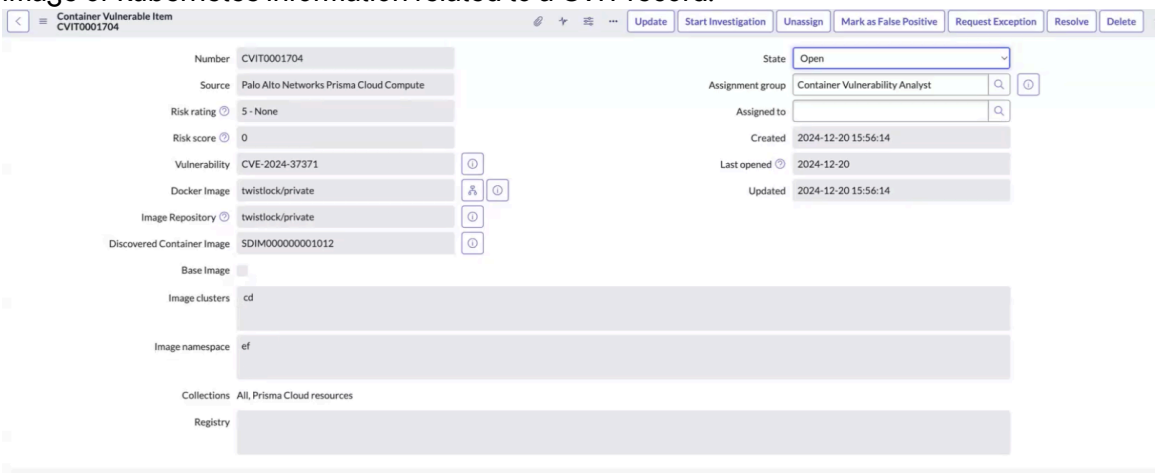
Starting with v2.12.1 of Container Vulnerability Response, you can also configure the granularity of container vulnerable items (CVITs) using Registry information and data sources. The namespace and cluster information is received from both scanner and Discovery. If you want this information only from Discovery, you can select **Discovery Information** from the **Data Source** field.



Depending on the chosen data source, you can view either

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

image or Kubernetes information related to a CVIT record.



If **Scanner information** is selected, the CVIT record shows **Image clusters** and **Image namespace** fields.

If **Discovery Information** is selected, the CVIT record shows **Kubernetes clusters** and **Kubernetes namespace** fields.

Prisma integration process

When the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute is run, it checks if a Common Vulnerability and Exposure (CVE) exists in the National Vulnerability Database (NVD) table. If it's already present, the existing information is used. However, if the CVE isn't found, placeholder records are generated in the NVD table. When creating these placeholder NVD records, initially only the CVE and its name are populated. Other details aren't populated with the assumption that the NVD integration fills in these details later. If the integration instance parameter *update_nvd* is set to true, it updates the placeholder NVD records. By default, the instance parameter is set to false. However, atleast until the NVD integration runs and populates these details, some understanding of the CVE, such as its severity or other details about the issue is needed. To meet this requirement, the fields **Exploit exists** and **Remediation notes** are populated with the details obtained from Prisma. Additionally, this configuration is made customizable, enabling you to specify any other fields you want to populate in the NVD entry based on the information provided by Prisma.

Preparing for the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

You can prepare for the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute by performing setup tasks.

Before you begin

To install and configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application, you may print the following checklist. Verify the items listed are completed before you install the application and import the vulnerability data into your ServiceNow AI Platform® instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist

Task	Description
☐	Verify that you have the following sets of information: • API base URL • Username and Password. These credentials are used to pull the vulnerabilities from the Prisma Cloud Compute integration. For more information, see https://pan.dev/compute/api/ **Note:** Mid Server is optional. The user credential used for Prisma Cloud Compute integration needs permission to monitor the images. See the following code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	If not already installed and activated, install the Vulnerability Response application before you install the third-party application. For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 16.1 of Vulnerability Response or later.
☐	Get entitlements and download the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application on your ServiceNow AI Platform® instance.
☐	Estimate the number of vulnerable items that you expect to import. Verify that your instance can accept the number of vulnerable items that you expect to import. An undersized instance can lead to long load times. If you don't know the size of your instance, or if you need assistance, contact ServiceNow Technical Support.
☐	Verify that you have the following groups or users to manage the integrations and to remediate the vulnerable items: **admin** Install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application. If not assigned, the admin assigns the container vulnerability admin (sn_vul_container.vulnerability_admin) and other roles. **sn_vul_container.vulnerability_admin** Completes the configuration of the Prisma Cloud Compute integration. This role has complete access to the Container Vulnerability Response (CVR) application and its records. This admin configures integrations and rules in Container Vulnerability Response. **Vulnerability Response Group**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist (continued)

Task	Description
	By default, the Vulnerability Response group is available. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all, sn_vul_container.read_all. **Container Remediation Owner Group** By default, the Container Remediation Owner group is available. Users assigned to this group inherit the sn_vul_container.remediation_owner. The Container Remediation Owner remediates container vulnerabilities assigned to them or to a group they belong to. **Vulnerability Analyst** Users assigned to Container Vulnerability Analyst group inherit sn_vul.vulnerability_analyst. The Vulnerability Analyst monitors remediation of all vulnerable items. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance. For more information, see Create a user group.
☐	Install the Vulnerability Response integration with NVD and run the NIST National Vulnerability Database Integration - API (CVE only).

You are ready to Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.

Install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Before you run the integration on your instance, complete the installation and configuration steps so that the Prisma Cloud Compute product properly integrates with Container Vulnerability Response. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin

Procedure

1. Log in to the instance you want to install the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute on.
2. Navigate to the ServiceNow Store.
3. In the ServiceNow Store, search for Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.
4. Click the application tile.
   Detailed information about the application you are installing is displayed.

Note: Read the **Other Requirements** and **Dependencies** sections, if needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Request App** and enter your Now Support login credentials.
6. Click **Get**.
7. Update the **Instance Name** and **Reason for the Instance** fields, and click **Validate Instance**.
8. Click **Request**.
   You receive an email with detailed installation instructions.
9. Navigate to **System Applications** > **Applications**.
10. Locate the application, select it, and click **Install**.

Result
Your application is automatically installed on your instance.

What to do next
Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute for your environment. See Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application.

Configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application

Install and configure the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute application. Import data from Prisma Cloud Compute. You can use the imported data to prioritize and remediate vulnerabilities for your docker images.

Before you begin
Role required: admin

Procedure
1. Open the email from ServiceNow that you received about the integration.
2. Log in to your instance as an admin.
3. Follow the instructions in the email to get the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navigate to **All** > **Prisma Cloud Compute Integration** > **Administration** > **Configuration**.
   On the Prisma Cloud Compute Configuration form, fill in the fields. For more information, see Prisma Cloud Compute Configuration form.
5. From the Projects list, select either **All Projects** or **Specific Projects** to configure either all projects or selected projects respectively.
   If you select **Specific Projects**, you can select the projects from the Available list.
6. Complete the configuration by clicking either **Finish** or **Save and Test Credentials**.
   - If you configured a project, click **Finish**.
   - If you did not configure a project, click **Save and Test Credentials**
7. View the newly created instance by navigating to **Prisma Cloud Compute Integration** > **Administration** > **Integration Instances**.
8. View the projects you configured earlier by clicking **Integration Instance Parameters**.
9. Run the newly created integration instance to import the following data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Docker Images: Lists the Docker images, which are created using an identification and reconciliation engine (IRE). Each Docker image also provides information on the relationship between the repositories and the versions installed.
- Discovered Container Images: The Discovered container images module provides information on the image ID, Docker image, and the image repository. It also stores the layer information and associates it with the discovered image. You can also view the projects and container count here. For a discovered container image, you can view cloud metadata such as cloud provider, cloud region, cloud account ID, and cloud resource IDs.
- Container Image Packages: It provides information about the packages where the vulnerabilities exist. The Binary package details are also provided as a comma-separated value.
- Container Image Layers: This screen displays the record for each image layer.
- Container Image Findings: This screen displays the list of findings along with information on the associated vulnerabilities, image layer, docker image, image repository, and discovered image. Currently, the vulnerability information is limited to just the ID. Additional information is populated when NVD integration is triggered.
- Container Vulnerable Items: Each finding has a corresponding vulnerability. The CVITs are further created based on the granularity.

10. Configure the granularity of a vulnerable item.

a. Navigate to **Prisma Cloud Compute Integration** > **Configure Image Vulnerability Keys**

b. Configure the granularity of the CVITs by selecting the required check boxes.
The vulnerable items are created based on the selected keys, during the next import.

> **Note:** By default, a CVIT is created for a combination of Image Repository, Vulnerability, and Image tag. You can add components to the key for further granularity. For example, you can create a CVIT for a combination of Image Repository, Vulnerability, Image tag, and Cluster. Once the vulnerable items or vulnerable item findings are created, the check boxes are no longer editable.

Exploring the Wiz Container Vulnerability Integration

Import container vulnerability data with the Wiz Container Vulnerability Integration that is included with the Wiz Vulnerability Response Integration.

Wiz Container Vulnerability Integration overview

The Wiz Container Vulnerability Integration imports container image vulnerabilities that are identified by the Wiz vulnerability scanner. Import data to help you identify, prioritize, and assign container vulnerabilities for remediation with the automated workflows of the ServiceNow AI Platform instance.

Findings are mapped to container vulnerable items (CVITs) to support triage, risk prioritization, and targeted remediation workflows for container-based workloads.

For more information about the other integrations that are included with the Wiz Vulnerability Response Integration and installation and configuration steps, see Understanding the Wiz Vulnerability Response Integration.

Please review more information about the Wiz integration at SecOps articles on the Security Operations Community.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediating container vulnerabilities

Monitoring remediation is a process that begins with reviewing status and ends with closing container vulnerable items (CVITs). Container Vulnerability Response offers tools and procedures to make that process more productive and efficient.

Container Vulnerability Response calculator rules

Vulnerability calculators automate the calculation of initial values for the fields on container vulnerable items. The condition for each calculator is evaluated in order, and the first matching calculator is used.

To view and create vulnerability calculators, navigate to **All** > **Container Vulnerability Response** > **Administration** > **Vulnerability Calculators**.

The Container Vulnerability Response base system includes two vulnerability calculators that set the base Risk Score on the container vulnerable item. The following calculator groups are available in the base system:

- Vulnerability Severity: Calculates the risk score for vulnerable items using the normalized vulnerability severity.
- Default Risk Calculator: It's based on the risk rule.

Note: Starting with version 2.10 of Container Vulnerability Response, in case of:

- **Default Risk Calculator** rule: Whenever the risk score on a container vulnerable item (CVIT) changes, the following details are documented in the Notes section of the CVIT:
  - Calculator group name
  - Calculator name
  - Field values that have a weightage greater than 1 and their risk score contribution.
  - Final risk score
- **Vulnerability Severity** risk rule: Whenever the risk score is updated on a CVIT, the **Notes** section is updated with the following details:
  - Calculator group name
  - Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, select any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If **Template** is selected, the risk score is updated according to the specified condition in the rule. If **Script** is selected, you can either add or update the existing script. The system property *sn_sec_cmn.risk_score_changes_add_worknotes* helps populate the work notes section. Starting with v2.12.2 of Container Vulnerability Response, the system property *sn_sec_cmn.risk_score_changes_add_worknotes* is inactive by default. If you enable it, only then you can see all the changes related to the risk score of a container vulnerable item in the Work notes section. Additionally, the work notes are updated only if there's a change in the risk score.

Vulnerability Risk Score Weights

All vulnerabilities are assigned a risk score and rating based on factors such as severity, criticality, exploit information, and so on. The business rule *Update Risk Rating from Risk Score* on the container vulnerable item table is responsible for calculating the risk rating. Whenever the risk score changes, the risk rating is calculated and populated on the container vulnerable items. Prior to version 17.1 of the Vulnerability Response (VR) application,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the following risk ratings were provided as part of script include `VulnerabilityUtils`, which were hard-coded.

Value (Risk Rating)	Weight (Risk Score)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Starting with the 18.0 version of Vulnerability Response,

- The risk rating types are shipped in the base table Risk Score Weights [sn_sec_cmn_risk_scorew_weights] as cvr_risk_rating. These types are passed as part of the business rules or script includes on each table where the risk rating is calculated.
- The script is modified so that you can query the entries in the Risk Score Weights table values for risk rating calculation.
- Add additional entries for an existing type or create a new type. When you create a new type, ensure that you add the labels for the new risk rating, and also modify the related scripts and business rules. You must also add a new style for the new risk score.
- Modify the script to query the records in the base table.

You can access the Risk Score Weights table by entering sn_sec_cmn_risk_score_weight (for versions below 30.0) or sn_sec_calculator_risk_score_weight (for versions 30.0 and above) in the filter navigator.

In addition, the risk score is automatically recalculated in the following scenarios:

- When a configuration item (CI) changes from non-internet facing to internet facing.
- When the associated Common Vulnerabilities and Exposures (CVEs) or third-party entries (TPEs) on the vulnerability items (VIs) are linked to a CVE Known Exploit Vulnerability (KEV).

For more information, see Vulnerability Response calculators and vulnerability calculator rules.

Container Vulnerability Response assignment rules

Define the criteria by which container vulnerable items are automatically assigned to an assignment group for remediation.

To create and view assignment rules for container vulnerable items, navigate to **All** > **Container Vulnerability Response** > **Administration** > **Assignment Rules**. When you create an assignment rule, you can set the conditions. When these conditions are met, the rule automatically assigns the container vulnerable items to the selected user group. Only the first assignment rule with a matching condition runs against a record. See Vulnerability Response assignment rules overview for more information about assignment rules.

Roles required: sn_vul_container.manage_assignment_rules to define and update rules and sn_vul_container.container_reapply to reapply rules.

Starting with version 2.13, fields for scanner information have been added to the records on the Discovered Container Image [sn_vul_container_image] table. You can use the following values as conditions when you create or update your assignment rules for container image vulnerable items (CVITs) to help you track ownership across your container environments.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Cloud account IDs
- Image namespaces
- Registry
- Hosts
- Labels
- Status (Vendor status for a resolved vulnerability)

Note: This value on Container Image Finding [sn_vul_container_image_findings] table the refers to the version in which a vulnerability was resolved, for example, `Fixed in 6.2.1`. This value is imported from the Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute integration.

Note: Container vulnerable items (CVITs) that are not in the Open state or have been manually assigned are always excluded from assignment rules. If you add values for these scanner fields to your assignment rules and rerun your rules, vulnerable items are not reassigned unless the assignment type is `Rule`. Items with Type `manual` are not considered by the assignment rules.

Important: As a vulnerability admin and analyst, you can obtain the latest assignments for selected CVITs in the Vulnerability Manager Workspace. This method is more efficient than reapplying the Assignment Rules for all CVITs in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Container Vulnerability Response remediation target rules

Remediation target rules define the expected time frame for remediating a container vulnerable item (CVIT). These rules are similar to how SLAs provide a time frame for remediating the vulnerability itself.

To create and view remediation target rules for container vulnerabilities, navigate to **All** > **Container Vulnerability Response** > **Administration** > **Remediation Target Rules**.

The remediation target rules define the target remediation time for selected container vulnerable items (CVITs). Set a deadline for remediating the vulnerability by selecting the number of days for the remediation. Set a reminder for remediation, and set the container vulnerable items the rule applies to. You can set a remediation target for the days within which it needs be remediated and also set a reminder before you approach the target date. For more information, see Vulnerability Response remediation target rules.

Important: As a vulnerability admin and analyst, you can obtain the latest remediation target date for selected CVITs in the Vulnerability Manager Workspace. This method is more efficient than running the Remediation Target Rules for all CVITs in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Exception management in Container Vulnerability Response

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions to an container vulnerable item (CVIT) that cannot be remediated according to the policy.

Some container vulnerabilities (CVIT) might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Life cycle of an exception

Definition of an exception

An exception is a request to defer the remediation of a CVIT or RT for a specified period. For example, as a remediation owner, you can request an exception if a patch is not available for a machine.

Requesting an exception

As the remediation owner, you can ask for an exemption for a CVIT or RT using the exception management process. After the exception approver approves this request, the CVIT or RT moves to a **Deferred** state.

Approving an exception request

CVIT or RTs that can't be remediated immediately are reviewed by vulnerability analysts, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level workflow. If only the first-level approver is present, the exception can be requested and approved. However, if there's no first-level approver, an exception can't be requested. See Add an exception approver for more information.

Note:

Starting from Vulnerability Response v15.0, if you are deploying the VR application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow. To configure approval rules for exception management and false positive, see Configure approval rules for Exception Management.

Once an exception request for a CVIT or RT is approved, you can perform the following actions:

- Reopen
- Delete
- Update the **Assignment to** or **Assignment groups** fields

Tracking an exception request

After raising the exception, you can track its status by using the **State Change Approvals** tab of the CVIT or RT. If an action is taken on an RT, you can't track the status of the individual CVITs in that RT.

Expiry of an exception request

When an exception request for a particular CVIT or RT expires, the impacted CVIT or RT reverts to its **Open** state.

If a single CVIT or all the CVITs in a RT pass in the next scan, then the CVITs and, where applicable, the RT **State** field changes to **Closed** with the substate **Fixed**.

Configure approval rules

View and configure approval rules by navigating to **All** > **Container Vulnerability Response** > **Administration** > **Approval rules**. Request an exception for the CVITs that cannot be remediated or deferred immediately, by identifying the impacted vulnerabilities, configuration items (CIs), or CVITs. Automate the CVIT deferral process. Defer the matching CVITs based on these rules when the system identifies these CVITs.

The following approval rules are shipped by default:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Approval for Exception Requests: A default configuration with two approval levels is provided in the base system. Whenever there is an exception request on a vulnerable item, the approval request is sent to the users or groups present in level 1. Once approved by level 1 approvers, it is sent to the level 2 approvers.

  Note: You can change the default levels and edit as required. Starting from Container Vulnerability Response v2.0.6, you can use the system properties provided in the base system for exception approvals via workflow in the System Properties [sys_properties] table. So, when an exception or false positive request is raised via workflow, it's sent for approval to the group IDs defined in the system property. Navigate to **All** > **System Properties** and select *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*, or *sn_vul_container.container_false_positive_approver_group* to change the property value.

- Approval for Exception Rules: It does not have configuration but two approval levels.
- Approval for False Positives: It has one configuration with one approval level.

Note: Starting from v2.5 of Container Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the container vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the container vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Requesting and approving an exception in Container Vulnerability Response

You can request to defer the remediation of a container vulnerable item (CVIT) for a specified period. For example, as a developer, you can request an exception if a patch is not available for a machine. Approvers who have access can approve requests from other users.

To request or approve an exception, see:

- Request an exception for a container vulnerable item
- Request an exception for container vulnerabilities using GRC: Policy and Compliance Management

Note:

Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested. Starting from v2.5 of Container Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the container vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the container vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request an exception for a container vulnerable item

Request an exception for a container vulnerable item (CVIT) that can't be remediated immediately. For example, as a remediation owner, you can request an exception if a patch isn't available for a machine.

Before you begin

Role required: Developer Group

About this task

You can request an exception for multiple CVITs simultaneously using the Bulk Edit feature in the Vulnerability Manager Workspace. For more information, see Request bulk exception in the Vulnerability Manager Workspace.

Procedure

1. Navigate to **Container Vulnerability Response** > **Container Vulnerable Items** > **All**.
2. Select the item that you want to request an exception for.
   The selected item must be in Open or Under Investigation state.
3. On the Container Vulnerable Item form, click **Request Exception**.

4. **a.** On the form, fill in the fields.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the duration selected in the **All** > **Container Vulnerability Response** > **Administration** > **Exception Management** screen. When the exception request expires, the group reverts to its Open state. **Note:** Starting with version 1.2 of Container Vulnerability Response, if a vulnerable item was deferred for remediation by using the exception management feature, then in case it is reopened by the scanner, the deferral date set on the vulnerability will still persist. To enable this functionality, set the value of the system property `sn_vul.container.auto_defer_cvit_in_act` to true. Also, the deferred until date persists even after the CVIT gets closed or the exception expires. The role required is sn_vul_container.manage_exception_configuration for both read and write.
Reason	Reason for the exception. Choices are as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	▪ Risk Accepted ▪ Awaiting Maintenance Window ▪ Fix Unavailable ▪ Mitigating Control in Place ▪ Other To see how to add new reason choices, see Define a policy reason mapping.
Additional information	Details that are related to the reason why this request is being made. This field is to be updated by the remediation owner.

b. Submit the exception request by clicking **Request Approval**.
The state of the container vulnerable item changes to In Review. Use the **State Change Approval** tab to track the status of the exception request.

Request an exception for a container remediation task

Request an exception to defer a container remediation task for a specified period if it can't be resolved immediately.

Before you begin

You can request exceptions from the Vulnerability Response Workspaces. See Request an exception in the IT Remediation Workspace.

Role required:

sn_vul.remediation_owner, sn_vul.app_security_champion, or sn_vul_container.remediation_owner.

You can also request exceptions for container remediation tasks in the classic environment.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Remediation tasks** > **All**.
2. Select the group that you want to request an exception for.
   The selected task must be in the Open, Under Investigation, or Awaiting Implementation state.
3. On the container remediation task record, select **Request Exception**.
4. On the form, fill in the fields.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the exception duration that is defined in the configuration.
Reason	Justification for requesting an exception.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Additional information	Details that are related to the reason why this request is being made. This field is to be updated by the remediation owner.

5. Click **Request Approval**.

Request an exception for container vulnerabilities using GRC: Policy and Compliance Management

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Container Vulnerability Response.

Before you begin

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Role required: sn_vul.remediation_owner

You can also request exceptions in the classic UI:

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Container Vulnerable Items** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.
2. On the selected form, click **Request Exception**.

   Note: If GRC: Policy and Compliance Management is selected in the Exception Management screen, then fill in the fields on the Request Exception form. For more information on the form fields, see Request Exception form.

   a. Submit the exception request by clicking **Request Approval**.
   The state of the vulnerable items changes to In Review and a policy exception is created.
   Use the **State Change Approval** tab to track the status of the exception request.

   b. View the policy exception by clicking the Policy Exceptions related list.

   c. Click the policy exception number.

   d. In the **Approver** field, select the name of the approver.

   e. Click the Source tab and select a control objective from the **Control objective** field.

   f. Click the Risk assessment tab and select the risk rating from the **Risk rating** field.

   g. Save the form.

   h. Click the **Impacted Controls** tab.

   i. Add the controls by clicking **Add**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

j. Save the form.

Note: You can raise a compliance review by clicking **Request compliance review**.

The approval form is sent to the approver.

The approver can either approve the request by clicking **Approve** or request additional approval by clicking **Request Additional Approval**.

The record state changes to Deferred. The reason stated is the one you selected when raising the exception request. The **Deferral** tab provides additional notes on the record.

Note: If the request gets rejected, the record moves to its previous state.

3. Click **Submit**.
   For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

Define a policy reason mapping

Define reason choices to be available to any user who requests an exception.

Before you begin

Role required: sn_vul.compliance.manager and sn_vul_container.manage_exception_configuration

Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Integration Registry**.

   Note: You can either select a reason from the reason choices available in the Reason Choices table or add a new reason.

2. Click the Container Vulnerability Response - CVIT integration registry.
3. In the Reason Choices list, click **New**.
4. Click the magnifying glass icon.
5. Add an existing reason choice to create a new one.
   - If you want to add an existing reason choice, then select a reason.
   - If you want to add new reason choice to the Reason Choices table, then click **New** and fill in the fields on the form.

Reason Choice List form

Field	Description
Label	Unique label for this choice.
Value	Unique value for this choice. This value is mapped in the Policy Reason Mapping table for the respective applications. To navigate to this table, enter `sn_vul_policy_reason_mapping.LIST` in the filter navigator.
Order	Order for this choice. Reasons are ordered based on this number.
Default	Option to indicate that this reason choice will be available whenever an on demand policy exception is requested. If the integration registry doesn't contain

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	any application-specific choices, then all reason choices that have the **Default** field selected will be available.
Active	Option to display the choice in the list of reason choices.

6. Click **Submit**.

Result
The reason choice is added. The reason choice will be available in the **Reason** field of the policy exception request form for the selected application.

Approve an exception request in Container Vulnerability Response

Approve exception requests for container vulnerable items or remediation tasks that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

Before you begin
Role required: sn_vul.exception_approver

About this task
You can approve the exception and false-positive requests in the Vulnerability Manager Workspace. See Approve or reject requests in the Vulnerability Manager Workspace.

You can also approve exception requests in the classic environment:

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Defer a container vulnerable item in Container Vulnerability Response

If you determine that the issue associated with a container vulnerable item (CVIT) is of low risk and can be immediately deferred without further analysis, you can use the **Defer** feature.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)
Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

About this task
A scheduled job runs every day checking for deferred vulnerable items that have reached their reopen date. On the day the CVIT's deferral is set to expire, the record is reopened.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Container Vulnerable Items**.
2. Open a vulnerable item.
3. Click **Request Exception**.
4. Fill in the fields on the form, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Until	Select the date when the Deferred state expires and the remediation task is reactivated. **Note:** Starting with version 18.0 of Container Vulnerability Response, if a deferred container vulnerable item (CVIT) is closed and reopened by a scanner before the exception window expires, the state of the CVIT reverts to deferred state honouring the active exception window. To enable this functionality, set the value of the system property *sn_vul.container.auto_defer_cvit_in_act* to true. Additionally, the deferred Until date persists even after the vulnerable item gets closed or the exception expires. The role required is sn_vul_container.manage_exception_configuration for both read and write. After the record is submitted, if email notifications are defined, members of the Container Vulnerability Response group receive an email when the expiration date is within one week. When the defer date expires, the vulnerable item is set back to Open and a second email notification is sent out.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ False positive ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Click **Submit**.
   The group is marked **In Review**. A **Reopen** related link appears. The reopen date and reason appear in work notes under the **State Change Approvals** tab.

   Starting with Container Vulnerability Response v2.3, you can add relevant information in the Work Notes field in the Notes section for a deferred container vulnerable item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request an extension for a deferred container vulnerable item

Request an extension for a deferred container vulnerable item before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Container Vulnerable Items**.
2. Open a deferred container vulnerable item.
3. Select **Request Extension**.

   Note: The Request Extension button is visible only when the state of the container vulnerable item is Deferred.

4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the deferred container vulnerable item must be extended for remediation.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   An email is triggered on submission of the request and subsequent action by the approver.

   Note:
   - The request goes through two levels of approval.
   - If a deferred container vulnerable item is extended again, the extend deferral count increases in the backend.

6. After the request is approved, the Until, Reason, and Deferral notes are updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Working with an exception rule in Container Vulnerability Response

You can request an exception for container vulnerable items (CVITs) that can't be remediated or deferred immediately. By automating the VI deferral process, you can defer the matching CVITs based on the rule when the system identifies them.

You can perform the following tasks for an exception rule:

- Create an exception rule in Container Vulnerability Response
- #unique_878
- Activating an exception rule in Container Vulnerability Response
- Reopen an exception rule in Container Vulnerability Response
- Update an approved exception rule in Container Vulnerability Response
- Delete an exception rule in Container Vulnerability Response
- Defer a container vulnerable item in Container Vulnerability Response

Note: Starting from v2.5 of Container Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the container vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the container vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Create an exception rule in Container Vulnerability Response

Create a rule to automatically request an exception for a specific condition for a group of container vulnerable items (CVITs), such as a rule with a condition that is based on the vulnerability severity of these CVITs. With this rule, you can defer new and existing CVITs automatically if they match the approved rule condition.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

The rule is applied from the "Valid from" until the "Valid to" date. The remediation task (VUL) is created when the rule is approved. The grouping method for this VUL is known as exception rules. The VUL is created in the Deferred state. You can't close, reopen, or delete this VUL. New and reopened CVITs are deferred and added to this VUL from the "Valid from" date until the group expires on the "Valid to" date.

Note:

Email notifications are sent at every stage of the exception rule work flow. These emails provide the status and other details of a request. For example, when an exception rule is requested, the requester receives an email that confirms that the request is submitted.

Note: If the rule is rejected, you can reopen it in the Draft state, update it, and then resubmit it for approval.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Rules**.
2. On the Exception Rule new record page, click **New** to create a rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the Exception Rule form, fill in the fields.

   Note: For more information on the form fields, see Exception Rule form.

4. Add the assignment group when you are creating the rule.
5. Submit the form for approval.
   The status of the request changes to In review. Until you submit the exception rule, it remains in the Draft state.
6. To view and create a group to manage exception rules:

   a. Navigate to **All** > **User Administration** > **Groups**.

   b. In an exception rule, click the **Requested Approvals** tab to view the status of the request.
   A scheduled job is run daily, which runs the exception rules on existing data. All the vulnerable items, which match the condition are moved to the Deferred state. If an approved exception rule is deleted, all the deferred vulnerable items revert to their previous state. For more information, see Working with an exception rule.

Activating an exception rule in Container Vulnerability Response

A rule is activated on its "Valid from" date. After activation, it automates the exception process for container vulnerable items (CVITs).

The exception rule follows this life cycle:

1. The new CVITs that you create or reopen, and that meet the specified condition, are deferred. If you enable the Execute on existing data option when you run the exception rule for the first time, all the active and non-deferred CVITs that match the exception rule condition are moved to the newly created remediation task (RT) and its state is changed to Deferred.
2. If a newly created CVIT matches the exception rule condition, it is moved to the deferred RT that is associated with the rule and the group rule is not run on it.
3. On the "Valid from" date, existing CVITs are added if you enable the Execute on existing data option.
4. The RT stops accepting new CVITs when the rule expires on the "Valid to" date. The RT remains in existence until the "Deferred until" date.
5. The exception rule expires on the "Valid to" date.

Reopen an exception rule in Container Vulnerability Response

Reopen an exception rule that has been rejected, but you want to resubmit. Reopening the rule moves it to the Draft state.

Before you begin

Role required: sn_vul.vulnerability_admin

About this task

You can then update and resubmit the rule for approval.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Rules**.
2. Find the rule that you want to reopen and click **Reopen**.
3. Update the form and resubmit it for approval.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Update an approved exception rule in Container Vulnerability Response

Cancel an approved rule to be able to update it. For example, before you can modify any dates or add a condition to an approved rule, you must cancel it so that the remediation task (VUL) is deleted, and the container vulnerable items (CVITs) move to the Open state.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Group rules are reapplied to these CVITs. Submit the rule after making the changes so that it goes through the approval process once again.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Rules**.
2. Open the exception rule that you want to cancel and click **Cancel**.
3. In the Cancel Rule dialog box, click **Cancel rule**.
   The rule moves back to the Draft state and the associated VUL is deleted. The related CVITs are reopened, and group rules are applied to the individual CVITs.

Delete an exception rule in Container Vulnerability Response

Delete an exception rule that is not required anymore. For example, you can delete a rule if you don't want to defer a container vulnerable item (CVIT) during ingestion.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
Deleting a rule cancels the associated remediation task (VUL). The related CVITs are reopened, and group rules are applied to the individual CVITs.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Rules**.
2. Open the exception rule that you want to delete and click **Delete**.
3. In the Delete Rule dialog box, click **Delete rule** to delete the selected rule.
   The associated remediation task is also deleted. The related CVITs are reopened, and group rules are applied to the individual CVITs.

Request an extension for a deferred remediation task in Container Vulnerability Response

Request an extension for a deferred remediation task (VUL) before it reaches its deferred until due date. As a remediation owner, you’re no longer required to wait until the deferred due date to make this request.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task
You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Remediation Tasks**.
2. Open a deferred remediation task.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date when the Defer state expires and the container vulnerable item is reactivated.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the changes on the remediation task are rolled down to the container vulnerable items as well, which are part of the remediation task. However, the container vulnerable items should be in the deferred state and their current until data precedes the updated until date. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred remediation task is extended again, the extend deferral count increases in the backend.

Request an extension for an exception rule in Container Vulnerability Response

Request an extension for a deferred exception rule before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.exception_approver

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Exception Rules**.
2. Select a deferred exception rule.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the exception rule must be extended.
Reason	Enter the reason for deferring the exception rule. Choices include: ○ Risk accepted ○ Awaiting maintenance window ○ Fix unavailable ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the Deferred until, Reason and Additional information fields get updated on the exception rule and the container vulnerable items. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- The Request Extension button is unavailable for remediation tasks that are created as part of an exception rule.
- If a deferred exception rule is extended again, the extend deferral count increases in the backend.

Marking and approving a false positive container vulnerability item

Container Vulnerable items (CVITs) and remediation tasks (VULs) can be marked as false positives. Approvers with write access can approve such requests from other users.

- Mark as a false positive in Container Vulnerability Response
- Approve a false positive

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

Email notifications are sent at every stage of the false positive workflow, providing the status and other details of a request. For example, when a CVIT or remediation task is marked as a false positive, the requester receives a confirmation email. Simultaneously, the approver receives an email stating that a CVIT or remediation task has been marked as a false positive. Starting from v2.5 of Container Vulnerability Response, you can configure the time frames for approving false positives and exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the container vulnerable item changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the container vulnerable item or remediation task reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Important: As a Vulnerability analyst and remediation owner, you can request and approve false positives from the Vulnerability Manager Workspace and IT Remediation Workspace respectively.

Mark as a false positive in Container Vulnerability Response

Mark a container vulnerable item (CVIT) or remediation task as a false positive if the warning given by the scanner is not actually an issue. For example, if a CVIT has been decommissioned but the scanner is still raising an issue related to it, mark it as a false positive.

Important: As a Vulnerability analyst and remediation owner, you can request false positives from the Vulnerability Manager Workspace and IT Remediation Workspace respectively.

Before you begin

Role required: remediation owner

Procedure

1. Navigate to **All** > **Container Vulnerability Response (or Remediation Tasks)** > **All**.
2. Open the CVIT you want to mark as a false positive and click **Mark as False Positive**.
   The CVIT must be in an **Open** state.
3. On the False Positive form, enter details in **Additional information** and click **Request Approval**.
   The request is sent for approval and the State of the CVIT changes to **In Review**. Both the requester and approver are notified via email.

Approve a false positive

As a false positive approver, you can approve false positive requests from other users.

Important: You can approve or reject false positive requests in the Vulnerability Manager Workspace. For more information, see Approve or reject requests in the Vulnerability Manager Workspace.

Before you begin

Role required: false_positive_approver

You can also approve exception and false positive requests in the classic environment:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Note: A false positive can be time bound. Only the approver can set the end date.

Container Vulnerability Response remediation tasks and task rules overview

Configure remediation tasks (CVULs) to help analysts and remediation specialists organize container vulnerable items (CVIT) and analyze them in bulk. The criteria by which remediation tasks are formed are configured so that CVITs are automatically assigned into remediation tasks. Using remediation tasks, you can monitor progress and drive the remediation process more efficiently.

Removing assignments from container vulnerable items and remediation tasks

Starting with version 2.13, you can clear the **Assigned to** and **Assignment group** fields on container vulnerable items (CVITs) directly from the CVIT and remediation task records that you determine might be incorrectly assigned to you or your groups.

See Removing assignments from container vulnerable items and remediation tasks and Remove assignments from vulnerable items and remediation tasks for more information.

Tracking deferral counts for container vulnerable items and remediation tasks

Track the number of times a vulnerable item, application vulnerable item, container vulnerable item, or remediation task is deferred. The set deferral counts scheduled job runs daily to post counts for the records that are deferred more than once in the Deferral count column. Records are displayed in the Multiple deferrals modules for VR, AVR, and CVR.

Understanding remediation task rules

Remediation task rules enable you to define how container vulnerable items are automatically grouped and assigned. A default rule **Vulnerability** is included in the base system that gathers CVITs based on their vulnerabilities. However, you can group by any other set of values in columns accessible from the CVIT. These values could include configuration item (CI), vulnerability entry, and the like.

There are task rules for Container Vulnerability Response that are included with the Vulnerability Response application that is available when you activate it.

You can create multiple conditions with the condition builder. In the Group by section, after you set a field pair, another row appears. You can have up to six **Group by** selections. You can automate group assignment as well.

For example, you can group your container vulnerable items by the configuration item, or by the product model. You can have one task rule for low severity vulnerabilities or low risk CIs. You can have another task rule for critical servers, and vulnerabilities that expose the company to more risk. See Create, edit, and delete Container Vulnerability Response remediation task rules for more information about the options that you have available to you.

A different set of rules can be used for container vulnerable items that expose the company to more risk. The remediation task name is appended to the remediation task rule **Group by** values to make the short description of the new record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When a new container vulnerable item is created, imported, or reopened after being closed, the rules are evaluated against it. A CVIT is only evaluated once, automatically, unless it's reopened after being closed or the rules are reapplied manually.

The following process is used for each new or reopened CVIT:

- For each remediation task rule, the CVIT is compared to the remediation task rule filter.
- For each rule where the remediation task rule condition matches, the rule pulls the data from the **Group by** selections on the CVIT. It builds a group name and field. In this case, **High Risk: QID-32342:Summary of QID-3242** (Name: vulnerability ID: vulnerability summary).

> **Note:** The short description field is limited to 160 characters. Longer vulnerability summaries are truncated.

The rule checks to see if there's a matching **Open** remediation task that is assigned to the same assignment group as the CVIT.

- If the task is found, the CVIT is added to the existing task in the **Open** State.
- If no task in the **Open** state is found, the rule creates a **High Risk: QID-32342** task, assigns it to the same assignment group as the CVIT, and places the CVIT in the remediation task.

More than one remediation task rule can be defined to group different kinds of vulnerabilities. Since each vulnerability is compared with the remediation task rule conditions before putting it in a remediation task, too many rules might impact performance. Set up your task rules so the conditions help you avoid creating duplicate remediation tasks.

By default, remediation task rules use the assignment group set by the **Assignment Rules** on the CVIT when grouping the items and assigns the remediation task to match the CVITs.

As part of the default task rule, the assignment of these remediation tasks is controlled by the rules in the **Assignment Rules** module. For more information on assignment rules, see Vulnerability Response assignment rules overview.

When a task rule is deleted from the form or list view, you have the option to delete all Open tasks created by that rule. Tasks not in the **Open** State are excluded.

Reapplying remediation task rules

When you want to change a remediation task rule, use the **Reapply** button on the remediation task rule page to rerun the changed rule on all active **Open** remediation tasks created by that rule. It deletes and recreates remediation tasks based on the changed rule automatically.

Reapply only checks existing remediation tasks.

After you select **Reapply**, the following message is displayed: Reapplying this remediation task rule will delete and re-create the remediation tasks for this rule. Remediation tasks that are not in the Open State aren’t deleted.

> **Important:** As a vulnerability admin and analyst, you can evaluate the remediation task rules for selected vulnerable items in the Vulnerability Manager Workspace. This method is more efficient than reapplying the Remediation Task Rules in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Remediation task rules and CVIT creation and update

If a CI from a scan is associated with a known vulnerability, a CVIT is created. After it's created, the CVIT is evaluated against the conditions of remediation task rules for a match. If there’s a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

match to an existing remediation task, the CVIT is added. If a matching remediation task isn't found, one is created for the CVIT.

If any property that is captured in the remediation task filtering conditions is updated or changed on a CVIT, the updated AVI is also evaluated against the remediation task rules for a match. If there's a match to an existing remediation task, the CVIT is added. If a matching remediation task isn't found, one is created for the CVIT.

State rollup and rolldown

If you update a remediation task to Open, or from Open to Under Investigation, the new state rolls down to all associated CVITs. State roll down occurs immediately after you change the State.

State rollup from CVITs to the remediation task only occurs if all the CVITs on the task are in **Deferred** or **Closed- fixed** states. Rollup is done with the Rollup container vulnerable item values to vulnerability and a group-scheduled job, which runs every 15 minutes. The state is not rolled up until the job runs. For a State to roll up to occur from the CVITs to the remediation task, all the CVITs must be in the same State.

Create, edit, and delete Container Vulnerability Response remediation task rules

You can create rules to automatically group container vulnerable items (CVIT) into remediation tasks (CVUL) based on filter conditions. These rules automatically group CVITs as they're imported or manually created.

Before you begin

If you create a new rule, it doesn't apply to existing data. After you submit it, it's run against new imports.

Role required: App-Sec Manager

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Administration** > **Remediation Task Rules.**.
2. Open the rule or select **New**.
3. Fill in the fields on the form or edit them.

Remediation Task Rule

Field	Description
Name	Name of the task rule.
Active	Indicates whether the task is active.
Description	Description of the rule.
Case sensitive	Determines whether a condition is case sensitive or not. **Note:** The default value is case insensitive.
Condition	Optional filter conditions for the rule. By default, (**Case sensitive** check box not selected), the search text you enter in the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	condition builder on task rules records and forms isn't case-sensitive. You have the option to enable case-sensitive searches on task records and forms. An example condition is **Vulnerability** > **is** > **VULNENT123451** (a known imported vulnerability). Any CVIT that have this vulnerability match this condition.
Group by (up to six condition sets are available)	
Group container vulnerable items from	The table the rule uses to group CVITs. Select the elements from the tree: ○ Container Vulnerable Item [sn_vuln_vulnerable_item] ○ Container Vulnerable Item - Docker Image ○ Container Vulnerable Item – Container Vulnerability **Note:** If you choose an extended table, the **Using field** is applied only for application vulnerable items that use that extended table.
Using field	Field on the table that the rule uses to group CVITs. Select conditions from the tree.
Assignment	
Assign remediation tasks by	When automatically assigning remediation tasks, the Assignment choice is used in addition to the **Group By** choices to group the vulnerable items. New tasks are created, as needed, so that each CVIT is placed in a task with a matching assignment group set. To automate the assignment of tasks created based on this rule, choose one of the options available. ○ Group by field: If you selected any user group field from the **Using field** values in the **Group by** section, they appear in the drop-down menu. ○ User Group: Use the lookup list to select a static user group.

Note: if you delete a rule from either the form or list view, you have the option to delete all Open remediation tasks created by that rule. Groups not in the Open state are excluded.

4. Select **Submit** for new rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you select **Submit**, your rule is displayed on the Remediation Task Rules list [sn_vul_grouping_rule]. The following situations initiate your rule.

- When new CVITs are created.
- When you select **Reapply**. You select **Reapply** to evaluate task rules on existing remediation tasks only.
- When CVITs are updated, either by you or by the system.

  If an CVIT is updated, task rules are evaluated for matches to existing remediation tasks. Some common updates that initiate a rules check are:

  - When the State changes from Closed to Open, or from Closed to Under Investigation.
  - The configuration item (CI) is changed.
  - The vulnerability is changed.

The system checks all the task rules for matches to the updated CVIT. If the conditions of a rule match the conditions of a remediation task, matching CVITs are assigned to it.

If no match is found, a new remediation task is created.

For more information about state roll up from CVITs to remediation tasks and state roll down from remediation tasks to CVITs, see Container Vulnerability Response remediation tasks and task rules overview.

For an example of a remediation task rule, see Application Vulnerability Response remediation task rule examples.

5. To delete a task rule, select the rule from the Remediation Task Rules list and select Delete. The following message is displayed: `The selected remediation task rule created n remediation tasks. Of the remediation tasks, n are in the Open state.`

Option	Description
Check box deactivated (default).	Only delete the rule. Tasks not in the Open state are excluded.
Check box selected.	Include the remediation tasks in the Open state when you delete the remediation task rule. Delete the rule and any remediation tasks in the Open state.

6. Choose one option and select **Delete**.

Create auto-close rules for Container Vulnerability Response

Use auto-close rules to close older container vulnerable items (CVITs) automatically based on the filter conditions that you set.

Before you begin

Role required: sn_vul.container_manage_auto_close_stale_vi

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Container Vulnerability Response** > **Container Vulnerable Items** > **Auto-Close rules**.

   The base system provides the following auto-close rules: **Container Vulnerabilities last scanned**: Vulnerabilities not reported within the last 90 days are transitioned to Stale State.

2. Select **New** to create auto-close rule.
3. Fill in the fields on the form.

Field	Value
Name	Name of the auto-close rule.
Active	Option to activate the rule. If activated, it closes any detections automatically that match its filter criteria.
Execution order	Unique value for the execution of the auto-close rule. This value determines the order of execution. The default value is 100.
Integration type	Container Vulnerability Integration **Note:** To scan host vulnerabilities using Prisma Cloud Compute integration, select **Vulnerability Scanner Integration**.
Description	Description of the auto-close rule.
Condition	Filter conditions used to identify detections that should be closed.

4. Select **Submit**.
   The **Auto-Close** rules scheduled jobs run on a daily basis. It identifies CVITs based on the specified conditions and transitions the matching ones to the **Stale** state. In cases where there are CVITs with both Closed and Stale statuses, the CVIT is closed with the sub state set as Fixed.

Removing assignments from container vulnerable items and remediation tasks

You can clear the **Assigned to** and **Assignment group** fields on container vulnerable items directly from the container vulnerable item and remediation task records that you determine might be incorrectly assigned to you or your groups.

Overview for the workflow

If you determine that container vulnerable items (CVITs) and remediation tasks (CVULs) aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups, you can remove yourself or your groups from the **Assigned to** and **Assignment group** fields on CVIT and CVUL records.

The unassign workflow is supported both classic and workspace views for CVITs and CVULs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have the option to send requests to clear the assignment fields for approval. See Approve or reject an unassign request in Vulnerability Response and Removing assignments from vulnerable items and remediation tasks for more information.

- The **Unassign** UI action is displayed on CVIT and CVUL records in any state other than the Closed or Resolved.

  Note: After the request to clear the fields is approved for a CVUL, all the **Assigned to** and **Assignment group** fields on CVITs that have the same assignment group are unassigned. If any CVIT on a CVUL has a different assignment group than its associated CVUL, it is not unassigned. In most cases these CVITs have been manually assigned. See Container Vulnerability Response remediation tasks and task rules overview and Removing assignments from vulnerable items and remediation tasks for more information.

- Any records that you update with either the UI action or manually are displayed on the Unassigned module for Container Vulnerability Response.

See Remove assignments from vulnerable items and remediation tasks for more information about the steps for how to clear the assignment fields.

System properties and approval notifications

If a remediation owner selects **Unassign** on a record, by default, the sn_vul.unassign_vr.approval_required system property triggers the approval flow and creates a state change approval record in the Review state, and the request is routed for approval. The request is displayed on the My Approvals list for users with the sn_vul_container.unassign_approver.

Note: As a vulnerability administrator [sn_vul.vulnerability_admin], you can set the *sn_vul.unassign_vr.approval_required* system property to **false** to disable the approval process.

Additionally, you can change the value in the *sn_vul.default_assignment_group* system property so if the assignment fields are cleared, a specific group is assigned. For example, if a user clicks **Unassign** on a record and you want to redirect it to a specific group for review, you can add the system ID for the group of your choice in the value field of the system property.

Note: If you change this value, notifications for all the VITs, AVITs, and CVITs that are unassigned are sent to the group you specify.

Close a remediation task

If you determine that the issue associated with an application remediation task can be immediately closed without further analysis, you can use the **Close** feature. Starting with v2.10 of Container Vulnerability Response, the **Close** button has been removed for an container remediation task.

Before you begin

Role required: admin

About this task

In the Vulnerability Response Workspaces, a remediation task transitions through the same states as a remediation task prior did in previous versions of Vulnerability Response. When all the vulnerable items (VITs) in a remediation task are closed, the remediation task transitions to the Inactive state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: You can manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a CHG has changed its state, or you add a CHG or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move remediation tasks from the `Closed` or `Deferred` states.

Procedure

1. Open the record that you want to request a review for.
2. Select the **Close** button.
3. Fill in the fields on the form, as appropriate.

Field	Description
State	Select the state as *Closed*.
Reason	Enter the reason for closing the issue.
Additional information	Enter any other relevant information.

4. Select **Submit**.
   The remediation task is marked **Closed**.

IT Operations Management and pattern discovery

When discovery is enabled, information is received from the Information Technology Operations Management (ITOM) team. If the ITOM Discovery is enabled, you can see Kubernetes Namespaces, Kubernetes Clusters, and Kubernetes Services when you open a container vulnerable item (CVIT). Else, you can see Prisma payload information.

The image labels from the Prisma payloads are stored as key value pairs under the docker image. The labels in a Prisma payload are stored in the cmdb_key_value table. To enable this feature, an identification rule is shipped for cmdb_ci_docker_image by the ITOM team. Open the Docker image to view the related items list. Most of the items are populated by the ITOM team. The identification entry for a docker image is shipped to show the values as key value pairs.

The business criticality is determined based on the service criticality information received from the ITOM team. A scheduled job is run to pull data from all the services associated with an image. It calculates the business criticality based on service mapping. As the risk score can depend on business criticality, the risk score is also calculated based on it.

Analytics and Reporting Solutions for Container Vulnerability Response

This Platform Analytics Solution contains prepackaged Platform Analytics content for use with other ServiceNow AI Platform products. This Platform Analytics Solution provides an exposure on how vulnerabilities are managed through the various charts.

Required roles

The following roles and tasks are associated with this Solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Analytics and Reporting Solution and make any necessary changes to system properties.
- Platform Analytics administrator (pa_admin): Review the indicators, breakdowns, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Analytics and Reporting Solutions

Container Vulnerability Response dashboard

Analytics and Reporting Solutions contain prepackaged Performance Analytics and Reporting content for use with other ServiceNow AI Platform products. This Platform Analytics Solution permits you to track the volume, performance, and progress of vulnerabilities from initial analysis and detection to containment, or remediation. You can filter reports by assignment group, exploits, risk rating, or state.

Required ServiceNow AI Platform roles

- ServiceNow AI Platform administrator (admin): Install and activate this Analytics and Reporting Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the indicators, breakdowns, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.

Access the Container Vulnerability Response dashboard

To open the dashboard, navigate to **All** > **Container Vulnerability Response** > **Overview**.

Important:

Starting with version 2.2 of Container Vulnerability Response, this dashboard can also be viewed in the Next Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and select the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, select the drop-down next to the dashboard name. For more information, see Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

Note:

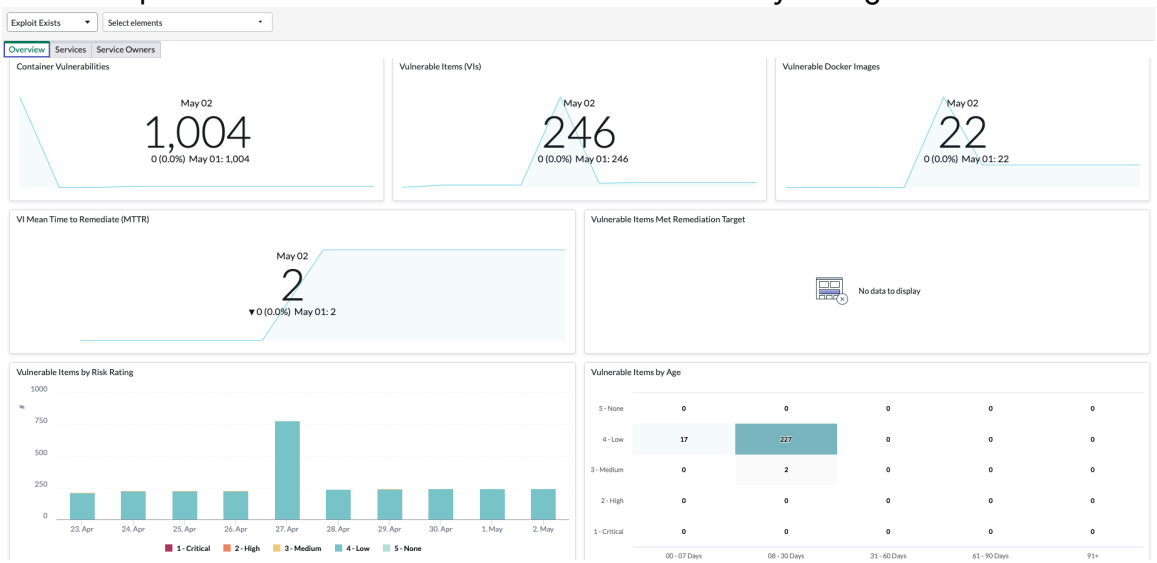
- If you're a new user, you can view the dashboards only from the workspaces.
- If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Container Vulnerability Management tabs

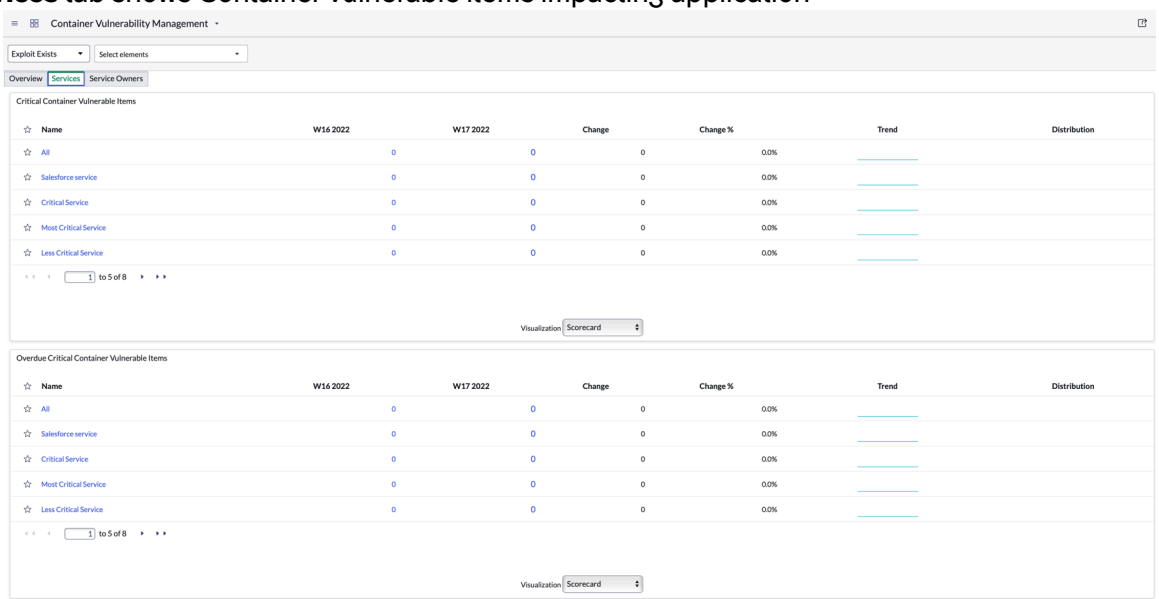
This dashboard lets you see the vulnerabilities that are present in containers. You can view the vulnerabilities and their related data by region, age, services, and other breakdowns.

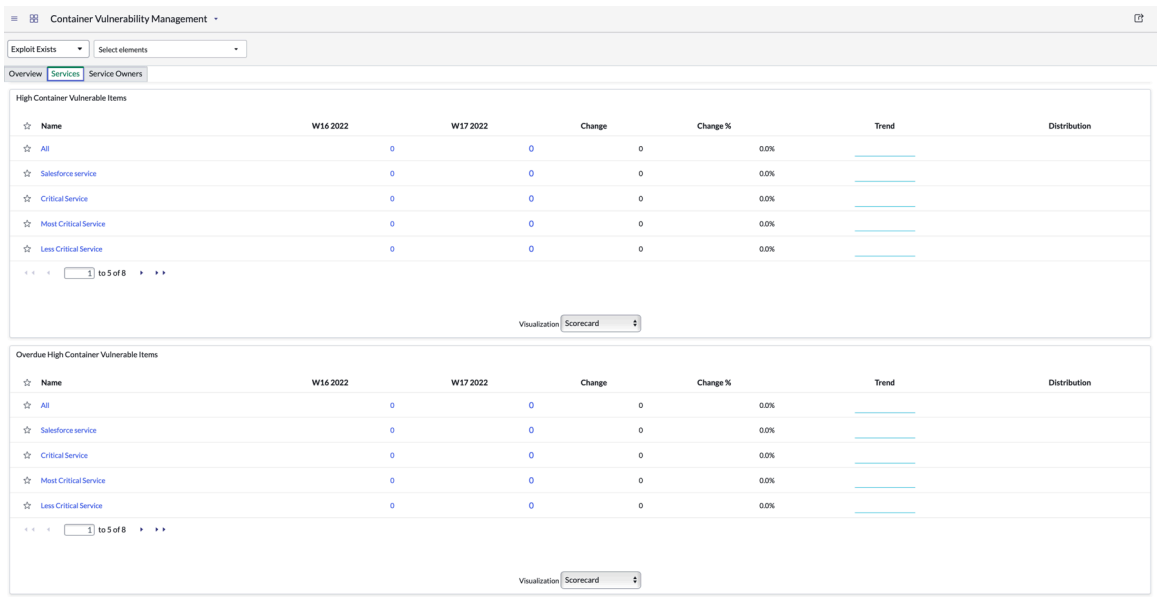
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Overview** tab provides the overall status of Container Vulnerability Management in the system.



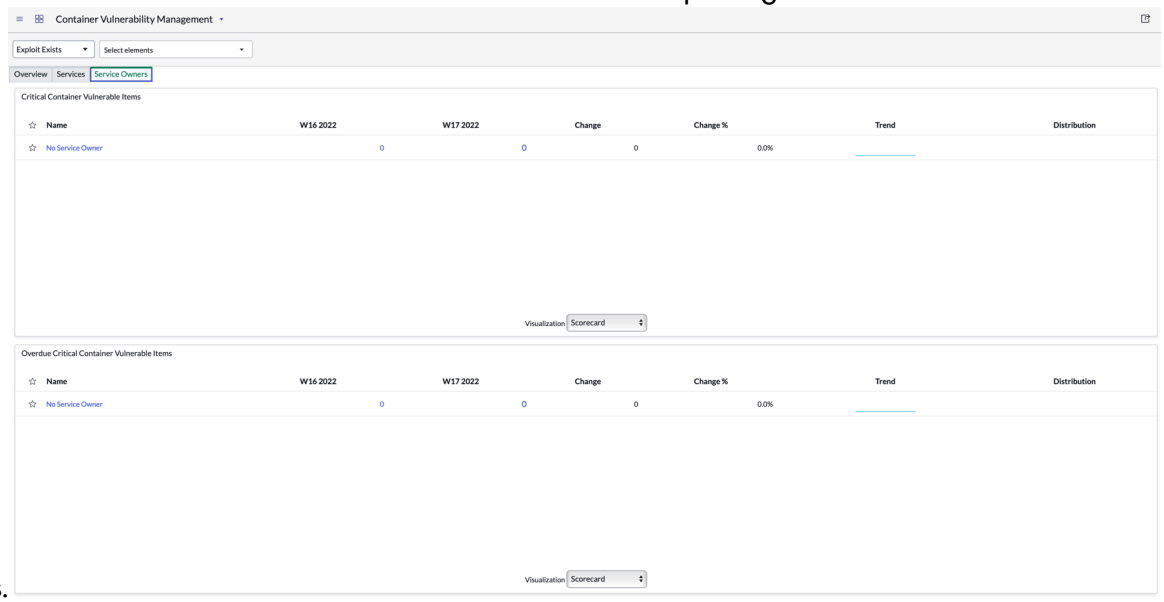
The **Services** tab shows Container vulnerable items impacting application services.

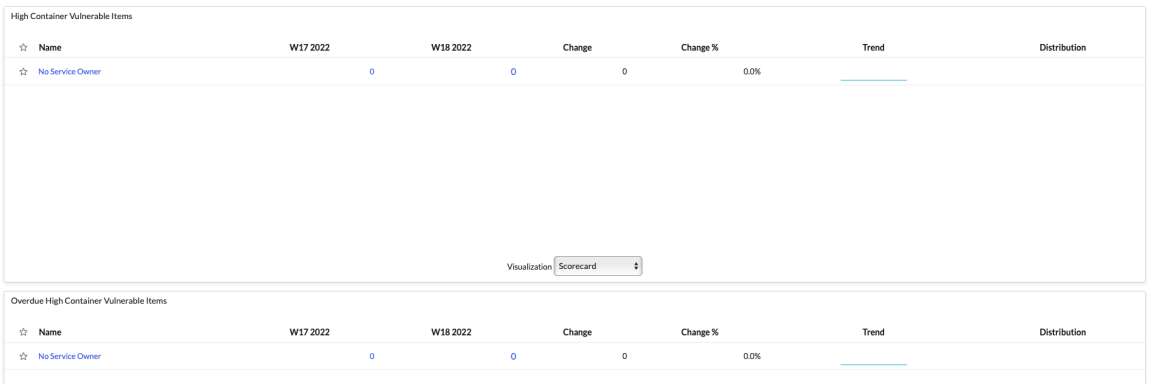




© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Service Owners** tab shows Container vulnerable items impacting service owners.





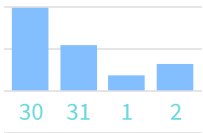
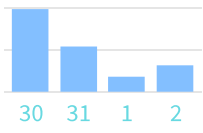
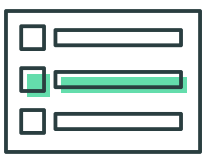
Breakdowns

- Exploit Exists
- Exploit Attack Vector
- Exploit Skill Level
- Remediation Target Status
- Risk Rating
- State
- Assignment Group

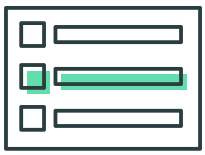
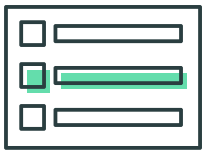
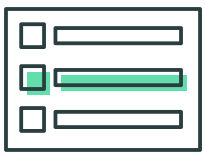
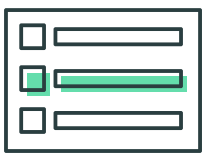
Data visualizations

Name	Type	Description
Container Vulnerabilities	42 Single score	Number of container vulnerabilities associated with one or more active container vulnerable items.

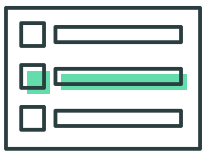
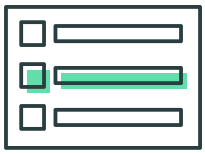
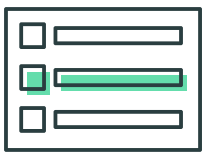
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Type	Description
Vulnerable Items (VIs)	Single score 	Number of active (non-closed) container vulnerable items.
Vulnerable Docker Images	Single score 	Number of docker images associated with active container vulnerable items.
VI Mean Time To Remediate (MTTR)	Single score 	The mean time to remediate (close) a vulnerable item, displayed as a 30-day running average.
Vulnerable Items Met Remediation Target	Single score 	Percentage of closed container vulnerable items that have met their remediation target dates in the current and previous quarters. Remediation targets are calculated from the Last Opened date plus the number of days.
Vulnerable Items by Risk Rating	 Bar	Number of active container vulnerable items grouped by risk rating over the selected time span.
Vulnerable Items by Age	 Bar	Number of active container vulnerable items grouped by risk rating and age (in days).
Critical Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a critical risk rating, grouped by service.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Type	Description
Overdue Critical Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a critical risk rating and past their remediation target dates, grouped by service.
High Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a high risk-rating, grouped by service.
Overdue High Container Vulnerable Items	List and  Line 	Number of active vulnerable items with a high risk-rating and past their remediation target dates, grouped by service.
Critical Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a critical risk rating, grouped by service owner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Type	Description
Overdue Critical Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a critical risk rating and past their remediation target dates, grouped by service owner.
High Container Vulnerable Items	List and  Line 	Number of active container vulnerable items with a high risk-rating, grouped by service owner.
Overdue High Container Vulnerable Items	List and  Line 	Number of active vulnerable items with a high risk-rating and past their remediation target dates, grouped by service owner.

Aggregated reports framework for Container Vulnerability Response

Using the aggregated reports framework, you can create reports for the data that involves complex and long-running on-the-fly queries for better performance.

The aggregated reports framework improves the performance by:

- using lesser resources and rendering reports faster,
- aggregating the data and reusing aggregations and breakdowns (Group By) and
- reducing the queries to the database

When you have more than one million container vulnerable items (CVITs), use the aggregated reports framework alongside the standard reports.

Required roles

The following roles and tasks are associated with this solution:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- ServiceNow AI Platform administrator (admin): Install and activate this Platform Analytics Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the aggregations, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.
- Admin (sn_vul_cmn.admin): Create aggregations.
- VR write(sn_vul_cmn.write): Edit the data in the Aggregations and Aggregated Results.
- VR read (sn_vul_cmn.read): Review the data in the Aggregations and Aggregated Results.
- Vulnerability analyst (sn_vul.vulnerability_analyst): Review Aggregated Results.

Related topics

Configure an aggregation for source data

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Create a report using an aggregation

Container Vulnerability Response reference

Reference topics containing information about tables, roles, and properties installed with the Container Vulnerability Response.

Components installed with Container Vulnerability Response

Several types of components are installed with activation of the Container Vulnerability Response application, including tables, user roles, and scheduled jobs.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Starting with v2.11 of Container Vulnerability Response, the most frequently used system properties are now accessible within the Container Vulnerability Response application. To view these system properties, navigate to **All** > **Container Vulnerability Response** > **Properties**.

Roles installed with Container Vulnerability Response

Roles are added with activation of Container Vulnerability Response.

Persona and granular roles are available to help you manage what users and groups can see and do in the Vulnerability Response application. For an initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant. For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

If you are an upgrade customer, access for the users and groups you assigned with the sn_vul.vulnerability_read and sn_vul.vulnerability_write permissions prior to v10.3 has not changed. Users and groups remain assigned with these roles until you change them. However, starting with v10.3, you may prefer assigning granular roles for more control over what users and groups can do and see in the Vulnerability Response application. For an overview and more information about managing these roles, see Vulnerability Response personas and granular roles and Manage persona and granular roles for Vulnerability Response.

Role title [name]	Description
sn_vul_container.delete	Deletes source records. Con the sn_vul_cmn.delete, and sn_vul_container.delete_vi ro
sn_vul_container.ci_manager	Manages reclassification of u configuration items (CIs).
sn_vul_container.configure_integrations	Configures container integra
sn_vul_container.configure_vi_granularity	Configures container vulnera granularity.
sn_vul_container.create_vi	Can create container vulnera manually.
sn_vul_container.delete_vi	Can delete manually created vulnerable items.
sn_vul_container.exception_approver	Approves exceptions, deferr closures of container vulnera Contains sn_vul.view_manager_worksp Starting with v2.3, the granul sn_vul_container.read_all, ha removed for this role so that access the container vulnera and remediation tasks assign and your group instead of all vulnerable items and remedi
sn_vul_container.false_positive_approver	Approves or rejects closing c vulnerable items as a false p Contains the sn_vul.view_manager_worksp
sn_vul_container.manage_assignment_rules	Defines and updates contain items assignment rules.
sn_vul_container.manage_auto_close_stale_vi	Configure the auto-close sta vulnerable items
sn_vul_container.manage_auto_exception_rule	Manage (create/read/update exception rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description
sn_vul_container.manage_normalized_severity	Can update the mapping to r severity.
sn_vul_container.manage_permissions	Can assign container vulnera response roles to users.
sn_vul_container.manage_remediation_target_rules	Defines and updates contain remediation target rules.
sn_vul_container.manage_risk_score_configuration	Defines and updates risk sco Calculators, risk rules, and vu Rollup Calculators for Contai Vulnerable Items.
sn_vul_container.read_all	Can view all container vulner and related information. Contains the sn_vul.view_manager_works
sn_vul_container.read_assigned	Can view container vulnerab assigned to you or your grou in the Classic UI or IT Remed Workspace. Contains the sn_vul.view_rer role. **Important:** Starting w of Vulnerability Respons sn_vul_container.read_a has the privilege to acce Remediation Workspace
sn_vul_container.read_assignment_rules	Can view container vulnerab Assignment Rules.
sn_vul_container.read_auto_exception_rule	Read Exception rules
sn_vul_container.read_discovered_image	Can view discovered items.
sn_vul_container.read_integrations	Can view results from integra
sn_vul_container.read_normalized_severity	Can view the normalized sev mapping.
sn_vul_container.read_remediation_target_rules	Can view Remediation Targe
sn_vul_container.read_risk_score_configuration	Can view risk score calculato and vulnerability rollup calcu Container Vulnerable Items.
sn_vul_container.remediation_owner	Reads and writes container v items assigned to them. Vuln records are also readable by this role.
sn_vul_container.update_assigned_to	Can update assignment of c vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description
	Requires sn_vul_container.w sn_vul_container.write_assig
sn_vul_container.update_assignment_group	Can update assignment grou container vulnerable items. Requires sn_vul_container.w sn_vul_container.write_assig
sn_vul_container.update_state	Can update states of vulnera Requires sn_vul_container.w sn_vul_container.write_assig
sn_vul_container.vulnerability_admin	Configures all rules, integrati so on for the Container Vulne Response product.
sn_vul_container.vulnerability_analyst	Monitors remediation of all c vulnerable items.
sn_vul_container.write_all	Can update all container vul and remediation tasks.
sn_vul_container.write_assigned	Can update container vulner remediation tasks assigned groups.
sn_vul_container.read_watch_topic	Can read Watch Topics for c vulnerabilities.
sn_vul_container.create_watch_topic	Can create Watch Topics for vulnerabilities.
sn_vul_container.edit_watch_topic	Can edit Watch Topics for co vulnerabilities.
sn_vul_container.manage_exception_configuration	Can manage exception mana configurations.

Tables installed with Container Vulnerability Response

Tables are added with activation of Container Vulnerability Response (CVR).

Table	Description
Container image finding sn_vul_container_image_findings	Stores information on the associated vulnerabilities, image layer, docker image,image repository, and discovered image. Starting with v2.11.3 of Container Vulnerability Response, you can also view the path where the finding is shown.
Container Image Layer sn_vul_container_image_layer	Contains the information of each image layer. An image is a static file with executable code that can create a container on a computing system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Container Image Package sn_vul_container_image_package	Provides information about the packages where the vulnerabilities exist. The Binary package details are also provided as a comma-separated value. Starting with v2.11.3 of Container Vulnerability Response, you can also view the package URL (PURL).
Container vulnerable item sn_vul_container_image_vulnerable_item	Contains details of each finding and the corresponding vulnerability. Starting with v2.11.3 of Container Vulnerability Response, you can also view information on the last scan date of an image running as a container.
Vulnerability Entry sn_vul_entry	Provides information on the severity of a CVE and any additional information sent by Prisma.
Discovered container image sn_vul_container_image	Provides information on the image ID, Docker image, and the image repository. It also stores the layer information and associates it with the discovered image. Starting with v2.11.3 of Container Vulnerability Response, it also provides information on Image digest of a docker image and last scan date of an image running as a container and a registry.
Finding Mappings sn_vul_container_finding_m2m_vul_item	M2M relationship of the container image findings and the container vulnerable items (CVITs).
Auto-close Vulnerable Items sn_vul_container_image_auto_close_config	Contains the information on how to close the stale container image findings and roll up the state to the CVITs.
Container Image Vulnerability Keys sn_vul_container_image_vulnerability_keys	Contains the granularity configuration for creation of CVITs from the container image findings.
Docker Related Services sn_vul_cmn_m2m_ci_services	Contains all the business services related with a container image.
VR Container Counts sn_vul_container_vr_container_counts	Contains the rolling average of container instances spun off from a container image over the last 90 days.
Container Remediation Task Item sn_vul_container_m2m_vul_group_item	M2M table between CVIT and container remediation tasks.
Container Remediation Task sn_vul_container_vulnerability	Contains container remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Container Remediation Task Manifest sn_vul_container_rt_manifest	Any updates on remediation task will be done by using this manifest table by scheduled jobs.

Scheduled jobs installed with Container Vulnerability Response

Scheduled jobs are added with activation of Container Vulnerability Response.

Scheduled job	Description
Associate existing Container VIs with Auto Exception Rule	Automatically associates the Auto Exception Rule with existing container vulnerable items (CVITs).
Check Container Vulnerable Item Deferment Expiration	Sends notifications if container vulnerable items or container vulnerabilities have expired (and if they expire in one week).
Vulnerability Response Container Count (Application - Vulnerability Response and Configuration Compliance for Containers)	Runs daily to populate the sn_vul_container_vr_container_counts table that calculates the 90-day rolling average for containers.
Auto-Close CVITs	Automatically closes container vulnerability items that match the condition defined in the auto-close configuration. Their status is changed to 'fixed'.
Calculate Business Criticality for CVIT	Processes all active CVITs and updates the Business Criticality field, based on the affected services of the docker image of the CVIT.
Close cancel CVITs that do not have a Docker Image associated	Automatically expires CVITs that don't have a CI associated with. Their state is set to Closed, and substate to Canceled.
Calculate Related VI Counts for Container Remediation Task	Calculates the counts on Container Remediation Task records.
Rollup container vulnerable item values to vulnerability and group	Calculates vulnerabilities and group roll ups for container vulnerable items. **Note:** Starting with v2.10 of Container Vulnerability Response, the scheduled job is enhanced to create background jobs with multithreading capabilities. This upgrade involves segmenting the job into several smaller child jobs, which are executed either in parallel or concurrently. This modification enables processing of multiple records simultaneously, thus significantly speeding up the overall task.

Container Vulnerability Response glossary

Learn about terms and concepts that are unique to Container Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key terms

Container

A unit of software, which packages the code and all its dependencies so that the application runs seamlessly and reliably from one computing environment to another.

Container image

A static file with executable code that can create a container on a computing system. A container image cannot be changed and thus can be deployed consistently in any environment.

Cluster

A set of worker machines, called nodes, that run containerized applications.

Docker

Software to create, deploy, and manage application containers on servers and the cloud.

Docker Image

A template file that contains code, required libraries, configurations, and so on. The file is used to launch container instances. It consists of a union of layered file systems.

Dockerfile

A text file containing instructions to create container images by adding multiple layers. For example, layering of Base Ubuntu, Nginx, and App code.

Docker Compose

A tool for defining and running complex applications with Docker. With Compose, you can define a multi-container application in a single file.

Docker Container

A Docker Container is a runtime instance launched from a Docker Image.

Image Layer

A layer is a modification to an image. It is represented by an instruction in the Dockerfile. Layers are applied in sequence to the base image to create the final image.

Image Repository

A collection of docker images with different tags or versions.

Image Labels

A set of key-value pairs stored with the image as metadata.

Namespace

An abstraction used by Kubernetes to support the isolation of groups of resources within a single cluster.

Pod

A set of running containers (another abstraction on top of a container).

Registry

A hosted service containing repositories of images.

Service

An abstract way to expose an application running on a set of pods as a network service.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tag

A tag is a label applied to a Docker image in a given image repository. Tags are how various images in a repository are distinguished from each other.

Container Vulnerable Item form fields

Container vulnerable items (CVITs) are automatically created during third-part vulnerability integration imports.

Container vulnerable item form fields

Except for the **Assignment group**, **Assigned to** fields and **Notes**, all other fields in the CVIT are read only.

Field	Description
Number	Automatically generated CVIT identifier for this record.
Source	Scanner that has identified the vulnerability.
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None.
Risk score	Calculated amount of risk the CVIT poses to your environment.
Remediation target rule	Remediation target rule according to which the remediation target date is calculated.
Remediation target	Date by which the CVITs should be remediated, since first identified. Only appears when applicable.
Remediation status	Status of the remediation for the CVIT.
Vulnerability	ID of the vulnerability associated with this application vulnerable item.
Docker Image	Template file that contains code, required libraries, configurations, and so on. The file is used to launch container instances. It consists of a union of layered file systems.
Discovered Container Image	Unique record for each image ID.
Base Image	A foundational image used to create containerized applications, containing the essential operating system and libraries. It serves as the starting point for building and customizing applications in environments like Docker.
Image Clusters	Groups of related images used in various contexts, such as clustering similar images in machine learning or container images in a repository.
Image namespace	Used to organize and isolate container images within a registry, enabling different teams or projects to maintain separate collections.
State	This field defaults to **Open** when created. See Application Vulnerable Item (AVI) states for more information on how states are mapped.
Assignment group	Group selected to work on this CVIT.
Assigned to	Individual from the selected assignment group that works on this CVIT. Can be manually added or edited by an App-Sec Manager.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created	Date and time at which a CVIT is created.
Last Opened	Latest date and time at which the CVIT is reopened.
Updated	Date and time at which the CVIT is last modified.
First found (v2.12.1)	Date the vulnerability was first found. Starting with v2.12.1, you can see the precise date and time when it was first discovered, ensuring clarity and accounting for different time zones. To populate the first found date and time details, the integration must be rerun.
Last found (v2.12.1)	Date the vulnerability was last found. Starting with v2.12.1, you can see the precise date and time when it was last found, ensuring clarity and accounting for different time zones. To populate the last found date and time details, the integration must be rerun.
Resolution date(v2.12.1)	Date the vulnerability was resolved. Starting with v2.12.1, you can see the precise date and time when it was resolved, ensuring clarity and accounting for different time zones. The resolution date is populated when the CVIT is resolved as part of the workflow.
Last opened (v2.12.1)	Date the vulnerability was last opened. Starting with v2.12.1, you can see the precise date and time when it was last opened, ensuring clarity and accounting for different time zones. The scheduled job *`Add default values for last_opened_dt_tm from last _opened`* populates the data in this field. It must be executed only once on-demand.
Vulnerability	
Summary	Description of the vulnerability.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for National Vulnerability Database (NVD) and with ServiceNow third-party integrations.
Vulnerability score (v3)	Common Vulnerability Scoring System (CVSS) v3 score.
Vulnerability score (v2)	CVSS v2 score.
Exploit exists	Yes, if at least one exploit is associated with the vulnerabilities associated with this vulnerable item.
Exploit attack vector	Most vulnerable attack vector of the exploits for the vulnerabilities associated with this vulnerable item.
Exploit skill level	Lowest skill level required to exploit the vulnerabilities associated with this vulnerable item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Threat	Relevant information about the threat. Pulled from the vulnerable entry record. **Note:** Any changes made here update the vulnerable entry record.
Remediation notes	Relevant solution to the threat, pulled from the vulnerable entry record.
Notes	
Work notes	Any relevant information. Select the text box for Work notes to add information.
Image Findings	Results of scanning container images for vulnerabilities.
Requested Approvals	Approvals request raised for the CVIT.
State Change Approvals	State change approvals request raised for the CVIT.

Age calculations of a CVIT:

- The Age column in the CVITs' list displays the duration (format: Days HH:MM:SS) for which a CVIT is active. The Age value is zero for a closed CVIT.
- The Age closed column in the CVITs' list displays the duration (format: Days HH:MM:SS) for which a CVIT is active before it's closed. For CVITs, other than in the Closed state, the Age closed value is zero.

For more information on how to customize the calculation of Age and Age closed durations, see the KB1703270 article.

Prisma Cloud Compute Configuration form

The Prisma Cloud Compute Configuration form is accessed from within the Prisma Cloud Compute Integration module.

To view the Prisma Cloud Compute Configuration form, navigate to **All** > **Prisma Cloud Compute Integration** > **Administration** > **Configuration**.

Prisma Cloud Compute Configuration

Field	Description
Integration Instance	Name of the new integration instance. You can create an instance or click the lookup icon to select an existing instance.
API Base URL	URL to integrate with Prisma Cloud Compute.
Username	Username to access Prisma Cloud Compute.
Password	Password to access Prisma Cloud Compute.
Mid Server	A Java application that runs as a Windows service or UNIX daemon on a server in your

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prisma Cloud Compute Configuration (continued)

Field	Description
	local network. The MID Server enables communication and the movement of data between a ServiceNow instance and external applications, data sources, and services.
Use Projects	Option to configure the projects. When you select the check box, you can select projects in the configuration page and run the integrations based on the projects configured to populate project-specific details. **Note:** If this check box is selected, the **Configure Projects** tab is enabled. Click **Next** to proceed with configuring the projects.

Request Exception form

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Container Vulnerability Response.

To view the Prisma Cloud Compute Configuration form, navigate to **All** > **Container Vulnerability Response** > **Container Vulnerable Items** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you're requesting an exception for.
Control objective	Control objectives that are associated with the policy you selected. If a policy isn't selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date can't be in the past.
Valid until	Date when the policy exception expires and when the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid can't exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request Exception form (continued)

Field	Description
Justification	Details that are related to the reason why this request is being made. This field must be filled in by the remediation owner.

Exception Rule form

Create a rule to automatically request an exception for a specific condition for a group of container vulnerable items (CVITs), such as a rule with a condition that is based on the vulnerability severity of these CVITs. With this rule, you can defer new and existing CVITs automatically if they match the approved rule condition.

To view the Exception Rule form, navigate to **All** > **Container Vulnerability Response** > **Administration** > **Exception Rules**.

Exception Rule form

Field	Description
Name	Name of the exception rule.
Valid from	Date from which this rule is active to defer the CVITs.
Valid to	Date from which the remediation task stops accepting new CVITs.
Reason	Reason to create this exception rule.
Assignment group	Group that the remediation task that was created for tracking the deferred CVITs is assigned to.
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.
Condition	Filter condition for the CVITs that can be defined while processing the CVITs.
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run.
Workflow stage	Current approval status of the exception rule.
State	State of the exception rule.
Execution order	Unique order for each exception rule.
Deferred until	Date until when the VULs and CVITs are deferred. On this date, the created VUL is closed, all the CVITs move out of the group, and group rules are reapplied.

Domain separation and Container Vulnerability Response

Domain separation is supported in Container Vulnerability Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

How domain separation works in Container Vulnerability Response

With domain separation you can standardize Container Vulnerability Response procedures, across the customer base you serve, with lowered operational costs and a higher quality of service.

Separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

Domain separation support in Container Vulnerability Response by version releases

Release	Support level	Notes
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	
Washingtondc	Standard	
Xanadu	Standard	

Domain separation for the Container Vulnerability Response application covers the following product functionality:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Ingests the container vulnerable items from third-party scanners (for example, the Palo Alto Prisma Cloud and Wiz products) in the correct domain. The data ingests in the same domain as that of the integration user, whose credentials are used for integration.
- Re-scans specific assets from Container Vulnerability Response in the domain from which it was requested.
- Uses the CMDB CI lookup process to ensure that the CI information from the scanners matches the CIs in CMDB of the integration user's domain.
- Calculates risk scores at the vulnerable item level as per the risk score calculator defined in the same domain as that of the integration user.
- Remediation target rules are executed on container vulnerable items as per the remediation target rules defined in the same domain as that of the integration user.
- Remediation task rule(s) can be defined, and stay in, the same domain as the domain of the integration user.
- Remediation tasks created using the remediation task rules stay in the same domain as where the group rules are created.
- Deferral workflow goes through the approval process in the same domain for which the deferral is requested.
- Reports and dashboards display the container vulnerable item-states such as age of vulnerable item, open vulnerable items by CI, container vulnerabilities by impact, and remediation target date status in the domain to which it belongs.
- Knowledge from third-party scanners can be ingested in the global domain and data can be shared across multiple clients.

Note: In all the above cases the overarching principles of visibility in separated domains in the ServiceNow AI Platform apply.

For more information on how to create and support domain-separated imports, see Create domain-separated imports for an integration and Create and support multiple domains in the background jobs framework.

Use cases

The Container Vulnerability Response application manages the life cycle of a container vulnerable item end to end. The following use cases are domain-separation aware:

- **Ingest** container vulnerable items (vulnerabilities on assets) from your third-party integration.
  - Ingest data from multiple instances
  - De-duplicate the container vulnerable item
  - Match up with CMDB CI
- **Enrichment** of container vulnerable item with risk scores and remediation target dates
  - Asset enrichment (CMDB)
  - Risk score and remediation target date enrichment
- **Group** container vulnerable items and assign the remediation task
  - Automatically group the container vulnerable items
  - Automatically assign the remediation task
- **Remediate**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Remediation tasks
  - Comprehensive remediation life cycle
  - Deferral workflow
- **Measure** the security posture of the organization and vulnerability management program
  - Vulnerability trend, most vulnerable asset, vulnerability by age
  - Remediation status by the remediation target date

Setup

Setting up domain separation for Container Vulnerability Response does not require any additional steps. All Container Vulnerability Response tables acquire the Domain column after the instance is domain separated. You can direct container vulnerability integration import data to specific domains. See Create domain-separated imports for an integration for more information.

Domain-separated data

Data can be domain separated, which means:

- A container vulnerable item ingested from third-party scanners stays in the same domain as the domain of the integration user, and is not accessible from any other domain.
- Container vulnerabilities, container vulnerable items (instances) or assets in one domain cannot be viewed from other domains.
- The risk scoring algorithm, the remediation task rules and the remediation target rules cannot be viewed by anyone outside the domain.
- Container vulnerability information from third-party scanners can exist in the global domain and be shared with all customers.
- Remediation tasks in one domain cannot be viewed from another domain.
- Deferral workflows created in one domain are not visible in another domain.
- All email notifications are contained within the domain they belong to.

Note:

The scheduled import templates available on the instance are by default set to "Domain: global". So, to avoid any conflicts when there are multiple domains on instances, adapt the following practice:

- Distribute the import templates available on the instance across the number of domains involved in the integration.
- Update the import template record's domain to the sys_id of the target domain.
- If necessary, create import templates for each domain.
- Ensure each domain has 2 import templates.

How vulnerability analysts manage their own application data

- Analysts create their own application installation, multi-source application management, and CI lookup rules.
- Analysts can configure specific integrations exclusively for use within the domain.
- Analysts can create their own deferral and change management workflows.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Analysts can create their own remediation task rules, risk-scoring logic to accurately prioritize vulnerabilities, auto-assign remediation tasks and assign to the correct assignment group.
- Domain users create a manual container vulnerability item and then close the item.

Business logic and processes that can be domain-separated by instance owner

- Container Vulnerability Response users and groups
- Container Vulnerability Response integrations
- Complete setup configuration (user and group management, application installation, multi-source application management, CI lookup rules, remediation task rules, risk calculators, remediation target rules etc.)
- Complete remediation life cycle including deferral
- Scheduled jobs

Related topics

Domain separation for service providers

Configuration Compliance

The ServiceNow® Configuration Compliance application is a Secure Configuration Assessment (SCA) application that aggregates scan results from integrations with third-party configuration scanning applications. You can prioritize configuration compliance issues using your Configuration Management Database (CMDB). Configuration Compliance tightly integrates with the IT change management process to remediate your non-compliant configurations.

Request apps on the Store

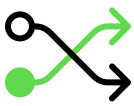
Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Configuration Compliance

Explore	Set up, Install and Configure	Integrate
		
Learn about Configuration Compliance concepts and features	Configure Configuration Compliance	Extend Configuration Compliance by integrating it with other applications

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance (continued)

Use the Vulnerability Response Workspaces  Learn how to monitor, manage and remediate configuration issues in the Vulnerability Manager, IT Remediation, and Vulnerability Assessment Workspaces.	**Remediate**  Learn how to remediate your non-compliant assets with Configuration Compliance	**Analytics & Reports**  View reports and dashboards in Configuration Compliance
Reference  Get details about Configuration Compliance components like fields, tables, and properties	**Upgrade Configuration Compliance to USEM**  Upgrade Configuration Compliance applications to Unified Security Exposure Management.	

Troubleshoot and get help

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring Configuration Compliance

Use test results obtained from third-party Secure Configuration Assessment (SCA) integrations to verify compliance with security or corporate policies. Identify, prioritize, and remediate non-compliant configuration items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

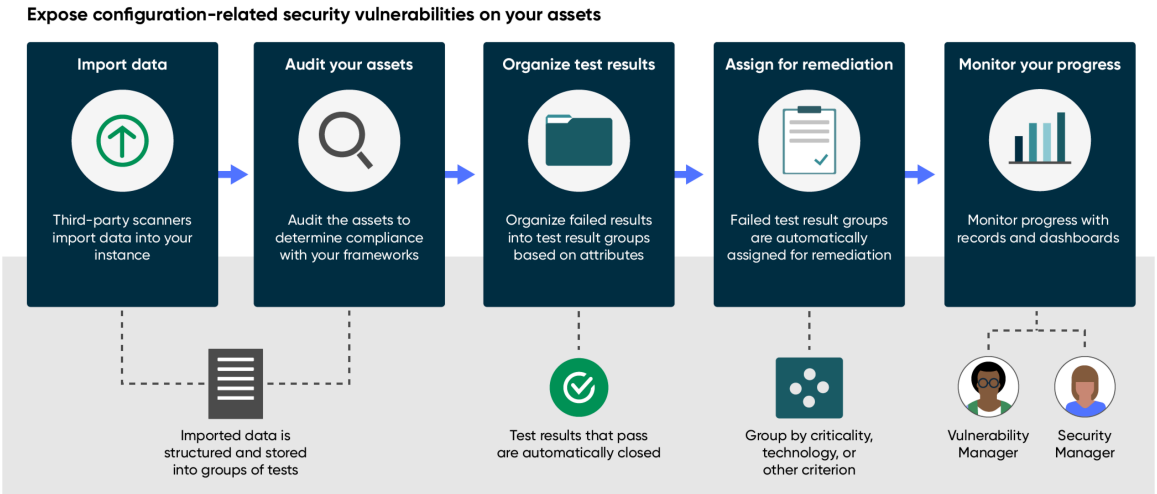
Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

What is Configuration Compliance

The ServiceNow® Configuration Compliance application enables you to prioritize and remediate the most critical configuration-related vulnerabilities in your environment quickly and efficiently. Configuration Compliance is available by subscription in the ServiceNow® Store.



Key features of Configuration Compliance

Use the Configuration Management Database (CMDB) in your ServiceNow AI Platform® to help you expose and fix your most critical configuration-related security vulnerabilities. Focus your remediation resources on activities with the greatest risk reduction. Streamline the remediation process across security, IT, and your business process stakeholders. The Configuration Compliance application includes the following key features:

- With supported third-party integrations, automatically import policies, tests, authoritative sources, and technologies. See Configuration Compliance integrations for more information about supported integrations.
- Correlate policies and tests to configuration items (assets) to identify configuration-related vulnerabilities and help you verify that your assets are in compliance with your policies and controls.
- Unify configuration assessment, assignment, and remediation across all of your assets.
- Configuration scanning content can be imported from leading Secure Configuration Assessment (SCA) ecosystem integration applications.
- Configuration findings, test failures, can be grouped and routed automatically based on remediation specialist skill sets and areas of responsibility. Intelligent workflows and tight integration with change management provide smooth task hand-offs between groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- When used with the ServiceNow Governance, Risk, and Compliance (GRC) application, configuration tests in Configuration Compliance can be rolled up to their corresponding GRC controls.
- With enhanced change management, create pre-populated change requests for IT directly from Configuration Compliance to help you with your remediation tasks that require additional resources.
- With dashboards, view remediation status metrics on remediation task, compliance test, and policy records.

Who uses Configuration Compliance

Configuration Compliance activities can involve many levels of management.

- System administrators
- Vulnerability administrators
- Vulnerability managers
- Vulnerability analysts
- Compliance administrators

Configuration Compliance tasks involve the following roles.

- sn_vulc.admin — can read, write, delete
- sn_vulc.write — can read and write
- sn_vulc.remediation_owner — Can read and update assigned records

  Note: The sn_vulc.remediation_owner role is also automatically assigned when any user is assigned the itil role.

- sn_vulc.read — can read

Configuration Compliance and Security Operations

When the Qualys Vulnerability Integration and the Tenable Vulnerability Integration are installed, access to Vulnerability Response becomes available. You can have multiple deployments of these integrations. Data sourced from each deployment is identified and available in a single instance of GRC.

Available versions for Xanadu

Release version	Release notes
Configuration Compliance v15.0, v15.1, v15.2, v15.3, 15.4	Configuration Compliance release notes For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Configuration Compliance imported data

The Configuration Compliance application imports policies, tests, authoritative sources, and test results from third-party integrations and stores them in modules for viewing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Supported integrations

Third-party integrations import configuration assessment findings, test groups, tests, technologies, authoritative sources, and test results into the Configuration Compliance application. Vulnerability managers or vulnerability analysts can use this data to identify and respond to the configuration-related vulnerabilities on your assets.

For more information about supported integrations, see Configuration Compliance integrations.

Test groups

Test Groups are related to authoritative documents and test records. A group of configuration tests define Test Groups. Test Groups typically align to a technology class, for example, Windows, Oracle databases, Cisco IOS, and are often derived from the primary industry standard. Test Groups can be modified to meet the needs of the organization. A single Configuration Test can belong to multiple test groups.

Integration	Description
Qualys Vulnerability Integration	Test groups are retrieved and Control IDs are populated by the scheduled job, **Qualys PC Policies** at 1:00AM. You can view the scheduled job by navigating to **Qualys Vulnerability Integration** > **Primary Integrations** > **Qualys PC Policies**. **Note:** If you choose to run the integration manually, run **Qualys PC Policies** first.
Tenable Vulnerability Integration	The scheduled job Tenable.io Compliance Results Integration imports policies. If you choose to run the integrations manually, run the integrations in the following order until you reconcile any ignored assets with assessment data: • Tenable.io Assets Integration • Tenable.io Compliance Results Integration • Tenable.io Compliance Results Backfill Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	• Tenable.io Assets Integration • Tenable.io Compliance Results Backfill Integration To view the policy record, navigate to **All** > **Configuration Compliance** > **Test Groups**. To correctly identify and create the test group records, audit information for test groups is imported and displayed in the **Short description** field.

Tests

Tests are libraries of data records that organize scans of computing assets. Configuration tests define how a class of technology assets should be governed.

A Configuration Compliance test is the mechanism third-party integration applications use to group assets by vulnerability type. Some third-party VA scanning solutions such as Qualys have very large libraries of tests (as many as 8,000) that are mapped to policies and "frameworks" of authoritative sources.

A Test can have many values, one-to-many, expected vs. actual, and so on. A test is anything that can be used to identify a class of software or hardware asset that is out of compliance. For example, a release or hardware number.

Integration	Description
Qualys Vulnerability Integration	The scheduled job, **Qualys PC Controls**, retrieves the tests. You can view the scheduled job by navigating to **Qualys Vulnerability Integration** > **Primary Integrations** > **Qualys PC Controls**. **Note:** If you choose to run the integration manually, run **Qualys PC Controls** after **Qualys PC Policies**.
Tenable Vulnerability Integration	The scheduled job Tenable.io Compliance Results Integration imports configuration tests (Tests). If you choose to run the integrations manually, run the integrations in the following order until you reconcile any ignored assets with assessment data: • Tenable.io Assets Integration • Tenable.io Compliance Results Integration • Tenable.io Compliance Results Backfill Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	• Tenable.io Assets Integration • Tenable.io Compliance Results Backfill Integration To view the Configuration Test record, navigate to **Configuration Compliance** > **Tests**. On the record, imported data is displayed in the **Short description** field and Remediation Status, Description, and Remediation tabs. Data is also displayed on the **Citations**, **Policies**, and **Test Results** Related Links.

Technologies

One of the techniques used by third-party vulnerability scanners to create test groups of software and hardware configuration items for analysis is to organize them by technology. Technologies are an imported library of OSes, network devices, databases, and apps that are associated with policies. Tests have multiple implementations for different technologies. Remediation is technology-specific, as well.

You can view the applicable technologies for a test, to better understand what kinds of software or hardware assets the control can be applied to. Examples of technologies that can be applied to controls include CentOS 7.x, Windows 8.1, Windows 2016 Server, and so on. The list of technologies is read-only and match the technologies defined in the Qualys Cloud Platform application.

Technologies are imported for database-related configuration assessments only. The *db_type* (if not empty) in the import is used to create a technology. View technologies populated on the Technologies section on configuration test records, test result records, policy records and at **Configuration Compliance** > **Supporting Data** > **Technologies**.

Authoritative sources

Configuration Compliance uses Authoritative sources and citations when generating vulnerability alerts for tests. Authoritative sources usually map to sections of published industry standards, such as "NIST 800-53 version 3 (2009) 3: 2009, SA-4".

Note: In the Qualys Vulnerability Integration, this combination is referred to as framework.

Authoritative sources and citations (also known as mandates) are imported from the third-party vulnerability scanners.

Authoritative source records contain references to information about known software and hardware configuration issues from experts in the field of computer security. They define requirements for security policies and procedures. Configuration tests can reference multiple authoritative sources through citations. Authoritative sources can report on compliance for a given standard in preparation for an audit.

Integration	Description
Qualys Vulnerability Integration	The scheduled job, **Qualys PC Policies Detail**, retrieves the authoritative sources and citations. You can view this scheduled job by navigating to **Qualys Vulnerability Integration**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	> **Primary Integrations** > **Qualys PC Policies Detail**. **Note:** If you choose to run the integration manually, run **Qualys PC Policies Detail** after **Qualys PC Policies**.
Tenable Vulnerability Integration	The scheduled job Tenable.io Compliance Results Integration imports authoritative sources as part of Citations data. If you choose to run the integrations manually, run the integrations in the following order until you reconcile any ignored assets with assessment data: • Tenable.io Assets Integration • Tenable.io Compliance Results Integration • Tenable.io Compliance Results Backfill Integration • Tenable.io Assets Integration • Tenable.io Compliance Results Backfill Integration Data is displayed on the **Citations** related link on configuration test records.

Test results

Configuration Compliance does not calculate the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using **Remediation Tasks**. See Configuration Compliance correlation for more information.

Integration	Description
Qualys Vulnerability Integration	You can retrieve the test results in one of the following ways: The scheduled job, **Qualys PC Results**, retrieves the test results. You can view this scheduled job by navigating to **Qualys Vulnerability Integration** > **Primary Integrations** > **Qualys PC Results**. **Note:** If you choose to run the integration manually, run **Qualys PC Results** after **Qualys PC Policies** and **Qualys PC Policies Detail**. The **Qualys PC Results** import uses the *`Start Time`* parameter in the **Integration Details** tab. All other Configuration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	Compliance imports bring in all available data regardless of *`Start Time`*. When the **Qualys PC Results** import is complete, an event is fired to trigger end-of-import calculations. For more information see, Configuration Compliance states. Alternatively, starting from V14.5, you can also run the following integrations to retrieve the test results: • Qualys PCRS Policy Host Integration - Retrieves the host IDs for each policy. To view this scheduled job, navigate to: Qualys Vulnerability Integration > Primary Integrations > Qualys PCRS Policy Host Integration. **Note:** If you choose to run the integration manually, run Qualys PCRS Policy Host Integration after Qualys PC Policies and Qualys PC Policies Detail. After this scheduled job is complete, it automatically triggers the Qualys PCRS Test Results Integration. • Qualys PCRS Test Results Integration - Retrieves the test results for each host ID. To view this scheduled job, navigate to Qualys Vulnerability Integration > Primary Integrations > Qualys PCRS Test Results Integration. **Note:** If you choose to run the integration manually, run Qualys PCRS Test Results Integration after Qualys PC Policies, Qualys PC Policies Detail and Qualys PCRS Policy Host Integration. This integration uses the Start Time parameter in the Integration Details tab.
Tenable Vulnerability Integration	The scheduled job Tenable.io Compliance Results Integration imports Test Results. If you choose to run the integrations manually, run the integrations in the following order until you reconcile any ignored assets with assessment data: • Tenable.io Assets Integration • Tenable.io Compliance Results Integration • Tenable.io Compliance Results Backfill Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
	• Tenable.io Assets Integration • Tenable.io Compliance Results Backfill Integration To view the Configuration Test record, navigate to **Configuration Compliance** > **Tests Results**. On the record, imported data is displayed in the**Test**, and **Configuration Item** fields. Data is also displayed on the **Expected Values**, **Actual Values**, and **Remediation** tabs. The **Remediation Tasks** and **Test Result History** Related Links are populated.

Configuration Compliance discovery

Configuration Compliance data is imported from third-party SCA scanner applications. They structure groups of software and hardware tests into data records to expedite conducting assessments.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

When an import is complete, an event is sent to indicate end-of-import actions. For every active remediation task, the following actions are taken:

- Resolved groups with failed results return to the **Awaiting Implementation** state.
- Remediation tasks where all results have passed, are **Closed**.
- The state of test results that are in active remediation tasks are updated.
- The flag indicating whether a result is part of an active remediation task is updated.

Configuration Compliance correlation

Configuration Compliance provides prioritization and test result grouping (into remediation task) to aid remediation of non-compliance issues.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Asset-Centric Prioritization

Configuration scans can produce large number of findings. Prioritize findings for greatest risk reduction. Priority includes both configuration test criticality and asset criticality. Configuration test result priority is expressed as a 0–100 scale risk score. Calculator groups compute risk score and can be customized.

When the third-party import is complete, Configuration Compliance sends an event to indicate end-of-import actions. For every active result group, the following actions are taken:

- Resolved remediation tasks with failed results return to the **Awaiting implementation** state.
- Remediation tasks where all results passed are **Closed**.
- The state of test results that are in active remediation tasks is updated.
- The flag indicating whether a result is part of an active remediation task is updated.

Remediation Tasks order of precedence

When test results belong to more than one remediation task, the **State** of a test result is derived according to an order of precedence.

The **State** and **Resolution** fields in the **Configuration Test** form and the **Result** field in the **Test Result** form, are calculated following this order of precedence.

Note:

The group membership precedence only applies to items where the item did not pass the configuration test. **Passed** items are always in the **Closed-Fixed** state.

The **Result** value determines the state. We ignore remediation tasks in the **Closed-Fixed** and **Closed-Canceled** state. The item state is computed from the states of all other remediation tasks it belongs to or is set to **Open**, if no other remediation task exists for the item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Remediation Tasks creation

Configuration Compliance Remediation Tasks are created manually.

There are two ways to create and populate **Remediation Tasks**.

- From the **Remediation Tasks** module and using filters that automatically populate the **Test Results** tab.

  This way is good for when you know what filtering you want to use. For example, capturing all failed test results that are moderate and higher criticality, affect the windows-based infrastructure, and apply only to the SAP supply chain application.

- By selecting test results in the **Test Results** list and creating a remediation task from the **Actions on selected rows...** menu.

  This method is good for results that are not easily filtered, or situations where you want to specify test results for remediation. For example, outliers that have nothing in common.

Note: If you create a remediation task from the **Test Results** list and you later decide to use a filter for that remediation task, your original entries are removed and replaced by the filter results.

Ungrouped Test Results

Ungrouped Test Results contain all non-pass test results that are not members of an active (non-**Closed**) remediation task. This module is updated after every import and whenever test results are added or removed from a remediation task.

Discovered Items for Configuration Compliance

Assets are automatically matched to configuration items (CIs) using CI lookup rules, when they are imported using the host and test results integrations. Discovered Items give you visibility into how asset identification is mapped to CIs in the CMDB.

Discovered Items are considered **Matched**, **Unmatched**, or **Reclassified**. Identified CIs are in the **Matched** state.

To make it easier to find potential matching issues, the CI Lookup Rule that matched the CI appears in the **CI matching rule** field.

Note: **CI matching rule** field support is available only for the Qualys integration.

If a match was not found, a CI is created in the *Unmatched CI* class [sn_sec_cmn_unmatched_ci], [cmdb_ci_unclassed_hardware], or

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

`[cmdb_ci_incomplete_ip]` of the CMDB. If the original unmatched CI was reclassified, Discovered item records are updated to reflect that state. For more information, see Unmatched CIs and View and reclassify unmatched configuration items for more information.

By default, the **Security Operations** > **CMDB** > **Discovered Items** module lists unmatched configuration items. You can view all discovered items from an import by removing the filter.

For a description of the fields in Discovered Items, see Discovered Items form fields.

CI changes for discovered items for Configuration Compliance

The default value of the property `sn_sec_cmn.update_on_ci_change` is `true`. So, when the configuration item (CI) for a discovered item is updated, the test results are updated as well.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

The external ID for the test result is updated and the risk score, assignment rules, remediation task rules, remediation target rule are reevaluated. If a test result exists with the same test and CI, the test results are updated with the existing test result and the current test result is closed with the substate `invalidCI`. Work notes are added accordingly.

If you do not want to update the CI for the existing test result, set the property to false. In this case, if a CI changes, a new test result is created and the existing one is closed as an `invalidCI`.

Reconcile unmatched discovered items for Configuration Compliance

Create a schedule job to reconcile unmatched discovered items. When a test result is created, the configuration item (CI) added to it at the time of creation might be an outdated one.

Before you begin

Role required: admin

About this task

If the information in the CMDB changes, unmatched CI information is not reconciled. To reconcile, apply CI lookup rules on the test results that are in an unmatched state when the CMDB is updated with the latest CIs.
A schedule job is run on demand to reapply the CI matching rule for the discovered items in an unmatched state. If the CI changes after reapplying the lookup rules, the discovered items are updated with the new CI. Impacted test results are also updated. For details, see CI changes for discovered items for Configuration Compliance.

Procedure

1. Navigate to **All** > **Security Operations > Reconcile Unmatched Discovered Items**.
2. On the Background Jobs page, click **Create reconciliation job**.
3. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can only edit the Parameters field.

Background Job

Field	Description
Number	Unique job number.
Created by	User who created the job.
Parameters	Parameters to reconcile the unmatched discovered items: ○ limit: Maximum number of discovered items to be reconciled. If you do not enter a value, 10,000 discovered items are reconciled. ○ firstDiscovereditem: First discovered item that must be reconciled. If you do not enter a value, the reconciliation process starts from the first discovered item.
State	Current state of the background job.
State description	Description of the current state of the background job.
Job type	Type of job. The value is **Reconcile unmatched discovered items**.
Started at	Time when the job started.
Ended at	Time when the job was completed.
Job duration	Total time taken to complete the job.
Substate	Substate for the selected state.
Notes	Number of records processed.

4. Click **Submit**.

Note:

- To stop running the job, click **Cancel**.
- You cannot reconcile unmatched CIs or reapply CI lookup rules while importing hosts or test results.

Reapply CI lookup rules on selected discovered items for Configuration Compliance

Reapply configuration item (CI) lookup rules on selected discovered items from the discovered item list view select actions. The administrator might have to edit or update a lookup rule for multiple reasons. If the lookup rule changes, they can reapply them on the discovered items.

Before you begin

Roles required:

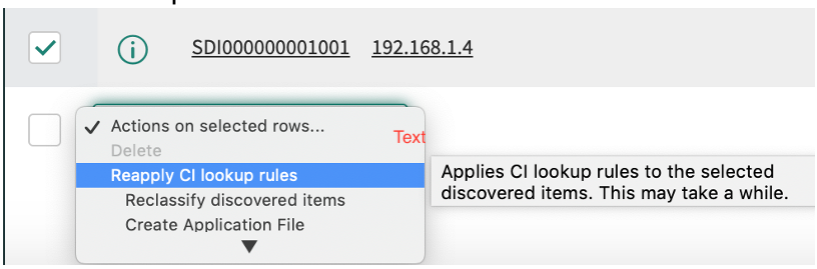
About this task

If the CI changes after reapplying the CI lookup rules, the discovered items are updated with the new CI and test results. For more information, see CI changes for discovered items for Configuration Compliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security operations** > **CMDB** > **Discovered Items**.
2. Select the required discovered items and click **Action on selected rows**.



3. Select **Reapply CI lookup rules** from the list.

   The rules are reapplied on these discovered items.

The Tenable Vulnerability Integration with Configuration Compliance

The Tenable.io product of the Tenable Vulnerability Integration imports policies, controls (test results), and configuration tests for processing in the Configuration Compliance application.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Tenable.io

The Tenable Vulnerability Integration is supported.

You can use imported data to:

- Identify configuration-related vulnerabilities on your assets listed in your Configuration Management Database (CMDB)
- Verify that your assets are in compliance with your policies and controls.

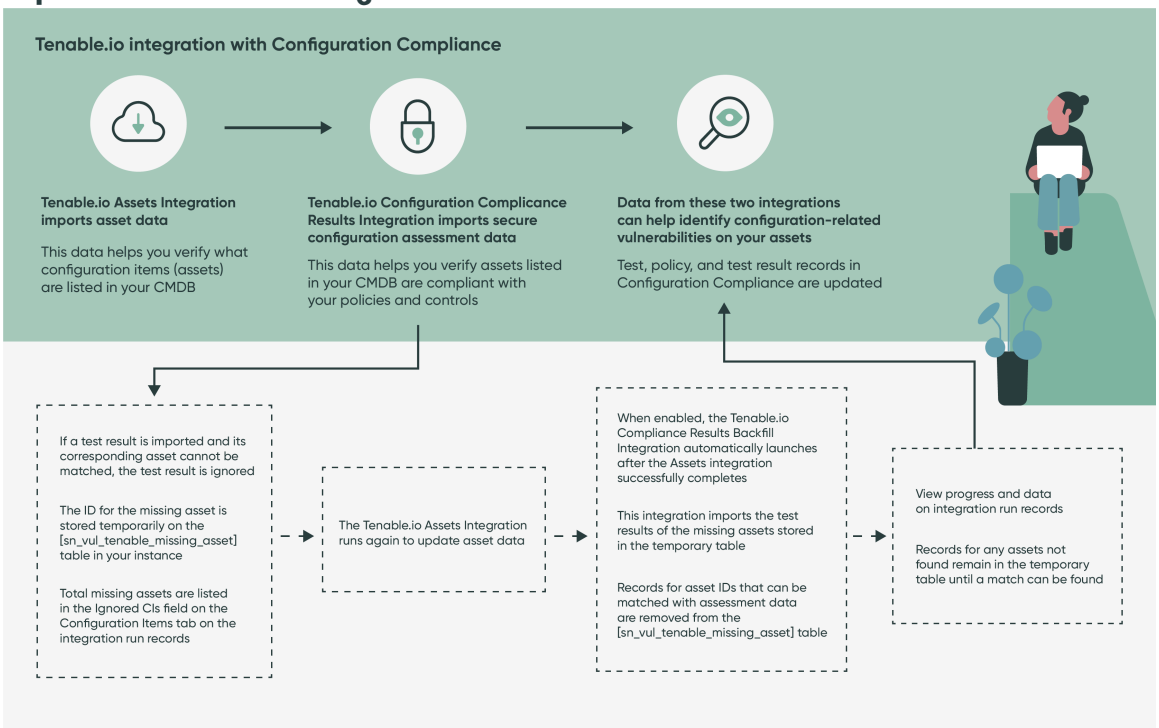
Assets data, policies, controls (test results), and configuration tests are imported with the following integrations:

- Tenable.io Assets Integration
- Tenable.io Compliance Results Integration
- Tenable.io Compliance Results Backfill Integration

The following image illustrates how the integrations work together to import asset and configuration assessment data and reconcile any ignored CIs overlooked during an import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Import flow for secure configuration assessment results



Data is imported, updated, and displayed on the test result, policy, and configuration test records in the Configuration Compliance application.

In some cases, the number of imported Configuration Items (CIs) is different for the Tenable.io Assets Integration and the Tenable.io Compliance Results Integration. When this occurs, temporary records are created and stored for the ignored asset IDs. These records can be matched later with imported assessment data by imports from the Compliance Results Backfill Integration.

For example, let's say the Assets Integration imports 80 assets on an integration run, but the Compliance Results Integration imports 100.

Note: You can verify the number of ignored CIs on integration runs by navigating to **Tenable Vulnerability Integration** > **Administration** > **Integrations**. Click the name of an integration to open the record. On the **Vulnerability Integration Runs** Related Link, open an integration run record and select the **Items** tab to see the value in the **Ignored CIs** field. This field tracks the total of ignored (missing) assets from the import.

By comparing values in the **Ignored CIs** fields on each integration run record, there is a difference of 20 ignored CIs. As a result, the backfill integration runs automatically as shown in the preceding image. This integration imports the configuration assessment information for the extra 20 assets found by the Compliance Results Integration but missed by the Assets Integration. Since assessment data for missing assets is not imported, the Tenable.io Compliance Results Backfill Integration imports up to 200 Asset IDs per integration run to reconcile the missing assets with their corresponding assessment data. All records created for missing or ignored assets and listed on the temporary table are deleted after these assets and their data are matched.

Note: It may take multiple runs of these integrations to import all the ignored assets.

For more information about how to enable and configure the Tenable.io Asset Integration, see Configure the Tenable Vulnerability Integration using Setup Assistant. See Understanding the Tenable Vulnerability Integration for more information about the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Tenable.io Compliance Results Integration and the Tenable.io Compliance Results Backfill Integration are inactive by default.

To activate them:

1. Navigate to **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
2. On the Tenable Integrations list, click an integration name to open the record and select the **Active** check box to enable it. You might prefer to leave the schedule settings in their default values for these integrations to start.

CI Lookup Rules for identifying configuration items from Configuration Compliance third-party vulnerability integrations

When data is imported from a third-party integration, Configuration Compliance automatically uses host data to search for matches in the Configuration Management Database (CMDB). It does this using **CI Lookup Rules**. These rules are used to identify configuration items (CIs) and add them to the test result record to aid in remediation.

As assets are imported, a lookup is performed first on the **Discovered Items** list using third-party IDs to find matches to configuration item (CIs) from prior imports. When a host ID match is found, it is used as the **Configuration item** field in the test result record.

You can see how imported assets are mapped to CIs using the **Discovered Items** list. If a match is not found, or the cmdb_ci field is empty, the rules use the other host information to attempt to correctly identify the CI. If a match is still not found, a placeholder CI is created and is designated as an **Unmatched CI**. See Unmatched CIs for more information on how those CIs are handled.

A new discovered item is created and mapped to this CI.

Note: CI lookup rules are available only for the Qualys Integration for Security Operations.

CI lookup rules can be domain separated and are source-specific. Each source can have multiple deployments. Qualys can have multiple deployments of the Qualys Integration. Each deployment has its own set of CI Lookup Rules.

Note: CI lookup rules are shared by all deployments of the vulnerability integration. If a rule is deleted or modified, the deletion or changes affect all deployments of the vulnerability integration.

When attempting a match, the first step is a vendor ID lookup for an exact match across source, source_instance, and vendor ID. Then, lookup rules are run in order, from lowest to highest and stop when a rule returns just a single CI as a match. If a rule is created in such a way that it returns more than one CI, only the first match is used.

Note: To avoid matching on low-level networking elements, if a matched CI is one of `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic`, or `cmdb_ci_ip_address`, the parent CI is returned.

A system property to exclude CI classes is available. This property is not available with upgrade. See Ignore CI classes for upgrade information and instructions on setting the property.

To make it easier to find matching issues, when a match is found, the CI lookup rule used to find it is added to the Discovered Item record in the **CI matching rule** field. Lookup rules are evaluated by lowest **Order** value first.

Some of the Qualys CI lookup rules shipped with the base system are:

- QUALYS HOST ID
- FQDN

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- NetBIOS
- DNS
- IP

Some of the Microsoft Defender CI lookup rules shipped with the base system are:

- S3 Bucket
- Name
- Resource Id

Some of the Palo Alto Prisma Cloud CI lookup rules shipped with the base system are:

- S3 Bucket
- Name
- Resource Id

Importing test results data can be taxing on an instance and performance issues with resources can occur if rules are not carefully constructed. The logic used to iterate through and perform matching within the CMDB can result in lengthy processing times. To avoid any potential degradation of resources or performance complications, test any custom-written CI Lookup Rules or modifications to pre-defined **CI Lookup Rules**. See Steps to help prevent duplicate or orphaned records after running Vulnerability Response CI lookup rules for more information on preventing duplicate orphan records, deleting data, and cleaning up data.

Reapplying updated CI lookup rules

When you change a CI lookup rule, click **Apply Changes** on the CI Lookup Rules list page to rerun all the rules on the discovered items that:

- Were matched by the updated rules
- Are not matched by any rule

If the configuration item (CI) changes after reapplying the lookup rules, the discovered items are updated with the new CI. The test results are also updated. For more information, see CI changes for discovered items for Configuration Compliance.

Deduplicating existing configuration items for Configuration Compliance

The Duplicate CI Remediator for deduplication tasks is updated with the `sn_sec_cmn_src_ci.cmdb_ci` property.

Whenever a deduplication task is used to update the configuration items (CIs), it also updates the discovered items related to those CIs. Hence, the test results are updated with the CI. For details, see CI changes for discovered items for Configuration Compliance.

Creating CIs for Configuration Compliance using the Identification and Reconciliation Engine

Starting with Configuration Compliance 11.1, you can create configuration items (CIs) in the Configuration Management Database (CMDB) using the Identification and Reconciliation engine (IRE) API. By using the IRE API to create CIs, you can prevent duplicate CIs from being created and you can reconcile CI attributes by allowing only authoritative data sources to write to CMDB.

A CI class (table) is the original table name in the instance database. CMDB contains base system classes that store data about CIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using IRE for CI creation

Prior to version 11.1, if a matched CI was not found either in the Discovered Items list or CMDB, a CI was created in the Unmatched CI class (`sn_sec_cmn_unmatched_ci`).

For more information, see Unmatched CIs.

Starting with version 11.1, you can use the IRE API to create CIs in CMDB. Instead of using the Unmatched CI class, a CI is created in the Unclassed Hardware or Incomplete IP Identified Device class.

CMDB CI classes

Note: To use the new classes, activate the CMDB CI Class Models plugin. Otherwise, CIs are created in the Unmatched CI class.

Starting with version 11.1, if the host that you imported from a third-party scanner can't be found in the Discovered Items list or CMDB, it is stored in one of the following new CMDB CI classes.

CMDB CI classes

CMDB CI Class	Description
Incomplete IP Identified Device (`cmdb_ci_incomplete_ip`)	CI is created in this table if only the IP address is available in the host information that is received from the scanner.
Unclassed Hardware (`cmdb_unclassed_hardware_ci`)	CI is created in this table if any of the following information is available in the host information that is received from the scanner: • Host name • IP address • DNS • NETBIOS • MAC address **Note:** If the MAC address is available, the network adapter entry is created and related to the unclassed hardware CI. If both the IP and MAC addresses are available, the IP address CI is also created and related to the unclassed hardware CI.

The system automatically uses an Unmatched CI class if one of the following occurs:

- The CMDB CI Class plugin is not activated.
- IRE raises an exception while creating a new CI.

Related topics

CMDB CI Class Models store app

Identification and Reconciliation engine (IRE)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance assignment rules overview

Define the criteria by which test results are automatically assigned to an assignment group for remediation.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

A default assignment rule, **Assign to CI support group**, is included in the base system assigning test results to the **CI Support Group**. Inactive by default.

The Assignment groups set by the Assignment Rules are used by **Remediation Task Rules** to assign owners to remediation tasks (RTs).

Assigning test results automatically

There are three different ways to assign test results using **Assign using**:

- Assignment group: This option allows you to select any of the existing ServiceNow AI Platform® user groups.
- Assignment Group Field: This option allows you to choose any assignment group field available using the cmdb_ci table. By default you see the following three group fields:
  - None: Indicates no default value for this mandatory field
  - Configuration Item: Approval Group
  - Configuration Item: Assignment Group
  - Configuration Item: Support Group
- Script: This option allows you to define the conditions using a script. This option requires coding or advanced ServiceNow® expertise.

See Create or edit Configuration Compliance assignment rules for more information on creating assignment rules.

With the sn_vulc.remediation_owner role, you can view and update test results and remediation tasks that are assigned to them or to their assignment groups. To view the modules, navigate to **All** > **Configuration Compliance** > **Test Results** > **My Open Test Results**, or **Configuration Compliance** > **Remediation Tasks** > **My Open Tasks**.

The sn_vulc.remediation_owner role can be assigned directly to a user, or, it is automatically assigned when you assign a user the itil role.

Assignment rule evaluation process

When a new test result is imported, or reopened after being closed, the assignment rules are evaluated against it. The assignment rules are evaluated after CI matching, and Risk Score calculations. A test result is only automatically evaluated upon initial import and when a rule is changed, unless it is reopened after being closed. You can manually reapply rules after changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following process is used for each new or reopened test result:

- For each test result assignment rule, the test result is compared to the assignment filter, lowest order rule first.
- Where the condition matches, the test result is assigned an assignment group. The lookup stops.
- Where the conditions do not find a match among all the rules, the test result remains unassigned.

Reapplying assignment rules

When you change an assignment rule, use the **Apply Changes** button on the Assignment Rules list page to rerun all the changed rules on all active Open test results, except those that were manually assigned.

Note: The assignment rules do not reevaluate manually created assignments.

The scheduled job [*Reapply all assignment rules*] is inactive, by default. When activated, it evaluates all the open test results against all active rules except those manually assigned. It can run Daily, Weekly, Monthly, Periodically, Once or On Demand.

Important: As an admin and analyst, you can obtain the latest assignments for selected test results in the Vulnerability Manager Workspace. This method is more efficient than reapplying the Assignment Rules for all test results in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Assignment rules and remediation task assignment

Usually, you would assign your remediation task (RT) to the same assignment group as the test results in it. That is what the remediation task rules do, by default.

For example, if your RT groups by configuration item class, the remediation task created can be broken apart by the different assignment groups. An Oracle Database TRG can be assigned to Group 1, and an Oracle Database TRG assigned to Group 2.

When the assignment group is changed at the remediation task level, all the test results in that remediation task which have same assignment group are updated to the new assignment group. The test results are marked as manually assigned and are not eligible for further rule evaluation.

Removing assignments from Configuration Compliance remediation tasks

You can clear the **Assigned to** and **Assignment group** fields on remediation tasks and their associated test results directly from the test result records and remediation tasks that you determine might be incorrectly assigned to you or your groups.

Overview of the workflow

Remediation owners can update records for reassignment with the **Unassign** button.

Use case for sn_vulc.remediation_owner

If you determine that RTs and their associated test results aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups, you can remove yourself or your groups from the **Assigned to** and **Assignment group** fields on those remediation task records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unassign module

The **Unassign** button is displayed on the remediation task and test result records in any state other than the Closed or Resolved states.

If you select **Unassign**, you are prompted that all the associated test results with the remediation task are reassigned and transition to the **Unassigned** assignment type.

Note: If any test result on a remediation task has a different assignment group than its remediation task, it is not unassigned. In most cases, these test results have been manually assigned.

Any records that you update with either the UI button or manually, are displayed on the Unassigned module under Configuration Compliance.

For the steps to reassign records using the *Unassigned* UI action, see Remove assignments from remediation tasks for you or your groups.

System property and notifications

If you are an administrator with the sn_vulc.vulnerability_admin role, when you select **Unassign** on a record, by default, the system property, *sn_vulc.unassign_test_result_group.approval_required* triggers the State Change Approval record and Requested Approval record. Also, the request displays in the My Approvals list of the approver.

Note: As a vulnerability administrator, you can set the *sn_vulc.unassign_test_result_group.approval_required* system property to **false** to disable the approval process.

- If the approver approves your request, by default, the system property, *sn_vulc.default_assignment_group* clears the Assigned to and Assignment group fields, and populates the Assignment type field with **Unassigned**. As a vulnerability administrator, you can change the value in the *sn_vulc.default_assignment_group* system property so that the assignment fields are cleared and a specific group is then assigned. For example, if a user selects **Unassign** on a record and you want to redirect it to a specific group for review, you can add a system ID for the group of your choice in the value field of the system property.
- If the approver rejects your request, the reason for rejection displays on the **Notes** tab.

Alternatively, if *sn_vulc.default_assignment_group* is not configured for a specific group, by default, users that you add to the Unassign notification user group are alerted when records are unassigned. The system property, *sn_vulc.default_notification_group* determines the notifications to this group.

The assignment type, whether it's **Manual**, **Rule**, or **Unassigned**, is available from the RT records and the list view. The **Unassigned** assignment type is displayed after the **Assigned to** and **Assignment group** fields are cleared by the system property of the feature.

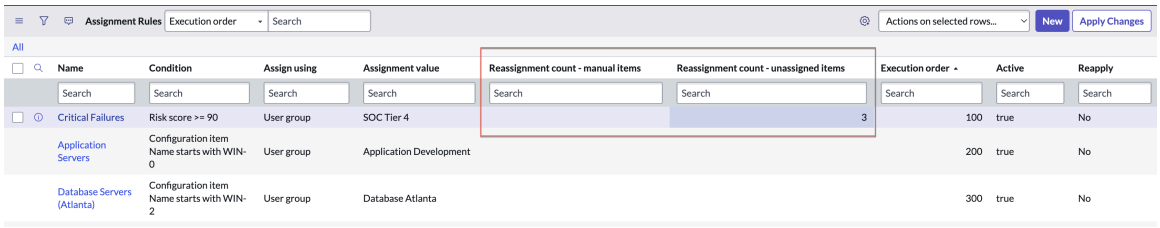
Monitoring your assignment rules with the scheduled job for this feature

A daily scheduled job counts the records when they transition to the **Unassigned** assignment type. With this count, vulnerability analysts can monitor and adjust any assignment rules that might not be performing well based on any assignment rules that have higher counts of unassigned RTs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The *Reassignment count for assignment rules* scheduled job runs daily and posts the total number of RTs that are unassigned by this feature for a particular assignment rule.

The job also counts any records that are manually unassigned. Both the manual counts and the counts that are gathered by this feature are posted on the Vulnerability Assignment Rules list in two columns: *Reassignment count - manual items* and *Reassignment count - unassigned items*.



1. As a vulnerability administrator, you can view these counts by navigating to **Configuration Compliance** > **Administration** > **Assignment Rules**.
2. Select the gear icon in the upper right of the list and select the **Reassignment count - manual items**, and **Reassignment count - unassigned items** for display.
3. Any RT that was originally assigned by a rule but later was automatically or manually reassigned, contains a reference to the original rule in the list view.

Configuration Compliance remediation tasks and remediation task rules overview

Automatically create Remediation Tasks (RTs) to analyze results in bulk using remediation task rules. The criteria by which groups are formed is configured so that you do not have to manually assign test results into groups.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Understanding remediation tasks

Remediation tasks represent a set of test results to remediate. Grouping test results has many advantages. You can move test results through the remediation states, mark them under investigation, defer them, mark them resolved in bulk by using groups. You can create conditions to automatically group all results with specified results, technologies, risk scores, and any other data related to the test results. Test results can belong to more than one remediation task giving you the flexibility to actively work with one remediation task and monitor another. It all depends on your organizational needs. For example, you could group by assignment, and also create a remediation task containing technologies.

Remediation tasks are created as follows.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Manually, using one of two options, to add test results to the remediation task.
  - **Manual**: creates a remediation task with no entries. Test results must be added manually.
  - **Filter**: creates a remediation task and uses conditions to automatically add test results to that remediation task.

  Note: Manually added test results are not automatically removed from remediation tasks by remediation task rules or remediation task conditions.

- Automatically, using remediation task rules. This option is the easiest option, once configured, remediation task rules create all desired remediation tasks.

From a remediation task, the group of test results may be assigned to a user, deferred until later, used to create a **Change Request**, and so on.

Note:

With the sn_vulc.remediation_owner role, you can view and update test results and remediation tasks that are assigned to you or to your assignment groups. To view the modules, navigate to **All** > **Configuration Compliance** > **Test Results** > **My Open Test Results**, or **Configuration Compliance** > **Remediation Tasks** > **My Open Tasks**.

When it is determined that a new test result can be added to a remediation task, the test result is included in the **Test Results** related list of the remediation task.

When updating the state of a remediation task, associated test results can have their state updated to match this remediation task. For more information on state changes, see Configuration Compliance states.

Understanding remediation task rules

Remediation task rules allow you to define how test results are automatically grouped and assigned. A default rule, **Assignment group, Test**, is included in the base system grouping test results based on a test result **Assignment group** and the **Test** field. This rule is disabled, by default. You can group by any other set of values in columns accessible from the test result. You can use up to six keys and any number of conditions. For more information, see Create or edit Configuration Compliance remediation task rules.

Important: As an admin and analyst, you can evaluate the remediation task rules for selected test results in the Vulnerability Manager Workspace. This method is more efficient than reapplying the remediation task rules in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

For example, you can group your test results by assignment group or technology and configuration item (CI). A different set of rules can be used for test results that expose the company to more risk. You can have one remediation task rule for low severity or low risk CIs. See Test Results fields for more information on available fields.

When a new test result is imported, or reopened after being closed, the remediation task rules are evaluated against it. A test result is only evaluated once, unless it is reopened after being closed.

Remediation task rules are evaluated after CI matching, risk score calculations, and assignment rules.

The following process is used for each new or reopened test result:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For each remediation task rule, the test result is compared to the condition filter.
- For each rule where the rule condition matches, it pulls the data from the group key columns on the test result. The rule checks to see if there is a matching **Open** remediation task that is assigned to the same assignment group as the test result.

  If the remediation task is found, the test result is added to the existing remediation task in the **Open** state.

- If no remediation task in the **Open** state is found, the rule creates a remediation task, assigns it based on the **User Group** or **Key** value in the rule, and places the test result in it.

More than one test result rule can be defined, to group different kinds of results. Since each result is compared with the rule conditions before putting it in a remediation task, too many rules may have a performance impact.

When a remediation task rule is deleted, you have the option to delete all open remediation tasks created by the rule. This applies to both the rule form view and list view.

When a remediation task assignment is made or changed, the **Assignment group** and the **Assigned to** fields roll down to all test results, except for those where the test result has a different assignment group than the RT. For more information on assignment rules, see Configuration Compliance assignment rules overview. These assignments are used automatically for this group on the next import.

Track deferral counts for test results and remediation tasks

Starting with v14.3, track the number of times a test result or a remediation task is deferred in the Multiple deferrals module. A scheduled job, **set deferral counts**, runs daily to post counts for records that are deferred more than once in the Deferral count column in the records that are listed in the Multiple deferrals module.

Configuring calculator groups and calculators for Configuration Compliance

Configuration Compliance calculators are used to update record values when pre- defined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Configuration Compliance calculators

The Configuration Compliance application includes two types of calculators, Risk Calculators and Risk Score Rollup Calculators. These calculator groups are enabled by default.

The Risk Score calculator group has been renamed to Risk Calculators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Risk Score Rollup Calculators includes rollup calculators for configuration tests and remediation tasks.

Configuring risk and rollup calculators for remediation of test results and remediation tasks includes the following tasks:

- Create a risk calculator
- Create a risk score rollup calculator

After you create a risk calculator, it is available for calculations with the next data ingestion. After you create it, you may also prefer to apply it on-demand.

For more information about calculators and calculator groups, see Configuration Compliance calculator groups.

Configuration Compliance Exception Management overview

When your organization can't comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception. Exception management entails requesting, reviewing, approving, or rejecting exceptions for a remediation task that cannot be remediated according to the policy.

Important: Exception management is supported in the Vulnerability Manager Workspace and IT Remediation Workspace.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Some vulnerabilities might not have an existing patch, fix, or solution. When an exception is approved, it also means that you're accepting a risk because you're acknowledging and agreeing to the consequences of not remediating the configuration-related vulnerability.

Life cycle of an exception

An exception is a request to defer the remediation of a remediation task for a specified period.

The life cycle of an exception is as follows:

- Requesting an exception
- Approving an exception request
- Tracking an exception request
- Expiry of an exception request

Requesting an exception

As the remediation owner, you can ask for an exemption for a remediation task using the exception management process. During the approval process, the remediation task remains in **In**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

review state. After the exception approver approves this request, the remediation task moves to a **Deferred** state.

Important: You can request an exception from the IT Remediation Workspace. For more information, see Request an exception in the IT Remediation Workspace.

Approving an exception request

Remediation tasks that can't be remediated immediately are reviewed, assessed for risk, and approved for deferral until they can be remediated. Approving an exception request can be a two-level workflow. If only the first-level approver is present, the exception can be requested and approved. However, if there's no first-level approver, an exception can't be requested. See Add an exception approver for Configuration Compliance for more information.

Important: You can approve or reject an exception request from the Vulnerability Manager Workspace. For more information, see Request exceptions for remediation tasks and records from the Vulnerability Manager Workspace.

Note:

Starting from Configuration Compliance v13.0, if you are deploying the CC application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow.

Once an exception request for a remediation task is approved, you can perform the following actions:

- Reopen
- Delete

Note: Rejection comments are shown in the Work notes for a remediation task. If an exception request is rejected, this remediation task reverts to its previous state.

Tracking an exception request

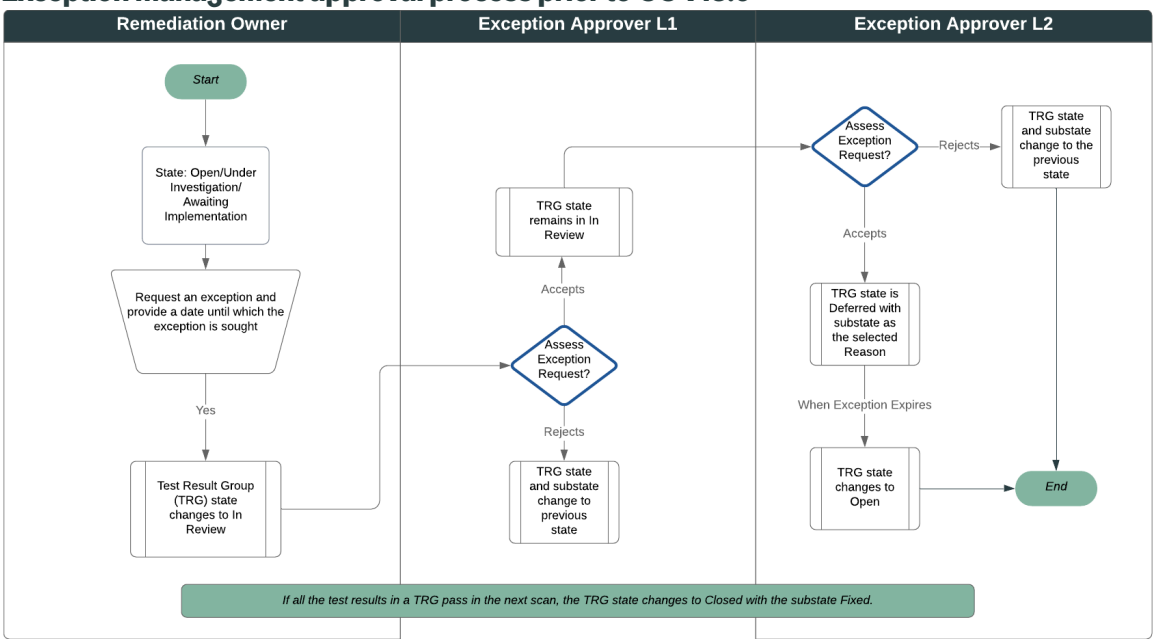
After raising the exception, you can track its status by using the **State Change Approvals** tab of the remediation task. If an action is taken on a remediation task, you can't track the status of the individual test results in that remediation task.

Expiry of an exception request

When an exception request for a remediation task expires, the remediation task reverts to its **Open** state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception management approval process prior to CC v13.0



Configuration Compliance change management

As an IT remediation owner, you can create and manage change requests (CHG) directly from remediation tasks (RTs) in the Configuration Compliance application.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Change requests and the Configuration Compliance workflow

Change requests and change management are part of the remediation process of the Configuration Compliance workflow. During this remediation phase, you might use change requests to help you prioritize, track, and remediate test results.

The Configuration Compliance application works with the ServiceNow AI Platform® IT change management process to help you remediate non-compliant software and technologies in your environment.

With change management in the Configuration Compliance application, you can associate test results to existing change requests, or split a remediation task and create a new remediation task only for selected test results.

For more information, see Create a change request in Configuration Compliance.

Key terms

Tests

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tests are libraries of data records that organize scans of computing assets. Configuration tests define how a class of technology assets should be governed. A test is anything that can be used to identify a class of software or a hardware asset that is out of compliance.

Test results

Test results are imported by third-party integrations. Once they are viewable in Configuration Compliance, they are remediated using **Remediation Tasks**. Groups are assigned for remediation according to assignment rules.

> **Note:** Starting with version 14.9 of Configuration Compliance, test result is labelled, Finding.

Remediation task

Test results are grouped into remediation tasks according to assignment rules and automatically assigned to remediation owners for remediation.

> **Note:** Starting with version 14.9 of Configuration Compliance, test result is labeled Remediation Task.

Test Groups

Test groups are related to authoritative documents and test records. A group of configuration tests define a Test group.

Change requests

Change requests help you implement controlled processes for remediation. You might use change requests with remediation tasks in Configuration Compliance to help you identify, track, and resolve non-compliant assets (configuration items) that require additional resources, or that you might target for deferral.

For more information about test results and remediation tasks, see Configuration Compliance remediation tasks and remediation task rules overview.

When to use change requests in Configuration Compliance

Change requests help you initiate and track remediation activities on your test results. When remediation owners have large numbers of unremediated test results or configuration items, they might use change requests to identify test results for deferral. Alternatively, they might identify and regroup test results and configuration items that require more resources than initially identified in the original remediation task.

Create change requests from a remediation task

Create a change request directly from a remediation task for all the test results in the remediation task, or use filtering to identify only test results that match specific criteria. Create a change request with pre-populated information to expedite your investigation for test results that require manual intervention.

Split a remediation task

From an existing remediation task, identify a subset of test results that you want to move to a new remediation task. By creating a new TRG, you can work with a specific group of test results without impacting the original remediation task.

Associate test results to an existing change request

Associate test results to existing tasks to avoid creating duplicate change requests as you work to resolve your remediation tasks. By associating a remediation task to a change request that is already available in your instance, you can use an existing lists of tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Types of change requests for a remediation task

You can create, approve, implement, review, and close change requests directly from remediation tasks that are assigned to you. You can create three types of change requests with pre-populated information from a remediation task:

- Standard. A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction.
- Normal. Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed.
- Emergency. A change to resolve a major incident.

Setting up, installing, and configuring the Configuration Compliance application

Before you run the application in your ServiceNow AI Platform® instance, you must first download and install the Configuration Compliance application from the ServiceNow® Store. This application is available as a separate subscription.

Complete the following setup checklist steps listed in the following table prior to installation. These setup tasks are required for a smooth installation and configuration.

For more information about released versions of the Configuration Compliance application, as well as third-party and ServiceNow applications that are compatible with it, see the Vulnerability Response Compatibility Matrix and Release Schema Changes [KB0856498] article in the HI Knowledge Base.

For more information about getting entitlements for store apps, see Security Operations and the ServiceNow Store.

Setup checklist tasks

Setup tasks	Description
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns the Configuration Compliance Admin [sn_vulc.admin] role. • The Configuration Compliance Admin [sn_vulc.admin] oversees configuration and verifies expected results. • The Remediation Owner [sn_vulc.remediation_owner] reads and updates assigned records. The sn_vulc.remediation_owner role is also automatically assigned when any user is assigned the itil role.
Supported integrations	Before you can use Configuration Compliance to remediate configuration items, you must

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup checklist tasks (continued)

Setup tasks	Description
	install a third-party scanner integration and perform at least one network scan. Verify that the Vulnerability Response application is installed and activated prior to configuring supported third-party integrations. See Install Vulnerability Response. To verify that integration applications are installed and activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. For more information about third-party integrations and a list of supported products, see Configuration Compliance integrations.

Qualys Vulnerability Integration

- If the Qualys Vulnerability Integration is already installed on your system, and your API credentials are different than the ones you want to use for Configuration Compliance, go into Setup Assistant (in Vulnerability Response) and assign them to each **Qualys PC** integration.
- Navigate to **Qualys Vulnerability Integration** > **Primary Integrations** and edit the **Qualys API Credentials** field under the **Qualys REST Details** tab.

For more detailed information on the Qualys Vulnerability Integration, see Understanding the Qualys Vulnerability Integration.

You are now ready to install the Configuration Compliance application. See Install Configuration Compliance.

Install Configuration Compliance

Before you run Configuration Compliance in your ServiceNow AI Platform® instance, you must first download and install the Configuration Compliance application from the ServiceNow Store. This application is available as a separate subscription.

Before you begin

Complete the following setup checklist prior to installation. See Setting up, installing, and configuring the Configuration Compliance application for setup tasks. These setup tasks are required for a smooth installation and configuration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To Opt in to ServiceNow products, follow the steps in Opt in to the ServiceNow Store products.
2. To install an application that you have purchased from the ServiceNow Store, follow the steps in Install a ServiceNow Store application.
3. **Optional:** Alternatively, if you want to manage your entitlement for the Configuration Compliance application on other ServiceNow AI Platform instances, follow the steps in Manage entitlements from your ServiceNow instance.
4. If you have already installed the Configuration Compliance application and you are updating it, see Install an update to a ServiceNow Store application.
5. Install supported applications.

   Separate third-party applications acquire and transform data in Configuration Compliance. Before you can use Configuration Compliance to remediate configuration items, you must install a third-party scanner integration and perform at least one network scan.

   For information about installing third-party integrations for Configuration Compliance, see Configuration Compliance integrations.

Components installed with Configuration Compliance

Several types of components are installed with activation of the Configuration Compliance plugin, including tables and user roles.

Starting with v15.1.5 of Configuration Compliance, the most frequently used system properties are now accessible within the Configuration Compliance application. To view these system properties, navigate to **All**Configuration Compliance**Properties**.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

View filtered lists for components installed with an application

Filter the Applications Files table so that only the roles, scheduled jobs, and tables that are installed with an application are displayed. The application you want to view these components for should be installed so that its files are loaded onto the instance and into the metadata table. Follow these steps to view filtered lists from the Applications Files table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. In the filter navigator, enter **sys_metadata.list** to navigate to the metadata table.
2. Select the condition builder (filter icon), and select, **Application** > **is** followed by the name of your application. For example, **Application** > **is** > **Vulnerability Response**.
3. In the condition builder, to add a second filter, select **AND**, then select, **Class** > **is a** and choose one of the following classes from the list: **Role**, **Scheduled job**, or **Table**.
4. Select **Run**.

The results for the class you selected are displayed in a filtered list.

Roles installed

Role title [name]	Description	Contains roles
Configuration Compliance administrator [sn_vulc.admin]	Able to modify application property, configuration, update rules, integrations of Configuration Compliance application. Starting with v15.0, an admin user cannot delete source records such as Expliots, CVEs, etc.	sn_vulc.write **Note:** Inherits the roles that are required for the administration of the records of the Configuration Compliance application.
read [sn_vulc.read]	Read lists and records in Configuration Compliance.	sn_sec_cmn.calc_read
write [sn_vulc.write]	Write lists and records in Configuration Compliance.	• sn_vulc.read • sn_vulc.remediation_owner
write assignment [sn_vulc.write_assignment	Write to Test Result assignment fields.	Contained in the sn_vulc.remediation_owner role.
remediation owner sn_vulc.remediation_owner	View and update permission for test results assigned to you or your group.	Contained in the itil role. Contains: • sn_sec_cmn.read • sn_vulc.write_assignment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
CC.System sn_vulc.import_admin	Runs all scheduled jobs in configuration compliance application. **Note:** This user is the default run-as user for every scheduled job in configuration compliance.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration
VRCommon.System sn_vul_cmn.admin	Default run-as user for all scheduled jobs in Vulnerability Response common application.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	Default run-as user for all scheduled jobs which are used for the background jobs capability in Security support common application	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7: sn_vulc.edit_watch_topic	Edit watch topics for Configuration Compliance.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Read watch topics for Configuration Compliance.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Create watch topics for Configuration Compliance.	sn_vulc.read_watch_topic
sn_vulc.auditor	Allow read for all configuration	sn_vulc.read

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	compliance modules	sn_vulc.advanced_read
sn_vulc.advanced_read	Allow read for all the configuration compliance administration modules	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	Allow read for test criticality mapping	
sn_vulc.read_task_rules	Allow read for remediation task rules	
sn_vulc.read_assignment_rules	Allow read for assignment rules	
sn_vulc.read_risk_score_configuration	Allow read for risk score configuration	
sn_vulc.read_auto_close_rules	Allow read for auto close configuration	
sn_vulc.false_positive_approver	Allows approving / rejecting closing remediation tasks as false positive	
V15.0: sn_vulc.delete	Deletes source records.	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled jobs installed

Scheduled job	Description
V15.0: Update test group on configuration tests	Updates test group on tests for Tenable and Microsoft Defender source. This is an one-time job.
V15.0: Populate existing test result fields	Updates values into newly added columns (such as Age, Age closed, Active, etc) in the test results table, saved filters and modules. This is an one-time job.
V15.0: Populate Vulnerable CIs table - Delete and Re-populate for Test Results	Populates total records in the Vulnerable CIs table. This is an one-time job.
Version 12.0 Calculate remediation metrics for all the test results groups	Calculates and updates values for status metrics on remediation task records.
Version 12.0: Calculate remediation metrics for all the test results	Calculates and updates values for status metrics on test results records.
Version 12.0: Change Request State Synchronization	On-demand job that synchronizes the states of all existing remediation tasks (RTs) with change requests (CHGs). As a change request moves through its life cycle, it also moves the states of any related remediation tasks automatically. Enables state synchronization going forward.
Version 11.1: Check Test Result Groups Deferment Expiration	Sends notifications if remediation tasks have expired (and if they expire in one week).
Configuration Compliance CI count	Populates distinct configuration item (CI) count and the 90 day rolling average in the Configuration Item Count [sn_vulc_cc_configuration_item_count] table.
Version 11.1: Evaluate and notify remediation targets	Sets or updates remediation target dates on all test results. Determines the status of remediation target dates against rules. Sends notifications
V14.7: Insert Test Result Groups Into Unified Remediation Task	One-time scheduled job to insert all the remediation tasks created in the classic UI into the Unified remediation task (sn_vul_remediation_task).
Version 12.0:	Populates change requests on remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Populate CR-TRG m2m for CR and CR-Parent	
Removed in v11.1: Re-open deferred test result groups **Note:** Deprecated for versions prior to 11.1. Do not use.	Reopens deferred groups when the due-date has passed.
Reapply all assignment rules	Reapplies all assignment rules.
Version 14.3: Reassignment count for assignment rules	Runs daily and posts the total number of test results and remediation tasks that are unassigned by this feature for a particular assignment rule.
Reassess the state of the test result groups	Reassesses the state of remediation tasks for entries where **assess_state** is false. Runs every 15 minutes.
Rollup test result risk score to test result group and configuration test	Runs hourly and calculates the rollup scores for the changed configuration tests and remediation tasks. • Calculates rollup risk score for all tests in sn_vulc_test_manifest and deletes the manifest record upon completion. • Calculates the rollup risk score for all the tests in sn_vulc_result_group_manifest and deletes the manifest upon completion.
Version 12.0: Update policy remediation metrics	Starting with v15.0 of Configuration Compliance, this scheduled job has been renamed to Update remediation metrics. • Calculates and updates values for status metrics on policy records. • Calculates test result compliance % of a CI on Discovered Item.
Version 14.3: Set deferral counts	Collects the number of times a test result or a remediation task is deferred.
Update Risk Rating for Test Results	Updates Risk Rating for Test Results.
Update Rollup risk score for all non closed Result groups and Configuration tests.	Updates the rollup risk score for all non-closed Result groups and Configuration Compliance tests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tables installed

Table	Description
Assignment Rule [sn_vulc_assignment_rule]	Contains the set of rules evaluated to set the assignment group on test results.
Authoritative Source [sn_vulc_auth_src]	Store imported authoritative sources.
Calculator [sn_vulc_calculator_risk_score]	Contains the calculator that sets certain test result fields when certain conditions are met.
CC Configuration Item Count [sn_vulc_cc_configuration_item_count]	Contains the total number of configuration items.
Version 12.0: Change request association [sn_vulc_action_associate_cr]	Staging table used for associating change requests to remediation tasks.
Version 12.0: Change request creation [sn_vulc_action_create_cr]	Staging table used for creating change request forms.
Version 12.0: Change request form [sn_vulc_cr_form]	Base table for change request management.
Citation [sn_vulc_citation]	Contains imported citations
Configuration Test [sn_vulc_test]	Contains imported configuration test data.
Configuration test manifest [sn_vulc_test_manifest]	Contains the configurations tests for which the rollup risk score needs to be calculated.
Version 12.2 Missing asset table [sn_vul_missing_asset]	Contains temporary asset records for imported configuration compliance assessment data with unmatched assets.
Configuration Test Technology [sn_vulc_test_technology]	Contains imported configuration test technologies.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Group Rule [sn_vulc_grouping_rule]	Contains the rules that define the criteria with which groups are automatically created for a set of test results.
Policy [sn_vulc_policy]	Contains imported policies.
Policy Configuration Test [sn_vulc_policy_test]	Contains imported policy configuration test data.
Remediation Target Rule [sn_vulc_ttr_rule]	Defines the expected time frame for remediating a test result.
Risk Calculators [sn_vulc_calculator_group]	Contains the grouping of Configuration Compliance calculators. The order of the calculator group determines which group is evaluated first, and in each group, one calculator at most is used.
Risk Score Rollup Calculator [sn_vulc_risk_score_rollup]	Contains rollup calculator configurations.
Split test result group [sn_vulc_action_split_trg]	Staging table used for splitting remediation tasks.
State Change Approval [sn_vulc_state_change_approval]	Contains approval state process data.
Technology [sn_vulc_technology]	Contains imported technologies.
Test Criticality Map [sn_vulc_test_criticality_map]	Contains criticality map data.
Test Result [sn_vulc_result]	Contains imported test results.
Test Result Group [sn_vulc_result_group]	Contains imported remediation tasks.
Version 12.0:	Contains change requests for remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Test Result Group Change Requests	
Test result group manifest [sn_vulc_result_group_manifest]	Contains the remediation tasks for which the rollup risk score needs to be calculated.
Test Result Groups [sn_vulc_m2m_result_result_group]	Contains remediation task data.
Test Result History [sn_vulc_result_history]	Contains imported test result history.
Test Result Remediation Status	Status of the test result against the closest applied remediation target rule.
V14.7: Watch Topic Test Counts [sn_vulc_wt_test_counts]	Cache table for the Distinct Configuration Tests tab in the Vulnerability Manager workspace.

Create or edit Configuration Compliance assignment rules

Create rules to automatically assign test results based on filter conditions. These rules assign test results as they are imported.

Before you begin
Role required: sn_vulc.admin

About this task
The base system ships with one Configuration Compliance assignment rule, **Assign to CI support group**, which assigns test results to the same assignment group as the CI support group. This rule is inactive by default. You can modify using filter conditions. With assignment rules, you define one or more conditions of assignment and the order of execution. Once a test result matches a rule condition, the assignment lookup stops.

Note: New or updated rules are automatically evaluated on the next import or manually using the **Apply Changes** button on the Assignment Rules list.

Procedure
1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Assignment Rules**.
2. Open the **Assign to CI support group** rule or click **New**.
3. Edit the **Assign to CI support group** rule, or if **New**, fill in the fields on the form, as appropriate.

Configuration Compliance Assignment Rule

Field	Description
Name	Name of the group rule.
Execution order	Order in which the rules are evaluated. The lowest number is evaluated first.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	High priority rules, test results that need special handling, where risk is critical, or a test result that should be handled by regulatory compliance, should be run first. Next, run your general rules, where no special handling is required, and you know who should be responsible for them. Finally, create a default rule to assign test results to the group that figures out what assignment group it should belong to. This group could add another rule to cover their decisions. This default rule would run last.
Active	Indicates whether the assignment rule is active.
Condition	
Condition fields	Conditions that must be met. Case sensitivity for the search text you enter in the condition builder is not supported on this record or form.
New Criteria	Adds more condition filter fields to choose from.
Description	Text describing the assignment rule.
Assign using	To automate the assignment of groups created based on this rule, choose one of the options available. ○ User group: Select a user group from the lookup table ○ User group field: Select a user group field from the drop-down menu. ○ Script: Create or edit a script. **Note:** Creating or edit a script requires ServiceNow expertise.
User group field	Select the user group responsible for remediating tests that match the conditions of the assignment rules.

4. Click **Submit**.

Configuration Compliance remediation target rules

With remediation target rules, you can set the expected time frames for remediating test results. You can send notifications to users and groups when target dates are approaching and when they are past due.

Important: As an Configuration Compliance admin or analyst, you can obtain the latest remediation target date for a specific set of test results in the Vulnerability Manager Workspace. This method is more efficient than running the Remediation Target Rules for all test results in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Roles required: Configuration Compliance administrator (sn_vulc_admin), or a manager with the sn_vulc.manage_remediation_target_rules role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

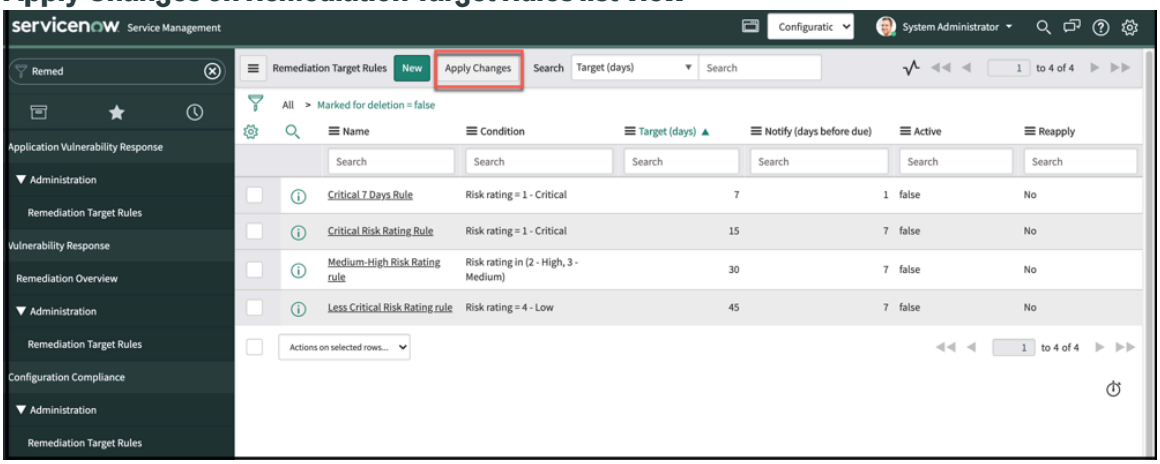
Remediation target rules

A scheduled job, *`Evaluate and notify remediation targets`*, runs daily and uses active remediation target rules to evaluate active test result records. Whenever test result records associated with remediation tasks are updated or changed, the modified values are evaluated by the target rules, and changes are rolled up and displayed on associated remediation tasks.

You can edit, disable, or delete existing remediation target rules and create new ones. When you change, disable, or create a new rule, you have the option to click **Apply Changes** from the Remediation Target Rules list view and manually apply the changes you introduced before the next scheduled job. With this option, you can reevaluate your test result records without having to wait. If you do not choose to apply your changes manually, the next daily scheduled job picks up your changes and applies them.

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Remediation Target Rules** to view remediation target rules.

Apply Changes on Remediation Target Rules list view



2. Click a rule in the Name column to open its record.
3. Select the **Active** check box on the Remediation Target Rule record to enable (`true`) any disabled rules (`false`).

Whenever you change or add a target rule, regardless of whether you choose to apply the changes manually or wait for the next scheduled job, your changes are used to evaluate all active test results along with any other target rules that are affected by your changes. When you choose to manually apply the changes, this evaluation may take some time if you have a large volume of active test results, because all the rules impacted by your changes are used for an evaluation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, the default value for targeted remediation days is 30. If you create a new rule that also has 30 for Targeted remediation days, this rule, and any target rules with 30 days or greater as target dates are each applied to your test results.

Deactivated and deleted target rules

When a rule is active, `true` is displayed in the Active column on the Remediation Target rules list view. After a rule is deactivated (`false`), it is no longer applied to new test results. However, the scheduled job continues tracking any existing test results the rule was applied to. If the deactivated rule or rules are subsequently reactivated, any test result with an empty **Remediation Target Date** field is evaluated against the reactivated rules. This includes test results created while the rules were deactivated.

When rules are deleted, the **Remediation Target Date** and related fields on closed test results are preserved. The **Remediation Target Date** and related fields on non-closed test results are cleared, and any dependent rules are reapplied.

To deactivate a rule, from the remediation target rule record, disable the active check box and click **Update**. `False` is displayed in the Active column on the Remediation Target Rules list view.

To delete a rule, click **Delete** on the form, or, alternatively, from the list view, select the rule or rules, and click **Delete** from the **Actions on rows** list. The rule is no longer displayed on the list and the next rule in the order of operation replaces the deleted rule.

If you deactivate or delete a rule and choose to apply your changes prior to the next scheduled job, the rule reference is cleared from the field, but the remediation date and status data are preserved. If you do not apply your changes manually, the rule reference is cleared from the field with the next scheduled job.

About Target rules and the Evaluate and notify remediation targets scheduled job

The *`Evaluate and notify remediation targets`* scheduled job runs once at 4:30:00 daily. It picks up any active remediation target rules and evaluates all active test results starting with the test results with the earliest remediation target date. It evaluates all test results that meet the following criteria:

- Are not in a **Closed** state.
- Have no remediation target date.
- Have remediation target dates that are later than the dates in the remediation target rules.
- Are created after a scanner import is completed. The scheduled job picks up and evaluates any new test results that are created as a result of an import.

After a target rule is defined, remediation target dates are calculated by the *`Evaluate and notify remediation targets`* scheduled job. The scheduled job adds a remediation target date, if one does not exist, or, if this rule contains an earlier date than the one in the record, it updates the existing target date.

Any expired records and reminder dates that match the target rules are picked up by the job and notifications are sent. For disabled rules, the job clears the remediation fields on test result records and stops sending notifications.

The sn_sec_cmn.evaluate_targetmissed_records property, when enabled, prevents the *`Evaluate and notify remediation targets`* scheduled job from evaluating Target missed Test Results. This property is enabled by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing target dates and status on the list and form views

Configuration Compliance managers can see the remediation target date from both the test result form and list views. Remediation target rules are also run after a scanner import and rerun if a test result is reopened.

The scheduled job updates the **Remediation target** and **Remediation status** in the test result list view, and the **Remediation target rule**, **Remediation target**, and **Remediation status** fields on test result form.

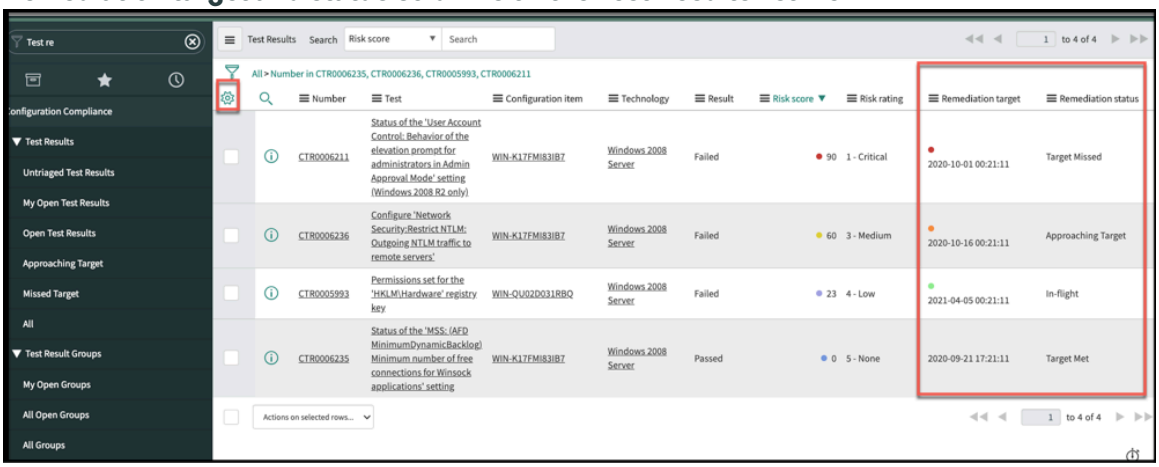
Note: By default, the **Remediation target** and **Remediation status** columns are not displayed on the Test Results list view. To display these columns, you also must add them to the list view. Similarly, add the **Remediation target rule**, **Remediation target**, and **Remediation status** fields to the test result form.

Use the slushbuckets in the Settings and Additional action menus, respectively, as shown in the following images to display these columns and fields. For the Additional action menu on the test result record, click the menu icon, followed by **Configure** and **Form layout** to view the slushbucket and move the fields from **Available** to **Selected**.

The Remediation target date is coded on the Test Results list view as colored dots:

- Test results that have not reached their notification date are shown in green.
- Test results approaching the remediation target date are shown in orange.
- Test results past the remediation target date are shown in red.

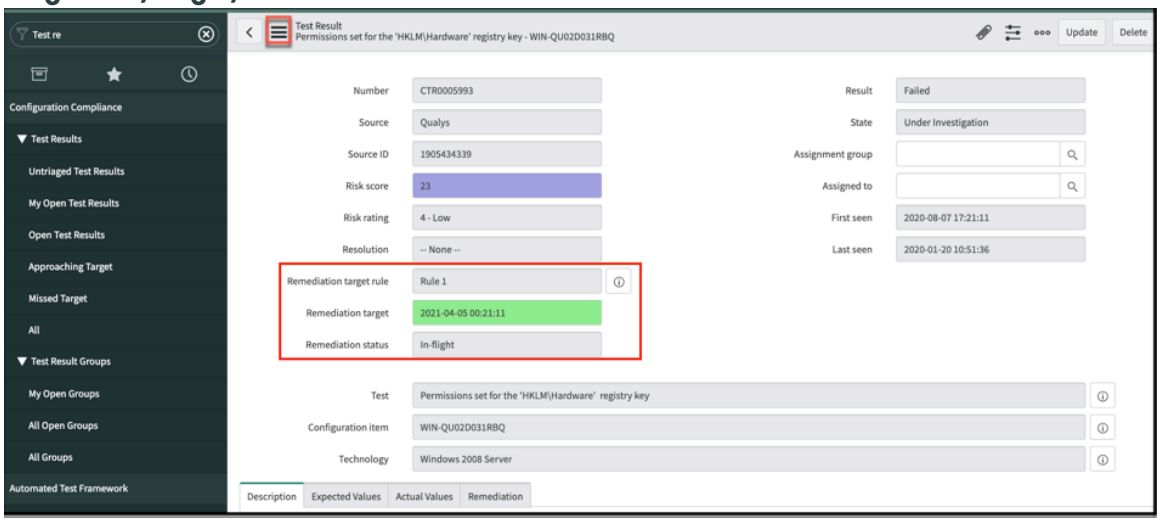
Remediation target and status columns on the Test Results list view



- `Target Missed`: the target date is past due
- `In-flight`: the test result is in progress

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Target rule, target, and status fields on the test result record



Test result records are also displayed visually on the Configuration Compliance Dashboard. Navigate to **All** > **Configuration Compliance** > **Overview** and check the dashboard for status. The Overview includes existing widgets and remediation status. The colors of the graphs match the colors displayed in the Test Results list view and Test Result record.

Remediation target rule scenario

When multiple remediation target rules are applied to the same test result, the most restrictive rule is applied.

For example, if a test result first identified on 03/01/2018 meets the conditions for two remediation target rules:

- Remediation target rule 1: Defined on 03/07/2018; remediation target is 15 days since first seen; calculated remediation target date is 03/16/2018 10:00:00.
- Remediation target rule 2: Defined on 03/10/2018; remediation target is 10 days since first seen; calculated remediation target date is 03/11/2018 10:00:00.

Note:

Remediation targets are calculated from the **Last seen** date plus the number of days (measured as 24-hour increments).

Starting from V14.5, remediation targets are calculated from the **Target from (date)**. The default value remains **Last Seen**. Starting from v14.12, the default value is **Last pass**.

In this scenario, Remediation target rule 2 applies to the test result, because it has the more restrictive date: 10 days since the test result was first identified versus 15 days.

Create or modify target rules and reapply changes

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Remediation Target Rules** to view, edit, and create new remediation target rules.
2. In the Name column, click a rule to open a target rule and edit the record, or, alternatively, click **New** to create a new target rule.
3. Fill out the form to define the expected remediation time frame, specify which test results this rule to applies to with conditions, and determine when to send reminders to users or groups, or both.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name for your rule.
Active	Enable or disable the rule. The rule is automatically enabled (true) by default and will be applied to your test results if you choose to apply changes manually or after the next scheduled job.
Target (days)	Set the targeted deadline date for remediation in number of days. The default value for targeted remediation days is 30. For example, if you create a new rule that also has 30 for a Target value, your new rule and any other existing rules that also have 30 days or greater as target dates will be applied to your test results.
V14.5: Target from (date)	Date from when the target dates are computed. You can specify only the date or the date and time type fields. Starting from v14.12, the default value is *Last pass*. Select one of the following: ○ Last seen ○ First seen ○ Created ○ Last pass If the last pass is empty, the Created date is considered for the calculation of remediation target. To customize the values for this field, see KB1642413.
Notify (days before due)	Set a number of days before the deadline date to remind users and groups.
Description	Short description of the rule.
Condition	Use the condition builder to specify the test results this rule applies to. For example, set a remediation target date of 30 days for all test results with risk scores greater than 70. Send reminders to users or groups, or both, seven days prior to the remediation date. Case sensitivity for the search text you enter in the condition builder is not supported on this record or form. Prior to v 12.0, case sensitivity is supported for the search text you enter in the condition builder.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
User and user groups or both	Select users or groups, or both to send notifications about the approaching and past due target dates you have set.

4. Click **Submit**. Alternatively, to save edited rules, click **Update**.

   The list view is displayed with your updated or new rule. Rules in the list are ordered and run starting with the rule with the lowest remediation target date. If you disable or delete a rule, the next rule in the order sequence replaces the inactive or deleted rule.

5. To apply your new changes now, click **Apply Changes**.

Important: As an admin or analyst, you can obtain the latest remediation target date for selected test results in the Vulnerability Manager Workspace. This method is more efficient than running the Remediation Target Rules for all test results in the classic UI, which is a time-consuming process. For more information, see Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace.

Configuration Compliance calculator groups

Configuration Compliance calculators are used to update record values when pre-defined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Configuration Compliance calculator groups

From the Default Risk Calculator record, calculator rules can be applied to all affected test results and collections on-demand. Vulnerability managers may use this feature adjust their risk calculator configuration. They might experiment with several prioritization schemes early in their deployment and apply those changes on-demand to view how they impact import findings.

The Risk Score calculator group has been renamed to Risk Calculators.

Risk Score Rollup Calculators are included with Configuration Compliance. There are two types of individual rollup calculators:

Configuration Test Risk Roll Up

Calculators that roll up risk scores for all Test Results with the same Configuration Test to provide an overall risk score for the Configuration Test. The rolled-up value is displayed in the Risk Score fields.

Remediation Task Risk Score Rollup

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These calculators roll up risk scores for all Test Results in a Remediation Task to provide an overall risk score for that remediation task. The rolled-up value is displayed in the Risk Score fields.

Both the Risk Score calculator group and Risk Score Rollup Calculators group are enabled by default.

For more information, review the following key terms for Configuration Compliance calculators:

Test result

A test result is the outcome of the configuration test on a configuration item (CI) and the associated technology. Test results in Failed, error, and Unknown states identify hardware, software, and assets that are out of compliance with your policies.

Remediation task

Test results are grouped together at the time of data import based on the pre-defined remediation task rules. These remediation tasks are similar to vulnerability groups in Vulnerability Response. Remediation Tasks organize test results into groups for bulk analysis and represent a set of items to remediate.

Risk score in a test result

A value calculated by risk score calculators that is based on the business context of an asset and the severity of the associated test. It is the average of the business criticality of the affected asset as defined in the CMDB, and the severity of the test as communicated by the scanner.

Each asset can have multiple services associated with it. The business criticality of an asset is determined by the service with the highest criticality.

The calculated value is displayed in the Risk Score fields of test results. The scores display values that range from 0-100. Fields are also color-coded to provide you with the severity at-a-glance.

Risk score in remediation task

This score is displayed on the Remediation Task record and is the rolled up value of the risk scores for all the active test results in a Remediation Task. This score changes as test results are remediated in the Remediation Task.

Risk score in configuration test

This score is displayed on configuration tests and is the rolled up value of the risk scores for all the active test results with that configuration test. This score changes as the test results associated with this configuration test are remediated.

Risk rating

The amount of risk a failed test result poses to your system. It is based on a range of risk scores on a 1-5 numeric scale that rates risks as Critical (1) to None (5). The score is based on a range of risk scores and is displayed in Risk Rating fields.

Risk rating ranges

Risk rating	Risk score
1- Critical	90 to 100
2- High	70 to 89
3- Medium	40 to 69
4- Low	1 to 39

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk rating ranges (continued)

Risk rating	Risk score
5- None	0

Risk score rollup calculators

There are two types of rollup calculators:

- Configuration Test Risk Roll Up: These calculators roll up risk scores for all Test Results with the same Configuration Test to provide an overall risk score for the Configuration Test. The rolled-up value is displayed in the Risk Score fields. You can edit the script values for weight and score for these calculators.
- Remediation Task Risk Score Rollup: These calculators roll up risk scores for all Test Results in a remediation task to provide an overall risk score for that remediation task. The rolled-up value is displayed in the Risk Score fields. You can edit the script values for weight and score for these calculators. For an example of a Risk score rollup calculator and how it calculates scores, see Risk rollup calculation example for Configuration Compliance (prior to v15.0).

Historical risk score

The inherent risk score across all the passed test results in a remediation task. This field displays the amount of risk that was remediated by a test group and is only displayed after a test group is in the 'Closed' state and the risk score is zero.

Scores are calculated whenever the risk score changes or when test results are added or removed from a remediation task.

Note: To work properly, this script requires the Service Mapping plugin. Service Mapping is available as a separate subscription and requires activation by ServiceNow personnel.

Create a Configuration Compliance calculator group

Configuration Compliance calculator groups are used to group calculators based on how you want to use them.

Before you begin

Role required: sn_vulc.admin

About this task

The Configuration Compliance base system includes one calculator group: **Risk Score**. As you create other calculators, you can add them to this group or create other groups and calculators. Within each group, the first calculator that matches the test result runs.

There are two calculator groups that are included with the Configuration Compliance application:

- Risk Calculators
- Risk Score Rollup Calculators

Risk Calculators calculate the risk score and risk rating of a Test Result.

Risk Score Rollup Calculators roll up risk scores for all Test Results and Remediation Tasks with the same Configuration Test to provide an overall risk score.

You also create new calculators directly from these groups.

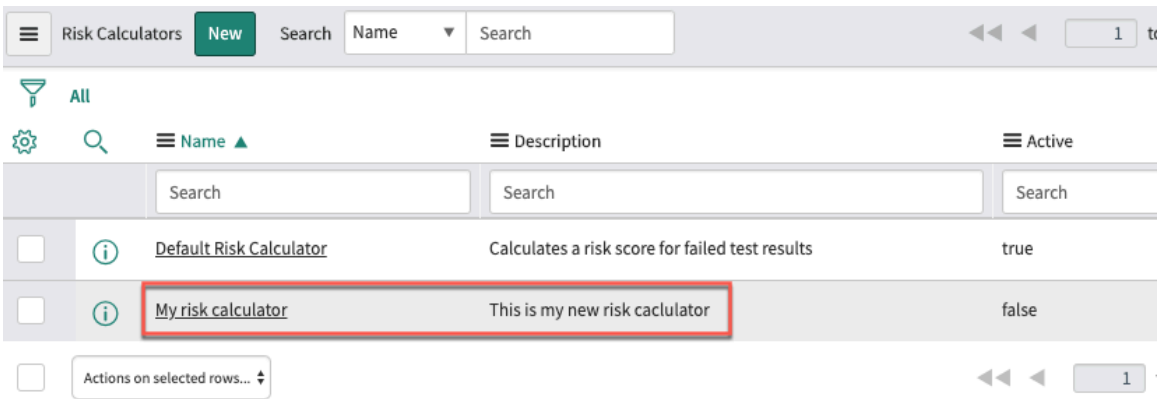
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Calculator Groups**.
2. Navigate to **All** > **Configuration Compliance** > **Administration** and select **Risk Calculators** or **Risk Score Rollup Calculators**.
3. Click **New**.
4. Fill in the fields on the form, as appropriate.

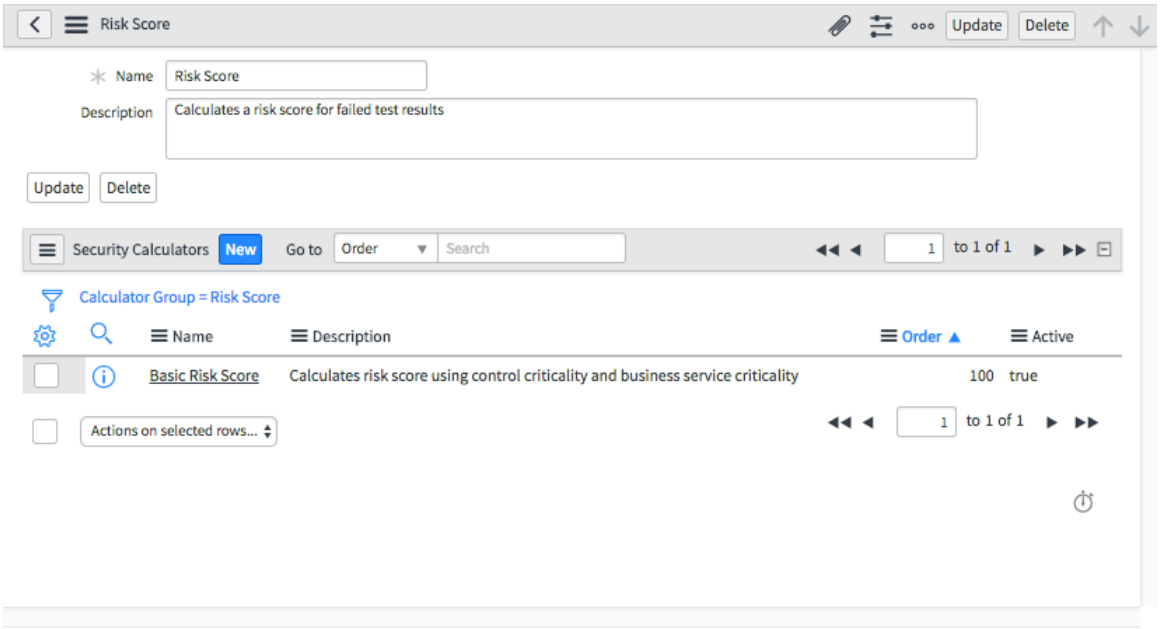
Field	Description
Name	The name of the calculator.
Description	A description of this calculator group.
Active	Enable or disable the calculator group.

5. Right-click **Save** in the form header or click **Submit**.
   The new calculator group is displayed on in the group list with the other calculators. Click the name of new calculator group to open the record. See Create, edit, and reapply risk calculators for Configuration Compliance for more information about setting conditions and displayed values and reapplying calculators.



The **Security Calculators** related list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Click **New** to add calculators along with their conditions to the group.

   Case sensitivity for the search text you enter in the condition builder is not supported on this record or form.

Configuration Compliance calculators and calculator rules

Configuration Compliance automate calculating initial values for the fields on test results. The condition for each calculator is evaluated in order, and the first matching calculator is used.

Configuration Compliance calculators

The Configuration Compliance base system includes one configuration compliance calculator (**Default Risk Calculator**) that sets the base **Risk Score** on the test result. Configuration Compliance calculators can be built to prioritize and rate the impact of test results based on any criteria by using condition filters. Whether it is the business impact of the vulnerability, the class of the configuration item (CI), you can create additional configuration compliance calculators to set other fields on test results or you can customize the existing configuration compliance calculators. A calculator can be written to reflect any set of priorities.

Each calculator contains a list of calculator rules, with a condition determining when to apply it. When the calculator is run, the condition for each calculator rule is evaluated in order, and the first matching calculator rule is used.

All enabled configuration compliance calculators set the selected fields each time a test result is created, when an associated CI or Configuration Test changes, or when the **Calculate Risk Score** related link in a test result is used. As an example, the Risk Score is automatically updated on test result records when the control.criticality value is updated on a test result that is imported. After a test result import has updated a test result score, you can recalculate the risk score of the test results by selecting the **Reapply Calculator** button.

From an existing test result, if you select the **Calculate Risk Score** related link and either of the calculators is enabled, the Risk Score field in the test result is updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The **Calculate Risk Score** related link is only visible when at least one configuration compliance calculator is enabled.
- Starting from v22.0 of Vulnerability Response, you can update the risk score for a test result in the Vulnerability Manager Workspace and IT Remediation Workspace by selecting the **Calculate Risk Score** button in its record view.
- Starting with version 14.13 of Configuration Compliance, whenever the risk score on a test result changes, the following details are documented in the Notes section of the test result:
  - Calculator group name
  - Calculator name: Depending on whether the calculator rule is based on a template or a script, the name is appended with the details in brackets. To modify or view the basis of the calculator rule, select any rule and select the **Advanced view** check box. From the **Value type** drop-down box, select the required option. If **Template** is selected, the risk score is updated according to the specified condition in the rule. If **Script** is selected, you can either add or update the existing script.
  - Field values with their weightage and risk score contribution
  - Final risk score
  - The system property *sn_sec_cmn.risk_score_changes_add_worknotes* helps populate the work notes section. Starting with v15.2.1 of Configuration Compliance, the system property *sn_sec_cmn.risk_score_changes_add_worknotes* is inactive by default. If you enable it, only then you can see all the changes related to the risk score of a test result in the Work notes section. Additionally, the work notes are updated only if there's a change in the risk score.

Configuration Compliance calculator rules

By default, a base system **Default Risk Calculator** is provided. If you want to create a risk rule for this calculator, you must set the target field of **Default Risk Calculator** to **Risk Score**. Select the **New Risk Rule** button to create a new risk rule . This creates a specialized test result calculator rule called a **Risk Rule**, which in turn, calculates the **Risk Score** based on multiple values. By default, the following values for calculating risk score are considered:

- Business Criticality
- Criticality

You can adjust the values to use in the **Default Risk Rule** and how much weight to give each of these values. Weights are used to adjust how much each element counts when setting the base **Risk Score**.

Starting with Configuration Compliance version 13.0, you can customize the criteria for the default risk rule. For more information, see Define fields and weights for the risk rule.

Assigning a weightage percentage

You can also assign weightage percentage (0-100) at the field value level. For example, you can assign a weightage percentage to each level of Severity (None to Critical). If the criticality weightage is 50 for the risk rule, and the following weightage values are assigned for the Criticality level:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign weightage percentage

Criticality	Risk Score
Critical	100
High	50
Medium	20
None	0

If the criticality is critical, the corresponding weightage is 50. If the criticality is high, the weightage is 25, and if the criticality is medium, the weightage is 10. If the criticality is none, the corresponding weightage is 0. For more information, see the Risk score calculation example for Configuration Compliance.

Each rule has an **Order** setting however, the first one to match the conditions updates the **Risk score** field in the test result. Non-scripted calculator rules typically create less of a performance impact than scripted calculator rules.

The base system Configuration Compliance calculator contains calculator rules that assign each level of criticality (None to Critical) a value (0-100) for **Risk Score** based on severity. Unknown severity is automatically assigned a risk score of 100. These values can be adjusted, like Default Risk Calculator, new calculator rules or new risk rules can be created.

Vulnerability Risk Score Weights

All vulnerabilities are assigned a risk score and rating based on factors such as severity, criticality, exploit information, and so on. The business rule *`Update Risk Rating from Risk Score`* on the vulnerable item table is responsible for calculating the risk rating. Whenever the risk score changes, the risk rating is calculated and populated on the vulnerable items. Prior to version 17.1 of the Vulnerability Response (VR) application, the following risk ratings were provided as part of script include `VulnerabilityUtils`, which were hard-coded.

Value (Risk Rating)	Weight (Risk Score)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Starting with the 18.0 version of Vulnerability Response,

- The risk rating types are shipped in the base table as cc_risk_rating. These types are passed as part of the business rule on each table where the risk rating is calculated.
- The script is modified so that you can query the entries in the Risk Score Weights table values for risk rating calculation.
- Add additional entries for an existing type or create a new type. When you create a new type, ensure that you add the labels for the new risk rating, and also modify the related scripts and business rules. You must also add a new style for the new risk score.
- Modify the script to query the records in the base table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can access the Risk Score Weights table by entering sn_sec_cmn_risk_score_weight in the filter navigator.

In addition, the risk score is automatically recalculated in the following scenarios:

- When a configuration item (CI) changes from non-internet facing to internet facing.
- When the associated Common Vulnerabilities and Exposures (CVEs) or third-party entries (TPEs) on the vulnerability items (VIs) are linked to a CVE Known Exploit Vulnerability (KEV).

Define fields and weights for the risk rule

Customize the parameters and weights for the risk rule so that you can generate risk scores that use the test and asset data that are unique to your organization. By selecting the fields that are included in the risk rule, you can define an effective risk scoring framework.

Before you begin

Role required: sn_vulc.admin

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Risk Calculators**.
2. Click **Default Risk Calculator**.
3. Select the target field as **Risk Score**.
   The **New Risk Rule** button displays on the Calculator Rule table.
4. Click the **New Risk Rule** button to navigate to the **Configuration Compliance Risk Rule** form.
5. In the Risk Calculator Criteria section, set the weight for each criterion according to its importance in the overall risk score calculation.
6. Clear the **Active** check box, to deactivate the rule.
7. Click **Add Criteria** to add risk rule fields to the Risk Calculator Criteria.
8. On the form, fill in the fields.

Risk rule field form

Field	Description
Choose reference table	The table that you use to define the risk score weightage. Select from the following options: ○ Test Result: Add fields that are you can directly dot walk to from the Test Result (TR). ○ Test Result - Configuration Item: Add dot walkable fields that are part of the base table extensions, such as the Hardware table. These fields are not part of the base cmdb_ci table. ○ Test Result - Test: Add dot-walkable fields that are part of the tables that extend the base table, for example, Third-party

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Entry. These fields are not part of the Configuration Test base table. ○ Test Result Reference Table: Add fields that are a part of the Related tables (m2m) or tables that have a reference to the test result. These fields are not directly dot-walkable from the Test Result. ○ Configuration Item Reference Table: Add fields that are a part of the Related tables (m2m) of cmdb_ci or tables that have a reference to cmdb_ci. These fields are not directly dot-walkable from the TR. ○ Test Reference Table: Add fields that are a part of the Related tables (m2m) of sn_vulc_test or tables that have a reference to sn_vulc_test. These fields are not directly dot-walkable from the TR. ○ Custom Conditions: Use this option to assign weights to the rule by evaluating the condition. For example, the Internet-facing filter determines if a configuration item (CI) is external or internal.
Field	The field used for risk score calculation for this rule.
Weight	Weightage of this field within the risk rule. The value must be an integer from 0 through 100.
Table	○ Test Result > Configuration Item ○ Test Result > Test ○ Test Result Reference Table ○ Configuration Item Reference Table ○ Test Reference Table This field appears only when any of the listed options is selected from the Choose reference table field.
Aggregation	Select the minimum or maximum value to be considered for calculations when field is selected from the Related tables (m2m). This field appears only when a reference table is selected from the Choose reference table field.
Define value weightage	Component to assign weights to each field value. For numeric fields, define field values as a range (for example, 1–5). The value must be an integer between 0–100.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	This field does not appear if the Custom Conditions option is selected from the Choose reference table field.
Condition table	Select a condition from the list. This field appears only when Custom conditions option is selected from the Choose reference table field.
Field name	Enter a name for the risk criteria. This field appears only when Custom conditions is selected from the Choose reference table field.
Condition	Preview the items in this table that match the defined conditions. This field appears only when Custom conditions is selected from the Choose reference table field.

9. Click **Submit**.

What to do next
In the Rule page, activate and reapply the rule to reevaluate the risk score on the active test result.

Edit risk rollup calculators for Configuration Compliance

Edit an existing risk rollup calculator.

Before you begin
Role required: Role required: sn_vulc.admin

Procedure
1. Navigate to **All** > **Configuration Compliance** > **Administration** and select **Risk Score Rollup Calculators**.
2. With the list of Risk Score Rollup Calculators displayed, click a calculator to open the record and edit the form.

Field	Description
Name	The name of the Configuration Test or Remediation Task rollup calculator.
Description	A description for the risk rollup calculator.
Table	Table on which the rollup calculator is applied.
Include deferral	Includes deferred test results during rollup of risk score.

3. Define the weightages in one of the following ways:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- In the Rollup Weights section, assign weightages for the following:

Rollup Weights

Field	Description	Default weight
Maximum risk score	Maximum risk score of the test results considered.	85
Average risk score	Aggregate of the risk scores of all the test results considered.	0
Count of test results	Number of test results.	15

- Select the **Advanced view** check box, and in the **Script values** editor, edit the values in the script as required.

> **Note:** Editing script requires advanced knowledge of the ServiceNow AI Platform and the Configuration Compliance application.

4. Click **Update** to save your edits.

Rollup calculators are scheduled jobs that run hourly to pick up changes. These scheduled jobs also overall risk scores for configuration tests and remediation task. The rolled-up values are displayed in the Risk Score fields.

For an example of how a risk rollup calculator determines scores, see Risk rollup calculation example for Configuration Compliance (prior to v15.0).

Create, edit, and reapply risk calculators for Configuration Compliance

Calculator rules can be applied to all affected test results and collections on-demand. Vulnerability managers may use this feature adjust their risk calculator configuration and apply changes on-demand to import findings.

Before you begin

Role required: sn_vulc.admin

Procedure

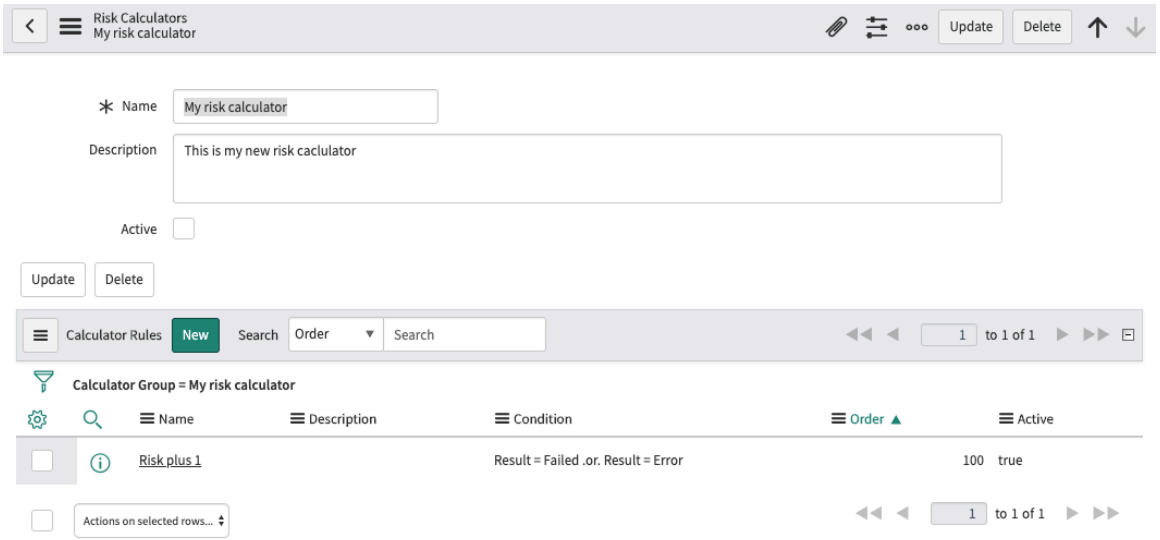
1. To create a new risk calculator, follow these steps.

   a. Navigate to **All** > **Configuration Compliance** > **Administration** and select **Risk Calculators**.

   b. In the Risk Calculator list, click **New**.

   c. Enter a name and description for your new calculator and click **Submit**.
   The new calculator is displayed on the Risk Calculator list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



d. In the list, click the new calculator to create the conditions under which the calculator runs and specify the fields and values you want displayed on test result records and remediation tasks.

e. In the record that is displayed, click **New**.

f. Fill in out the fields in the tabs as appropriate.

Tab	Description
When this condition is met	Use the conditions builder to create the conditions under which the calculator runs. An example is: `Result is Failed or Result is Error`.
Set these values	Use the template to select the fields and values you want displayed.

g. Click **Submit**.
The record is displayed with the new calculator rules and the group it belongs to.

2. To reapply an existing calculator to test results or edit the rules and displayed values for an existing risk calculator, follow these steps.

a. From the Risk Calculators or Risk Rollup calculator lists, select the calculator you want to edit.

b. To reapply a risk calculator to your existing test result data from the record, click **Reapply Calculator**.
All test results that meet the conditions of the calculator are updated.

Note: Depending on the number of test results, this update may take time.

c. To edit the conditions and values, in the lower left in the Name column, click the calculator name.
For risk calculators, the record and the **When this condition is met** and **Set these values** tabs are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Fill in the form as appropriate.

Tab	Field Description
When this condition is met	Use the filter conditions builder to create the conditions under which you want the calculator to run.
Set these values	Choose one to continue. ▪ Value type - Template. Choose fields from the list and corresponding values. ▪ Script - Enter your changes using the editor. **Note:** Editing script requires advanced knowledge of the ServiceNow AI Platform and the Configuration Compliance application.

3. **Optional:** To apply the new rules on-demand to your existing test result data, follow these steps.

   a. With the Risk Calculators list displayed, click a calculator you want to apply.
   The record is displayed.

   b. Click **Reapply Calculator** to test and apply your changes on-demand to your import findings.

4. View your changes on test results and continue to edit your calculators as required.

Examples for Configuration Compliance risk score calculation

Starting with v13.0 of Configuration Compliance, you can customize the criteria for the default risk rule. Use risk scores provided by third-party vendors like Qualys and Tenable for risk score calculations.

Third-party vendors, like Qualys and Tenable, provide their own scores. These scores are populated in the Criticality field on the sn_vulc_test table. Use this field for risk score calculations. To use this score to compute the risk score, follow the procedure:

Add source criticality as a criterion for a risk rule

Use scores based on criticality provided by third-party vendors to compute risk scores.

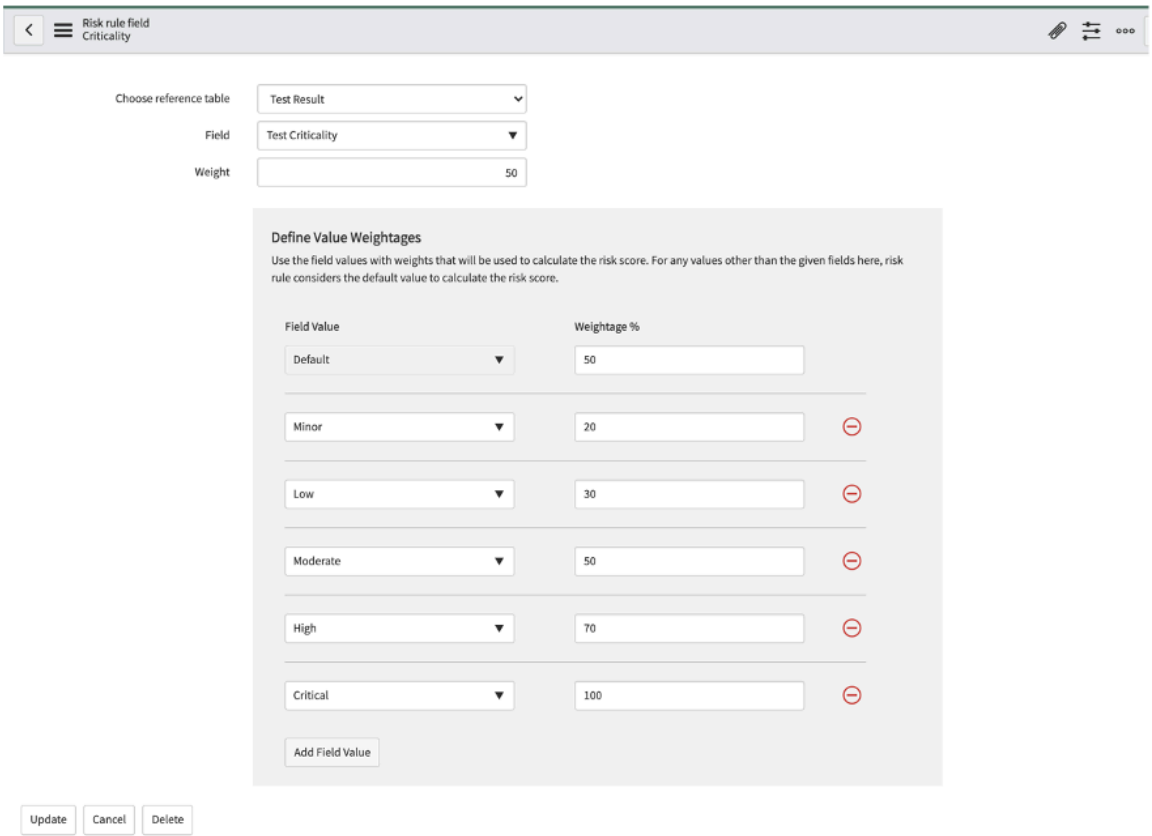
Before you begin
Role required: sn_vulc.admin

About this task
Third-party vendors, like Qualys and Tenable, provide their own risk scores. These scores are populated in the Criticality field on the sn_vulc_test table. Use this field for risk score calculations and computing the risk score.

Procedure
1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Risk Calculators**.
2. Navigate to the Risk rule form.
3. Clear the **Active** check box, to deactivate the rule.
4. Click **Add Criteria**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. From the **Choose reference table** list, select **Test Result**.
6. From the **Field** list, select **Test.Criticality**.
7. In the **Weight** field, specify the relative importance of this field.
   The value must be an integer from 0 through 100.
8. In the **Define Value Weightages** section, add field values, and assign a weightage percentage to the fields.



9. Click **Submit**.

Add business criticality as a criterion for a risk rule

Specify a criticality value to business services and use the business criticality to compute the risk scores.

Before you begin

Role required: sn_vulc.admin

About this task

Assuming your organization has many business services and a configuration item (CI) is being used by the following services:

Criticality of the business services

Business Service	Criticality
Cloud Management	1 - Most critical
E-commerce	2 - Somewhat critical

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Criticality of the business services (continued)

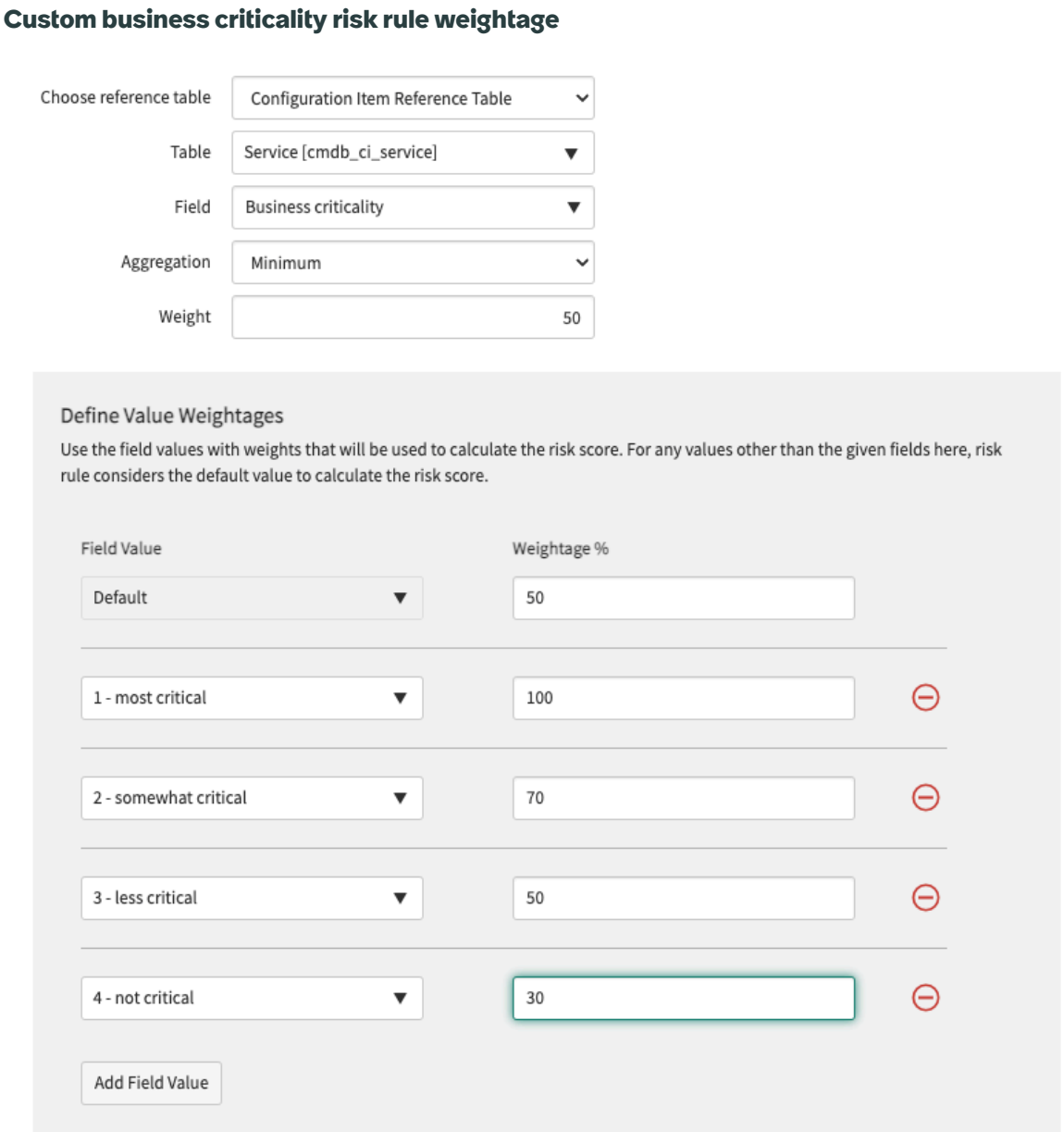
Business Service	Criticality
Client services	3 - Less critical
Travel and Expense	4 - Not critical

The mapping between the CI and services is stored in the Services [cmdb_ci_services] table. When a CI does not pass a Configuration Test, a Test Result (TR) is created. You can use the value of the business criticality from the affected services to compute the risk score for this TR. Follow the procedure to use the criticality value of these services to compute the risk score.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Risk Calculators**.
2. Navigate to the Risk rule form from the **Calculator Rules** section.
3. Clear the **Active** check box, to deactivate the rule.
4. Click **Add Criteria**.
5. From the **Choose reference table** list, select **Configuration Item Reference Table**.
6. From the **Table** list, select **Service [cmdb_ci_service]**.
7. From the **Field** list, select **Business Criticality**.
8. In the **Aggregation** field, select **Minimum** to retrieve the most critical service for this use case (1- Most critical value) or **Maximum** to retrieve the least critical service for this use case (4 – Not critical value).
9. In the **Weight** field, specify the relative importance of this field.
   The value must be an integer from 0 through 100.
10. In the **Define Value Weightages** section, add field values and assign weightages.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



11. Click **Submit**.

Add conditional criterion to the risk calculator

Use custom conditions to the risk rule for risk score calculation.

Before you begin

Role required: sn_vulc.admin

About this task

Assuming that your organization has multiple configuration items (CIs), of which only a few can be accessed by an external user. Users can add risk score weightages for these outward-facing CIs.

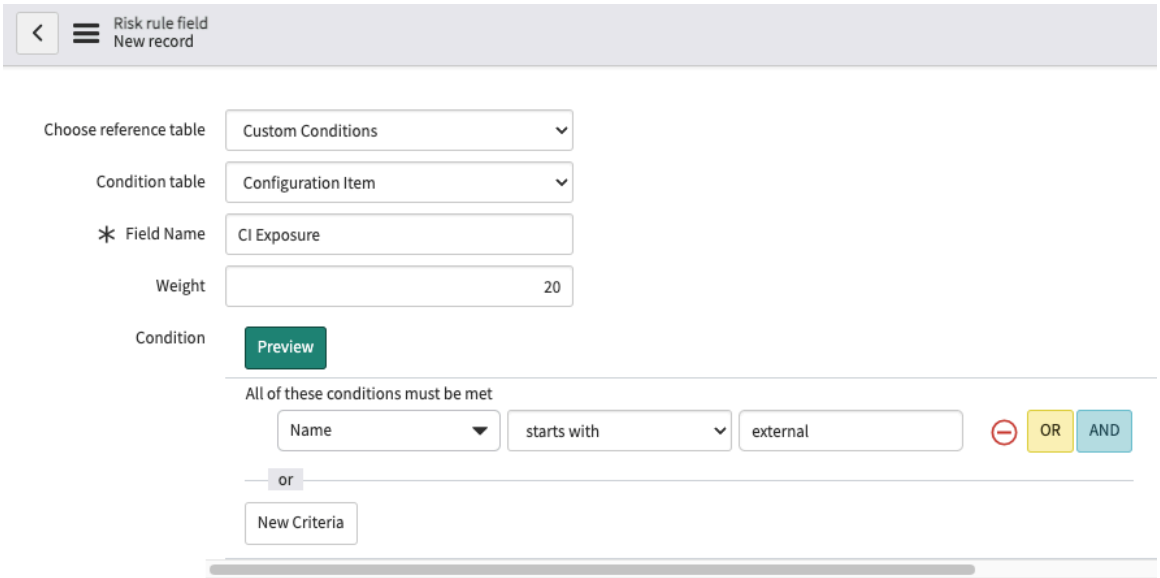
Note: You can identify these CIs by their name. The names start with 'external'.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Risk Calculators**.
2. Navigate to the Risk rule form.
3. Clear the **Active** check box, to deactivate the rule.
4. Click **Add Criteria**.
5. From the **Choose reference table** list, select **Custom Conditions**.
6. From the **Condition table** list, select **Configuration Item**.
7. In the **Field Name** field, enter `CI Exposure`.
8. In the **Weight** field, specify the relative importance of this field.
   The value must be an integer from 0 through 100.
9. In the **Condition** field, select **Name > starts with**, specify the value as `external`.

Custom conditions for new risk rule



10. Click **Submit**.

Related topics

Configuration Compliance calculator groups

Risk score calculation example for Configuration Compliance

Determine the risk score calculators to generate risk scores that use the test and asset data specific to your organization.

Example of determining risk rule calculators scores

The following example demonstrates how scores for risk rule calculators are determined. Assume that a risk rule calculator is configured with the fields in this table.

Determine risk rule calculator scores

Field	Weightage	Weight breakdown
Control.Criticality	50	Default: 0

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Determine risk rule calculator scores (continued)

Field	Weightage	Weight breakdown
		Minor: 20 Low: 30 Moderate: 50 High: 70 Critical: 100
Business_Criticality	50	Default: 0 Minor: 20 Low: 30 Moderate: 50 Hight: 70 Critical: 100

Assume that the Test Results that are shown in this table are present in the system.

Test Results mapping

ID	Business Criticality	Control Criticality
CTR0000001	1 – Most Critical	Minor
CTR0000002	1 – Most Critical	Low
CTR0000003	2 – Somewhat Critical	Minor
CTR0000004	2 – Somewhat Critical	Moderate
CTR0000005	3 – Less Critical	Low

The risk score calculation for the test result is calculated based on the formula:

Risk Score = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100 where W is the weight and FV is the weight percentage of the field value.

The resulting risk score for these test results is as described in this table:

Risk score based on Test results

ID	Business Criticality (50%)	Control Criticality (50%)	Resultant risk score
CTR0000001	1 – Most Critical (50% x100)	Minor (50% x 20)	60
CTR0000002	1 – Most Critical (50% x 100)	Low (50% x 30)	65

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk score based on Test results (continued)

ID	Business Criticality (50%)	Control Criticality (50%)	Resultant risk score
CTR0000003	2 – Somewhat Critical (50% x 70)	Minor (50% x 30)	45
CTR0000004	2 – Somewhat Critical (50% x 70)	Moderate (50% x 50)	60
CTR0000005	3 – Less Critical (50% x 50)	Low (50% x 30)	40

If the weightage percentage is changed for one of the field values, see this table for the results:

Results for changed weightage percentage

Field	Weightage	Weight breakdown
Control.Criticality	50	Default: 0 Minor: 20 Low: 30 Moderate: 60 Hight: 70 Critical: 100
Business_Criticality	50	Default: 50 1 – Most Critical: 100 2 – Somewhat Critical: 70 3 – Less Critical: 20 4 – Not Critical: 30

The risk score for the test results after reapplying the calculator is shown in this table:

Risk score for TR on reapplying calculator

ID	Business Criticality (50%)	Control Criticality (50%)	Resultant risk score
CTR0000001	1 – Most Critical (50% x 100)	Minor (50% x 20)	60
CTR0000002	1 – Most Critical (50% x 100)	Low (50% x 30)	65
CTR0000003	2 – Somewhat Critical (50% x 70)	Minor (50% x 30)	45
CTR0000004	2 – Somewhat Critical (50% x 70)	Moderate (50% x 60)	65

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk score for TR on reapplying calculator (continued)

ID	Business Criticality (50%)	Control Criticality (50%)	Resultant risk score
		*Revised value	*Revised value
CTR0000005	3 – Less Critical (50% x 20) *Revised value	Low (50% x 30)	25 *Revised value

Risk rollup calculation example for Configuration Compliance (prior to v15.0)

The following example demonstrates how scores for risk rollup calculators are determined.

For the following remediation task rollup calculator, the formula for calculating the Remediation Task Risk Score is:

(Maximum risk score/100) * 85 + (factor * 15).

The factor in the previous equation is determined by the number of test results as shown in the following table.

Test result count	Factor
<10	0.2
10-99	0.4
100-1000	0.6
1001-9999	0.8
>1000	1

For the following Remediation Task, TRG0003066, with three test results Risk scores, the maximum score is 90.

Number	Risk score	Remediation task	Result	Status
CTR000123	90	TRG0003066	Failed	Open
CTR000124	70	TRG0003066	Failed	Open
CTR000125	40	TRG0003066	Failed	Open

For the Remediation Task, TRG0003066:

The Risk Score is 79, (90/100) * 85 + 0.2 * 15 = Math.floor (76.5 +3) =79.

The historical risk score is null, because the Remediation Task is still 'Open'.

After the data ingestion, the test results are 'Passed', and the Remediation Task transitions to 'Closed' as shown in the following table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Number	Risk score(Prior to v15.0)	Remediation task	Result	Status
CTR000123	0	TRG0003066	Passed	Closed
CTR000124	0	TRG0003066	Passed	Closed
CTR000125	0	TRG0003066	Passed	Closed

Test results History is displayed in the following table.

Number	Risk score	Latest result	Result
CTRH000111	90	CTR000123	Failed
CTRH000112	70	CTR000124	Failed
CTRH000113	40	CTR000125	Failed

The Risk Score is zero, because there are no active test results in the Remediation Task.

For the Remediation Task, TRG0003066:

The Historical Risk Score is 79: (90/100) * 85 + 0.2 * 15 = Math.floor (76.5 +3) =79.

Risk rollup calculation example for Configuration Compliance (v15.0 and later)

The following example demonstrates how scores for risk rollup calculators are determined.

For the following remediation task rollup calculator, the formula for calculating the Remediation Task Risk Score is:

(Maximum risk score* 80/100) + (Average risk score* 5/100) + (Factor * 15)

Where, the weights are as follows:

- Maximum risk score: 80
- Average risk score: 5
- Factor: 15

The default weight of the Average risk score is 0. For more information on how to set the weights, see Edit risk rollup calculators for Configuration Compliance.

The factor in the previous equation is determined by the number of test results as shown in the following table.

Test result count	Factor
<10	0.2
10-99	0.4
100-1000	0.6
1001-9999	0.8
>10000	1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For the following Remediation Task, TRG0003066, with three test results Risk scores, the maximum risk score is 90 and the average risk score is 66.67.

Number	Risk score	Remediation task	Result	Status
CTR000123	90	TRG0003066	Failed	Open
CTR000124	70	TRG0003066	Failed	Open
CTR000125	40	TRG0003066	Failed	Open

For the Remediation Task, TRG0003066:

The Risk Score is 81, (90* 80/100) + (66.67* 5/100) + (0.2 * 15) = Math.floor (78.3 +3) = 81.

The historical risk score is null, because the remediation task is still 'Open'.

After the data ingestion, the test results are 'Passed', and the Remediation Task transitions to 'Closed' as shown in the following table. Starting with v15.0 of Configuration Compliance, the Risk Score of a passed test result is populated to determine the risk mitigated.

Number	Risk score	Remediation task	Result	Status
CTR000123	90	TRG0003066	Passed	Closed
CTR000124	70	TRG0003066	Passed	Closed
CTR000125	40	TRG0003066	Passed	Closed

Test results History is displayed in the following table.

Number	Risk score	Latest result	Result
CTRH000111	90	CTR000123	Failed
CTRH000112	70	CTR000124	Failed
CTRH000113	40	CTR000125	Failed

The Risk Score of the Remediation Task is zero, because there are no active test results in the Remediation Task.

For the Remediation Task, TRG0003066:

The Historical Risk Score is 81: (90* 80/100) + (66.67* 5/100) + (0.2 * 15) = Math.floor (78.3 +3) = 81.

Create or edit Configuration Compliance remediation task rules

You can create rules to automatically group test results based on filter conditions. These rules automatically group test results as they are imported. Use the filter to limit the test results grouped by this rule, such as selecting all test results with exploits.

Before you begin

Role required: sn_vulc.admin

About this task

The base system ships with one remediation task rule, **Assignment group, Test**, which groups test results by assignment group (pre-populated from **Assignment Rules**) and the test result **Test** field. This rule can be modified using filter conditions and group keys. Group keys are columns in

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

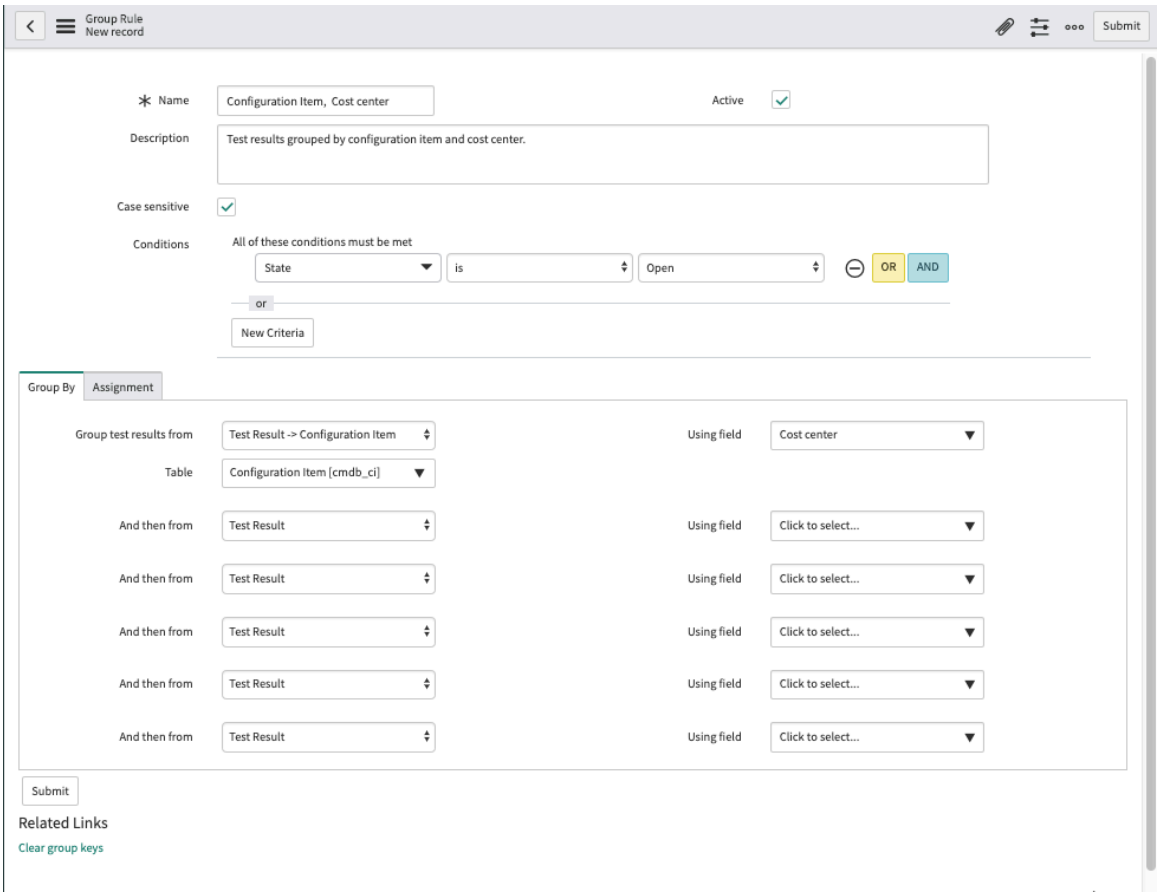
the test results table. Select up to six keys to indicate what values should be used to group the test results.

Starting with version 14.7 of Configuration Compliance, the **Assignment group, Test** remediation task rule is deactivated for new implementations.

Note: New or updated rules are automatically evaluated on the next import or manually using the **Reapply** button on the Group Rule form.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Remediation Task Rules**.
2. Open the **Assignment group, Test** rule or click **New**.



3. If **New**, fill in the fields on the form, as appropriate.

Configuration Compliance Remediation Task Rule

Field	Description
Name	Name of the group rule.
Active	Indicates whether the group is active.
Description	Text description of this remediation task rule.
Case sensitive	Determines whether the rule matching is case sensitive or not. **Note:** The default value is case insensitive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Conditions	Conditions that must be met. By default, (**Case sensitive** check box disabled), the search text you enter in the condition builder on group rules records and forms is not case-sensitive. You have the option to enable case-sensitive searches on group records and forms.
Group By	
Group test results from	Automate the creation of groups based on this rule. Choose one of the options available. ○ Test Result | Using field ○ Test Result->Configuration Item | Table | Using field If an extended **Table** field is selected, test results that don't use the corresponding extended table are grouped in a separate remediation task.
Assignment	
Assign test result groups by	Automate the assignment of groups created based on this rule. Choose one of the options available. ○ Group key When selected, a Key value field appears, available fields are listed in a drop-down menu. ○ User group When selected, a User group lookup field appears.

4. Click **Submit**.

Note: **The Clear Group By Keys** related link removes the group keys from the Group By tab on the form.

Specify the duration of an exception requested for a remediation task

Use system properties to limit the duration for which an exception is requested for a remediation task. Remediation of the remediation task is deferred for the specified period.

Before you begin
Role required: sn_vulc.admin

About this task
The `sn_vulc.exception_max_request_days` property is used to specify the maximum number of days for which an exception for a remediation task can be requested. The default value is 365 days.

Note: You can use the `sn_vulc.exception_approval_required` property to disable the exception approval work flow for the remediation task if it is not required. By default, this property is enabled and its value is `true`.

Procedure

1. Navigate to **All** > **System Properties** > **All Properties**.
2. On the System Properties page, search for `sn_vulc.exception_max_request_days`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click on the property name to open the System Property record.
4. To be able to edit this record, ensure that Configuration Compliance is selected as the current application.
5. Enter a positive **Value** and click **Update**.
   The record is updated and saved.

Configure Exception Management for Configuration Compliance

Limit the duration of an exception requested and add a questionnaire to the exception using the Configuration Compliance module. By default, an exception is requested using the ServiceNow® Vulnerability Response module. You can also request an exception using the GRC: Policy and Compliance Management integration.

Before you begin

Role required: sn_vulc.admin

About this task

If Vulnerability Response is enabled, you can limit the duration for which an exception can be requested. Similarly, if the GRC: Policy and Compliance Management module is installed, you can select GRC: Policy and Compliance Management on the configuration screen. Enabling this option lets you request an exception that specifies the Policy and Control objective from GRC.

If you add a questionnaire, it's sent to the person raising the exception or the false positive request. You can either use the default questionnaire or create one based on your requirements.

It's useful for the exception approver to understand the reason for requesting the exception.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Exception Management**.
2. On the Exception Management Configuration form, select how you want to manage an exception by selecting an option from the Manage exceptions using list.
   - Vulnerability Response

     Note: Starting from 22.0 of Vulnerability Response, you can set up questionnaire for false positive requests for the Vulnerability Response option also.

   - GRC: Policy and Compliance Management

     Note: You must activate the GRC plugin to use GRC: Policy and Compliance Management to request an exception.

   Note: Changing the configuration doesn't impact the existing data.
3. Fill the fields on the form.

Settings for CC Exception Management form

Field	Description
Duration	Period for which an exception can be requested.
Unit	Unit of time for the specified period.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Enable questionnaire to request exception	Option to add a questionnaire to the exception request being raised.
Questionnaire to request exception	Option to display the questionnaire selected by you to request an exception. The Exception Questionnaire is displayed by default.
Enable questionnaire to mark false positive	Option to add a questionnaire to the false positive request being raised.
Questionnaire to mark false positive	Option to display the questionnaire selected by you to mark as a false positive. The questionnaire for a false positive request is displayed by default.

4. Select **Save**.

Add an exception approver for Configuration Compliance

Add users to the approver groups so that you can request an exception for a remediation task in Configuration Compliance.

Before you begin
Role required: sn_vulc.admin

About this task
An exception request for a remediation task is approved using the default two-level approval workflow. Adding users to the first-level group is mandatory. If there are no users in the second level, the request is automatically approved after the first-level approval.

Note: If there's no first-level approver, an exception can't be requested.

Note: Upto Configuration Compliance v13.0, if there's no first-level approver, an exception can't be requested. However, starting from Configuration Compliance v13.0, if you are deploying the CC application for the first time, the flow designer for exception management is enabled by default. If you are already using the workflow, you can update to the flow designer. In both cases, you cannot change it back to workflow.

Procedure

1. Navigate to **All** > **System Security** > **Users and Groups** > **Groups**.
2. In the Name column, search for **Exception**, and click **Exception Approver - Level 1 CC**.

   Note: Starting from Configuration Compliance v14.7.5, you can use the system properties provided in the base system for exception approvals via workflow in the System Properties [sys_properties] table. So, when an exception request is raised via workflow, it's sent for approval to the group IDs defined in the system property. Navigate to **All** > **System Properties** and select *sn_vulc.exception_approver_L1_CC* or *sn_vulc.exception_approver_L2_CC* to change the property value.

3. On the Group Exception Approver - Level 1 CC form, navigate to **Group Members** > **New** (or **Edit**).
4. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User form

Field	Description
User ID	Unique identifier for the user.
First name	User's first name.
Last name	User's last name.
Title	User's job title. Enter a title or job description, or select one from the list.
Department	User's department.
Password	Password assigned to the user. This password can be permanent or temporary.
Password needs reset	Option to enable the user to reset the password to ensure security.
Locked out	Option to lock the user out of the instance and terminate all the user's active sessions. The system prevents users with the admin role from locking themselves out.
Active	Option to make this user active. Only you can see an inactive user in these areas: ○ Lists of users ○ Selection list on reference fields (magnifying glass icon) ○ Auto-complete list that appears when you type into a reference field
Web service access only	Option to designate this user as a non-interactive user.
Internal Integration User	Option to designate this user as an internal integration user.
Email	User's email address.
Language	User's preferred language.
Calendar integration	Calendar used to manage the work schedule. For example, Outlook.
Time zone	Time zone for this user's location.
Date format	User's preferred format for dates.
Business phone	User's business phone.
Mobile phone	User's mobile phone.
Photo	Photo that you can upload by clicking on **Click to add...**.

5. Click **Submit**.
6. **Optional:** Repeat steps 1–5 to create an Exception Approver - Level 2 CC.

Note: While creating a second level approver, select **Exception Approver - Level 2 CC**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. **Optional:** If you select **Edit**, move users from the **Collection** to the **Group Members** panel and click **Save**.
   The approver must navigate to **All** > **Configuration Compliance** > **My Approvals** and approve requests.

Create a Configuration Compliance criticality map

Configuration Compliance criticality mapping provides a transform map for third-party source criticality fields to recognizable fields in Configuration Compliance severity.

Before you begin

Role required: sn_vulc.admin

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Criticality Mapping**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field mapping

Field	Description
Source	The name of the source for the criticality mapping.
Source value	The source criticality value.
Target value	The target value. Choices are: **Critical** The configuration issue associated with the control is causing a disruption to one or more business-critical CIs. **High** The configuration issue associated with the control is a threat, but is not causing a shutdown of critical network resources. **Moderate** The configuration issue associated with the control is a risk, but is not an immediate threat. **Low** The configuration issue associated with the control is a low-level threat and can be ignored in favor of CIs that are at greater risk. **Minor** The configuration issue associated with the control is a minor risk and can be ignored if necessary.

4. Click **Submit**.

Create email notifications

Vulnerability administrators can edit the notification or add new ones, specifying when to send the notification, who receives the notification, and what content is in the notification.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vulc.admin

About this task
You can create email templates for different types of email notifications. For more on how to create email templates, see Define Vulnerability Response email templates.

Procedure
1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Notifications**.
2. Select the remediation target notification record or select **New**.
3. Fill in the fields on the form, as appropriate.
   For more information on the form fields, see Create an email notification.
4. Select **Preview Notification** to view the message.

Result
Starting from v14.11 of Configuration Compliance, when a recipient clicks the links in an email notification, the records open in the Vulnerability Manager Workspace or IT Remediation Workspace based on their role.

- Links open in the Vulnerability Manager Workspace for the users with the sn_vulc.admin role.
- Links open in the IT Remediation Workspace for the users with the sn_vulc.remediation_owner role.

If the recipient doesn't have any of the preceding roles, the links in an email notification open in the classic UI.

Configure approval rules for Exception Management in Configuration Compliance

Use the flow designer to approve exception requests for exception management and exception rules. If you are deploying Configuration Compliance for the first time, the flow designer is activated by default.

Before you begin
Role required: sn_vulc.admin

About this task
The value of the system property *sn_vulc.flow_designer_activation* is set to true. This means that the flow designer is enabled by default.

If were using Configuration Compliance prior to v13.0, the value of this system property was set to false.

Note: You cannot revert to using the workflow after activating the flow designer. For a detailed comparison between the workflow and flow designer, see Exception management workflow versus flow designer in Configuration Compliance.

To use the flow designer, create rules using the Approval Rules module. Using this module, you can configure approval rules for each of the following exception management workflows.

- Exception approval rules for test result groups
- Approval rule for auto-exception rules

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can also define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow. For information on configuring approval levels, see Create approval levels for Exception Management in Configuration Compliance.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Approval Rules** > **Exception approval rules for test result group**.
2. On the Approval Rules page, select the group for which you want to set the approval rule.
3. On the form, fill in the fields.

Approval Rule form

Field	Description
Name	Approval configuration name.
Table	Table on which the rule is applied.
Application	Default value is Configuration Compliance.
Rule type	Specifies the rule type. For example, exception management, or exception rule.
Active	Enabled by default, signifying that the approval rule is in use.
Description	Short description of the approval rules.
Approval expiry (days)	Date until when the approver can approve the request.
Notify approver (days)	Date after which the approver is notified to take action.

4. Select **Update**.
   In the Approval Configurations tab, there are two levels of approvers set up by default. You can select a rule to define the conditions based on different use cases within a rule. For more information, see Create configurations for an approval rule in Configuration Compliance .

Note: In each configuration page, you can create multiple approval levels. For more information, see Create approval levels for Exception Management in Configuration Compliance .

Example:

Based on different use cases, you can define different approval processes for the same test results found on different remediation tasks.

Create configurations for an approval rule in Configuration Compliance

Define the conditions to filter out matching remediation tasks for an approval level.

Before you begin

Role required: sn_vulc.admin

About this task

In the Approval Configurations module, you can configure multiple levels of approval for different configurations. Define condition-based rules, with each rule containing multiple levels of approval.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Use the Approval rules module to configure approval rules for the exception management workflows. For information on configuring approval rules, see Create approval levels for Exception Management in Configuration Compliance.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Approval Rules**.
2. Select an approval rule and navigate to the **Approval Configurations** tab.
3. Select a configuration.
4. On the form, fill in the fields.

Approval Configuration form

Field	Description
Name	Approval configuration name.
Approval rule	Contains the table and type details for the approval rule.
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 is run before a configuration with an order entry of 200.
Active	Enabled by default, signifying that the approval configuration is in use.
Description	Short description of the approval configuration levels.

5. Set a condition for the test results or remediation tasks in one of the following ways:

Field	Description
Condition	Identifies the matching test results or remediation tasks.
Advanced condition	Script that defines the condition for the test results or remediation tasks. **Note:** This field appears when you select the **Advanced** check box.

6. Select **Update**.
   You can define conditions containing multiple levels of approval within a rule. The flow designer automatically inherits the rules created in this module and processes the matching approval workflow. For information on configuring approval levels, see Create approval levels for Exception Management in Configuration Compliance.

Example:
You can define different approval paths for different types of remediation tasks.

Create approval levels for Exception Management in Configuration Compliance

Define the levels of users and user groups that are going to approve the exception requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_vulc.admin

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Approval Rules**.
2. Select an approval rule and navigate to the **Approval Configurations** tab.
3. Select a configuration.
4. In the **Approver Levels** section, select an approver level.
5. On the form, fill in the fields.

Approver Level form

Field	Description
Name	Approval level name.
Required approval	Select how many approvals are required for the selected level: ○ One approver required ○ All users must approve
Active	Enabled by default, signifying that the approval level is in use.
Order	Execution order of various configurations within a rule. For example, a configuration with an order entry of 100 runs before a configuration with an order entry of 200.
Approval rule	Contains the table and type details for the approval rule. This field is read-only.
Approval configuration	Contains the approval configurations. This field is read-only.
Assign using	Select an option from: ○ User and user group ○ Approval table field ○ Script
Groups	Approver level group consisting of multiple users. The user must have one of the following roles for exception management and exception rules: ○ sn_vulc.exception_approver ○ sn_vulc.read ○ sn_vulc.read_auto_exception_rule
Users	Edit the users listed in the groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To save the changes, select **Update**.

> **Note:** Prior to v13.0, the workflow process is functional if there are users only in Exception level 1. However, starting from v13.0, there must be at least one user in each level.
>
> Prior to v13.0, in the workflow, if there was no user in the second level, the remediation task was deferred. However, v13.0 onwards, if there is no user in the second level, the approval request is automatically rejected.

Example:
There can be different approval levels for remediation tasks for Linux and Windows servers.

Exception management workflow versus flow designer in Configuration Compliance

Starting with Configuration Compliance (CC) v13.0, if you are deploying CC for the first time, the flow designer for approving exception requests in exception management is enabled by default. If you are an existing CC user, the default option is workflow.

Workflow versus flow designer

Considerations	Workflow	Flow designer
Version	Prior to v13.0 of CC.	Starting from v13.0 of CC.
Default option	Default option if you are an existing CC user.	Default option for new CC users starting from v13.0.
Setting the approval process	Exception management includes exception requests along with exception rules.	Includes defining various levels and adding different approvers for different use cases. Easier to implement than the workflow. Exception management includes exception requests along with exception rules.
Upgrading to flow designer	You can upgrade to flow designer from workflow. However, existing requests can only be approved using the workflow.	Flow designer is enabled by default.
System property *sn_vulc.flow_designer_activation*	If you have been using the workflow for exception management prior to v13.0, the system property is set to false. To activate the flow designer, set this property to true. **Note:** You cannot revert to using the workflow after activating the flow designer.	If you are using CC for the first time for v13.0 or later, the system property value is set to true by default.
Approval rules module	After setting the system property to true, the **Enable module approval rules**	If you have deployed CC for the first time from CC v13.0,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Workflow versus flow designer (continued)

Considerations	Workflow	Flow designer
	scheduled job runs within 24 hours. This scheduled job enables the **Approval rules** module. To activate this module instantly, run this job manually.	this module is available by default.
Approval levels	Provides the option to set only two levels of approvers.	Provides multiple options such as setting any number of configurations, approver levels, and dynamically adding approvers for each rule.

Configuration Compliance integrations

Third-party integrations import configuration assessment findings, policies, tests, technologies, authoritative sources, test results along with other vulnerability data into the Configuration Compliance application.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

The Configuration Compliance application supports the following third-party integrations:

- Starting with v14.11, drive remediation for security gaps in your enterprise assets identified by the Security Posture Control application by publishing findings as test results in the Configuration Compliance application. The Security Posture Control application and its supported applications are available with separate subscriptions from the ServiceNow® Store. See Security Posture Control for more information.
- Microsoft Defender for Cloud Integration for Security Operations
- Palo Alto Prisma Cloud Vulnerability Integration
- Qualys integration with Configuration Compliance
- The Tenable.io product of the Tenable Vulnerability Integration

Additional notes for integrations

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

error. To avoid this miscommunication, starting from version 14.8.5 of Configuration Compliance, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Microsoft Defender for Cloud Integration for Security Operations

The Microsoft Defender for Cloud Integration product is an infrastructure security management system that enhances the security posture of your cloud environments.

Microsoft Defender for Cloud Integration for Security Operations integrates with the Configuration Compliance application to map tests to configuration items (CIs) to create test results. It continuously discovers new cloud resources deployed across workloads and determines whether they are configured according to security standards such as the Center for Internet Security (CIS).

Starting with version 2.2, Microsoft Azure Security Center is renamed to Microsoft Defender for Cloud Integration for Security Operations.

Available versions

Application	Version
Microsoft Defender for Cloud Integration for Security Operations	2.3
Configuration Compliance	14.3
Security Support Common	13.2
Vulnerability Response	16.2

Multiple deployments of the Microsoft Defender for Cloud Platform

If you have multiple deployments of the Microsoft Defender for Cloud Platform application, you can add an integration for each deployment. Resources that are identified by multiple third-party deployments, are consolidated and reconciled with your Configuration Management Database (CMDB). This consolidation takes place even when scan processes overlap between the multiple deployments.

ServiceNow Microsoft Defender for Cloud Integrations

The Microsoft Defender for Cloud Integration for Security Operations enriches the compliance data on your instance by retrieving data from Microsoft Defender for Cloud. A series of scheduled jobs invokes the integrations automatically. You can also run these scheduled jobs manually. Scheduled jobs simplify the test results remediation life cycle by keeping the instance synchronized with Microsoft Defender for Cloud.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

There is a configured run-as user for each integration record, with the default value **VR.System**. This value must remain the same.

Note: If you do not set a valid run-as user, duplicate or multiple data retrieval attachments are created for the data source records. The number of attachments increases each time the integration is run. This increases the processing time, resulting in inconsistent transform results.

Microsoft Defender for Cloud Platform integration tasks involve the following roles.

- sn_vul_asc.configure_integration: Ability to read, write, and delete records.
- sn_vul_asc.read_integration: Ability to read records.

Viewing the Microsoft Defender for Cloud Integrations

View the integrations by navigating to **All** > **Microsoft Defender for Cloud Integration** > **Integrations**.

The following integrations are included in the base system.

Integration	Description
Policy Definition Integration	Retrieves policies and creates policy entries in your instance.
Assessment Metadata Integration	Retrieves assessment metadata and creates tests in your instance.
Compliance Standards & Controls Integration	Retrieves standards and controls and creates the authorization source and citations. It then links them to the tests created.
Assessment Integration	Retrieves assessments and processes them in your instance. The output of this integration is test results.

Create CIs using the Identification and Reconciliation Engine

Use the Identification and Reconciliation Engine (IRE) to create CIs, when an existing CI cannot be matched with a host imported from a third-party scanner.

If a CI is not matched in the CMDB, a CI is created in the *cmdb_ci_cmp_resource* class. Later, when a discovery finds the same CI, it enriches the CI or creates another one.

Note: Automatic reconciliation does not happen for cloud resources.

Install and configure Microsoft Defender for Cloud Integration for Security Operations

Install and configure the Microsoft Defender for Cloud Integration for Security Operations, so that you can use the data that is imported from Microsoft Defender for Cloud to prioritize and remediate any misconfigurations on your assets.

Before you begin

Create a new app registration on Azure Active Directory for the Microsoft Defender for Cloud Integration. For more information on how to register a new application on Azure Active Directory, see the Microsoft product documentation site. For more information on Azure roles, see Azure roles.

Role required: sn_vulc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Definition** > **Plugins**.
2. In the search bar, search for `Microsoft Defender for Cloud Integration for Security Operations`.
3. Select **Install**.

   Any dependencies that will be installed are displayed.
4. Navigate to **All** > **Microsoft Defender for Cloud Integration** > **Administration** > **Configuration** > **Microsoft Defender for Cloud Configuration**.
5. On the form, fill in the fields.

Microsoft Defender for Cloud Configuration form

Field	Description
API URL	Resource URL of the instance. Example: https://management.azure.com (Azure public cloud)
Tenant ID	Tenant identity of your organization.
Integration instance	Default instance. You can also create an instance for bringing the data from multiple Microsoft Defender tenants or subscriptions.
Client ID	Client identity that is generated after the Microsoft Defender for Cloud Integration application is registered.
Client secret	Client secret that is generated after the Microsoft Defender for Cloud Integration application is registered.
Import Findings from	Resources and assessments that correspond to the selected management group IDs and subscription IDs that are to be retrieved.
Management Group IDs	Resources and assessments that correspond to the management Group IDs that are to be retrieved. **Note:** This field appears only when you select **Specific Management Groups** from the **Import Findings from** field.
Subscription IDs	Identification numbers of the subscriptions for which the resources and assessments are to be retrieved. **Note:** This field appears only when you select **Specific Subscriptions** from the **Import Findings from** field.
Validation status	Whether the credentials and subscription ID that are provided are valid.

6. Configure or run the integrations by selecting **Save and test**.

Configuration Compliance imported data for Microsoft Defender for Cloud Integration

Configuration Compliance imports policies, tests, authoritative sources, and test results from third-party integrations and stores them in modules for viewing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Test groups

A group of configuration tests constitutes a test group. Test groups are related to authoritative documents and test records, and they can be modified to meet the needs of your organization. One configuration test can belong to multiple test groups.

If the Microsoft Defender for Cloud Integration is installed, test groups are retrieved and populated by the scheduled job, **Policy Definitions Integration**. You can view the scheduled job by navigating to **All** > **Microsoft Defender for Cloud Integration** > **Administration** > **Integrations** > **Policy Definitions Integration**.

Note: If you choose to run the integration manually, run the **Policy Definitions Integration** first.

Tests

Tests are libraries of data records that organize scans of computing assets. Configuration tests define how assets must be governed.

A Configuration Compliance test is the mechanism third-party integration applications use to group assets by test results type.

If the Microsoft Defender for Cloud Integration is installed, the scheduled job, **Assessment Metadata Integration**, retrieves the tests. You can view the scheduled job by navigating to **Integration** > **Primary Integrations** > **Assessment Metadata Integration**.

Note: If you choose to run the integration manually, run the **Assessment Metadata Integration** after the **Policy Definitions Integration**.

Starting with v15.0 of Configuration Compliance, the test group to which a test belongs to populates in the **Test Groups** column of the Tests list.

Authoritative sources

Configuration Compliance uses authoritative sources and citations when generating vulnerability alerts for tests. Authoritative sources usually map to sections of published industry standards, such as **ISO 27001** and **PCI DSS 3.2.1**.

These source records contain references to information about known software and hardware configuration issues from experts in the field of computer security. They define requirements for security policies and procedures.

If the Microsoft Defender for Cloud Integration is installed, the scheduled job, **Compliance Standards & Controls**, retrieves the authoritative sources and citations. You can view this

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

scheduled job by navigating to **All** > **Microsoft Defender for Cloud Integration** > **Integrations** > **Compliance Standards & Controls Integration**.

Note: If you choose to run the integration manually, run the **Compliance Standards & Controls Integration** after the **Assessment Metadata Integration**.

Assets

The **Assessment integration** provides vital information such as resource tags and cloud attributes. This information is displayed in the Discovered Item form. #It is used primarily for filtering in#Configuration Compliance Assignment and Remediation Task Rules.

- Resource tags: All cloud resource tags are imported as host tags as part of the#**Assessment integration**. The cloud tags for any cloud resource type are stored here, whether the resource is a host or not.
  - Tag storage is not case-sensitive. If a#Tokyo#tag is created, then a#**TOKYO**# tag cannot be stored in the Host tag table. **Tokyo** and **TOKYO** are considered to be the same host tag. Whichever tag was imported first wins.
  - Using host tags as a group key in a remediation task rule can have unexpected results. Host tags are intended for use only in the condition builder.
- Cloud attributes for assets: Following are the cloud attributes that the integrations retrieve from Microsoft Defender for Cloud:
  - Cloud Account
  - Cloud Region
  - Cloud Resource Type
  - Cloud Service Provider

Test results

Configuration Compliance does not calculate the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using **Remediation Tasks**.

If the Microsoft Defender for Cloud integration is installed, the scheduled job, **Assessment Integration**, retrieves the test results. You can view this scheduled job by navigating to **All** > **Microsoft Defender for Cloud Integration** > **Integrations** > **Assessment Integration**.

The **Assessment Integration** import is the only integration that uses the *`Start Time`* parameter in the **Integration Details** tab. All other Configuration Compliance imports bring in all available data regardless of *`Start Time`*.

When the **Assessment Integration** import is complete, an event is started to trigger end-of-import calculations.

The **Assessment Integration** pulls the data assessments only if there is a status change from the last successful integration run for the last one day by default. So, if the assessment fails continuously for the past few days, the integration will not fetch the assessment as there is no status change for the assessment. To keep the test results up to date with the defender assessments, a new **Comprehensive Assessment Integration** is added which pulls the data from the past seven days. It runs weekly and pulls all the test results, which are not passed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CI lookup rules for identifying CIs from Microsoft Defender for Cloud integrations

When data is imported from a third-party integration, Configuration Compliance automatically uses resource data to search for matches in the Configuration Management Database (CMDB), using CI Lookup Rules. These rules are used to identify the configuration items (CIs) and add them to the test result record to aid in remediation. Base system CI lookup rules are available for Resource ID, Name, and S3 Bucket. For more information on CI lookup rules, see CI lockup rules for Microsoft Defender for Cloud Integration for Security Operations.

Understanding the Vulnerability Response Integration with Palo Alto Prisma Cloud

Prisma Cloud is an API-based cloud infrastructure security solution. It connects to your cloud environment and monitors the resources deployed on the public cloud environments, such as Amazon Web Services (AWS), Microsoft Azure, and so on. You get complete visibility and control over risks within your public cloud infrastructure.

The Vulnerability Response Integration with Palo Alto Prisma Cloud application facilitates ingestion of policies and alerts from Prisma Cloud, as tests and test results respectively, in the Configuration Compliance application. With the right configuration, the test results can be managed seamlessly by assigning appropriate risk scores, and grouping and assigning them to relevant users and groups.

Available versions

The table lists the applications that Vulnerability Response Integration with Palo Alto Prisma Cloud depends on, along with the version of the application.

Application	Version
Prisma Cloud integration for Security Operations	2.3
Configuration Compliance	14.7
Security Support Common	13.5
Vulnerability Response	18.0

ServiceNow Prisma Cloud Integrations

The Vulnerability Response Integration with Palo Alto Prisma Cloud application helps import the Prisma data to your ServiceNow instance to enrich your instance for better management. A series of scheduled jobs invoke the integrations automatically. You can also run these scheduled jobs manually. Scheduled jobs simplify the test results remediation life cycle by keeping the instance updated by retrieving data periodically from Prisma Cloud.

Prisma Cloud integration tasks involve the following roles.

- sn_vul_prismacloud.configure_integration: Ability to read, write, and delete records.
- sn_vul_prismacloud.read_integration: Ability to read records.

Viewing the integrations

You can view the integrations that are part of the Vulnerability Response Integration with Palo Alto Prisma Cloud by navigating to **Prisma Cloud Integration** > **Integrations**.

The following integrations are available in the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run Sequence	Schedule	Integration	Description
1	Weekly	Prisma Policy Integration	• Retrieves policies from Prisma Cloud and creates test entries in your instance. • It does not provide incremental support. If you run the integration for the last 10 days, it shows the result for previous integration runs as well.
2	Daily	Prisma Alerts Integration	• Retrieves alerts from Prisma Cloud and creates test results entries in your instance. • Provides incremental support. The integration runs daily after the last integration run time.

Preparing for installing the Vulnerability Response Integration with Palo Alto Prisma Cloud

Prepare for installing the Vulnerability Response Integration with Palo Alto Prisma Cloud by performing setup tasks.

Before you begin

To integrate Vulnerability Response with Palo Alto Prisma Cloud, you must be assigned a permission group in Prisma that provides read-only access to Policy and Alerts data. You can find more information on permission groups at Prisma Cloud Administrator Roles.

For detailed information on the roles assigned to different permission groups, refer to the page Prisma Cloud Administrator Permissions.

In addition, access keys must be created to enable reading the alerts. For more information on creating access keys, see Create and Manage Access Keys.

To install and configure the Vulnerability Response Integration with Palo Alto Prisma Cloud, use the following checklist. Before you install the application, verify that the items listed are completed.

Integration preparation checklist

Task	Description
☐	Verify that you have the following sets of information: • API base URL • Access key ID • Secret key • Username and Password for accessing Prisma Cloud. These credentials are used to connect to the Prisma Cloud instance from the ServiceNow AI Platform® instance. The access key ID and secret key must be generated from the Prisma Cloud portal after registration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration preparation checklist (continued)

Task	Description
☐	If not already installed and activated, install the Vulnerability Response application before you install the Vulnerability Response Integration with Palo Alto Prisma Cloud application. For more information about installing and activating the Vulnerability Response application, see Install Vulnerability Response. This integration requires version 15.2.0 of Vulnerability Response or later.
☐	If you don't already have the application on your instance, get entitlements and download the Vulnerability Response Integration with Palo Alto Prisma Cloud application to your ServiceNow AI Platform® instance. See .
☐	Ensure you have installed the following plugins for a smooth integration run: • Vulnerability Response • Configuration Compliance • Vulnerability Response Integration with Palo Alto Prisma Cloud The following plugins are optional but can be useful: • Cloud Provisioning and Governance • Discovery and Service Mapping Patterns
☐	Estimate the number of test results that you expect to import. Verify that your instance can accept the number of test results that you expect to import. An undersized instance can lead to long load times. If you don't know the size of your instance, or if you need assistance, contact ServiceNow Technical Support.
☐	Verify that you have an administrator to manage the integrations and to remediate the test results: The admin installs the Vulnerability Response Integration with Palo Alto Prisma Cloud application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles.

You are ready to Install and configure the Vulnerability Response Integration with Palo Alto Prisma Cloud application.

Install and configure the Vulnerability Response Integration with Palo Alto Prisma Cloud application

Install the Vulnerability Response Integration with Palo Alto Prisma Cloud application to use the imported data from Prisma Cloud. Use this data to prioritize and remediate misconfigurations on your assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

Procedure

1. Navigate to **System Definition** > **Plugins**.
2. In the search bar, search for `Vulnerability Response Integration with Palo Alto Prisma Cloud`.
3. Click **Install**.

   Any dependencies that will be installed are displayed.
4. Navigate to **All** > **Prisma Cloud Integration** > **Administration** > **Configuration** > **Prisma Cloud Configuration**.
5. On the form, fill in the fields.

Field	Description
Integration Instance	Name of the new integration instance. You can create an instance or click the lookup icon to select an existing instance.
API URL	URL to integrate with the Prisma Cloud.
Access key ID	Unique key to authenticate the access request to the Prisma Cloud. **Note:** You must generate the key after logging in to the Prisma Cloud portal.
Secret key	Private key to authenticate the access request to the Prisma Cloud. **Note:** You must generate the secret key after logging in to the Prisma Cloud portal.

6. Click **Save and Test**.

What to do next
After you complete the installation, navigate to **Prisma Cloud Integration** > **Configuration** to continue with the configuration.

Configure the Vulnerability Response Integration with Palo Alto Prisma Cloud application

Configure the Vulnerability Response Integration with Palo Alto Prisma Cloud application. Use the imported data from Prisma Cloud to prioritize and remediate misconfigurations on your assets.

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Prisma Cloud Integration** > **Configuration**.
2. On the form, fill in the fields.

Prisma Cloud Configuration

Field	Description
Integration Instance	Name of the new integration instance. You can create an instance or click the lookup icon to select an existing instance.
API URL	URL to integrate with Prisma Cloud.
Access key ID	A unique key to authenticate the access request to the Prisma Cloud. You must generate the key after logging in to the Prisma Cloud portal.
Secret key	A private key to authenticate the access request to the Prisma Cloud. You must generate the secret key after logging in to the Prisma Cloud portal.

3. Click **Save and Test**.

What to do next

After you complete the configuration, navigate to **Prisma Cloud Integration** > **Integrations** to verify that the integration run is successful.

Verify the Vulnerability Response Integration with Palo Alto Prisma Cloud import run status

Use the Vulnerability Response Integration with Palo Alto Prisma Cloud import run status to verify the success of your integration runs and to identify any issues.

Before you begin

Role required: admin

About this task

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 14.8.5 of Configuration Compliance, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **Prisma Cloud Integration** > **Integrations**.
2. Click **Prisma Policies Integration**.
3. Click **Execute Now**.
   When this integration is run, the following tables are populated in this order:
   a. sn_vulc_test.list (Configuration Tests)
   b. sn_vulc_auth_src (Authoritative Source
   c. sn_vulc_citation (Citations)
4. Under the **Items** tab, view the number of new tests created, updated, and ignored by clicking the vulnerability integration run.

   Note: Policies are defined in Prisma Cloud for the selected cloud instance. The instance is scanned based on the defined policies.

5. Click **Prisma Alerts Integration**.
6. Click **Execute Now**.
   The following tables are populated based on the integration:
   - Test Results
   - Discovered Items: If the configuration items are unavailable in the system, they are created. The class is always Cloud Resource. On the Discovered Item page, three new fields are created: **Cloud resource type**, **Cloud service provider**, and **Asset Category**.

     Under the **Items** tab, click the vulnerability integration run to view the number of new tests results imported, updated, and ignored. The **Configuration Items** tab also gets populated based on the number of test results created.

Data mapping

The data from Prisma Cloud is imported in the Configuration Compliance module of the ServiceNow instance.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The data from Prisma Cloud is imported with a different name in Configuration Compliance as mentioned in the table.

Mapping of Prisma Cloud data in Configuration Compliance

Prisma Cloud	Configuration Compliance
Policy	Test
Alert	Test result
Compliance standard	Authoritative source
Sections	Citation
Asset	Discovery item/ Configuration item (CI)

Tests

A policy in Prisma Cloud is imported as a test in Configuration Compliance. Policies are related to authoritative documents and test records, and they can be modified to meet the needs of your organization. You can view the tests by navigating to **Configuration Compliance** > **Tests**.

If **Vulnerability Response Integration with Palo Alto Prisma Cloud** is installed, the integration job, *`Prisma Policy Integration`* retrieves the tests. You can view this integration job by navigating to **All** > **Prisma Cloud Integrations** > **Prisma Policy Integration**.

Test Results

An alert in Prisma Cloud is imported as a test result in Configuration Compliance. Alerts are remediated using **Remediation Tasks**. You can view the test results by navigating to **Configuration Compliance** > **Test Results**.

The Configuration Compliance imports test results as part of a third-party integration. After they're viewable on the Configuration Compliance application, they are remediated using Remediation Tasks.

If **Vulnerability Response Integration with Palo Alto Prisma Cloud** is installed, the integration job **Prisma Alert Integration** retrieves the test results. You can view this integration job by navigating to **All** > **Prisma Cloud Integration** > **Integrations** > **Prisma Alert Integration**.

The **Prisma Alert Integration** is an integration job that runs daily and pulls the test results with status change after the time that is defined in the **Start Time** field in the **Integration** tab.

Note: If you run the integration job, **Prisma Alert Integration** manually, run it after you run the integration job, **Prisma Policy Integration**.

When the **Prisma Alert Integration** completes importing the data, an event is started to trigger end-of-import calculations. If the alert fails continuously for the past few days, the integration won't fetch the alerts as there's no status change for the alert. So, to keep the test results data up to date with the Prisma alerts, a new integration job, **Prisma Comprehensive alert Integration** is added which pulls the alerts that are updated in the past seven days. It runs weekly and pulls all the test results, which aren't passed.

Authoritative Sources

Configuration Compliance uses authoritative sources and citations when generating vulnerability alerts for tests. Authoritative sources usually map to sections of published industry standards, such as ISO 27001 and PCI DSS 3.2.1.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These source records contain references to information about known software and hardware configuration issues from experts in the field of computer security. The references define requirements for security policies and procedures. Navigate to **Configuration Compliance** > **Authoritative Sources** to view the authoritative sources.

Assets

If the Vulnerability Response Integration with Palo Alto Prisma Cloud is installed, the scheduled job *`Prisma Alerts Integration`* captures the alert related information in the Discovered Items module or table. You can view this scheduled job by navigating to **Prisma Cloud Integration** > **Integrations**.

The Prisma Alerts integration imports additional types of information, such as resource tags and cloud attributes that are stored in tables. This information is displayed in the Discovered items form.

- Host tags: A resource can have multiple tags. The host tags are available in key value pair format. For example, the operating system is Windows 10 and the Java version is 1.8.
- Cloud attributes for assets: The following cloud attributes are available:
  - Cloud account: Provides the account ID from the integration. The information is populated from the Cloud Accounts [sn_sec_cmn_cloud_account.LIST] table.
  - Cloud region: Provides the location where the resource has been hosted. The information is populated from the Cloud Regions [sn_sec_cmn_region.LIST] table.
  - Cloud resource type: Provides information on the type of resource such as whether it is a virtual machine or a database instance, and so on. The information is populated from the Cloud Resource Type [sn_sec_cmn_cloud_resource_type.LIST] table.
  - Cloud service provider: Provides information on the cloud service provider whether it's Amazon Web Services (AWS), Oracle Cloud, and so on. The information is populated from the Cloud Service Provider [sn_sec_cmn_cloud_service_provider.LIST] table.
  - Cloud account groups: Provides information on the account groups. The information is populated from the Cloud Account Groups [sn_vul_prismacloud_account_group.list] table.

    Note: The Cloud account groups attribute is available only for Prisma.

CI lookup rules

The base system CI lookup rules are available for Resource ID, Name, and S3 Bucket. For more information on the CI lookup rules, see CI lookup rules for Microsoft Defender for Cloud Integration for Security Operations and Palo Alto Prisma Cloud.

Prisma Cloud REST Messages

Prisma REST messages are used to make calls to the Prisma Application Programming Interface (API) to fetch the compliance data.

The following REST messages are shipped with the base system.

Prisma Cloud integrations

All Prisma Cloud integrations use the JSON Web Token (JWT) for authentication and authorization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prisma Login REST message

Endpoint	Description	Method	Body	API documentation link
/login	Obtains the JWT token for use in all subsequent integrations.	*POST*	`{ "username": <<access key id >>, "password": <<secret access key>>}`	https://pan.dev/prisma-cloud/api/cspm/app-login/

Prisma Refresh Token REST message

Endpoint	Description	Method	Body	API documentation link
/auth_token/extend	Automatically renews the JWT token on expiration. The default duration for token expiry is 60 minutes.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Prisma Policy REST message

Endpoint	Description	Method	Body	API documentation link
/v2/policy	Retrieves all the policy data from Prisma.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Prisma Alert REST Message

Endpoint	Description	Method	Body	API documentation link
/v2/alert	Retrieves all alerts from Prisma.	*POST*	`{ "detailed": "false", "filters": [ { "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" } ], "sortBy": [ "resource.id" ], "pageToken": "", "offset": 0, "limit": 2000, "timeRange": { "type": "absolute",`	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prisma Alert REST Message (continued)

Endpoint	Description	Method	Body	API documentation link
			"value": { "startTime": <<Import since at integration level>>, "endTime": <<Current integration run time>> } } }	

For Prisma Comprehension Alert integration, the filters in the above POST body must be replaced as follows:

```
"filters": [
 {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "open"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "dismissed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "snoozed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "pending_resolution"
                },
                {
                    "name": "timeRange.type",
                    "operator": "=",
                    "value": "ALERT_UPDATED"
                }

    ],
```

Qualys integration with Configuration Compliance

The Qualys Policy Compliance collects the data and automatically sends it to the Qualys application, which continuously analyzes and correlates the information. It easily integrates as the Qualys Integration for Security Operations to map configuration findings to CIs and business services to determine the impact and priority of potential misconfigurations.

If you have multiple deployments of the Qualys Cloud Platform application, you can add an integration for each deployment. Assets, identified by multiple third-party deployments and their

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

vulnerabilities, are consolidated and reconciled with your CMDB. This consolidation happens even when scan processes overlap between the multiple deployments. Data sourced from each deployment is identified and available in a single instance of Vulnerability Response.

Note: You cannot delete the original vulnerability integration, but you can disable it. Integrations created from inactive templates are disabled by default.

Host tags

All host tags are imported as part of the Qualys Host List integration. Host tags are used primarily for filtering in Vulnerability Response Assignment and Vulnerability Group Rules. They are displayed in the Discovered Item form.

Note: The Qualys Host List integration should be run prior to creating the Assignment or Remediation Task Rules in Vulnerability Response so that all tags can be present in the rules and before vulnerable items are imported and grouped.

- Tag storage is not case-sensitive. If a **San Diego** tag is created, then a **SAN DIEGO** tag cannot be stored in the Host tag table. “San Diego” and “SAN DIEGO” are considered to be the same host tag. Whichever tag was imported first wins.
- Using host tags as a Group Key in a Remediation Task Rule can have unexpected results. Host tags are intended for use only in the condition builder.
- Host tags are controlled by the global system property **sn_vul.import_host_tags**. This property is set to true by default. Turning off tags turns them off across all instances.

Host tags (also called asset tags) are used for organizing and tracking the assets in your organization. You can assign tags to your host assets. Then, when launching scans, you can select tags associated with the hosts you want to scan. The Host Tags module enables you to download host tag data from Qualys to your instance on a scheduled basis.

Associating a Test with its Test Group

To populate the Test group field on a Test form, enable the *sn_vulc.add_policy_as_key* system property. For more information on how a test is associated to its test group, impact of enabling this system property and post-requisites, see KB1644268 article.

Warning: You cannot disable the *sn_vulc.add_policy_as_key* system property once it is enabled. So, review the Impact section in the KB1644268 article before you enable this system property.

When you enable this system property, after the next ingestion, the **Test group** field is added on the Test table and it populates the test group to which a test belongs to. Therefore, you can easily:

- identify the Test Group to which a Test Result belongs to by dot-walking from Test to Test Group.
- differentiate Test records with same Test id that are associated with different Test Groups.

Integrating Qualys with the ServiceNow® Configuration Compliance application

Ignore passed test results

Starting with v15.2.5 of Configuration Compliance, the ignore_passed_result integration instance parameter for the Qualys Integration for Security Operations has been added.This parameter is set to `false` by default so that passed test results imported by Qualys are not ignored.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Set the parameter to `true` to ignore passed test results on import.
- If activated, this parameter does not impact the closure of the test results.

  For example, if you activate the parameter, and a failed test result from a previous import has since passed, it will be closed correctly.

API credentials

If the Qualys Vulnerability Integration is already installed on your system, and your API credentials are different than the ones you want to use for Configuration Compliance, go into Setup Assistant (in Vulnerability Response) and assign them to each **Qualys PC** integration.

Navigate to **All** > **Qualys Vulnerability Integration** > **Primary Integrations** and edit the **Qualys API Credentials** field under the **Qualys REST Details** tab.

Configure the PCRS parameters

Starting with v12.6.3 of Qualys Integration for Security Operations, you can use the Qualys PCRS Policy Host Integration and Qualys PCRS Test Results Integration for importing test results with new sets of Qualys APIs. These integrations need a gateway URL to fetch information from Qualys.

Before you begin

Role required: admin

About this task

When you install the Qualys Integration for Security Operations for Vulnerability Response, you can configure the **gateway_url** and **posture_api_version parameters**for the new PCRS integrations in Configuration Compliance. For more information on how to find the gateway URL for your API URL, see Identify your Qualys platform.

The gateway URL must be added in your ServiceNow instance.

Note: Starting with v12.21.0 Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, you can configure the `posture_api_version` integration instance parameter to select the API version for PCRS integrations.

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Integration Instances**.

   Note: Ensure that the scope you are in is Qualys for Security Operations.

2. Open the instance that is used by the PCRS integrations.
3. On the Integration Instance Parameters tab, add the gateway url for **gateway_url** configuration.

   Note: The Qualys PCRS Test Results Integration is dependent on the Qualys PCRS Policy Host Integration. So, if you backdate the integration Qualys PCRS Test Results, you might have to run them in the same order again.

4. **Optional:** On the Integration Instance Parameters tab, locate the **posture_api_version** parameter and set the value to 2.0 or 5.0 as required.

Components installed with the Qualys Integration for Security Operations

The following roles, scheduled jobs, and tables are installed with the Qualys Integration for Security Operations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

View filtered lists for components installed with an application

Filter the Applications Files table so that only the roles, scheduled jobs, and tables that are installed with an application are displayed. The application you want to view these components for should be installed so that its files are loaded onto the instance and into the metadata table. Follow these steps to view filtered lists from the Applications Files table.

1. In the filter navigator, enter **sys_metadata.list** to navigate to the metadata table.
2. Select the condition builder (filter icon), and select, **Application** > **is** followed by the name of your application. For example, **Application** > **is** > **Vulnerability Response**.
3. In the condition builder, to add a second filter, select **AND**, then select, **Class** > **is a** and choose one of the following classes from the list: **Role**, **Scheduled job**, or **Table**.
4. Select **Run**.

The results for the class you selected are displayed in a filtered list.

Roles installed

Role title [name]	Description	Contains roles
sn_vul_qualys.read	Has read access to the Qualys Vulnerability Integration records.	
sn_vul_qualys.user	User for Qualys Vulnerability Integration. Can read and write records	sn_vul_qualys.read
sn_vul_qualys.admin	Administrator forQualys Vulnerability Integration. For example, you can modify integration start dates and perform some advanced configuration settings.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Can configure the Qualys Vulnerability Integration	sn_vul_qualys.admin

Scheduled jobs installed

Scheduled job	Description
Qualys PC Policies	Retrieves Policies from Qualys. The output is stored in the sn_vulc_policy table. The API used in this integration does not support pagination, so all policies are downloaded on a single page.
Qualys PC Policies Detail	Retrieves the complete policy details, such as technologies and sections, for example.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
Qualys PC Controls	Retrieves compliance controls information for different control IDs from Qualys.
Qualys PC Results	Retrieves compliance posture records from Qualys. The output of this integration is Test Results. By default, the parameter details are passed to import host information, last scan dates/times, control ID, and evidence information.
Qualys PC Comprehensive Results	Retrieves compliance posture records from Qualys based on the last evaluation date for the test results that are not passed. This job runs once a week. The output of this integration is test results. By default, the parameter details are passed to import the host information, last scan dates/times, control ID, and evidence information.
Qualys PCRS Policy Host Integration	Retrieves host data from Qualys and processes it in your instance. When `posture_api_version` is set to 5.0, this integration uses the Start Time value as the StatusChangedSince parameter while fetching data. The output of this integration is policy host IDs. The Qualys host data is imported in this integration. **Note:** • This scheduled job appears only when Configuration Compliance is installed. • Configure the gateway_url and pcrs_page_size integration instance parameters before running this integration. These two integrations will be inactive OOB. If you activate either one of these integrations, the PC Results integrations will get deactivated. These two integrations are added based on the new streaming APIs from Qualys.
Qualys PCRS Test Results Integration	Retrieves the test results for each host ID. This integration uses the Start Time parameter in the Integration Details tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
	Note: • This scheduled job appears only when Configuration Compliance is installed. • Configure the gateway_url and pcrs_page_size integration instance parameters before running this integration. • If you choose to run the integration manually, run Qualys PCRS Test Results Integration after Qualys PC Policies, Qualys PC Policies Detail and Qualys PCRS Policy Host Integration.
Qualys Comprehensive PCRS Policy Host Integration	Retrieves host data from Qualys and processes it in your instance. The output of this integration is policy host IDs. **Note:** • This scheduled job appears only when Configuration Compliance is installed. • Configure the gateway_url and pcrs_page_size integration instance parameters before running this integration. • This integration is inactive out of the box. When you set `posture_api_version` to 5.0, activate this integration if the corresponding Qualys PCRS Policy Host Integration is also active.
Qualys Comprehensive PCRS Test Results Integration	Retrieves test results for each host ID. This integration uses the Start Time parameter in the Integration Details tab. **Note:** • This scheduled job appears only when Configuration Compliance is installed. • Configure the gateway_url and pcrs_page_size integration instance parameters before running this integration. • If you run the integration manually, run Qualys PCRS Test Results Integration after Qualys PC Policies, Qualys PC Policies Detail, and Qualys PCRS Policy Host Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Qualys PCRS Policy Host and Qualys PCRS Test Results integrations are inactive by default. These two integrations are based on the new streaming APIs from Qualys. If you activate any one of these integrations, the PC Results integration will be deactivated and vice versa.

Tables installed

Table	Description
Qualys PC Result Import sn_vul_qualys_pc_result_import	Table extending the import set row. Field maps transformation is skipped and the response attachment is processed directly with the onComplete script.
Policy Host Id sn_vul_qualys_policy_host_id	Table storing the mapping between the Policy and the host for which this policy was scanned. This table is used in the new Qualys PCRS integration. **Note:** This table is appears only when Configuration Compliance is installed.
Qualys PCRS Policy Host Import sn_vul_qualys_pcrs_policy_host_import	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script. **Note:** This table appears only when Configuration Compliance is installed.
Qualys PC Policy Import sn_vul_qualys_pc_policy_import	Table extending the import set row. Field map transformation is skipped and the response attachment is processed directly with the onComplete script.

Update configuration items with the network partition identifier for the Qualys Integration

Create unique configuration items (CIs) for assets in your environment that share IP addresses. Identify the distinct assets across your environment and automatically update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.

Before you begin

Role required: admin

About this task

By default in the Vulnerability Response application, one way to identify your assets is by IP address. In certain cases, assets can share IP addresses, but they are stored as one CI in your CMDB.

For example, as shown in the following tables, multiple assets (CI)s in your environment can share IP addresses but have unique network and repository ids. However, by default, these assets are typically identified and stored as a single CI `(CI 1)` during the IP address lookup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Default IP lookup and CI creation

Source	IP address	NETWORK_ID	Configuration item
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	IP address	REPOSITORY_ID	Configuration item
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

You can create individual CIs for assets that have the same IP address so that you can identify them as distinct assets. Starting from a fresh data import, you can update your existing CIs with more granularity that includes the network partition identifier [network_partition_identifier] by running the scheduled job, *`Update existing discovered items with network partition identifier`*.

This scheduled job is deactivated by default. Activate this feature for the Assets and Fixed and Open Vulnerabilities Integrations for Qualys Vulnerability Integration in the Setup Assistant to view this identifier on your records.

When activated, this scheduled job adds the Network Partition Identifier [network_partition_identifier] to existing CI records from imported data. Existing CIs created by the IRE are also updated. The scheduled job also creates CIs that include the network partition identifier starting with the next import. Alternatively, you can launch the job on-demand to update your existing data.

Starting with v14.0 of Vulnerability Response and v12.1 of the Qualys Vulnerability Integration Vulnerability Integration, the CMDB CI Class Models (1.0.21.) is supported. The class models have the network partition identifier [network_partition_identifier] in the Identification and Reconciliation (IRE) identification rules.

Option	Description
Run the scheduled jobs on-demand.	Update your existing discovered items. CIs for your existing Qualys Vulnerability Integration data are created or updated to include the network partition identifier granularity. Discovered items, vulnerable items, and detection records are all updated with the new CIs.
Wait for imports of fresh data from the integrations with the next scheduled jobs.	Create CIs for each new asset using the network partition identifier starting with the next scheduled job. CI, vulnerable item, and

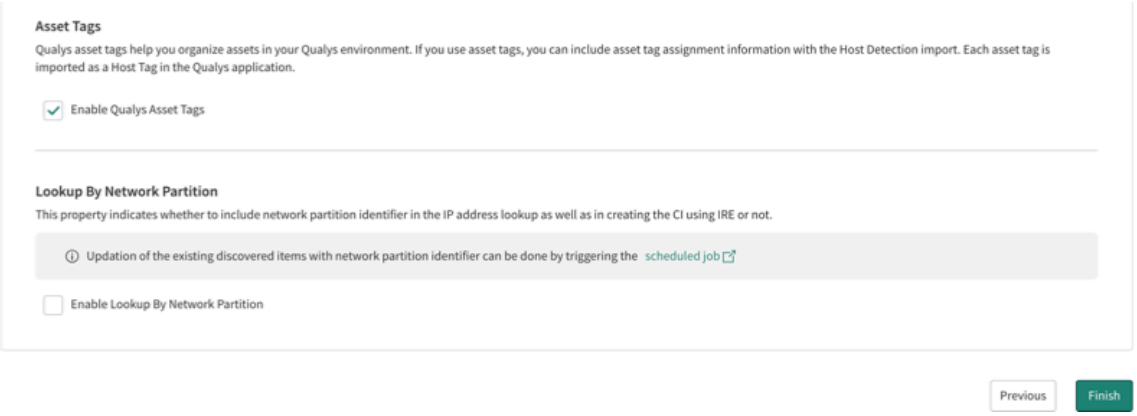
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Option	Description
	detection records are all updated to include the new granularity. New CIs are created when an exact match is not found.

Procedure

1. Navigate to **Vulnerability Response** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.
2. Choose Qualys Vulnerability Integration.
3. **Edit** the required integration.
4. Choose **Host Detection Configuration**.
5. Choose **Enable Lookup By Network Partition** check box from the **Lookup By Network Partition**



section.

6. Click **Finish**.

Network partition identifiers NETWORK_ID and REPOSITORY _ID included in IP lookup and CI creation

Source	IP address	NETWORK_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Qualys Vulnerability Integration: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Qualys: Assets and Fixed	123.12.12.141	12	CI 1	CI 1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
and Open Vulnerabilities Integrations				
	123.12.12.141	13	CI 1	CI 2

The IP Address and Incomplete IP Address CI identification lookup rules include the network partition identifier attribute automatically for a data import from the Assets and Fixed and Open Vulnerabilities Integrations for Qualys Vulnerability Integration.

After you activate the scheduled job and save the records, you alternatively can update your existing discovered items with CIs that include the network partition identifier by launching scheduled jobs on-demand. The CIs on your existing discovered item, vulnerable item, and detection records are automatically updated.

Set additional filter parameters for Qualys imports

Customize the filtering parameters for your scheduled queries with the Qualys Vulnerability Integration to help you further refine the vulnerability data you import with the supported Qualys integrations.

Before you begin

Use cases: As a vulnerability manager or analyst, you might want to filter out data from your queries so that you can review only specific vulnerability details. For example, say you want to view imported vulnerabilities that are filtered by specific IPs or IP ranges. Or, you want to import only machines that are under your scope, for example, only machines within your corporate network that are not external devices.

To help you gather this data, you might add Qualys parameters to help you import the specific vulnerability details you need.

Without adding additional API calls or coding, this feature permits you to customize your HTTP Request information with Qualys parameters in your ServiceNow AI Platform. You modify or add these values on your HTTP Method record under the REST method for the supported Qualys integrations of the Qualys Vulnerability Integration.

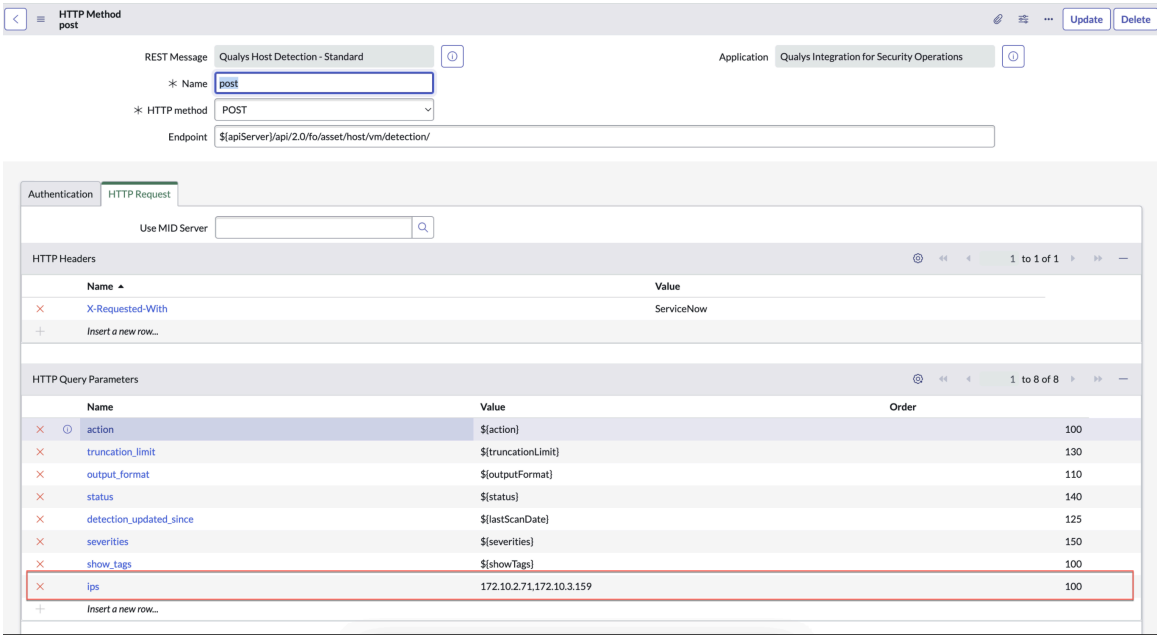
Role required: sn_vul.vulnerability_admin

Procedure

1. Locate the parameters supported by the Qualys product on the developer site that you want to use for your filtering.
   Parameters and values you enter from the Qualys product are supported only at the integration instance level in your ServiceNow AI Platform. All Qualys Integrations support filtering using query parameters.
2. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.
3. On the Qualys Integrations list page, click the record for the integration that you want to open the record.
4. With the Qualys REST Details tab selected, locate and click the information icon (ⓘ) for REST method followed by **Open Record** to open the HTTP Method record.
5. Select the **HTTP Request** tab.
6. In the HTTP Query Parameters for the request body, add the values you got from the Qualys developer site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following image, as an example, the parameter that ingests only certain IP addresses/ranges, *ips={value}* has been added. In this case, **value** is one or more IPs/ranges that you specify. Multiple entries are comma separated, `172.10.2.71, 172.10.3.159`, and a range is specified with a hyphen, `10.10.10.1-10.10.10.100`. Refer to the Qualys developer site for more information.



If you want to enter more than one parameter, refer to the Qualys documentation for more information about how to separate each value.

Note: You should be aware of you API requirements. You might have to add these API properties to the Query Parameters, or to the body content.

Some other parameters you might find useful from the Qualys developer site:

- *ag_ids* - Asset Group list IDs to retrieve. This parameter ensures only machines under your scope are brought in.
- *qids* - This parameter limits results to only certain vulnerabilities (QID in Third-Party Entry table). This setting prevents flooding your system with informational records.
- *arf_filter_keys* - Filters and returns host detections based on the specified values. Acceptable values: non-running-kernel, non-running-service, and config-not-exploitable. You can use any single value or comma-separated values. When you use this parameter in the REST parameters, set the following instance parameters to false because they are mutually exclusive: include_kernel_metadata, include_service_metadata, include_exploitable_config_metadata.
- *show_arf_data* - Displays ARF-affected data for host detections along with the arf_filter_keys parameter. Acceptable values: 0 or 1. If you set the value to 0, the output does not include the ARF filter output data. When you use this parameter in the REST parameters, set the following instance parameters to false because they are mutually exclusive: include_kernel_metadata, include_service_metadata, include_exploitable_config_metadata.
- *code_modified_after* - Returns QIDs modified after the specified date in the Knowledge Base integrations.
- *code_modified_before* - Returns QIDs modified before the specified date in the Knowledge Base integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- *assetDeploymentType* - Returns host IDs of the specified deployment type for PCRS Policy Host integrations. Acceptable values: ON-PREM, CLOUD, or ALL. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *assetState* - Returns host IDs of the specified state for PCRS Policy Host integrations. Acceptable values: TERMINATED, ACTIVE, or ALL. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *cloudMetaDataRequired* - Fetches cloud metadata in the PCRS Test Results Integration response. Acceptable values: 0 or 1. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *status* – Filters results based on result status. Acceptable values: Passed, Failed, and Error. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *previousStatus* – Filters results based on the previous result status. Acceptable values: Passed, Failed, and Error. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *criticalityLabels* – Filters results based on criticality level. Acceptable values: UNDEFINED, MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT. You can provide multiple comma-separated values. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *criticalityValues* – Filters results based on criticality level. Acceptable values: 0–5. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.
- *extendedEvidenceRequired* – Fetches extended evidence data. Acceptable values: 0 or 1. This parameter is available when the posture_api_version integration instance parameter is set to 5.0.

7. Click **Update**.

Resolving Qualys Vulnerability Integration issues

Some commonly encountered issues, along with workarounds are discussed.

Attachments not appearing after import

If attachments are not appearing as expected for data sources or on a security incident after third-party integration imports, check your IP restrictions.

IP access restrictions can prevent attachments from being seen unless you are logged in from a safe IP. Since a new attachment is added with each import, this can result in duplicates you have to remove.

For example, when you run a third-party host import integration, if you do not see any attachments on your data sources, check your IP restrictions and add users to the safe list prior to import.

Modify transform maps

Transform maps are provided with base configurations and are sufficient usually. You can modify transform mappings depending on the needs of your organization.

Before you begin

Role required: sn_vul_qualys.admin + import_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Import Sets** > **Administration** > **Transform Maps** to view the REST messages.
2. Filter the resulting list by application, and limit the list to the **Qualys Vulnerability Integration** application.
3. Modify the transform maps per the customer requirements.

   For details on the data provided by the Qualys API, see the Qualys API documentation.

Check XML attachment property size

Verifies that the XML attachment property is sufficient for large files.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **System Properties** > **Import Export**.
2. Scroll down to **Import Properties** > **XML Format** at the bottom of the page.



3. If necessary, change the value to 250 and click **Save**.

Related topics

Available system properties

Data retrieval limitations

By default, there are no restrictions on how data is retrieved from Qualys. Many records can be related to low severity vulnerabilities that a customer is not willing to remediate using their vulnerability response process. Updating the corresponding REST message/method parameters can modify this behavior.

The REST message/method responsible for this update is **Qualys Host Detection – Standard/post**. To update the values, add a new HTTP Query Parameter to the post method with the following values:

- Name: severities
- Value: 3-5 (or whatever appropriate severities are desired)

Qualys Knowledge Base Integration is failing

Resolve Qualys Knowledge Base Integration failure by reducing the payload attachment size received from Qualys to the specified limit.

Before you begin
Role required: sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Ensure that the payload attachment size is within the specified limit.
   a. Navigate to **All** > **Qualys Vulnerability Integration** > **Integration Instances**.
   b. Select the **Integration Instance Parameters** tab.
   c. Select **max_delta_days** and modify the default value to 3.
2. If the integration still fails, perform the following steps:
   a. Navigate to **All** > **Qualys Vulnerability Integration** > **Primary Integrations**.
   b. Select **Qualys Knowledge Base**.
   c. Select the **Integration Details** tab.
   d. In the **Start time** field, select the current date to skip the execution of the run for that day.
   e. Navigate to **All** > **Qualys Vulnerability Integration** > **Integration Instances**.
   f. Select the **Integration Instance Parameters** tab.
   g. Select **kb_backfill_full_import** and modify the default value to true.

Result

Running the Qualys Knowledge Base Backfill integration updates all the third-party entries (TPEs) in the system. While the Qualys Host Detection integration creates a placeholder entry, the Qualys Knowledge Base Backfill integration updates it.

Qualys integration run status chart

The Qualys Integration Run Status module is a graphical view of the status of Qualys integration runs.

To view the status of integration runs, navigate to **Qualys Vulnerability Integration** > **Integration Run Status**.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

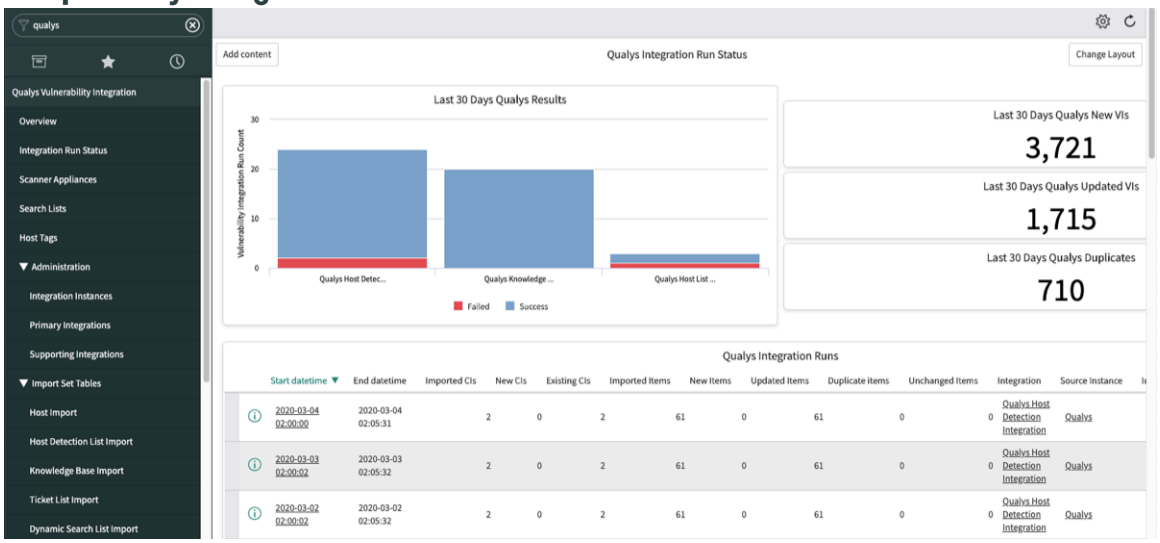
In the chart, point to any part (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

The Qualys Integration Run Status displays the vulnerability integration run status for the last 30 days. The Qualys[qualys] updated VIs count indicates the count for any unique detections in the same asset. The VI then gets updated with the new detection.

Note: The vulnerability integration run count is displayed only for the integrations, which are set to active state. Navigate to **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations** and set the state to active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample Qualys Integration Run Status chart



- The values in the Imported Items column represents the total number of records that are created from an integration run.
- The New items column displays the number of records that are created from an integration run.
- The Duplicate items column is no longer populated. You may prefer to remove this column from the display.
- The Updated items column displays the number of times records are updated during an integration run. This value is not the number of unique records that are updated. If for example, a record is updated two times during the integration run, it is counted two times and displayed as 2 updated items.
- The Unchanged items column displays records found during the integration run that already exist in the database but were not updated, because none of the relevant field values had changed.

Note: Integration runs with zero results for all four of the following values: **New CIs**, **Existing CIs**, **New Items**, and **Updated Items** are filtered out of the **Qualys Integration Runs** list.

Qualys integration run status chart reports

Name	Description
Last 30 Days Qualys Results	The number of integration runs completed for each integration. Shows both successful and failed runs. Run in a bar visual.
Last 30 Days Qualys New VIs	The number of new records imported in the last 30 days. Shown as an integer.
Last 30 Days Qualys Updated VIs	The number of updated records imported in the last 30 days. Shown as an integer.
Last 30 Days Qualys Duplicates	The number of duplicate records imported in the last 30 days. Shown as an integer.
Qualys Integration Runs	The integration run records in a list.

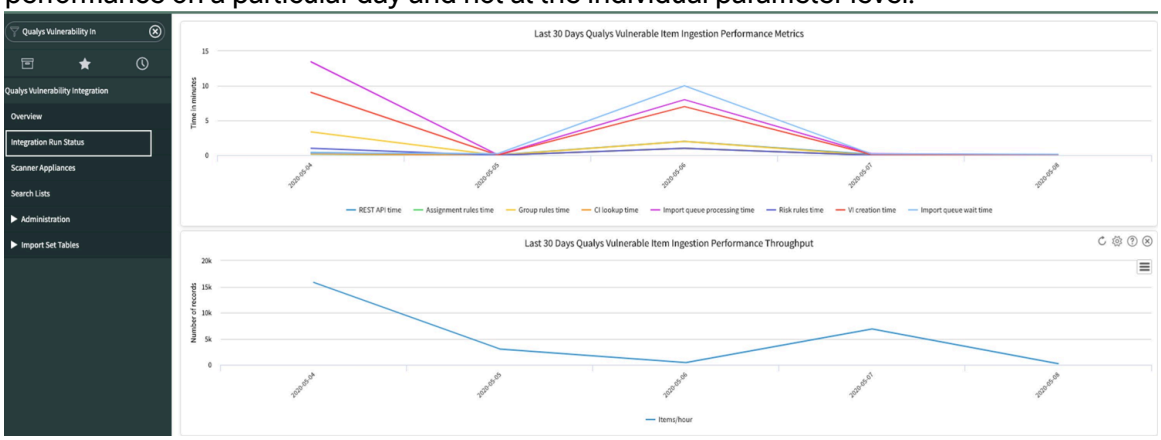
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys integration run status chart reports (continued)

Name	Description
	Note: V16.1: To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.
Last 30 Days Qualys Vulnerable Item Ingestion Performance Metrics	Daily performance metrics for vulnerable items compared for the last 30 days.
Last 30 Days Qualys Vulnerable Item Ingestion Performance Throughput	Daily vulnerable item ingestion throughput measured for the Qualys Host Detection integration for the last 30 days.

Multiple factors can impact the performance of the integration run, like the amount of data and time taken to process this data. Two graphs compare the performance metrics:

- Qualys Vulnerable Item Ingestion Performance Metrics: Compare daily performance metrics for assignment rules, group rules, risk rules, queue wait time, queue processing time, and other statistics for vulnerable items for the last 30 days, to identify the cause for any deviations in performance. The performance is calculated based on the time taken for each activity. These parameters are calculated and associated at the integration run level. Each parameter is color coded for easy identification.
- Qualys Vulnerable Item Ingestion Performance Throughput: Compare daily vulnerable item ingestion throughput for the Qualys Host Detection integration. Throughput is measured in items per hour. This report shows the overall performance on a particular day and not at the individual parameter level.



Qualys REST messages

Qualys REST messages are used to make calls to the Qualys API to fetch the compliance data.

The following rest messages are shipped with the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys PC Policies REST message

The Qualys PC Policies REST message retrieves policy data from Qualys. The changes to the REST message method record impact the request made to Qualys to retrieve policy information.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys PC Policies REST message parameters

Parameter Name	Value	Description
action	list	Indicates the type of operation requested. Required parameter.
details	All	Indicates the level of detail shown for policies retrieved. It is safe to modify as per your requirement.

Qualys PC Controls REST message

The Qualys PC Controls rest message retrieves compliance controls information for different control IDs from Qualys.

Qualys PC Controls REST message parameters

Parameter Name	Value	Description
action	list	Indicates the type of operation requested. Required parameter.
details	All	Indicates the level of detail shown for controls retrieved. It is safe to modify as per your requirement.

Qualys PC Policies Detail REST message

The Qualys PC Policies Detail REST message retrieves the complete policy details, such as technologies and sections.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys PC Policies Detail REST message parameters

Parameter	Value	Description
action	list	Indicates the type of operation being requested. Required parameter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys PC Policies Detail REST message parameters (continued)

Parameter	Value	Description
show_user_controls	Boolean	• Set to 1 to include user-defined controls (UDCs) in the XML output. • When not specified, UDCs are not included. This is an optional parameter. It is safe to modify as per your requirement.
show_appendix	Boolean	(Optional) Set to 1 to show the appendix section in the XML output. When unspecified.

Qualys PC Results REST message

The Qualys PC Results rest message retrieves compliance posture records from Qualys.

Qualys PC Results REST message parameters

Source Field	Value	Description
action	list	Indicates the type of operation requested. Required parameter. Changes are not recommended.
show_extended_evidence	Boolean	• Set to 1 to show the extended evidence information in the output. • Set to 0 or when unspecified, the extended evidence information is not shown in the output. **Note:** • You cannot specify `show_extended_evidence=1` in the same request as `hide_evidence=1`. This results in an error. The extended evidence is a part of the evidence data and it's shown only when evidence data is shown. • This parameter is not shipped with the base system.
cause_of_failure	Boolean	If you pass '1', Qualys will return the cause of failure. If you pass '0', Qualys will not return these attributes. **Note:** This parameter is not shipped with the base system.
policy_id		Shows compliance posture information records for a specified policy. A valid policy ID is required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys PC Results REST message parameters (continued)

Source Field	Value	Description
details	All	Indicates the level of detail shown for postures retrieved. It is safe to modify as per your requirement.
show_remediation_info		(Optional) Set to 1 to show remediation information in the XML or CSV output. By default, the output does not include the remediation information. When not specified, the remediation information is not included in the output.

Qualys PCRS Policy Host Integration REST message

The Qualys PCRS Policy Host Integration retrieves host data from Qualys and processes it in your instance.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys PCRS Policy Host Integration REST message parameters

Parameter Name	Value	Description
policyId	${lastRunDatetime}	Policy IDs for compliance evaluation.

Qualys PCRS Test Results Integration

The table shows the request parameters that are sent.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys PCRS Test Results Integration REST message parameters

Parameter Name	Value	Description
evidenceRequired	1	• The default value is 1, which indicates that evidence data will be retrieved for the host posture. • Set the value to 0 to retrieve the evidence data. **Note:** Changing the value to 1 increases the time required to fetch posture data.
compressionRequired	0	• The default value is 0, which indicates that the output will not be compressed. • Set the value to 1, if you want the data to be compressed. **Note:** Not compressing the data increases the time required to fetch posture data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Qualys Comprehensive PCRS Policy Host Integration REST message

The Qualys Comprehensive PCRS Policy Host Integration retrieves host data from Qualys and processes it in your instance.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Comprehensive PCRS Policy Host Integration REST message parameters

policyId	${policyId}	Policy IDs for compliance evaluation.

Qualys Comprehensive PCRS Test Results Integration

The table shows the request parameters that are sent.

Starting with v12.21.0 of Qualys Integration for Security Operations and v30.3.0 of Unified Security Exposure Management, the API version has been updated to version 5.0.

Qualys Comprehensive PCRS Test Results Integration parameters

Parameter Name	Value	Description
evidenceRequired	1	• The default value is 1, which indicates that evidence data will be retrieved for the host posture. • Set the value to 0 to retrieve the evidence data. **Note:** Changing the value to 1 increases the time required to fetch posture data.
compressionRequired	0	• The default value is 0, which indicates that the output will not be compressed. • Set the value to 1, if you want the data to be compressed. **Note:** Not compressing the data increases the time required to fetch posture data.

Understanding the Tenable Vulnerability Integration

The Vulnerability Response Integration with Tenable application developed by ServiceNow engineering for the Tenable Vulnerability Integration uses data imported from the Tenable.io, Tenable.sc, and Tenable.cs products to help you prioritize and remediate vulnerabilities for your assets. The application is available with a separate subscription from the ServiceNow® Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

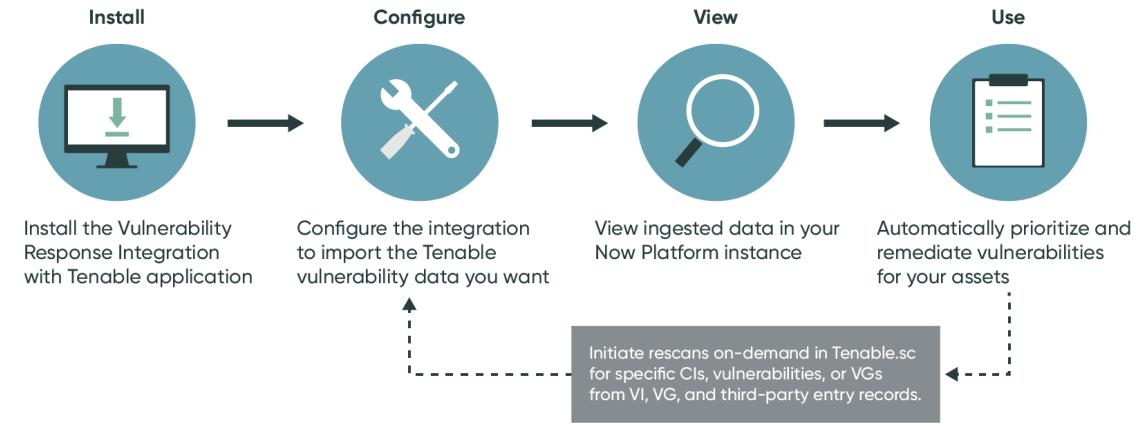
The Tenable Vulnerability Integration employs three Tenable integrations, Tenable.io, Tenable.sc and Tenable.cs, to import third-party scanner data about your assets and vulnerabilities. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13 and Tenable.cs product starting with version 5.0.1.

- Tenable.io is a cloud-based enterprise integration.
- Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Tenable.sc product and your ServiceNow AI Platform instance are in the same environment.
- If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server.
- Tenable.cs is a cloud-based enterprise integration.

The Vulnerability Response Integration with Tenable application is available on the ServiceNow Store with a separate subscription.

For lists and descriptions of the integrations in the Tenable Vulnerability Integration, see Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications and Tenable.sc integrations with the Vulnerability Response application.

Tenable Vulnerability Integration



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available versions for Xanadu

Release version	Release notes
Vulnerability Response Integration with Tenable v3.13.1, v4.1, v5.0.1	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes

Terms and Key features of the integrations

Vulnerable items and vulnerabilities

A vulnerable item is created in your ServiceNow AI Platform instance when:

- An imported vulnerability from a third-party scanner is matched to an existing asset (a configuration item in your CMDB). The Tenable product refers to these matches as **vulnerabilities**.
- An imported vulnerability from a third-party scanner isn't matched to an existing asset in your CMDB. In this case, an unmatched CI is also created along with a vulnerable item.

  For unmatched CIs, you can also use the Identification and Reconciliation Engine (IRE) to create CIs in two new classes when an existing CI can't be matched with a host. Otherwise, unmatched CIs are created in the Unmatched CI classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine.

Third-party vulnerability entries and plugins

Third-party vulnerability entries are imported from third-party scanners and listed in the Third-Party Vulnerability Entries table in your ServiceNow AI Platform instance. Starting with v24.0 of Vulnerability Response, the Softwares column in the Third-Party Vulnerability Entries table populates the Common Platform Enumerations (CPEs) associated with a third-party entry. Third-party vulnerability entries from Tenable are ingested into Vulnerability Response and matched to existing assets listed in your CMDB. Tenable refers to third-party vulnerability entries as **Plugins**.

Configuration item (CI)

Configuration items are the existing assets listed in your CMDB.

Discovered item

Assets ingested from the Tenable asset import are matched to existing configuration items in your CMDB. Imported assets are updated.

If a match isn't found, a CI is created in the Unmatched CI class of the CMDB. If the CMDB CI Class Models plugin is enabled, the Identification and Reconciliation Engine (IRE) creates CIs using new classes. For more information, see Creating CIs for Vulnerability Response using the Identification and Reconciliation engine. If the original, unmatched CI is reclassified, discovered item records are updated to reflect the state. Discovered items give you visibility into how assets are identified and mapped to CIs in the CMDB.

CI lookup rules

When data is imported from a third-party integration, Vulnerability Response automatically uses host (asset) data to search for matches in the Configuration Management Database (CMDB). CI lookup rules are used to identify CIs and add them to VI records when VITs are created to aid you with remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rescan and remediation scan

You can initiate a targeted rescan command on a specific configuration item, remediation task, or third-party entry directly from vulnerable item, remediation task, and third-party vulnerability entry records in your ServiceNow AI Platform instance. Tenable refers to this rescan as a **remediation scan**.

Automatically close older VIs

With the Auto-Close Stale Vulnerable Items module in your ServiceNow AI Platform, you can clean up older, stale vulnerable items (VI)s not recently found by your third-party integrations. Moving these VIs to **Closed** helps you reduce the number of active vulnerable items and remediation tasks and reconcile assets in your CMDB. You can use all the integrations with the Vulnerability Response Integration with Tenable to close stale VIs automatically.

Instance

This term refers to a distinct occurrence of your ServiceNow AI Platform® application.

Integration

An integration is a product-specific reference to an integration, such as the Tenable.io Assets Integration, or the Tenable.sc Plugin Integration. These are the separate integrations that belong to specific Tenable products in the Tenable Vulnerability Integration in your instance.

Integration instance

This term refers to the separate Tenable integrations listed by their Tenable.io and Tenable.sc products.

Deployment

When an integration supports multi-source, a single, distinct integration existence is referred to as a deployment of your integration. The term is used to refer to the integration(s) and products across your environment. For example, you might have multiple deployments of various integrations of the Tenable.io and Tenable.sc products in your environment.

The Tenable.io, Tenable.sc, and Tenable.cs integrations also include the following key features:

- Configuration assessment findings, that is, test results along with policies, configuration tests (controls), and citations with authoritative sources can be imported into the Configuration Compliance application with the Tenable.io product. See Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications and Exploring Configuration Compliance for more information about how this integration works with the Configuration Compliance application.
- Starting with v2.1 of the Tenable Vulnerability Integration, create unique configuration items (CIs) that include different network partition identifiers for assets in your environment that share the same IP address. Identify the distinct assets across your environment and update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.
- You can schedule when you want the jobs to run for all the Tenable.io, Tenable.sc and Tenable.cs integrations. You can also execute scheduled jobs manually on-demand.
- For asset imports with Tenable.io, you can enable asset tags to organize and track the assets listed in your CMDB in the Tenable.io environment.
- The Tenable.io, Tenable.sc and Tenable.cs integrations permit you to configure CI Lookup Rules to define how asset data from third-party sources are used to identify Configuration Items (CIs) in your ServiceNow AI Platform CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Tenable.io, Tenable.sc and Tenable.cs integrations permit you to set import filters on the vulnerabilities import so that you import only the vulnerabilities from Tenable that you want. For Tenable.io, you have the option to import **Fixed** vulnerabilities from Tenable with the vulnerabilities import.
- For Tenable.sc, you have the option to initiate rescans on-demand directly from a vulnerable item, remediation task, and third-party entry records in your ServiceNow AI Platform instance. If VIs have been transitioned to **Closed/Fixed** but aren't yet updated in your instance, you can verify vulnerabilities on specific configuration items have been remediated. See Initiate rescan for the Tenable.sc integration.

The following sections list more details about the Tenable integrations.

Required ServiceNow AI Platform roles

The integration tasks require the following roles in your ServiceNow AI Platform instance.

admin

The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant.

sn_vul.vulnerability_admin

Once assigned, the vulnerability admin completes the configuration of the Tenable integrations in Setup Assistant. This role has complete access to the Vulnerability Response (VR) application and its records. The vulnerability admin configures all VR applications and rules for installed third-party integrations.

sn_vul_tenable.configure_integration

This role contains the sn_vul_tenable.read_integration granular role and users with this role can configure the Vulnerability Response Integration with Tenable application.

sn_vul_tenable.read_integration

Users with this roles can view (read) but not edit records of the Vulnerability Response Integration with Tenable application.

Vulnerability Response group

By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically.

Vulnerable items

Vulnerable items are grouped into remediation tasks according to remediation task rules and assigned for remediation based on your assignment rules. For more information, see Vulnerability Response remediation tasks and remediation task rules overview and Vulnerability Response assignment rules overview.

Configuration item (CI) lookup rules

CI Lookup Rules identify CIs and determine when to add them to a vulnerable item. For more information on how CI lookup rules work, see CI lookup rules for identifying configuration items from Vulnerability Response third-party vulnerability integrations.

Note: Rules, once removed, can't be recovered. Rather than removing existing rules, disable them when creating ones.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following Tenable.io lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Note: The Tenable.io CI lookup rules prioritize and populate the non-empty network interface values (FDQN, IPV4, and MacAddress) over the regular FDQN, IPV4, and MacAddress values for a discovered item. When these network interface values are empty, the regular FDQN, IPV4, and MacAddress values are populated for a discovered item.

The following Tenable.sc lookup rules are shipped with the base system.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Note: Multiple values for ip_address, mac_address, fqdns and network_interfaces are used for an asset. All values are considered in CI lookup rules for matching. All values are used to create multiple network adapters using IRE.

The Tenable.cs lookup rule Cloud Resource Id is shipped with the base system.

For more information on how to configure the categorization of unmatched cloud resources into your preferred CI class, see Updating CI class for unmatched cloud assets.

New properties to ignore IP addresses

In Tenable.io, there are two properties available if you want to ignore multiple IP addresses or multiple Mac addresses as part of your CI lookup rules:

ignoreIPAddress

A list of IP addresses to be ignored for CI lookup and CI creation.

ignoreMacAddress

A list of MAC addresses to be ignored for CI lookup or CI creation.

Discovered items

This module lists configuration items detected during import from the Tenable Vulnerable Item integrations and the Tenable Asset integrations.

Note: The default filter for this list is set to `Unmatched`. You can view all discovered items from an import by removing the filter.

For more information on the Discovered Items module, see Discovered Items.

Asset tags

Asset tags (also referred to as host tags) are used for organizing and tracking the assets in your organization. You can assign tags to your assets. Then, when launching the scans, you can

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

select tags associated with the assets you want to scan. The Asset Tags module enables you to download asset tag data from Tenable.io to your instance on a scheduled basis. Asset data that includes asset tags is pulled from Tenable.io and transformed using the Tenable.io Asset Transform integration transformation maps.

All Asset tags are imported as part of the Tenable.io Asset integration. Asset tags are used for filtering in Vulnerability Response assignment rules and Remediation Task Rules. The tags are displayed in the Discovered Item form.

Note: Run the Tenable.io Asset Integration prior to creating Vulnerability Response assignment rules or remediation task rules in the Vulnerability Response application so that all tags are available for these rules before vulnerable items are imported and grouped. Also note the following points about tags:

- Tag storage isn't case-sensitive. For example, if you create a tag to describe assets in your San Diego location, and you create the `San Diego` tag, you can't also create a `SAN DIEGO` tag and store it in the Asset tag table. `San Diego` and `SAN DIEGO` are considered to be the same asset tag by the system. Whichever tag is imported first is the tag that is stored and recognized going forward.
- Using asset tags as a Group Key in a remediation task rule may have unexpected results. Asset tags are intended for use only in the condition builder.
- Asset tags are controlled by the global system property sn_vul.import_asset_tags. This property is set to `true` by default. Disabling tags disables them across all ServiceNow AI Platform® instances.

Data retrieval filters

Data retrieval settings help you determine specifically the type and scope of data you want to import from the Tenable application to your ServiceNow AI Platform® instance. For a list of the most commonly used settings, see Data retrieval settings for the Tenable Vulnerability Integration.

Vulnerability Priority Rating (VPR)

The Vulnerability Priority Rating (VPR) is an attribute from the Tenable product that is imported and used with a new default risk calculator in Vulnerability Response. The Tenable Risk Rule is installed with the Vulnerability Response Integration with Tenable application as part of the Default Risk Calculator in the Vulnerability Calculators from Vulnerability Response.

This risk rule is inactive by default.

By enabling the Tenable risk calculator rule, the imported VPR values are used to calculate the Risk Score for vulnerable items. The default weight distribution for this risk calculator: VPR = 70%, Asset=15%, and Business Criticality=15%. Enabling this Tenable Risk Calculator rule may impact your data ingestion performance. For more information about Vulnerability Response calculators and the Tenable risk calculator rule, see Vulnerability Response calculators and vulnerability calculator rules.

Installation and configuration

After you download the Vulnerability Response Integration with Tenable from the ServiceNow® Store, installation and configuration is supported by the Setup Assistant in Vulnerability Response. See Configuring Vulnerability Response using the Setup Assistant for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications

The Tenable.io integrations in the Vulnerability Response Integration with Tenable with Tenable application are available for use with both the Vulnerability Response and Configuration Compliance applications.

List of Tenable.io integrations

The Tenable.io and Tenable.sc integrations support multi-source deployments. You can add and deploy multiple instances of these integrations across your environment using Setup Assistant in Vulnerability Response. You also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

Tenable.io is a cloud-based enterprise integration. The following sections describe the supported Tenable.io integrations and their behavior.

Starting with v 6.1.3, the Tenable.io Compliance Results Integration is replaced by two separate integrations, the Tenable.io Fixed Compliance Results Integration and the Tenable.io Open Compliance Results Integration. The original Tenable.io Compliance Results Integration is no longer available. Compliance results are now imported separately based on their status, improving ingestion performance for your environment if you have large volumes of compliance data.

Tenable.io integrations

The following table lists the supported integrations for the Tenable.io product.

Integration	Description
Tenable.io Assets Integration	Retrieves all asset data, including asset tags, from the Tenable.io product. Creates unique CIs for unmatched assets.
Tenable.io Compliance Results Integration	Retrieves secure configuration assessment data from Tenable.io and processes it in your ServiceNow AI Platform instance. Imported data includes compliance test results along with associated policies, configuration tests (controls), and citations with authoritative sources. Starting with v 6.1.3, this integration is replaced by the Tenable.io Fixed Compliance Results Integration and Tenable.io Open Compliance Results Integration.
Tenable.io Fixed Compliance Results Integration	Retrieves compliance test results in a fixed state (Passed, Skipped) and processes associated policies, tests, and citations.
Tenable.io Open Compliance Results Integration	Retrieves compliance test results in an open state (Failed, Warning, Error, Unknown) for investigation and remediation. Triggered after the Tenable.io Fixed Compliance Results integration.
Tenable.io Compliance Results Backfill Integration	Matches compliance results with assets that were previously missing. Runs automatically after the Assets Integration and removes resolved entries from the missing asset table.
Tenable.io Scan Credential Integration	Retrieves scan credentials configured in Tenable.io for use in rescan requests. Runs weekly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration	Description
Tenable.io Template Integration	Retrieves available Tenable.io credentials for rescans. Stores a single template record temporarily.
Tenable.io Plugin Integration	Retrieves plugin data from Tenable.io to keep Tenable Identifiers (Ten IDs) current.
Tenable.io Fixed Vulnerabilities Integration	Retrieves vulnerability data based on severity filters. Outputs Closed/Fixed vulnerable items. Scheduled; chains to Open.
Tenable.io Open Vulnerabilities Integration	Retrieves open vulnerability data. Triggered after the Fixed Vulnerabilities integration. Outputs New/Reopened VIs.
Tenable.io Scan Metadata Integration	Retrieves scan metadata from the `/scans` endpoint using the `last_schedule_id` from existing asset data and associates scan records with discovered items and vulnerabilities.

Tenable.io Assets Integration

Retrieves all asset data, including asset tags, from the Tenable.io product and processes it in your instance.

- Starting with v3.0, if the Tenable.io Compliance Results Integration is activated, you can import secure configuration assessment data along with imported asset data. This data can help you identify and respond to configuration-related vulnerabilities on your assets.
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Asset API.
- The output of this integration is discovered items.
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.
- Starting with v2.2, Last Scan Time is imported and updated only for assets that have vulnerabilities.

Tenable.io Compliance Results Integration

Note: Deprecated starting with v 6.1.3. This integration is replaced by the Tenable.io Fixed Compliance Results Integration and the Tenable.io Open Compliance Results Integration.

This integration retrieves all secure configuration assessment data and processes it in your ServiceNow instance. Imported data includes test results along with policies, configuration tests (controls), and citations with authoritative sources.

- Assessment data for missing assets or assets without asset IDs aren't imported.
- If a test result is imported and its corresponding asset couldn't be matched in your instance, the test result is ignored and the ID for the missing asset is stored in a temporary record in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets are listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Tenable.io Fixed Compliance Results Integration

Retrieves secure configuration assessment data for compliance test results with a status of Passed or Skipped and processes it in your ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Imported data includes test results along with associated policies, configuration tests (controls), and citations with authoritative sources.
- This integration is scheduled and executes first in the compliance chain. Upon successful completion, it automatically triggers the Tenable.io Open Compliance Results Integration, provided the Open integration is active and configured in the **Next Integration** field.
- Assessment data for missing assets or assets without asset IDs isn't imported.
- If a test result is imported and its corresponding asset can't be matched in your instance, the test result is ignored and the missing asset ID is stored in a temporary record in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets is listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Tenable.io Open Compliance Results Integration

Retrieves secure configuration assessment data for compliance test results with a status of Failed, Warning, Error, or Unknown and processes it in your ServiceNow instance.

- This integration is triggered upon successful completion of the Tenable.io Fixed Compliance Results Integration.
- By default, this integration is configured to run on demand. You can modify the scheduling configuration from the integration record in **Tenable Vulnerability Integration** > **Integrations**.
- Assessment data for missing assets or assets without asset IDs isn't imported.
- If a test result is imported and its corresponding asset can't be matched in your instance, the test result is ignored and the missing asset ID is stored in the `sn_vul_tenable_missing_asset` table.
- The total number of ignored (missing) assets is listed in the **Ignored CIs** field on the **Configuration** tab of the integration run record.

Execution behavior for the split compliance results integrations

- The Fixed Compliance Results Integration is designed to execute first. When active, it automatically triggers the Open Compliance Results Integration upon successful completion, provided the Open integration is active and configured in the **Next Integration** field of the Fixed integration record.
- If the Fixed Compliance Results Integration is inactive or encounters an error during execution, the Open Compliance Results Integration isn't triggered. You must execute it manually or configure its own schedule.
- Execution details and error information are captured in the integration run record.

Upgrade considerations

- If you are upgrading from an earlier release, your existing compliance data remains unchanged. The Fixed and Open Compliance Results integrations preserve their configured Start time and continue fetching data incrementally from where the previous integration left off.
- To continue ingesting compliance results, ensure that both integrations are active.
- You can modify scheduling behaviour or disable automatic chaining as needed.

Both the Fixed and Open Compliance Results integrations use the same Tenable.io Compliance Results Transform map and import data into the Tenable.io Test Results Import [sn_vul_tenable_io_tr_import] table. The data mapping behaviour remains unchanged.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results Backfill Integration

When activated, this integration runs automatically after the Assets integration completes as part of a chained integration run. It matches configuration assessment data with missing assets listed in the `sn_vul_tenable_missing_asset` table.

- Imports up to 200 asset IDs for any missing assets discovered or present in your instance after the Assets integration import completes successfully.
- Removes the temporary records from the `sn_vul_tenable_missing_asset` table when assets can be matched with corresponding configuration assessment data.
- Coordinates the REST message calls to the Compliance Export API.

Tenable.io Scan Credential Integration

Retrieves the scan credentials configured in Tenable.io for use in rescan requests initiated from the ServiceNow AI Platform.

- Coordinates the REST message calls to the Credentials API.
- The output of this integration is scan credentials populated in the `sn_vul_tenable_scan_credential` table.
- The imported credentials are used to access the scanner when you initiate scan requests from the ServiceNow AI Platform.
- This integration is scheduled to run weekly.

Tenable.io Template Integration

A template record is sent to Tenable.io during rescan. This integration retrieves available Tenable.io credentials to use for rescans. Credentials are instance-specific, and a single template record is imported and securely stored temporarily on the `sn_vul_tenable_io_template` table.

Tenable.io Plugin Integration

Retrieves the plugin data from the Tenable.io product to keep Tenable Identifiers (Ten IDs) current.

- Retrieved data is based on the date that the plugins were last updated by a Tenable.io integration run.
- Coordinates the REST message calls to the Plugin API.
- The output of this integration is third-party vulnerabilities.

Tenable.io Fixed Vulnerabilities Integration

Retrieves vulnerability data based on severity filters from the Tenable.io product and processes it in your instance.

- Vulnerable items are created for detection records in the Open and Reopened states because these records require remediation. Existing vulnerable items are updated if detections are Fixed, but vulnerable items aren't created for Fixed detections by default because Tenable considers Fixed vulnerabilities Mitigated.
- When you activate the flag **Create vulnerable items for Fixed Vulnerability detections** in Setup Assistant, new VIs are created in the Fixed state so you have visibility into the detections that created them. Since VIs are created for Fixed detections that don't exist in your instance,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

this might negatively impact your import performance. You may prefer to leave this feature deactivated so that Fixed detections only update the states of existing vulnerable items.

- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Vulnerabilities API.
- The output of this integration is Closed/Fixed vulnerable items (VIs). It also creates assets and third-party entries if they don't exist.
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.

This integration run is scheduled. It's a chained integration, which means after a run is successfully completed, the Open Vulnerabilities integration is triggered.

Starting from Tenable v3.3, you can view the following information for vulnerability integration runs:

- **Total chunks**: The total number of chunks being generated by Tenable.
- **Available chunks**: Number of chunks available for download for ServiceNow.

Tenable.io Open Vulnerabilities Integration

This integration is triggered upon successful completion of the Tenable.io Fixed Vulnerabilities Integration.

- Retrieves vulnerability data based on the severity filters from the Tenable.io product and processes it in your instance.
- Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share the same IP address.
- Coordinates the REST message calls to the Vulnerabilities API.
- The output of this integration is New/Reopened vulnerable items (VIs). It also creates configuration items and third-party entries if they don't exist. Tenable considers active vulnerabilities Cumulative (current).
- Data is imported in chunks and stored in the `sn_vul_tenable_chunk_status` table. Table cleaner automatically removes stored data from this table after 30 days.

Starting from Tenable v3.3, you can view the following information for vulnerability integration runs:

- **Total chunks**: The total number of chunks being generated by Tenable.
- **Available chunks**: Number of chunks available for download for ServiceNow.

Tenable.io Scan Metadata Integration

Retrieves metadata from the /scans endpoint. It pulls scan information based on the last_schedule_id from the existing asset data in Tenable.io.

- Table Creation: A new custom table, `sn_vul_tenable_scan`, stores scan metadata retrieved from the Tenable.io /scans endpoint, including scan ID, name, status, start time, end time, and scan type.
- Data Association: A reference field is established between discovered items (configuration items or vulnerabilities) and the corresponding latest scan record in the `sn_vul_tenable_scan` table. This linkage enables you to:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- View the most recent scan information associated with each discovered item.
- Improve the context for vulnerability triage and remediation decisions.
- Enhance auditability and reporting capabilities by maintaining a historical record of scan activities.

Activate Tenable.io integrations

The Tenable.io Compliance Results Integration and the Tenable.io Compliance Results Backfill Integration are inactive by default. Follow these steps to activate an integration:

1. Navigate to **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
2. From the **Tenable Integrations** list, open the integration record.
3. Select the **Active** check box.
4. Select **Update**.

You can keep the default schedule settings when activating these integrations initially.

Note: Starting with v 6.1.3, the original Tenable.io Compliance Results Integration is no longer available. You must activate both the Fixed and Open Compliance Results integrations to continue ingesting compliance data.

Tenable.sc integrations with the Vulnerability Response application

The Tenable.sc integrations in the Vulnerability Response Integration with Tenable application.

Starting with Vulnerability Response v20.0, if an asset is scanned by an agent, the "Agent exists" column in the Discovered Items list displays the value as "true." This indicates that the scan is authentic.

List of Tenable.sc integrations

Multi-source is supported for all the Tenable.io and Tenable.sc integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You can also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

- Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Tenable.sc product and your ServiceNow AI Platform instance are in the same environment.
- If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required to use a MID Server.

Tenable.sc integrations

Integration	Description
Tenable.sc Assets Integration	To avoid creating duplicate discovered items with imported asset data, the Asset Integration of the Tenable.sc product is comprised of two integrations. **The Tenable.sc Open Assets Integration** This integration imports vulnerability data about your assets that Tenable considers **Cumulative** (current), or **Open**. The vulnerable items (VIs) that are created in your instance with this imported

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
	asset data are considered open, that is, in the **Open** state. These vulnerable items require investigation and might need remediation. **The Tenable.sc Fixed Assets Integration** This integration imports vulnerability data about your assets that Tenable considers **Mitigated** (no longer vulnerable) or **Fixed**. The vulnerable items for these assets transition from the **Open** state to the **Closed/Fixed** state in your instance, because the results of scans show they're no longer vulnerable. • Retrieves all asset data from the Tenable.sc product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Assets API. • The output of this integration is discovered items. • The Tenable query filter that you select in the Setup Assistant also applies to the Tenable.sc Assets Integration. Only the assets with the vulnerabilities that match the conditions of the query filter are imported.
Tenable.sc Plugin Integration	• Retrieves the plugin data from the Tenable.sc product. Retrieved data are based on the date that the plugins were last updated by a Tenable.sc integration run. • This import ensures that the Tenable.sc Identifiers (Ten IDs) are current and only active vulnerabilities are imported. • Coordinates the REST message calls to the Plugins API. • The output of this integration is third-party vulnerabilities.
Tenable.sc Fixed Vulnerabilities Integration	• Retrieves vulnerability data based on severity filters from the Tenable.sc product and processes it in your instance. Vulnerable items are created for detection records which are in the **Open** and **Reopened** states, because these records require remediation. Existing vulnerable items are updated by Vulnerability Response if detections are **Fixed**, but vulnerable items aren't created for **Fixed** detections by default, because Tenable considers **Fixed** vulnerabilities **Mitigated**. • When the flag **Create vulnerable times for Fixed Vulnerability detections** is activated in Setup Assistant, it creates VIs in the **Fixed** state so you have visibility into the detections that created them. As VIs are created for **Fixed** detections that don't exist in your instance, this might

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
	negatively impact your import performance. You may prefer to leave this feature deactivated so that **Fixed** detections only update the states of existing vulnerable items. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is **Closed/Fixed** vulnerable items (VIs). It also creates assets and third-party entries if they don't exist. This integration run is a scheduled run. It's a chained integration which means after a run is successfully completed, the Tenable.sc Open Vulnerabilities Integration described next is triggered. **Note:** By default, the family IDs 0 and 39 are excluded from this integration.
Tenable.sc Open Vulnerabilities Integration	• This integration is triggered on successful completion of the Tenable.sc Fixed Vulnerabilities Integration. • Retrieves vulnerability data based on the query filters selected from the Tenable.sc product and processes it in your instance. • Creates corresponding vulnerable items for active vulnerabilities. • Creates unique CIs for unmatched assets, or updates existing CIs with the network partition identifier attribute for assets across your environment that share IP address. • Coordinates the REST message calls to the Vulnerabilities API. • The output of this integration is **Update/Create new** vulnerable items (VIs) if they don't exist. It also creates configuration items and third-party entries if they don't exist. **Note:** By default, the family IDs 0 and 39 are excluded from this integration.
Tenable.sc Scan Credential Integration	• This integration retrieves the scan credentials configured in Tenable.sc. • Coordinates the REST message calls to the Credentials API. • The output of this integration is scan credentials populated in table, [sn_vul_tenable_scan_credential].

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.sc integrations (continued)

Integration	Description
	• The imported credentials are used to access the scanner when scan requests are initiated from the ServiceNow AI Platform. • This integration is scheduled to run weekly.

Tenable.sc Backfill Vulnerabilities Integration	• This backfill integration imports any open and fixed vulnerabilities that might have been missed during an import.
	• This integration imports both open and fixed vulnerabilities from the last seven days to update your detections and vulnerable items.
	• This integration might impact your performance.
	• This integration is inactive by default.
	• To update your vulnerability data and avoid potential performance problems, you might prefer to schedule the Tenable.sc Fixed Vulnerabilities and Open Vulnerabilities Integrations to run when no other scans are running.
	• The output of this integration is:
	  ○ **Closed/Fixed** vulnerable items (VIs). It also creates assets and third-party entries if they don't exist.
	  ○ to **Update/Create new** vulnerable items (VIs) if they don’t exist. It also creates configuration items and third-party entries if they don't exist.

User authentication and Tenable.sc

User authentication is supported by your ServiceNow AI Platform® instance and version 5.13 of the Tenable.sc product. User authentication is required if you’re using version 5.12 and earlier of the Tenable.sc product.

When you select user authentication for the Tenable.sc integrations, tokens might expire and be replaced during integration runs. In the Notes column on the Vulnerability Integration Run record (VIN), the following message is displayed for a process when a token expires, `Error: Token validation is failed`. No action is required if this message is displayed. Expired tokens are automatically refreshed in the background and the message doesn’t indicate a pause or error with the integration process.

Tenable.cs integrations with the Vulnerability Response and Container Vulnerability Response application

The Tenable.cs integrations in the Vulnerability Response Integration with Tenable application are available in the Vulnerability Response and Container Vulnerability Response applications.

Starting with v20.0 Vulnerability Response, if an asset is scanned by an agent, the "Agent exists" column in the Discovered Items list displays "true," indicating that the scan is authentic.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

List of Tenable.cs integrations

Multi-source is supported for all the Tenable.io, Tenable.sc, and Tenable.cs integrations. You can add and deploy multiple instances of the following integrations across your environment from Setup Assistant in Vulnerability Response. You can also install and configure the Vulnerability Response Integration with Tenable application from Setup Assistant.

Tenable.cs is a cloud-based enterprise integration. See the following table for the names and descriptions of the supported integrations for the Tenable.cs product.

Tenable.cs integrations

Integration	Description
Tenable.cs Cloud Container Assets Integration	• Retrieves all container asset data from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. Coordinates the REST message calls to the Asset API. The output of this integration is Discovered Container Images, Docker Images, and Container Repositories.
Tenable.cs Open Cloud Container Vulnerabilities Integration	When activated, this integration runs automatically after the container assets integration is successfully completed as part of a chained integration run. • Retrieves container vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopenedcontainer vulnerable items (CVIs). If they don't exist, it also creates discovered container images, docker images, container repositories, image findings, third-party entries, and Common Vulnerabilities and Exposures (CVE).
Tenable.cs Fixed Cloud Container Vulnerabilities Integration	This integration is triggered on successful completion of the Tenable.cs Open Cloud Container Vulnerabilities Integration. • Retrieves container vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopened container vulnerable items (CVIs). If they don't exist, it also creates discover container images, docker images, container

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs integrations (continued)

Integration	Description
	repositories, image findings, third-party entries, and CVEs. Image findings are created in closed state.
Tenable.cs Open Cloud Host Vulnerabilities Integration	• Retrieves vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is New/Reopened vulnerable items (VIs). If they don't exist, it also creates configuration items, third-party entries, and CVEs. Vulnerability Detections are created in open state.
Tenable.cs Fixed Cloud Host Vulnerabilities Integration	This integration is triggered on successful completion of the Tenable.cs Open Cloud Host Vulnerabilities Integration. • Retrieves vulnerability data based on the severity filters from the Tenable.cs product and processes it in your instance. • Creates unique CIs for unmatched assets, or updates existing CIs. • Coordinates the REST message calls to the Vulnerabilities API. The output of this integration is close vulnerable items (VIs). If they don't exist, it also creates configuration items, third-party entries, and CVEs. Vulnerability Detections are created in closed state.

User authentication and Tenable.sc

User authentication is supported by your ServiceNow AI Platform® instance and version 5.13 of the Tenable.sc product. User authentication is required if you're using version 5.12 and earlier of the Tenable.sc product.

When you select user authentication for the Tenable.sc integrations, tokens might expire and be replaced during integration runs. In the Notes column on the Vulnerability Integration Run record (VIN), the following message is displayed for a process when a token expires, `Error: Token validation is failed`. If this message is displayed, no action is required. Expired tokens are automatically refreshed in the background and the message doesn't indicate a pause or error with the integration process.

Preparing for the Tenable Vulnerability Integration

Prepare for the ServiceNow® Tenable Vulnerability integration by performing the following setup tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

A successful integration requires planning and careful execution of pre-integration tasks. For a smooth installation and configuration of the Vulnerability Response Integration with Tenable application, you may prefer to print the following checklist and verify the items listed are completed before you install the application and import vulnerability data into your ServiceNow AI Platform® instance.

Note: If you have been importing data with the Tenable-built integration, and you want to start using the ServiceNow® Vulnerability Response Integration with Tenable, see the

For current data cleanup and migration information from the Tenable-built integration to the integration built by ServiceNow, see the Guidelines to migrate from the Tenable Vulnerability Response Integration to the ServiceNow Vulnerability Response Integration with Tenable [KB0960667] article.

Role required: Admin to download and install the application.

Task	Description
☐	(Optional) If not already installed and activated, you may prefer to install the Vulnerability Response application prior to installing the third-party application. For more information about installing and activating the Vulnerability Response application, see, Install Vulnerability Response. This integration requires version 12.1 of Vulnerability Response or later.
☐	If you don't already have it on your instance, get entitlements and download the Vulnerability Response Integration with Tenable application to your ServiceNow AI Platform® instance. The Vulnerability Response Integration with Tenable application supports the Tenable.sc product starting with version 5.13 and Tenable.cs product starting with version 5.0.1. .
☐	Estimate the number of vulnerable items that you expect to import. Verify that your instance can accept the number of vulnerable items you expect to import. An undersized instance can lead to long load times. If you don’t know the size of your instance, or, if you need assistance, contact ServiceNow® Technical Support.
☐	Verify that you have groups or users to manage the integrations and remediate vulnerable items. **admin** The system admin uses Setup Assistant to install the Vulnerability Response Integration with Tenable application. If not assigned, the admin assigns the vulnerability admin (sn_vul.vulnerability_admin) and other roles in Setup Assistant. **sn_vul.vulnerability_admin**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	Once assigned, the vulnerability admin completes the configuration of the Tenable integrations. This role has complete access to the Vulnerability Response (VR) application and its records. Configures all VR applications and rules and configures third-party integrations. **sn_vul_tenable.configure_integration** Can configure the Tenable Vulnerability Integration. This role contains the sn_vul_tenable.read_integration granular role. **sn_vul_tenable.read_integration** Can view (read) records of the Tenable Vulnerability Integration. **Vulnerability Response group** By default, the Vulnerability Response group is available in Setup Assistant. Users assigned to the Vulnerability Response group inherit the sn_vul.read_all and sn_vul.remediation_owner roles automatically. The system admin performs the initial assignment of roles to users and groups in Setup Assistant for the integration. By default, the Vulnerability Response group is available. If not already created, you may prefer to create additional groups and add users with the User Administration module in your instance prior to using Setup Assistant. See Create a user group. Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.
☐	To promote improved performance for your first import, you may prefer to disable certain features, rules, or jobs in your instance. • Disable vulnerability calculators if you don't use them. These calculators, plus any you have defined, run every time a vulnerable item record is created or updated. See Disable vulnerability calculators. • During the initial import of records, certain notification-related business rules can cause many notifications to be generated, impacting performance. Prior to your initial import, you may prefer to Disable notification-related business rules as described in Import modifications for the Tenable Vulnerability Integration.
☐	Verify you have enabled any features, rules, dependency plugins, or jobs in your instance required for the integration. • Tenable.sc is an on-premises integration that gives you the option to use a MID Server if the Vulnerability Response Integration with Tenable product and your ServiceNow AI Platform instance are in the same environment. If the Tenable.sc product and your ServiceNow AI Platform instance aren't in the same environment, you're required

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	to use a MID Server. For more information about MID Servers in your instance, see MID Server. • Verify the IntegrationHub plugin is installed and activated. This plugin enables base system components to call external systems using integration APIs and activates protocol steps like REST. Navigate to **System Applications** > **All Available Applications** > **All** and locate the plugin. If not installed in your instance, install and activate it.
☐	Obtain Tenable credentials. Verify you have any account names, passwords, and other service information required by your Tenable products so that you have access to them. Tenable.io requires Administrator access with a permission attribute greater than or equal to 64. Tenable.sc requires Security Analyst or Manager access. **Note:** Starting with v3.8 of Vulnerability Response Integration with Tenable, accessing Tenable.io no longer needs administrator privileges. A basic user with a permission attribute equal to 16 can also access the product.

You're ready to Install the Vulnerability Response Integration with Tenable application using Setup Assistant.

Install the Vulnerability Response Integration with Tenable application using Setup Assistant

Before you run the ServiceNow® Tenable Vulnerability Integration, you need to download the Vulnerability Response Integration with Tenable application from the ServiceNow Store and install and configure it using the Setup Assistant in the Vulnerability Response application.

Before you begin

Before you install the Tenable application, verify you have completed all the items in the checklist in Preparing for the Tenable Vulnerability Integration.

Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

Roles required: admin for initial assignment of the sn_vul.vulnerability_admin role and installing the Tenable application in Setup Assistant. Vulnerability admin (sn_vul.vulnerability_admin or sn_vul.admin (deprecated) to configure the application in Setup Assistant after it is installed.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant** > **Integration application Installation**.

   After a few moments, the applications that are available for installation on your instance are displayed.

2. Locate the **Tenable (Tenable Platform)** tile and click **Install**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This action installs the Vulnerability Response Integration with Tenable application you downloaded from the ServiceNow Store.

3. Follow the prompts provided in the Setup Assistant to continue with the installation.
4. For more information about installing applications using Setup Assistant, see Install Vulnerability Response third-party applications using Setup Assistant.

What to do next

After you complete the installation in Setup Assistant, navigate to **Integration Configuration>Scanner Integrations** in Setup Assistant to continue with the configuration. If you want more information to supplement the prompts provided in Setup Assistant, see Configure the Tenable Vulnerability Integration using Setup Assistant.

Data retrieval settings for the Tenable Vulnerability Integration

The following data retrieval settings help you determine specifically the type and scope of data you want to import from the ServiceNow® Tenable Vulnerability Integration to your ServiceNow AI Platform® instance.

The settings described in the following sections help you control the data you want to import. Additionally, you can set the values of these filters in Integration Instances. To view integration instances, navigate to **Tenable Vulnerability Integration** > **Integration Instances** and select your integration, Tenable.io, Tenable.sc, or Tenable.cs.

On the Integration Instance page that is displayed, select the Integration Instance Parameters to display a list of parameters, or the Vulnerability Integrations tabs for a schedule, REST Details, Integration details, Data Sources, and integration run information.

Common severity and retrieval settings and filters for Tenable.io, Tenable.sc and Tenable.cs in your ServiceNow AI Platform instance

The following settings are available for the Tenable.io, Tenable.sc, and Tenable.cs integrations in your ServiceNow AI Platform instance. These and other configuration settings are displayed on the Integration Instance page of your ServiceNow AI Platform instance. You may prefer to leave these settings in their defaults for the first few integration runs.

Tenable.io

insert_fixed

If you enable the **insert_fixed** flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created for detections in the **Fixed** state that don't exist in your instance.

severity_critical

This filter is enabled by default (true) to receive critical severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_high

This filter is enabled by default (true) to receive high-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_info

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

severity_low

This filter is inactive by default (false). Enable this filter to receive low-level severity Vulnerabilities from the Tenable.io Open Vulnerabilities and Tenable.io Fixed Vulnerabilities Integrations.

size

This setting defines the number of plugin records to include in the result set from the Tenable.io Plugins Integration. Must be in the int32 format. The default value is 1,000. The maximum size is 10,000.

num_assets

The maximum number of vulnerabilities per exported chunk from the Tenable.io Fixed Vulnerabilities and Tenable.io Open Vulnerabilities Integrations. The default value is 50.

chunk_size

Specifies the number of assets per exported chunk by the Tenable.io Assets Integration. The default is 1,000.

Tenable.sc

async_request

This parameter is inactive by default (false). Enable or disable this parameter to make asynchronous or synchronous API calls with Tenable.sc respectively. For synchronous calls, if there's a timeout at 30 seconds, contact support for the Tenable product to tune the box. This parameter once enabled is applicable for all the integrations of Tenable.sc. For existing customers using asynchronous calls, a fix script is available, which adds a new async_request parameter to the existing Tenable.sc integration instances. To view the fix scripts, navigate to **System Definition** > **Fix Scripts**.

insert_fixed

If you enable the **insert_fixed** flag in Setup Assistant for the Vulnerabilities Import integration, new VIs are created fordetections in the **Fixed** state that don't exist in your instance.

offset

Specifies the number of assets, plugins, and vulnerabilities imported in one integration run.

Query filters

Query filters are configured from within the Tenable console. These query filters have IDs that can be selected from Setup Assistant or from the Integration Instances page in your ServiceNow AI Platform instance. These filters are applied while retrieving the data from the Tenable.sc integrations.

Tenable.cs

compute_severity_critical

This filter is enabled by default (true) to receive critical severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_high

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This filter is enabled by default (true) to receive high-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_info

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

compute_severity_low

This filter is inactive by default (false). Enable this filter to receive low-level severity Vulnerabilities from the Tenable.cs Open Cloud Host Vulnerabilities Integration and Tenable.cs Fixed Cloud Host Vulnerabilities Integration.

container_severity_critical

This filter is enabled by default (true) to receive critical severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_high

This filter is enabled by default (true) to receive high-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_medium

This filter is inactive by default (false). Enable this filter to receive medium-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_info

This filter is inactive by default (false). Enable this filter to receive info-level severity Vulnerabilities from the Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

container_severity_low

This filter is inactive by default (false). Enable this filter to receive low-level severity Container Vulnerabilities from the Tenable.cs Open Cloud Container Vulnerabilities Integration and Tenable.cs Fixed Cloud Container Vulnerabilities Integration.

asset_page_limit

This setting defines the number of container asset records to include in the result set from the Tenable.cs Cloud Container Assets Integration. The default value is 1,000. The maximum size is 1,000.

vuln_page_limit

This setting defines the number of vulnerabilities records to include in the result set from the Tenable.cs Open Cloud Host Vulnerabilities Integration, Tenable.cs Fixed Cloud Host Vulnerabilities Integration, Tenable.cs Open Cloud Container Vulnerabilities Integration, and Tenable.cs Fixed Cloud Container Vulnerabilities Integration. The default value is 1,000. The maximum size is 10,000.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

REST messages for the Tenable Vulnerability Integration

The ServiceNow® Tenable Vulnerability Integration REST messages are used to make calls to the Tenable API.

Tenable.io Assets REST message

The Tenable.io Assets REST message retrieves Assets information for the Tenable.io Asset Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve assets information. The export job for assets is submitted with the following filters:

- "is_deleted": false
- "is_licensed": true

Tenable.io Plugins REST message

The Tenable.io Plugins REST message retrieves Plugin information for the Tenable.io Plugin Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve plugins information.

Tenable.io Vulnerabilities REST message

The Tenable.io Vulnerabilities REST message retrieves vulnerability information for both Open and Closed vulnerabilities from the Tenable.io Vulnerability Integration. Changes to the REST message method record impact the requests made to Tenable.io to retrieve vulnerabilities information.

Tenable.sc Queries REST message

The Tenable.sc Queries rest message retrieves the query filter information for the Tenable.sc Asset integration and Tenable.sc vulnerabilities integration where the query filter is configured.

Tenable.sc Plugins REST message

The Tenable.sc Plugin REST message retrieves plugin information for the Tenable.sc Plugins Integration. Changes to the REST message Get Plugins method record impact the requests made to Tenable.sc to retrieve plugins information.

Parameter name	Value	Description
type	active	Indicates the source Tenable pulls data from. Used by code. Changes aren't recommended.
fields	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso,	Indicates the list of fields imported from Tenable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parameter name	Value	Description
	solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	

Tenable.sc Vulnerabilities REST message

The Tenable.sc vulnerabilities REST message retrieves vulnerability information from the Tenable.sc Integration. Changes to the REST message Fetch Vulnerabilities or Fetch Patched Vulnerabilities method or, starting with v14.0 Vulnerability Response and v2.2 of the Tenable Vulnerability Integration, Fetch Backfill Vulnerabilities record impact the requests made to Tenable.sc to retrieve vulnerabilities information.

Tenable.sc Scan Credentials REST message

Tenable.sc Policy REST message

The Tenable.sc policy POST REST message adds a policy for requested plugins. Generated policy is used in Tenable.sc scan requests.

Tenable.sc Scan REST message

The Tenable.sc scan POST REST message adds a scan that is dependent on the access and permission defined in the request body of the rest message. It uses policy, plugin id, and IP(s) in the request body for the scan request.

Tenable.sc Scan Result REST message

The Tenable.sc Scan Result GET REST message provides scan details of the scan generated using the Scan REST message. It uses the scanResultId in the response of the scan REST messages and retrieves scan details for the triggered scan.

Tenable.sc Scan Credentials

The Tenable.sc scan credentials REST message retrieves the credentials information from Tenable.sc. Changes to the REST message 'Import' method record impact the requests made to Tenable.sc to retrieve the credentials information.

Parameter name	Value	Description
fields	id,name,description,type	Indicates the list of fields imported from Tenable.sc
filter	usable	Indicates that the integration pulls only usable credentials from Tenable.sc Changes to either of the parameters isn't recommended.

Tenable.cs GraphQl REST message: The Tenable.cs GraphQl REST message retrieves container asset information, host, and container vulnerability information for Tenable.cs Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Changes to the REST message Fetch Container Assets, Fetch Container Vulnerabilities, Fetch Compute Vulnerabilities method record impact the requests made to Tenable.cs to retrieve asset and vulnerabilities information.

Data transformation for the Tenable Vulnerability Integration

After you identify the data to import, it's retrieved from the Tenable product and processed through a set of data sources and transforms in your instance.

During installation, normalized severity maps are installed in the Normalized Severity Mapping module. These maps transform imported Tenable severity levels to standard severity levels for processing in your instance. For information about creating severity maps, see Create a Vulnerability Response severity map in the Vulnerability Response documentation.

Tenable.io Asset Import

Imported asset data is first loaded into the Tenable.io Asset Import [sn_vul_tenable_io_asset_import] Table.

The Tenable.io Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for `Tenable.io Asset Transform`.

The following table lists the transform map fields by integration.

Tenable.io Asset transform map fields

Source field	Target field	Description
u_id	source_id	Tenable provides a unique id for assets and maps to the discovered item record and is used for CI lookup.
u_ipv4s	ip_address	Maps the first ip value to the ip_address field on the discovered item record.
u_mac_addresses	mac_address	Maps the first mac_address value to the mac address field on the discovered item record.
u_fqdns	fqdn	Maps the first fqdn value to the fqdn field on the discovered item record.
u_netbios_names	netbios	Maps the first netbios value to the netbios field on the discovered item record.
u_plugin.cvss4_base_score	v4_base_score	CVSS v4 base score is mapped to the v4 base score in third party entry record.
u_plugin.cvss4_threat_score	v4_threat_score	CVSS v4 threat score is mapped to the v4 threat score in third party entry record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Asset transform map fields (continued)

Source field	Target field	Description
u_operating_systems	os	Maps the first OS value to the os field on the discovered item record.
(Prior to v14.0 Vulnerability Response and v2.2 of the Tenable Vulnerability Integration)u_last_scan_time	last_scan_date	Maps to the last_scan_date field on the discovered item record.
u_last_authenticated_scan_dat	last_auth_scan_date	Maps to the last_auth_scan_date field on the discovered item record.
[script]	name	Maps the host name using the script's logic.
u_tags		The Tags are saved in sn_sec_cmn_host_tag. The mapping from tags to assets is saved in sn_sec_cmn_m2m_src_ci_tag.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.io Asset transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored.This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.io Plugins Integration

The Tenable.io plugins transform map is used to transform plugins imported from Tenable.io.

Note: Changes to this transform map alters how data received from the Tenable plugins is processed.

To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the Tenable.io Plugin Transform.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The tenable.io plugins payload contains all the fields in the u_attributes column of the sn_vul_tenable_io_plugin_import table. The attributes field is parsed and mapped to the third-party entry table records as listed in the following table.

Source field	Target field	Description
id	id	Maps id from source and adds the TEN-prefix to it. For example, if the id received is 12345, the id in the target table is TEN-12345.
Description	summary	Maps the description of the plugin to the summary column.
[script]	source	The source for imported third-party entry (TPE) is Tenable.io.
[script]	source_instance	Reference to the Tenable deployment that imports this record.
family	category	Maps the family of plugin to the category column
plugin_modification_date	last_modified	Maps the plugin_modification_date to the last modified field.
plugin_publication_date	date_published	Maps the plugin_publication_date to the published date.
has_patch	remediation_type	Maps the remediation type from has_patch value.
synopsis	threat	Maps the threat information about this vulnerability.
cvss_base__score	score	Maps the Common Vulnerability Scoring System (CVSS) base score to the score column in third-party entry table.
solution	solution	Maps the solution provided by scanner to the solution column in the third-party entry table.
exploit_available	exploit	Maps the exploit_available provided by scanner to the exploit column in the third-party entry table.
vpr.score	source_risk_score	Maps the vpr score provided by scanner to the source_risk_score in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
vpr.drivers.age_of_vuln	age_of_vuln	Maps the age of the vulnerability from the scanner to the age_of_vuln column in the third-party entry table.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
vpr.drivers.product_coverage	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
vpr.drivers.threat_sources_last28	threat_sources	Maps threat sources in the last 28 days from the scanner to the threat_sources in the third-party table.
vpr.drivers.threat_intensity_last28	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
vpr.drivers.threat_recency	threat_recency	Maps the threat recency information from scanner to threat_recency in the third-party entry table.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Maps cvss3 impact score to v3_impact_subscore column in the third-party entry table.
cvss_temporal_score	cvss_temporal_score	Maps the temporal score for CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Maps the temporal score for CVSS v3.
risk_factor	source_severity	Maps to the source severity in the third-party entry table.
name	name	Maps the name of the plugin to name in third-party entry table.
stig_severity	stig_severity	Maps the vpr score provided by the scanner to the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		source_risk_score in the third-party entry table.
plugin_type	check_type	Maps the plugin type to check_type in third-party entry table.
unsupported_by_vendor	unsupported_by_vendor	Maps the unsupported_by_vendor field to the unsupported_by_vendor column.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same Common Vulnerabilities and Exposures (CVE) in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.
bid	The list of bug traqs is added as a reference.
see_also	The list of URLs is added as a reference.
xrefs	The list of X-REF is added as a reference.
[script]	The list of exploits for that plugin and inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates the values in the third-party entry, and verify if the third-party entry exists. Based on the results, modifies the values in a third-party entry. This script is for internal use, and modifying or deleting them isn't recommended.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the script is run	Purpose
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

The TenableIOPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from Tenable.io plugins integration and transforms it into ServiceNow AI Platform third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.io plugins data in the third-party entry table.

Tenable.io Vulnerabilities Import

The Tenable.io Vulnerable Item transform map is used to transform open and fixed vulnerabilities information imported from Tenable.io.

Note: Changes to this transform map alter how data from the Tenable Vulnerabilities Import is processed.

The same transform map is used for both the Tenable.io Fixed Vulnerabilities Integration and the Tenable.io Open Vulnerabilities Integration. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the `Tenable.io Vulnerable Item transform map`.

Source field	Target field	Description
u_asset.uuid	id	Uuid is mapped to the id field of the cmdb_ci record.
u_asset.ipv4	ip_address	The ipv4 field is mapped to the ip address field of the cmdb_ci record.
u_asset.last_authenticated_results	last_auth_scan_date	The last authenticated scan date is mapped to the last auth scan date of the cmdb_ci record.
u_asset.mac_addess	mac_address	Mac address is mapped to the host mac address field of the cmdb_ci record.
u_asset.netbios_name	netbios	Netbios is mapped to the netbios field of cmdb_ci record.
u._plugin.cvss3_base_score	v3_base_score	CVSS v3 base score is mapped to the v3 base score of the third-party entry record. These changes will be implemented as part of Tenable 5.2.1 Version.
u._plugin.cvss3_temporal_score	v3_temporal_score	CVSS v3 temporal score is mapped to the v3

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		temporal score in the third-party entry record. These changes will be implemented as part of Tenable 5.2.1 Version.
u._plugin.cvss_base_score	score	CVSS base score is mapped to the score field of the third party entry record.
u._plugin.cvss_temporal_score	temporal_score	Temporal Score is mapped to the temporal score in the third-party entry record.
u_plugin.description	summary	Description is mapped to the summary field in the third-party entry record.
u_plugin.family	category	Maps the family of plugin to the category column of the third-party entry record.
u_plugin.modification_date	last_modified	Last modified date is mapped to the plugin last modified date in the third-party entry record.
u_plugin.publication_date	date_published	Publication date is mapped to the date published field of the third-party entry record.
u_plugin.risk_factor	source_severity	Risk factor is mapped to the source_severity field of the third-party entry record.
u_plugin.solution	solution	Solution is mapped to the solution field of the third-party entry record.
u_plugin.synopsis	threat	Synopsis is mapped to the threat field of the third-party entry record.
u_severity_id	priority	Priority is mapped to the severity id from the payload. The default value is 5.
u_plugin.exploit_available	exploit	Maps the exploit_available provided by the scanner to the exploit column in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
vpr.score	source_risk_score	Maps the vpr score provided by the scanner to the source_risk_score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Maps the age of vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
u_plugin.vpr.drivers.product_coverage	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party entry table.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_plugin.vpr.drivers.threat_recency	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-party entry table.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Maps CVSS3 v3 impact score to v3_impact_subscore column in the third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.type	check_type	Maps the plugin type to check_type in third-party entry table.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Maps the unsupported_by_vendor field in plugin to the unsupported_by_vendor column.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.
U_plugin.on_cisa_kev	cisa_exists	Maps on_cisa_kev field with cisa_exists in third-party entry table.
u_plugin.family_id	Family_id	Maps the plugin Family id to family_id column in third-party entry table.
port	port	Port is mapped to the port field of the vulnerable item record.
protocol	protocol	Protocol is mapped to the protocol field of the vulnerable item record.
u_first_found	first_found	First found is mapped to the first found field of the vulnerable item record.
u_last_found	last_found	Last found is mapped to the last found field of the vulnerable item record.
u_state	state	State is mapped to the State field in the vulnerable item record
[script]	source	The source of the integration is populated. The vulnerable items created from this integration have Tenable.io as the source.
[script]	integration_instance	The integration_instance is the name of the instance from which the vulnerable item is imported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.name	name	Maps the name of the plugin to name in third party entry table.
u_plugin.stig_severity	stig_severity	Maps the stig severity of the plugin to stig severity column in third-party entry table
u_plugin.vpr_v2.malware_observations_intensity_last30	vprv2_malware_observations_intensity_last30	Maps the VPRv2 malware_observations_intensity_last30 value to the vprv2_malware_observations_intensity field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.targeted_industries	vprv2_targeted_industries	Maps the VPRv2 targeted_industries value to the vprv2_targeted_industries field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.targeted_regions	vprv2_targeted_regions	Maps the VPRv2 targeted_regions value to the vprv2_targeted_regions field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.threat_summary	vprv2_threat_summary	Maps the VPRv2 threat_summary value to the vprv2_threat_summary field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.remediation	vprv2_remediation	Maps the VPRv2 remediation value to the vprv2_remediation field in the Tenable TPE Additional Attributes table.
u_plugin.d2_elliot_name	d2_elliot_name	Maps the d2_elliot_name value to the d2_elliot_name field in the Tenable TPE Additional Attributes table.
u_plugin.canvas_package	canvas_package	Maps the canvas_package value

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		to the canvas_package field in the Tenable TPE Additional Attributes table.
u_plugin. checks_for_default_account	checks_for_default_account	Maps the checks_for_default_account value to the checks_for_default_account field in the Tenable TPE Additional Attributes table.
u_plugin.checks_for_malware	checks_for_malware	Maps the checks_for_malware value to the checks_for_malware field in the Tenable TPE Additional Attributes table.
u_plugin.exploitability_ease	exploitability_ease	Maps the exploitability_ease value to the exploitability_ease field in the Tenable TPE Additional Attributes table.
u_plugin.exploithub_sku	exploithub_sku	Maps the exploithub_sku value to the exploithub_sku field in the Tenable TPE Additional Attributes table.
u_plugin.in_the_news	in_the_news	Maps the in_the_news value to the in_the_news field in the Tenable TPE Additional Attributes table.
u_plugin.metasploit_name	metasploit_name	Maps the metasploit_name value to the metasploit_name field in the Tenable TPE Additional Attributes table.
u_plugin.ms_bulletin	ms_bulletin	Maps the ms_bulletin value to the ms_bulletin field in the Tenable TPE Additional Attributes table.
u_plugin.usn	usn	Maps the usn value to the usn field in the Tenable TPE Additional Attributes table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_plugin.version	version	Maps the version value to the version field in the Tenable TPE Additional Attributes table.
u_plugin.vuln_publication_date	vuln_publication_date	Maps the vuln_publication_date value to the vuln_publication_date field in the Tenable TPE Additional Attributes table.
u_plugin.workaround	workaround	Maps the workaround value to the workaround field in the Tenable TPE Additional Attributes table.
u_plugin.workaround_type	workaround_type	Maps the workaround_type value to the workaround_type field in the Tenable TPE Additional Attributes table.
u_plugin.workaround_published	workaround_published	Maps the workaround_published value to the workaround_published field in the Tenable TPE Additional Attributes table.
u_plugin.vendor_unpatched	vendor_unpatched	Maps the vendor_unpatched value to the vendor_unpatched field in the Tenable TPE Additional Attributes table.
u_plugin.has_workaround	has_workaround	Maps the has_workaround value to the has_workaround field in the Tenable TPE Additional Attributes table.
u_plugin.vendor_severity	vendor_severity	Maps the vendor_severity value to the vendor_severity field in the Tenable TPE Additional Attributes table.
u_plugin.vpr_v2.cve_id	vprv2_cve_id	Maps the VPRv2 cve_id value to the vprv2_cve_id field in the Tenable TPE

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		Additional Attributes table.
u_plugin.epss_score	epss_score	Maps the epss_score value to the epss_score field in the Tenable TPE Additional Attributes table.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping can be found in sn_vul_m2m_entry_cve.
bid	The list of bug traqs is added as a reference.
see_also	The list of URLs is added as a reference.
xrefs	The list of X-REF is added as a reference.
[script]	The list of exploits for that plugin and Inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	TTriggers Tenable IO Vulnerabilities Processor which imports data from Tenable.io using the import set and loads each record into the CMDB CI table, the Vulnerable Items table, and the Third-party vulnerability table. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Checks if the Third-Party Entry and Detections exist. If not, these records are created in their respective tables. isn'tThis script is for internal use, and modifying or deleting them is not recommended.
onComplete (when an import set has completed transformation).	Updates the count of CIs, VITs, and Detections as imported from Tenable.io. This script is for internal use, and modifying or deleting them isn't recommended.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results Integration

Tenable.io Compliance Results transform map enables you to import secure configuration assessment findings from Tenable.io into ServiceNow. This integration leverages Tenable's compliance export APIs to retrieve test results on assets, supporting regular differential imports to keep data up to date.

Imported data is first loaded into the Tenable.io Test Results Import [sn_vul_tenable_io_tr_import] table.

To access the transform map, navigate to **System Import Sets** > **Transform Maps**. Search for *`Tenable.io Compliance Results Transform`*.

The following table lists the transform map fields by integration.

Tenable.io Compliance Results fields

Source field	Table	Target field	Description
asset_uuid	sn_vulc_result	sn_sec_cmn_src_ci -> source_id	Unique identifier for the asset in Tenable.io, mapped to the corresponding CMDB CI in ServiceNow after transformation.
first_seen	sn_vulc_result	first_seen	Date and time when the compliance check was first observed on the asset.
last_seen	sn_vulc_result	last_seen	Date and time when the compliance check was last observed on the asset.
audit_file	sn_vulc_policy	short_description	Name or identifier of the audit file used for the compliance check.
check_id	sn_vulc_test	source_id	Unique identifier for the compliance check within Tenable.io.
check_name	sn_vulc_test	short_description	Human-readable name of the compliance check.
check_info	sn_vulc_test	description	Detailed information about the compliance check, including its purpose and context.
expected_value	sn_vulc_result	expected_values	The value expected for the configuration setting according to the compliance policy.
actual_value	sn_vulc_result	actual_values	The actual value found on the asset

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.io Compliance Results fields (continued)

Source field	Table	Target field	Description
			during the compliance check.
status	sn_vulc_result	result	Result of the compliance evaluation. Possible values (from Tenable): PASSED, FAILED.
see_also	sn_vulc_result	remediation	Additional references or links for remediation guidance.
reference.framework	sn_vulc_auth_src	short_description	Compliance framework associated with the check (e.g., CIS, NIST).
reference.control	sn_vulc_citation	section	Specific control or section within the compliance framework.
solution	sn_vulc_test	remediation	Recommended steps to remediate the compliance failure.
profile_name	sn_vulc_citation	section_name	Name of the compliance profile or benchmark applied.
db_type	sn_vulc_technology	name	Database type or technology associated with the compliance check.

Note: Tenable does not provide a risk score for compliance test results. ServiceNow calculates risk scores using Configuration Compliance calculators and applies the default Medium risk value of 20 when no risk score is available. To ensure accurate prioritization, review and customize the risk calculator rules to reflect your organization's priorities.

For more information, see Configuration Compliance calculators and calculator rules.

Tenable.sc Asset Import

Asset data imported from Tenable.sc is first loaded into the Tenable.sc Asset Import table (sn_vul_tenable_sc_asset_import). The Tenable.sc Asset Integration transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable Asset import is Processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for the `Tenable.sc Asset Transform`.

Source field	Target field	Description
u_uuid	id	The uuid isn't populated from the Tenable API, so the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		'u_uniqueness' attribute is used to create a unique uuid field for assets and map it to the cmdb_ci record.
u_ip	ip_address	Maps ip field from API to the ip_address field on a cmdb_ci record.
u_macaddress	mac_address	Maps the mac address field from the API to the address field on the cmdb_ci record.
u_dnsname	fqdn	Maps the dnsname field from the API to the fqdn field on the cmdb_ci record.
u_netbiosname	netbios	Maps the netbios field from the API to the netbios field on the cmdb_ci record.
u_oscpe	os	The OS information is extracted from the oscpe attribute in the payload and maps it to the os field on the cmdb_ci record.
u_lastauthrun	last_auth_scan_date	Maps the lastauthrun field from the API to the last_auth_scan_date field on the discovered item record.
u_lastauthrun and u_lastunauthrun	last_scan_date	The lastauthrun is extracted from the Tenable API or lastunauthrun. The last_scan_date field on the discovered item record is populated based on the value that appears in the payload.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	Initializes the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Updates the values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Sets the values of new CIs created, and CIs that have been updated and ignored. This

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the script is run	Purpose
	script is for internal use, and modifying or deleting them isn't recommended.

Tenable.sc Plugins import

Plugins data imported from Tenable.sc is first loaded into the Tenable.sc Plugins Import table (sn_vul_tenable_sc_plugin_import). The Tenable.sc Plugin Transform Map is used to transform the plugins information that has been imported. Changes to this transform alter how data from the Tenable Plugin import is Processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for `Tenable.sc Plugin Transform Map`.

Source field	Target field	Description
u_id	id	Maps id from source and adds the TEN-prefix. For example, if the id received is 12345, the id in the target table is TEN-12345.
u_description	summary	Maps the description of the plugin to the summary column.
[script]	source	Imported TPE from this integration has Tenable.sc as the source.
[script]	source_instance	Reference to the Tenable deployment that imports this record.
u_family	category	Maps the name field in family object of plugin to the category column.
u_plugin_modification_date	last_modified	Maps the plugin_modification_date to the last modified field.
u_plugin_publication_date	date_published	Maps the plugin_publication_date to published date.
u_has_patch	Remediation_type	Maps the remediation type from has_patch value.
u_synopsis	threat	Maps the threat information about this vulnerability.
u_cvss_base_score	score	Maps the CVSS base score to the score column in third-party entry table.
u_solution	solution	Maps the solution provided by the scanner to the solution column in the third-party entry table.
u_cvss_temporal_score	cvss_temporal_score	Maps the temporal score for CVSS v2.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_cvss_v3_temporal_score	v3_temporal_score	Maps the temporal score for CVSS v3.
u_risk_factor	source severity	Maps to the source severity in the third-party entry table.
u_cvss_v3_base_score	v3_base_score	Maps the CVSS base score in the third-party entry table.
u_exploit_available	exploit	Maps the exploitAvailable provided by the scanner to the exploit column in the third-party entry table.
u_vpr_score	source_risk_score	Maps VPR score from the scanner to the Source risk score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9–10 – Critical • 7–9 – High • 4–7 – Medium • 0–4 - Low
u_vpr_context[id=age_of_vuln]	age_of_vuln	Maps the age of the vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
u_vpr_context[id=product_coverage]	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Maps threat sources in the last 28 days from scanner to threat_sources in the third-party table.
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_vpr_context[id="threat_recency"]	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-part entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Maps CVSS v3 impact score from the scanner to v3_impact_subscore in the third-party entry table.
u_name	name	Maps the name of the plugin to the name column in the third-party entry table.
u_stig_severity	stig_severity	Maps the stig_severity field in the plugin to stig_severity in the third-party entry table.
u_check_type	check_type	Maps the check type to check_type in the third-party entry table.
u_family.id	family_id	Maps the plugin family_id to family_id in the third-party entry table.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third-party entry table is populated based on exploit_available and v3_attack_vector of columns.

In addition to the direct fields, other information is added as related lists to third-party entries.

Source field	Description
u_cpe	The list of CPEs is added as a reference.
u_see_also	The list of URLs is added as a reference.
u_exploit_frameworks	The list of exploits for that plugin and inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Function used to update the values in the third-party entry and verify if the third-party entry exists. Based on the results, modifies the values in a third-party entry. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of Plugins created and ignored. This script is for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the script is run	Purpose
	internal use, and modifying or deleting them isn't recommended.

The TenableSCPluginsImportProcessor script include is called from the onBefore transform script. It takes the output from the Tenable.sc plugins integration and transforms it into ServiceNow third-party vulnerability entries. Any changes to this script include may alter the transformation of Tenable.sc plugins data in the third-party entry table.

Tenable.sc Vulnerabilities import

The Tenable.sc Open Vulnerabilities transform map is used to transform imported data from the Tenable.sc Open Vulnerabilities integration, and the Tenable.sc and Fixed Vulnerabilities transform map is used to transform imported data from the Tenable.sc Fixed Vulnerabilities Integration.

Note: Changes to these transform maps alter how data from the Fixed/Open Tenable Vulnerabilities Import is processed.

To access the Tenable.sc Open and Fixed Vulnerabilities transform maps, navigate to **Tenable Vulnerability Integration** > **Administration** > **Integration Instances** > **Tenable.sc Fixed/ Open Vulnerabilities Integration** > **Data Sources** > **Tenable.sc Open/Fixed Vulnerabilities** > **Tranforms**.

Source field	Target field	Description
u_pluginID	Id	Used as the identifier for the plugin. This field is mapped to the plugin Id in the third-party entry record.
u_riskfactor	source_severity	This field is mapped to source_severity in the third-party entry record.
u_severity	priority	The priority field is mapped with the severity. The default value is 5.
u_hasbeenmitigated	state	Has been mitigated is mapped to the state field of vulnerability record. For the Fixed vulnerabilities integration, all the VIs are in the 'Closed' state.
u_ip	ip_address	Ip address is mapped to the host ip field of cmdb_ci table.
u_port	port	Port is mapped to the port field of the vulnerable item record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_protocol	protocol	Protocol is mapped to the port field of the vulnerfable item record.
u_firstSeen	first_found	The first seen value is mapped to the first found field of the VI record.
u_lastSeen	last_found	The last seen value is mapped to the last found field of the VI record.
u_exploitAvailable	exploit	ExploitAvailable is mapped to the exploit field in the third-party entry record.
u_synopsis	threat	Synopsis is mapped to the threat field in the third-party entry record.
u_description	summary	Description is mapped to the summary field in the third-party entry record.
u_solution	solution	Solution is mapped to the solution field in the third-party entry record.
u_basescore	score	BaseScore is mapped to the score field in the third-party entry record.
u_temporalScore	temporal_score	Temporal Score is mapped to the temporal score in the third-party entry record.
u_cvssv3basescore	v3_base_score	Cvssv3basescore is mapped to the v3 base score in the third-party entry record.
u_cvsstemporalscore	v3_temporal_score	Cvssv3temporal score is mapped to the v3 temporal score in the third-party entry record.
u_pluginpubdate	date_published	Plugin published date is mapped to the plugin published date in the third-party entry record.
u_pluginmoddate	last_modified	Last modified date is mapped to the plugin last modified date in the third-party entry record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_dnsname	fqdn	DnsName is mapped to the FQDN field of the cmdb_ci record.
u_macaddress	mac_address	MacAddress is mapped to the mac_address field of the cmdb_ci record.
u_netbiosName	netbios	NetbiosName is mapped to the NETBIOS field of the cmdb_ci record.
u_ip	ip	IP is mapped to the IP field of cmdb_ci record.
hostUniqueness	uuid	Host uniqueness is not mapped to any field but is used to determine uuid for the host.
u_family	category	Maps the name field in the family object of the plugin to the category column of third-party entry record.
u_plugintext	proof	Plugin text is mapped to proof in tpe record.
[script]	source	The source of the integration is populated. The vulnerable items created from this integration have Tenable.sc as the source.
[script}	integration_instance	The integration_instance is the name of the instance from which the vulnerable item is imported.
u_vpr_score	source_risk_score	Maps VPR score from the scanner to the Source risk score in the third-party entry table.
[script]	source_risk_rating	Maps the vpr score to the standard risk rating based on the score ranges: • 9 - 10 – Critical • 7 – 9 – High

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
		• 4–7 – Medium • 0–4 - Low
u_vpr_context[id=age_of_vuln]	age_of_vuln	Maps the age of the vulnerability from the scanner to age_of_vuln in the third-party entry table.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Maps exploit code maturity from the scanner to exploit_code_maturity in the third-party entry table.
u_vpr_context[id=product_coverage]	product_coverage	Maps product coverage from the scanner to product_coverage in the third-party entry table.
u_vpr_context[id="threat_sources_last_28]	threat_sources	Maps threat sources in the last 28 days from the scanner to threat_sources in the third-party table.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Maps threat intensity in the last 28 days from the scanner to threat_intensity in the third-party entry table.
u_vpr_context[id="threat_recency"]	threat_recency	Maps the threat recency information from the scanner to threat_recency in the third-part entry table.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Maps CVSS v3 impact score from the scanner to v3_impact_subscore in the third-party entry table.
u_pluginname	name	Maps the name of the plugin to name column in third-party entry table.
u_stigseverity	stig_severity	Maps the stig_severity field in the plugin to stig_severity in third-party entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Source field	Target field	Description
u_checktype	check_type	Maps the check type to check_type in third-party entry table.
u_family.id	family_id	Maps the plugin family.id to family_id in the third-party entry table.
[script]	exploit_attack_vector	The exploit_attack_vector column in the third_party_entry table is populated based on exploit_available and v3_attack_vector of columns.

Source field	Description
u_cve	Inserts CVE-related data into the reference table (sn_vul_nvd_entry). If the same CVE in the NVD entry table (sn_vul_nvd_entry) is found, it associates the current vulnerability to the NVD entry. The mapping is found in sn_vul_m2m_entry_cve.
u_bid	The list of bug traqs is added as a reference.
u_cpe	The list of CPEs is added as a reference.
u_seealso	The list of URLs is added as a reference.
u_xrefs	The list of X-REFs is added as a reference.
u_exploitframeworks	The list of exploits for that plugin and Inserts mapping for applicable exploit framework and plugin to sn_vul_m2m_framework_vul.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Function used to update the values in the vulnerability and verify if the vulnerability exists. Based on the results, modifies the values in a vulnerable items table. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of new VIs created, and VIs that have been

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the script is run	Purpose
	updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Asset Import

Imported asset data is first loaded into the Tenable.cs Container Asset Import [sn_vul_tenable_cs_container_asset_import] Table.

The Tenable.cs Container Asset transform map is used to transform the imported assets information. Changes to this transform alter how data from the Tenable.cs Container Asset import is processed. To access this transform map, navigate to System Import Sets > Transform Maps. Search for Tenable.cs Container Asset Transform.

The following tables lists the transform map fields by integration.

Tenable.cs Container Asset transform map fields

Source field	Target field	Description
u_digest	Image_id	Tenable provides a unique digest for the container assets and maps to the discovered container image and docker image record and is used for CI lookup.
u_digest	Image_digest	Tenable provides a unique digest for the container assets and maps to the discovered container image and docker image record and is used for CI lookup.
u_name	name	Maps to the name field of the docker image record.
u_repositoryuri	name	Maps to the container repository record
u_repositoryuri	repo	Maps to the discovered container image record.
u_virtualmachines	host_list	Maps to the discovered container image record
u_labels	Image_labels	Maps the first OS value to the os field o discovered item record.
u_clusters	image_cluster	Maps to the discovered container image record
u_imagetags	tags	Maps to the discovered container image record
u_cloudprovider	cloud_providers	Maps to the discovered container image record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Asset transform map fields (continued)

Source field	Target field	Description
u_accountid	cloud_account_ids	Maps to the discovered container image record
u_region	cloud_regions	Maps to the discovered container image record
u_operatingsystem	os	Maps to the discovered container image record
u_scantime	last_scan_date	Maps to the discovered container image record

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Container Asset transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	This transform is used to initialize the values in the import_set for the integration process. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	A function used to update values in the host and verify if the host exists. Based on the results, modifies the values in an import_set. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	This transform is used to set the values of new CIs created, and CIs that have been updated and ignored. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Vulnerability Import

Imported container vulnerability data is first loaded into the Tenable.cs Container Vulnerability Import [sn_vul_tenable_cs_container_vuln_import] Table.

The Tenable.cs Container Vuln transform map is used to transform the imported container vulnerability information. Changes to this transform alter how data from the Tenable.cs Container Vulnerability Import is processed. To access this transform map, navigate to **System Import Sets** > **Transform Maps**. Search for Tenable.cs Container Vuln Transform.

The following tables list the transform map fields by integration.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
[script]	Image_id	Digest is extracted from the Resource.Id field from the API

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
		and mapped to image_id field of discovered container image and docker image record.
[script]	Image_digest	Digest is extracted from the Resource.Id field from the API and mapped to image_digest field of discovered container image and docker image record.
[script]	name	Repository information is extracted from name field and mapped to docker image and container repository record.
[script]	repo	Repository information is extracted from name field and mapped to discover container image record.
u_resource.Labels	Image_labels	Maps to the discovered container image record
u_resource.CloudProvider	cloud_providers	Maps to the discovered container image record
u_resource. AccountId	cloud_account_ids	Maps to the discovered container image record
u_resource.Region	cloud_regions	Maps to the discovered container image record
u_vulnerability. Id	id	Maps id from source and adds the TEN- prefix. For example, if the id received is 12345, the id in the third party entry table is TEN-12345.
u_vulnerability. Description Id	summaryid	Maps to the third party entry record. or CVE record.
u_vulnerability.Severity	v4_base_severity	Maps to the third party entry record.
u_vulnerability.VprScore	source_risk_score	Maps to the third party entry record.
u_vulnerability.VprSeverity	source_severity	Maps to the third party entry record.
u_vulnerability.AttackVector	v4_attack_vector	Maps to the third party entry record.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Maps to the third party entry record.
[script]	source	he source for imported TPE is Tenable.cs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
u_vulnerability.Id	name	Maps to the vulnerability references record
u_vulnerability. Links	url	Maps to the vulnerability references record
	vulnerability	Reference of TPE or CVE in vulnerability references record
u_software.Name	name	Maps to the container image package record
u_software.Version	version	Maps to the container image package record
u_software.Type	package_type	Maps to the container image package record
u_softwarepaths	path	Maps to the container image package record
u_resolved	status	Maps to the container image finding record
u_firstscantime	first_found	Maps to the container image finding record
u_resource.ScanTime	last_found	Maps to the container image finding record
u_vulnerability.Description	proof	Maps to the container image finding record
u_resolved	state	Maps to the container vulnerable item record
u_firstscantime	first_found	Maps to the container vulnerable item record
u_resource.ScanTime	last_found	Maps to the container vulnerable item record
[script]	source	The source for container vulnerable item record is Tenable.cs.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Container Vuln transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Triggers TenableCS Container Vulnerabilities Processor which imports data from Tenable.cs using the import set and loads each record into the CMDB CI table, the Vulnerable Item table, Third-party Vulnerability Entry table, Vulnerability Reference table, Container

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map script timing and purpose (continued)

When the script is run	Purpose
	Image Package, Container Image Finding, and Container Vulnerable Item. Modifying or deleting isn't recommended.
onBefore (before an import set has completed transformation)	Checks if the third party Entry and Image Findings exist. If not, these records are created in their respective tables. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation)	Updates the count of CIs, VITs, and Findings as imported from Tenable.cs. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Compute Vulnerability Import

Imported host vulnerability data is first loaded into the Tenable.cs Compute Vulnerability Import [sn_vul_tenable_cs_compute_vuln_import] Table.

The Tenable.cs Compute Vuln transform map is used to transform the imported host vulnerability information. Changes to this transform alter how data from the Tenable.cs Compute Vulnerability Import is processed. To access this transform map, navigate to **System Import Sets** > **System Import Sets**. Search for Tenable.cs Compute Vuln Transform.

The following table lists the transform map fields by integration.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
u_resource.Id	object_id	Maps to the CMDB Ci record.
u_resource.Name	name	Maps to the CMDB Ci record.
	asset_category	Cloud is mapped as Asset Category in discovered item record.
U_resource.CloudProvider	cloud_service_provider	Maps to the discovered item record
u_resource.Region	cloud_region	Maps to the discovered item record
u_resource.AccountId	cloud_account	Maps to the discovered item record
u_resource. CloudProvider	cloud_resource_type	Maps to the discovered item record
u_resource.Id	resource_id	Maps to the discovered item record
u_resource.Name	resource_name	Maps to the discovered item record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
u_vulnerability.Id	id	Maps id from source and adds the TEN- prefix. For example, if the id received is 12345, the id in the third party entry table is TEN-12345. Maps id to CVEs as well.
u_vulnerability. Description	summary	Maps to the third party entry record.
u_vulnerability.Severity	v4_base_severity	Maps to the third party entry record.
u_vulnerability.VprScore	source_risk_score	Maps to the third party entry record.
u_vulnerability.VprSeverity	source_severity	Maps to the third party entry record.
u_vulnerability.AttackVector	v4_attack_vector	Maps to the third party entry record.
u_vulnerability.ExploitMaturity	v4_exploit_maturity	Maps to the third party entry record.
[script]	source	The source for imported TPE is Tenable.cs.
u_vulnerability.Id	name	Maps to the vulnerability references record
u_vulnerability.Links	url	Maps to the vulnerability references record
	vulnerability	Reference of TPE or CVE in vulnerability references record
u_resolved	status	Maps to the vulnerable item detection record
u_firstscantime	first_found	Maps to the vulnerable item detection record
u_resource.ScanTime	last_found	Maps to the vulnerable item detection record
u_softwarepaths	proof	Maps to the vulnerable item detection record
u_softwareresolutionversions	solution_summary	Maps to the vulnerable item detection record
u_resolved	state	Maps to the vulnerable item record
u_firstscantime	first_found	Maps to the vulnerable item record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tenable.cs Container Vuln transform map fields (continued)

Source field	Target field	Description
u_resource.ScanTime	last_found	Maps to the vulnerable item record
[script]	source	The source for vulnerable item record is Tenable.cs.

There are three transform scripts executed during the transformation process. The following table lists when each script runs and its purpose.

Tenable.cs Compute Vuln transform map script timing and purpose

When the script is run	Purpose
onStart (when an import set has started transformation)	Triggers Tenable CS Compute Vulnerabilities Processor which imports data from Tenable.cs using the import set and loads each record into the CMDB CI table, the Vulnerable Items table, and the Third-party vulnerability table. This script is for internal use, and modifying or deleting them isn't recommended.
onBefore (before an import set has completed transformation).	Checks if the third-party entry and detections exist. If not, these records are created in their respective tables. This script is for internal use, and modifying or deleting them isn't recommended.
onComplete (when an import set has completed transformation).	Updates the count of CIs, VITs, and detections as imported from Tenable.cs. This script is for internal use, and modifying or deleting them isn't recommended.

Tenable.cs Container Vuln transform map fields

Source field	Target field	Description
u_digest	Image_id	A unique digest provided by Tenable for the container assets. It maps to the discovered container image and docker image record and is used for CI lookup.
u_name	name	Maps to the name field of the docker image record.

Standardized logic for calculating source_risk_score and source_risk_rating

As part of the standardized data-transformation, the Tenable integration uses a centralized business rule to populate both **source_risk_score** and **source_risk_rating**.

During the integration run, if either **vprv1_risk_score** or **vprv2_risk_score** is updated, the system automatically recalculates and populates **source_risk_score** and **source_risk_rating** using the values from the **vprv2_risk_score** and **vprv1_risk_score** fields in the Third-Party Entry table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If **vprv2_risk_score** is present, it takes precedence over**vprv1_risk_score**.
- If the **vprv1_risk_score** and **vprv2_risk_score** are empty, then source_risk_score will not be changed.
- **source_risk_rating** is derived from the finalized **source_risk_score** using the standardized thresholds:
  - 9-10 → **Critical**
  - 7-9 → **High**
  - 4-7 → **Medium**
  - 0-4 → **Low**
  - NaN → **None**

Note: The above changes will be implemented as part of Tenable 5.2.1 Version.

Set additional filter parameters for Tenable.io imports

Customize the filtering parameters for your scheduled queries with the Tenable Vulnerability Integration to help you further refine the vulnerability data you import with the Tenable.io product.

Before you begin

Use cases: As a vulnerability manager or analyst, you might want to filter out data from your queries so that you can review only specific vulnerability details. For example, say you want to view imported vulnerabilities that are filtered by *`cidr_range`*, *`num_assets`*, *`indexed_at`*, and *`plugin_family`*. Or, say you want to run a Tenable.io integration such that one run imports only critical vulnerabilities every four hours, and another runs every 24 hours to fetch all the other non-critical vulnerabilities.

To help you gather this data, you might add tenable-supported parameters to help you import the specific vulnerability details you need.

Without adding additional API calls or coding, this feature permits you to customize your HTTP Request information with Tenable parameters in your ServiceNow AI Platform. The following Tenable.io Integrations support filtering by providing JSON content in the request body:

- Assets Integration
- Fixed Vulnerability Integration
- Open Vulnerabilities Integration

You should know how to use JSON strings for this feature.

Role required: sn_vul.vulnerability_admin

Procedure

1. Locate the parameters supported by the Tenable.io product on the developer site that you want to use for your filtering.

   Parameters and values you enter from the Tenable.io product are supported only at the integration instance level.

2. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
3. On the Tenable Integrations list page, click the record for the Tenable.io integration that you want to open.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. With the Tenable REST methods tab selected, click the information icon (I) for REST method followed by **Open Record**.
5. Select the **HTTP Request** tab.
6. To edit the record, at the top of the page, click the link in, To edit the record click **here**.
7. In the REST Method record in the Content field, enter the JSON content that you want as part of the request body.

   As an example, you might set the severity parameter for imported vulnerabilities as, `{"filters": {"severity": ["critical"]}}` for the Tenable.io Assets Integration so it imports only critical vulnerabilities (CVSS score of 10.0).

   If you want to enter more than one parameter, refer to the Tenable.io documentation for more information about how to separate each value.
8. Click **Update**.

Tenable Vulnerability Integration reporting

View reports about vulnerabilities and vulnerable items on the Vulnerability Response dashboards.

Data visualizations in the Vulnerability Response Workspaces

The Vulnerability Response Workspaces include data visualizations that can help you monitor your remediation progress. You can determine the threat level to your organization by viewing the number and severity of active vulnerabilities that are important to your organization on dynamic data visualizations that are updated as vulnerability data changes. See Vulnerability Response Workspaces, Exploring the Vulnerability Manager Workspace and Exploring the IT Remediation Workspace for more information about the dynamic data visualizations that are available.

Previous versions of Vulnerability Response

The Vulnerability Response overview dashboard (Vulnerability Management) provides an executive view into vulnerabilities and vulnerable items, helping the Vulnerability Admin pinpoint areas of concern quickly. The Vulnerability Response remediation dashboard (Vulnerability Remediation) allows a remediation specialist to focus on the remediation tasks and vulnerable items they own.

See Using the default Vulnerability Response dashboards for more information.

Role required: Remediation owner.

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

to view the dashboard, navigate to **Vulnerability Response** > **Remediation Overview**.

Integration run status chart for the Tenable Vulnerability Integration

The Tenable Integration Run Status module provides you with a graphical view of the status of Tenable integration runs.

In the chart, point to any part of the graph to display a summary of data specific to that part. If you click any part on the bar graph, a list opens to provide more detailed information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: Vulnerability admin.

Persona and granular roles are available to help you manage what users can do and see in the Vulnerability Response application. For initial assignment of the persona roles in Setup Assistant, see Assign the Vulnerability Response persona roles using Setup Assistant.

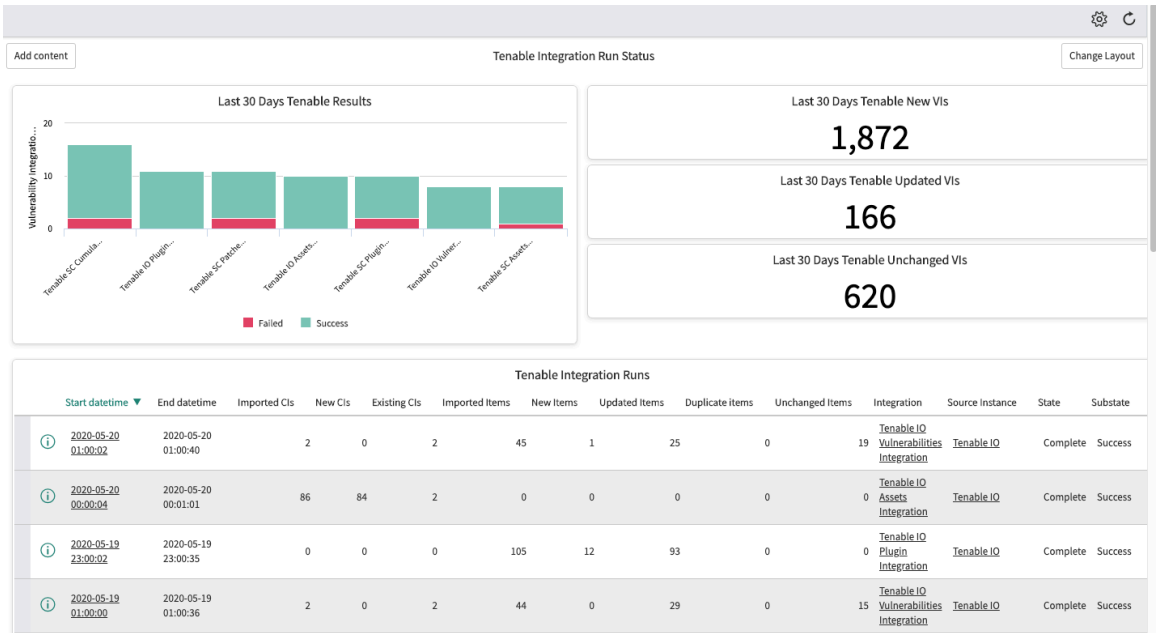
For more information about managing granular roles, see Manage persona and granular roles for Vulnerability Response.

To view the data, navigate to **All** > **Tenable Vulnerability Integration** > **Integration Run Status**.

Starting with version 19.0 of Vulnerability Response, this dashboard is available in the New Experience UI.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

Run status



Tenable integration run status chart reports

Name	Description
Last 30 days Tenable Results	The number of integration runs completed for each integration. Shows both successful and failed runs. Each run displayed as a bar in the graph.
Last 30 Days Tenable New VIs	The number of new vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Tenable Updated VIs	The number of updated vulnerable items imported in the last 30 days. Shown as an integer.
Last 30 Days Tenable Unchanged VIs	The number of duplicate vulnerable items imported in the last 30 days. Shown as an integer.
Tenable Integration Runs	The integration run records in a list.

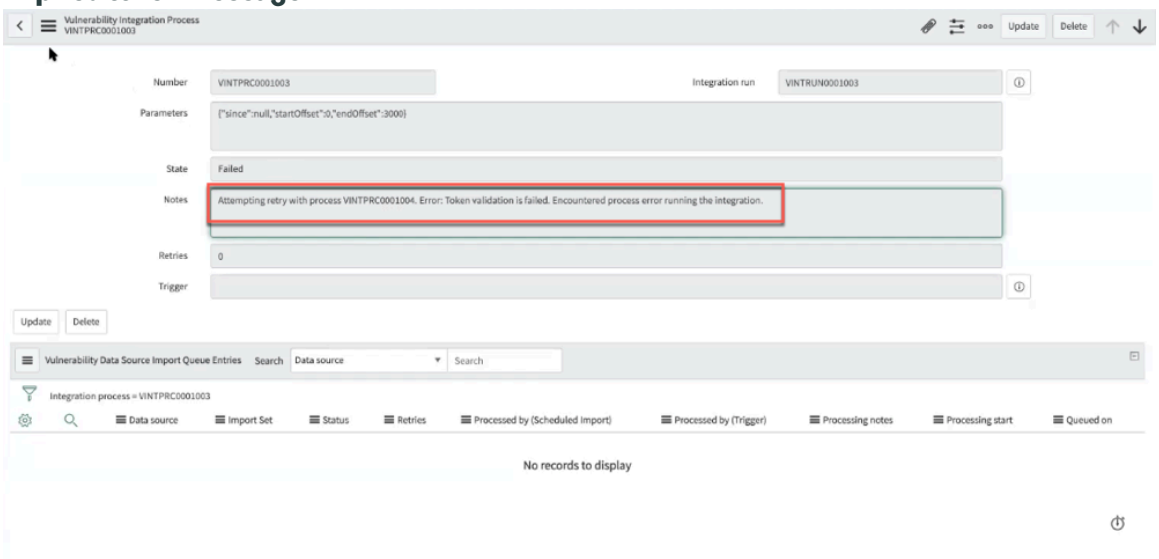
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	Note: V16.1: To verify detections for this integration, compare the detections or findings with the ServiceNow detection data in the *sn_vul_detection* table. While the integration is in progress, there might be a change in the detection or findings count. This report displays the count of detections in the 'Till date count' column in the instance, after the completion of the integration run.

Token validation expiration

If a Tenable.sc integration run fails for any reason, the authentication token for Tenable.sc automatically expires and a message is displayed on the Vulnerability Integration Process record.

Expired token message



A new token is automatically generated for the next integration process. All the integration processes, failed and successful, are displayed on the Vulnerability Integration Process tab on the Vulnerability Integration Process record.

Initiate rescan for the Tenable.sc integration

Verify your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Tenable platform. You can initiate a rescan on-demand for vulnerable items for the Tenable.sc product from your ServiceNow AI Platform® instance.

Before you begin

Roles required: sn_vul.write_all or sn_vul.write_assigned

Note: Tenable.sc does not support launching rescan on agent based machines.

Verify your scanner is activated before you begin. Navigate to **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.

About this task

To initiate rescan from the workspaces, see Rescan Tenable.io and Tenable.sc vulnerable items from the Vulnerability Response workspaces.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Follow the steps listed below to initiate a rescan in the classic environment.

To help reduce the overhead and volume involved with scheduled, full scans, remediation owners, IT specialists, vulnerability analysts, or vulnerability managers can initiate targeted rescans on-demand for specific vulnerabilities on assets (configuration items) in their environments. You can initiate rescans from vulnerable item (VI), remediation tasks (RT)s, third-party entry (TPE), or discovered item records from your ServiceNow AI Platform instance.

Rescans permit your remediation owners and vulnerability analysts to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

As an example, your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Tenable.sc vulnerable items.

Note: When requesting rescan from your ServiceNow AI Platform® instance, selecting the Vulnerability Response Integration with Tenable credentials is optional. The ServiceNow® Tenable.sc Scan Credential Integration imports and updates scanner credentials from the Tenable.sc product in your instance. This integration runs weekly to import and securely store your Tenable credentials data.

Note that this imported data does not include Tenable passwords or other sensitive Tenable account information. The ServiceNow® Tenable.sc Scan Credential Integration is enabled (`Active`) automatically from within the Setup Assistant in your instance when you configure the Tenable.sc Vulnerabilities integrations (Tenable.sc Open and Fixed Vulnerabilities Integrations).

Note the following information about the credentials you import so that your users can see them as needed from your ServiceNow AI Platform instance:

- Credentials created with the Tenable.sc administrator user role are available to users across all your organizations.
- Credentials created with the Tenable.sc organizational users role are only available to users within that organization. These credentials are not imported into the ServiceNow AI Platform for users outside of the creator's organization unless they are shared with the user's account being used to connect to the instance.

See the Tenable.sc documentation website for more information.

See Configure the Tenable Vulnerability Integration using Setup Assistant for more information about configuring the Tenable.sc application. To view more information about the Scan Credential Integration, navigate to **All** > **Tenable Vulnerability Integration** > **Integrations** > **Tenable.sc Scan Credential Integration**.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: You can only initiate rescans for VIs with Tenable.sc as the source. Verify Tenable.sc is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the **Personalize List** icon (Gear icon) and use the Slushbucket to move **Source** from **Available** to **Selected**.

3. Alternatively, navigate to **All** > **Vulnerability Response** > **Remediation Tasks** or **Vulnerability Response** > **Libraries** > **Third-Party** for the remediation task or third-party entry records, respectively, that you want to use for the rescan.

   Depending on your choice, the **Rescan** button is available on the following records:

   - On a single VI record, the VI must be from the Tenable.sc product and in any state other than **Closed**. For multiple VI records, all the VIs must be from the Tenable.sc product and in any state other than **Closed**.
   - On an RT record, the remediation task can be in any state other than **Closed**, and all the associated VIs must be from the Tenable.sc product.
   - On a third-party entry (TPE) record, the record must have at least one associated VI record from the Tenable.sc product in any state other than **Closed**.

4. In the upper right of the record, click **Rescan**.
   You are prompted to choose the scanner credentials to access the scanner. These are the credentials imported by the Tenable.sc Scan Credential Integration.
5. In the dialog, select the filters and credential types you want.
6. Click **Request Scan**.

   A message is displayed that indicates your scan is being processed. Status for all rescans can be found at any time under the Scan related lists on the VI, RT, TPE records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

   The State field on the parent scan record is marked as complete after all the child scans are successfully completed. The child scans import data. The parent scan record is a container for the child scans.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to **Closed/Fixed** are imported with the next scheduled import of the Tenable.sc Fixed Vulnerabilities Integration.

Initiate rescan for the Tenable.io integration

Verify that your vulnerable items have been remediated between scheduled scanning cycles by initiating rescans in the Tenable platform. You can initiate a rescan on-demand for vulnerable items for the Tenable.io product from your ServiceNow AI Platform® instance.

Before you begin

Roles required: sn_vul.write_all or sn_vul.write_assigned

Verify your scanner is activated before you begin. Navigate to **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.

About this task

- See and Rescan records and remediation tasks in the Vulnerability Manager Workspace and Rescan vulnerable items and remediation tasks in the IT Remediation Workspace to initiate a rescan in the Vulnerability Response workspaces.
- Follow the steps listed below to initiate a rescan in the classic environment.

Note: Tenable.io does not support launching rescan on agent based machines.

To help reduce the overhead and volume involved with scheduled, full scans, as a remediation owner, IT specialist, vulnerability analyst, or vulnerability manager, you can initiate targeted rescans on-demand. you can scan for specific vulnerabilities on assets (configuration items) in your environments. You can initiate rescans from vulnerable item (VI), remediation tasks (VUL), third-party entry (TPE), or discovered item (SDI) records from your ServiceNow AI Platform instance. Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When requesting rescan from your ServiceNow AI Platform® instance, selecting the Vulnerability Response Integration with Tenable credentials is optional. The ServiceNow® Tenable.io Scan Credential Integration imports and updates scanner credentials from the Tenable.io product in your instance. This integration runs weekly to import and securely store your Tenable credentials data.

Note that this imported data does not include Tenable passwords or other sensitive Tenable account information.

The following information describes the credentials you import so that your users can see them as needed from your ServiceNow AI Platform instance:

- Credentials created with the Tenable.io administrator user role are available to users across all your organizations.
- Credentials created with the Tenable.io organizational users role are only available to users within that organization. These credentials are not imported into the ServiceNow AI Platform for users outside of the creator's organization unless they are shared with the user's account being used to connect to the instance.

  See the Tenable.io documentation website for more information.

- The Tenable.io Template Integration and the Tenable.io Scan Credential Integration are required to be activated prior to initiating rescans. To view more information about the Scan Credential Integration, navigate to **Tenable Vulnerability Integration** > **Integrations** > **Tenable.io Scan Credential Integration**.

  By default, the Template and scan Credential Integrations are deactivated. When you enter your credentials for Tenable.io, all Tenable.io integrations are automatically activated. To manually activate or deactivate these integrations:

  1. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
  2. On the list that is displayed, locate the Tenable.io integration records you want.
  3. Open each record and select the **Active** check box to activate the integration.
  4. Click **Update** to save your changes.
  5. Return to the Setup Assistant to continue with your configuration for the Tenable Vulnerability Integration with Vulnerability Response.

See Configure the Tenable Vulnerability Integration using Setup Assistant for more information about configuring the Tenable.io and Tenable.sc products.

Say your entire environment is scanned once every three weeks. The most recent full scan was completed a week ago, but you applied a patch yesterday to fix a critical vulnerability. Due to the nature of this vulnerability, you cannot wait two weeks for the next scheduled scan to verify that it has been remediated. To verify that your patch successfully fixed a critical vulnerability discovered during an earlier scan, you can initiate a targeted rescan from your ServiceNow AI Platform for Tenable.io vulnerable items.

You can view updated results on the records you initiated the scans from after the next scheduled import of the Fixed Vulnerabilities Integration.

During integration execution, multiple processes are generated, and data is received in the form of pages. Each process can contain one or more import queue entries with attached data in pages. These entries must process the data within the one-hour time limit. However, if the payload size is large, the processing time may exceed one hour or get stuck, resulting in an integration timeout error. The integration continues to process the data despite the timeout error. To avoid this miscommunication, starting from version 18.2.4 of Vulnerability Response, timestamps (heartbeats) are sent periodically to indicate if the queue is active and processing

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

data. The **Last Record Processed** field in the Import Queue Entry page is updated based on the count of records the import queue creates or updates. In case an import queue entry exceeds the one-hour time limit, the system checks the **Last Record Processed** field to see if it is also older than one hour. If it is, this indicates that the import queue entry is stuck, and it is timed out to prevent any further delays in processing.

Note: The **Last Record Processed** field is updated based on what is defined in the following system properties:

- *sn_sec_cmn.record_threshold_heartbeat*: Defines the number of processed records, after which the heartbeat (timestamp) is sent to the import queue entry.
- *sn_sec_cmn.maximum_heartbeat_delay*: Defines the time after which the import queue entry must be timed out.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerable items**.
2. Locate the vulnerable item record that you want to trigger a rescan from and open it.

   Note: If you are using the Tenable.io Scanner, you can only initiate rescans for VIs with Tenable.io as the source. Verify Tenable.io is displayed in the **Source** column on the VI List views, or in the **Source** fields on individual records. You can use the condition builder to group VIs by Source. Or, if the Source column is not displayed on the VI List view, in the upper left of the list, click the **Personalize List** icon (Gear icon) and use the Slushbucket to move **Source** from **Available** to **Selected**.

3. Alternatively, navigate to **All** > **Vulnerability Response** > **Remediation Tasks** or **Vulnerability Response** > **Libraries** > **Third-Party** for the records that you want to use for the rescan.

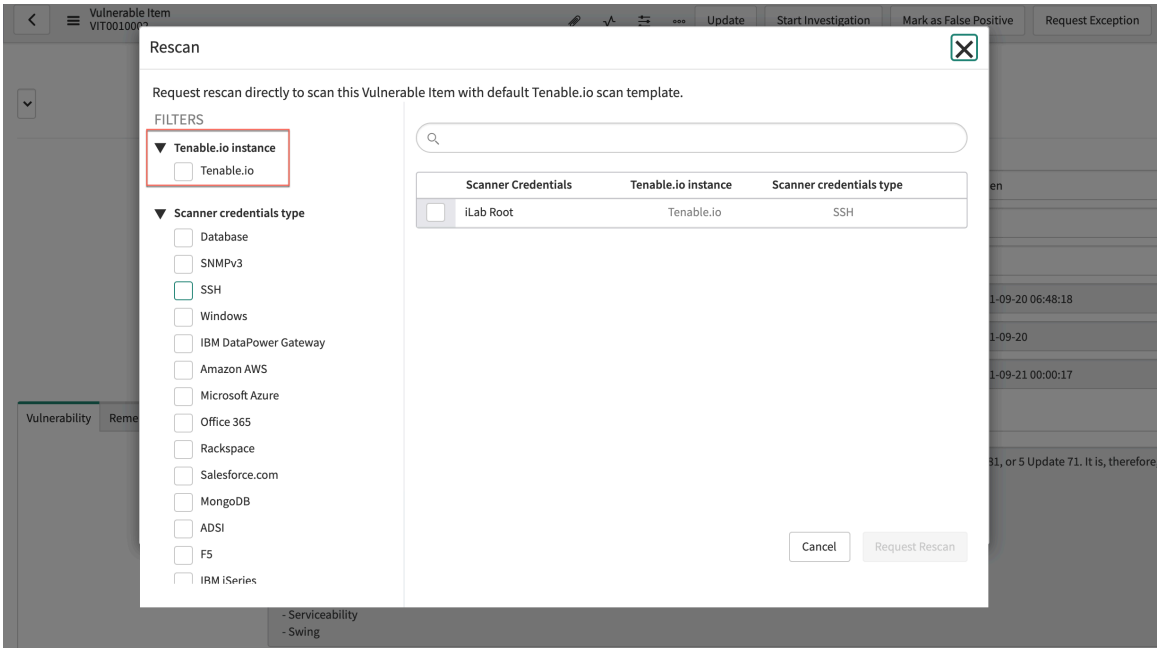
   Depending on your choice, the **Rescan** button is available on the following records:

   - On a single VI record, the VI must be in any state other than **Closed**. For multiple VI records, all the VIs must be from the Tenable.io product and in any state other than **Closed**.
   - For remediation task records, only remediation tasks in any state other than **Closed** are supported. All the associated VIs must be in any state other than **Closed** and use Tenable.io as the source.
   - On a third-party entry (TPE) record, the record must have at least one associated VI record from the Tenable.io product in any state other than **Closed**.
   - On Discovered Items records, the record must have at least one associated VI record from the Tenable.io product in any state other than **Closed**.
   - From the Vulnerable items list, you can select individual vulnerable items that you want to rescan. Use the Actions on selected rows menu in the lower left of the screen to launch the rescan. You are prompted to enter your credentials.

4. In the upper right of a record, click **Rescan**.
   You are prompted to choose the instance or instances for the rescan and the scanner credentials you want to use to access the scanner. The displayed credentials are those imported by the Tenable.io Scan Credential Integration.
5. In the dialog, select the instance and or instances and the credential types that you want to use.

   In the following image, one integration instance, `Tenable.io` is displayed. If you have more than one Tenable.io instance, they are all displayed under the `Tenable.io` section on the form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Field	Description
Tenable.io instance	Choose a Tenable.io integration instance that you want to initiate the rescan from. All your integration instances for Tenable.io are displayed. If a VI exists in more than one integration instance, you can use this filter to limit or expand the instances you want to scan. **Note:** If you choose to rescan VIs from a remediation task record for a single in tegration instance, only the active VIs that are associated with that remedia tion task, for that instance, using the cre dential(s) that you select are scanned.
Scanner credentials type filter	Use this filter to display credentials by type.
Pane with Scanner Credentials, Tenable.io instance, Scanner credentials type	These are the available scanner credentials imported from the Tenable.io products. Choose one or more credentials to use for the scan.

6. Click **Request Rescan**.

   A message is displayed that indicates your scan is being processed and a parent scan record is created. Status for all the child scans can be found at any time under the Scan related lists on the VI, remediation task, TPE, and SDI records you used to launch the rescans. In the message, click **View details** to view the status of the rescan and view any other rescans launched from a given record.

   The State field on the parent scan record is marked as complete after all the child scans are successfully completed. The child scans import data. Each scan supports a unique

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

combination of integration instance, TPE, IP, and Network ID. You might see multiple child scans on a parent scan record. For example, the maximum number of IP Addresses a child scan can support is 1000. If there are 1002 IPs for a vulnerable item, two child scans are created and listed on the Scans related list to support the request. The parent scan record is a container for the child scans and its state of reflects the status of the child scans.

Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first. The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped. All VIs that have transitioned, or will transition, to **Closed/Fixed** are imported with the next scheduled import of the Tenable.io Fixed Vulnerabilities Integration.

For scans that error out, you can check the child scans on the parent scan record. View the error in the response payload of the child scan.

You can view updated results on the records you initiated the scans from after the next scheduled import of the Fixed Vulnerabilities Integration.

Update configuration items with the network partition identifier for the Tenable Vulnerability Integration

Create unique configuration items (CIs) for assets in your environment that share IP addresses. Identify the distinct assets across your environment and automatically update the CIs on your existing discovered item, vulnerable item, and detection records to give you more details about your vulnerabilities.

Before you begin

Role required: admin

About this task

By default in the Vulnerability Response application, one way to identify your assets is by IP address. In certain cases, assets can share IP addresses, but they are stored as one CI in your CMDB.

For example, as shown in the following tables, multiple assets (CI)s in your environment can share IP addresses but have unique network and repository ids. However, by default, these assets are typically identified and stored as a single CI `(CI 1)` during the IP address lookup.

Default IP lookup and CI creation

Source	IP address	Network_id	Configuration item
Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	IP address	Repository_id	Configuration item
Tenable.sc: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can create individual CIs for assets that have the same IP address so that you can identify them as distinct assets. Starting from a fresh data import, you can update your existing CIs with more granularity that includes the network partition identifier [network_partition_identifier] by running the scheduled job, *`Update existing discovered items with network partition identifier`*.

This scheduled job is deactivated by default. Activate this feature for the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products in the Setup Assistant to view this identifier on your records.

When activated, this scheduled job adds the Network Partition Identifier [network_partition_identifier] to existing CI records from imported data. Existing CIs created by the IRE are also updated. The scheduled job also creates CIs that include the network partition identifier starting with the next import. Alternatively, you can launch the job on-demand to update your existing data.

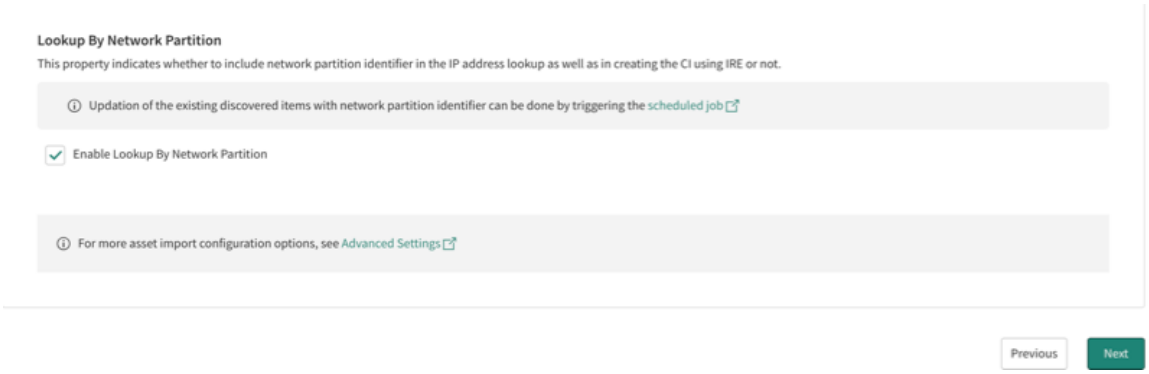
When you upgrade starting with v14.0 of Vulnerability Response and v2.2 of the Tenable Vulnerability Integration, the CMDB CI Class Models (1.0.21.) is supported. The class models have the network partition identifier [network_partition_identifier] in the Identification and Reconciliation (IRE) identification rules.

Option	Description
Run the scheduled jobs on-demand.	Update your existing discovered items. CIs for your existing Tenable data are created or updated to include the network partition identifier granularity. Discovered items, vulnerable items, and detection records are all updated with the new CIs.
Wait for imports of fresh data from the integrations with the next scheduled jobs.	Create CIs for each new asset using the network partition identifier starting with the next scheduled job. CI, vulnerable item, and detection records are all updated to include the new granularity. New CIs are created when an exact match is not found.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Setup Assistant** > **Integration Configuration** > **Scanner Integrations**.
2. Select Tenable.io integrations or Tenable.sc integrations.
3. **Edit** the required integration.
4. Select **Asset Import Configuration**.
5. Select **Enable Lookup By Network Partition** check box from the **Enable Lookup By Network Partition** section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Click **Next**.

Network partition identifiers NETWORK_ID and REPOSITORY _ID are included and update existing CIs or create CIs with the next scheduled job.

Network partition identifier attribute included in IP lookup and CI creation

Source	IP address	NETWORK_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Tenable.io: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	IP address	REPOSITORY_ID	CI for assets without network partition identifier	CIs Assets with network partition identifier
Tenable.sc: Assets and Fixed and Open Vulnerabilities Integrations	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

With the next scheduled job, the IP Address and Incomplete IP Address CI identification lookup rules include the network partition identifier attribute automatically for a data import from the Assets and Fixed and Open Vulnerabilities Integrations for the Tenable.io and Tenable.sc products.

After you enable the system property and save the records, you alternatively can update your existing discovered items with CIs that include the network partition identifier by launching the scheduled jobs on-demand.

Import modifications for the Tenable Vulnerability Integration

Configure optional modifications and streamline some of the data specifically for the Tenable Vulnerabilities import integration in the ServiceNow® Tenable Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_admin

About this task
This set of tasks requires coding and advanced knowledge about the ServiceNow AI Platform.

Follow these steps to create domain-separated imports for the Tenable Vulnerabilities Integrations. The following example is for the Tenable.io Open Vulnerabilities integration, but this content is applicable to the other Tenable integrations.

Procedure
1. Create a domain.
2. For every domain you create, create a user and assign the user to that domain.

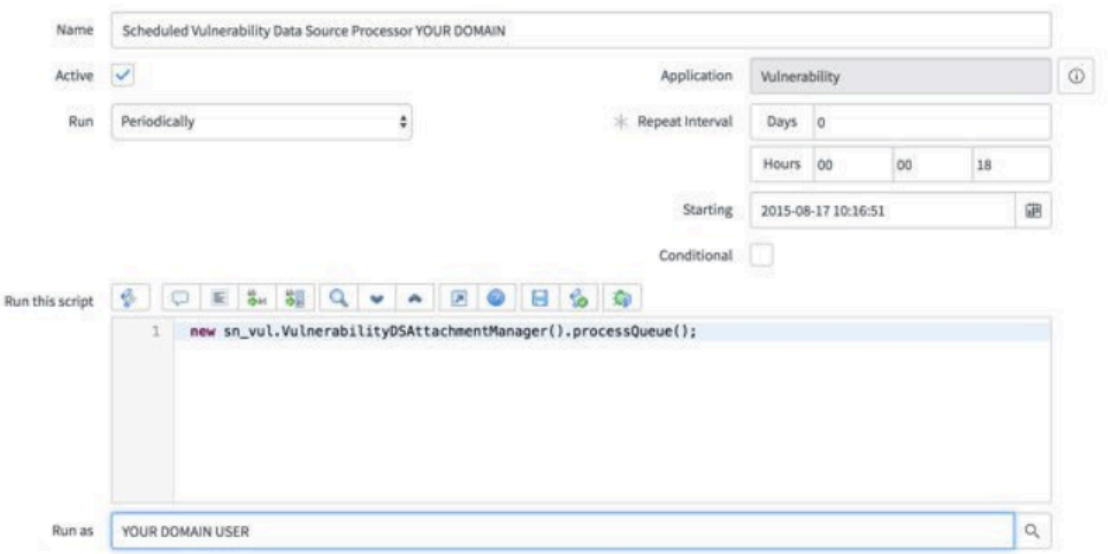
   Think of this user as a run_as placeholder for the domain in Tenable.io.

3. Open Vulnerabilities Integration.
   The user is the equivalent to the VR.System user in the global domain and must have the following roles: sn_vul.tenable_configure_integration, import_admin, and sn_vul.vulnerability_write. This user requires access to data sources, transform maps, and vulnerability data.

   Note: Consider this user as specific to this role. The user should not have any other purpose

4. In each domain, create a scheduled job by copying Scheduled Vulnerablity Data Source Processor found under **System Definition** > **Scheduled Jobs**.
5. Append the domain to the name to identify the scheduled job.
6. Change the run_as user to the user you created in the previous step.

   Note: Edit the following UI action so that the integration runs in the run_as user domain.



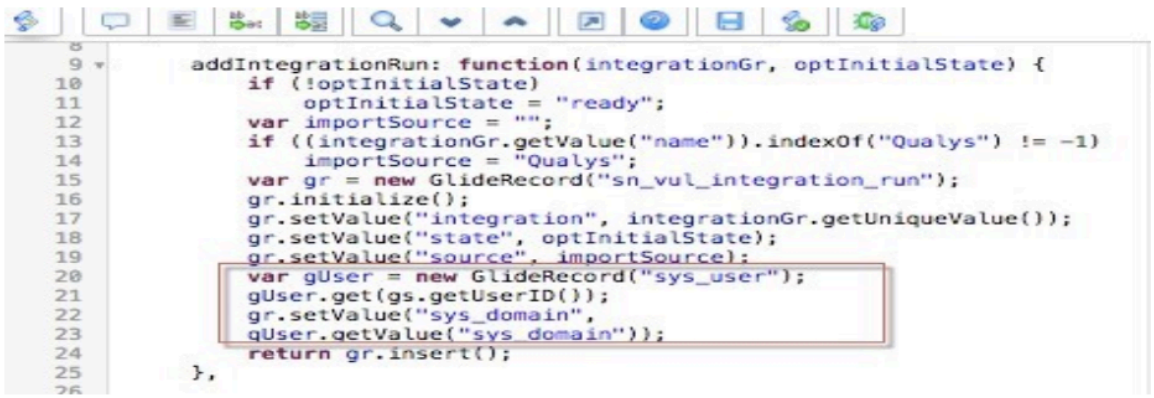
7. Edit the Execute Now UI action in the Tenable.io Open Vulnerabilities Integration to add this code block to the top of the file.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
//sys id below is of Tenable.io integration if(current.sys_id
== "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as =
gs.getUserID(); }
```

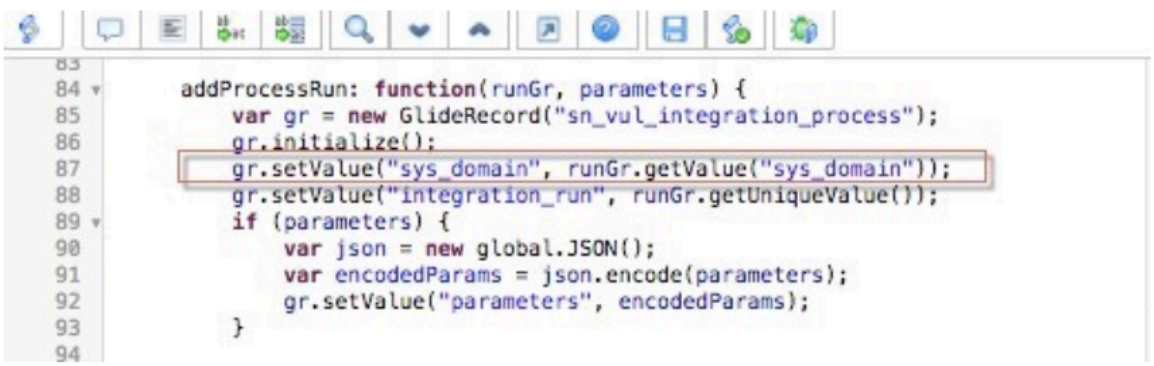
Note: Edit the following script includes so that integration runs in the run_as user domain.

8. Edit the VulnerabilityIntegrationUtils script include method addIntegrationRun to add the highlighted code.



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edit the VulnerabilityIntegrationUtils script include method addProcessRun to add the highlighted code.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edit the DataSourceVulnReportRefreshProcessor script include method _processFromDataSourceGroups to change this original code: Original _processFromDataSourcesGroups code to Edited _processFromDataSourcesGroups code.
11. Edit the VulnerabilityDSAttachmentManager script include method, queueItem to add the following highlighted code blocks queueItem, _getNext, _processQueueEntry function.

    You are ready for domain-separated host detection imports.

    Disable calculators prior to import

    Follow these steps to disable the default calculator if not used. If you do not use vulnerability calculators, it is best to disable the default calculators in addition to any others you have defined. Vulnerability calculators run every time a vulnerable item record is accessed and can impact instance performance.

    Role required: sn_vul.vulnerability_admin.

12. Navigate to **All** > **Vulnerability** > **Administration** > **Vulnerability Calculators**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

13. Open the Vulnerability Impact group.
14. Open the Score and Service Based Impact calculator.
15. Deselect the Active field to deactivate the calculator.
16. Click Update.

    You have disabled the default calculator.

    Disable notification-based business rules prior to initial import

    Follow these steps to disable Disable notification-related business rules prior to initial record import. During the initial import of records, certain notification-related business rules can generate many notifications, impacting performance. These business rules should be modified to disable them during the import.

    Role required is sn_vul.vulnerability_admin.

17. Navigate to **All** > **System Definition** > **Business Rules**.
18. Search for Affected ci notifications.
19. Open the business rule and insert the following condition: `current.sys_class_name != "sn_vul_vulnerable_item"`.
20. Click **Update**.
21. Repeat this procedure for the following business rules:
    - Affected cost center notifications
    - Affected group notifications
    - Affected location notifications

    Note: After the completion of the initial record import, you have the option of re-enabling these business rules. However, consider leaving them disabled. They can generate large numbers of notifications and impact the performance of your instance.

    Modify an initial start date

    Follow these steps to Modify an initial start date. During installation using Setup Assistant, you set an initial start date for the Tenable integrations. You can reset that start date in Setup Assistant or from the primary integration as shown in the following steps.

22. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Integrations**.
23. Click any integration.
24. Click Integration Details.
25. Set the Start time field to a value in the past, so all scanned and detected vulnerabilities since that time are detected.

    If you configured Tenable using Setup Assistant, the Start time field is pre-populated, initially to three months prior today's date, and subsequently to today's date. Note: Consider setting the value to a maximum of a month in the past. This keeps large amount of data from exceeding the Tenable API rate limitations, as well as triggering execution timeouts.

26. Click **Submit** or **Update**.
27. **Optional:** Click **Execute Now** to run immediately.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Split Tenable detections based on the vulnerability instance to split vulnerable items

ServiceNow® Vulnerability Response enables the splitting of detections from Tenable scanners, enabling for the creation of a unique vulnerable item (VIT) for each detected vulnerability instance. This split enables the assignment of VITs to various remediation teams, enhancing the management and tracking of vulnerabilities.

Before you begin

Role required: admin

About this task

The Tenable scanner's payload contains detection data, with each path within the proof used to split the detections. The output tag in the payload identifies the vulnerability's location, facilitating accurate identification and management of vulnerabilities according to their specific paths.

After a plugin is added to the [sn_vul_proof_key_vulnerability] table, run the integration to split existing VITs. To verify, inspect the VITs for distinct detection paths.

Scenario 1: Detection exists before plugin is added

- Before Adding Plugin: Detection A with 4 file paths → VIT1
- After Adding Plugin & Ingestion Run: The existing VIT is updated with new proof, and three additional VITs are created.
- Closure Behavior: If a path is no longer seen in Tenable data, ServiceNow closes the corresponding detection and its VIT using a hash-based comparison of the file path.

Scenario 2: Detection ingested after plugin is added

Detections are split during ingestion.

Note: Splitting occurs automatically during the ingestion run after plugin configuration.

Procedure

1. In the Third-party Integrations table [sn_sec_int_integration], set the **Include proof in VI key** column value to true for Tenable.io, Tenable.sc, and Tenable.cs.
2. Navigate to **All** > **Vulnerability Response** > **Administration** > **Configure VI granularity**.
3. For Tenable.cs product, navigate to **Detection Key Configuration** [sn_vul_detection_key_config] table, select Tenable.cs record and update,
4. **Optional:** On the Include port form, select the **Include port** check box and select the **click here** link (applies only to Tenable.io and Tenable.sc).
5. On the Add proof to VI keys list, select **New**.
6. On the Add proof to the VI key- New record form, in the **Vulnerability** field, add the Tenable ID for which you want to include the proof.

   Note: You can split the detections based solely on path information or by combining path and version details. For additional details, refer to the section 'Splitting detections from Tenable scanners' on this page.

7. In the **Regular Expression to Split Tenable VITs** field:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Split the detection based on only the path by entering Path\s+:\s+([A\n]+).
- Split the detection based on path and installed and fixed versions by entering Path\s+:\s+([A\n]+)\n\s+Installed\s+version\s+:\s+([A\n]+)\n\s+Fixed\s+version\s+:\s+([A\n]+).

8. Select **Submit**.

Example: Splitting detections from Tenable scanners

The following detection from a Tenable scanner shows proof in the output tag that includes both path and version information.


```
{
  "results": {
    "asset": {
      "agent_uuid": "92124caabdb9459baa9d053186df48b9",
      "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df",
      "device_type": "aws-ec2-instance",
      "fqdn": "ip-ac0a0004.secops.com",
      "hostname": "ip-ac0a0004",
      "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
      "ipv4": "18.220.145.158",
      "last_authenticated_results": "2024-05-17T03:34:04.424Z",
      "mac_address": "0a:3e:8b:ed:63:e6",
      "netbios_name": "IP-AC0A0094",
      "operating_system": [
        "Microsoft Windows Server 2019 Datacenter Build 17763"
      ],
      "network_id": "00000000-0000-0000-0000-000000000008",
      "tracked": true
    },
    "output": "\n  Path: C:\\Program Files (x86)\\Common
 Files\\Oracle\\Java\\javapath_target_1190440625\\\n
 Installed version : 1.8.0_361.9\n Fixed version : Upgrade
 to version 8.0.401 or greater\n  Path : C:\\Program
 Files\\Java\\jre1.8.0_361\\\n  Installed version :
 1.8.0_361.9\n  Fixed version : Upgrade to version 8.0.401 or
 greater\n  Path : C:\\Program Files\\Java\\jdk1.8.0_351\\\n
 Installed version : 1.8.0_351.10\n  Fixed version : Upgrade to
 version 8.0.401 or greater\n"
    "plugin": {
      "bid": 123456,
      "checks_for_default_account": false,
      "checks_for_malware": false,
      "coe": "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b",
      "cvSs3_base_score": 7.8,
      "cvss3_temporal_score": 7.0,
      "cvss3_temporal_vector": {
        "exploitability": "Proof-of-Concept",
        "remediation_level": "Official Fix",
        "report_confidence": "Confirmed",
        "raw": "E:P/RL:O/RC:C"
      }
    }
  }
}
```


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure Tenable test result granularity

Configure the Tenable test result granularity to ensure the system imports results at a more detailed level based on your selected configuration keys. In addition to the default keys, you can configure additional keys based on your requirements to increase granularity. Granular imports allow teams to manage their respective assets independently and prevent data from being overwritten when multiple records share common identifiers.

Before you begin

Role required:

- sn_vulc.admin

Procedure

1. Navigate to **All** > **Tenable Vulnerability Integration** > **Administration** > **Configure Tenable Test Result Granularity**.
2. In the Key Configuration form, confirm that:
   - **Source integration** is `Tenable.io`.
   - **Table** is set to `Test Result`.
3. In the **Configuration Key** section, choose the field for which you want to create unique test results.
   For example, selecting *`instance`* creates unique test results for each instance within a database.

   Note: Use this feature with caution. Each additional configuration key increases integration time. To maintain optimal performance, limit your use to no more than three extra keys.

4. Enter *true* next to *`instance`* to enable granularity, or *false* to disable it.
5. Select **Update** to save your changes.

Exploring the Wiz Test Results and Issues Integrations with Configuration Compliance

Import cloud configuration data with the Wiz Test Results and Issues Integrations with Configuration Compliance that are included with the Wiz Vulnerability Response Integration.

Wiz Test Results Integration

Import configuration test results from Wiz to detect non-compliant cloud configurations and help you enforce security policies and standards across your cloud environment.

Findings are mapped to cloud test results (CTRs) in the Configuration Compliance application.

Note: Prior to v1.1, host configurations from Wiz are not imported.

Wiz Issues Integration

Import issues data from Wiz to help vulnerability managers, analysts, and cloud security and risk teams identify combinations of vulnerabilities that might reveal a potential attack path in your cloud infrastructure.

These findings are also mapped to CTRs with `Wiz Issues` labeled as the source in the Configuration Compliance application to help you track and remediate assets that may pose complex multi-vector risks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about the other integrations that are included with the Wiz Vulnerability Response Integration and installation and configuration steps, see Understanding the Wiz Vulnerability Response Integration.

Configuration Compliance remediation

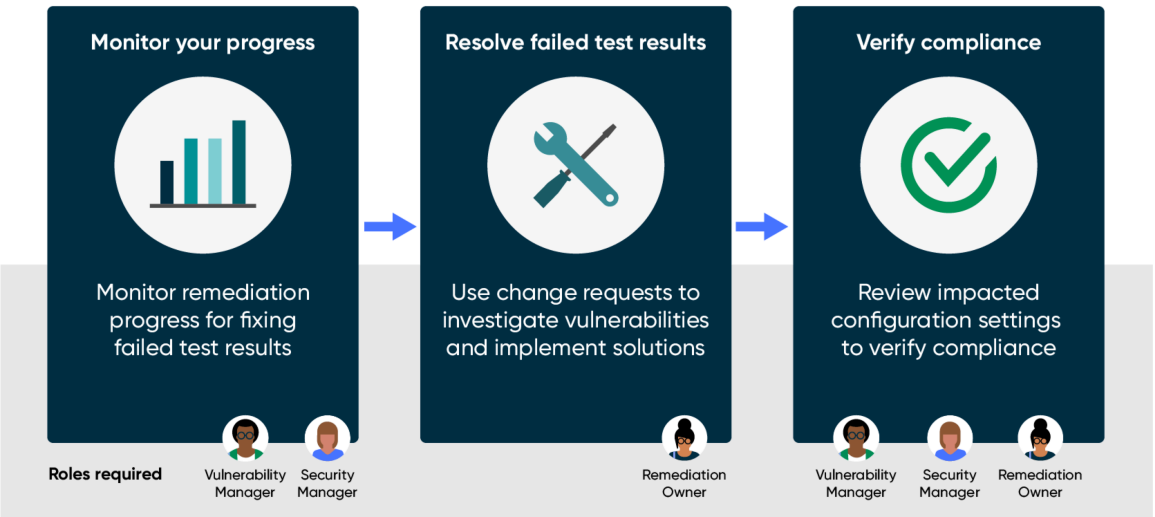
Configuration Compliance remediation is primarily a manual process augmented by scheduled jobs (integrations), remediation tasks, workflows, and change requests.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Remediation of test result groups



Separate third-party SCA plugins acquire and transform data in Configuration Compliance. Before you can use Configuration Compliance to remediate configuration items, you must install a third-party scanner integration and perform at least one network scan.

Use change requests to remediate individual test failures from remediation tasks.

The states of remediation tasks automatically transition as associated change requests move through their life cycles with State synchronization between change requests and remediation tasks. Users with the itil role can create and manage change requests directly from remediation tasks.

Related topics

- Manually create a Configuration Compliance remediation task
- Manually create a Configuration Compliance remediation task from the Test Results list
- Create a change request in Configuration Compliance
- Associate a remediation task to an existing change request

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remove assignments from remediation tasks for you or your groups

Automatic closing of test results

Close a remediation task

Configure approval rules for Exception Management in Configuration Compliance

Manually create a Configuration Compliance remediation task

You can manually create a remediation task from the **Remediation Tasks** module and perform remediation.

Important: You can create remediation tasks in the:

- Vulnerability Manager Workspace as a user with the sn_vulc.admin role.
- IT Remediation Workspace as a user with sn_vulc.remediation_owner role.

Before you begin

Role required: sn_vulc.admin

About this task

Using remediation task rules automatically populates the **Test Results** tab. Manual creation is useful for a group that doesn't need a rule or to be repeated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

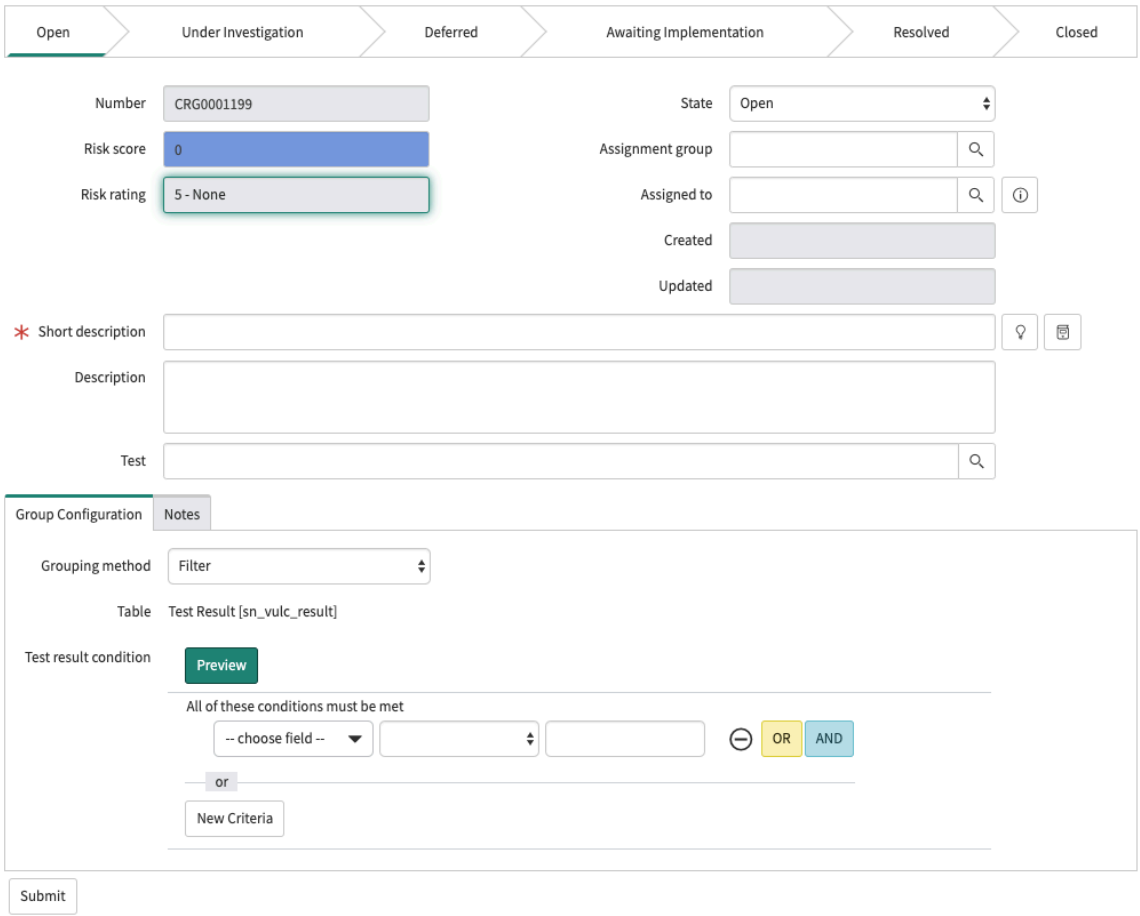
Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Remediation Tasks**.
2. In the navigation panel, click on **My Open Tasks** or **All Open Tasks** to view the list.
3. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task form



4. Fill in the fields on the Remediation Task form, as appropriate.

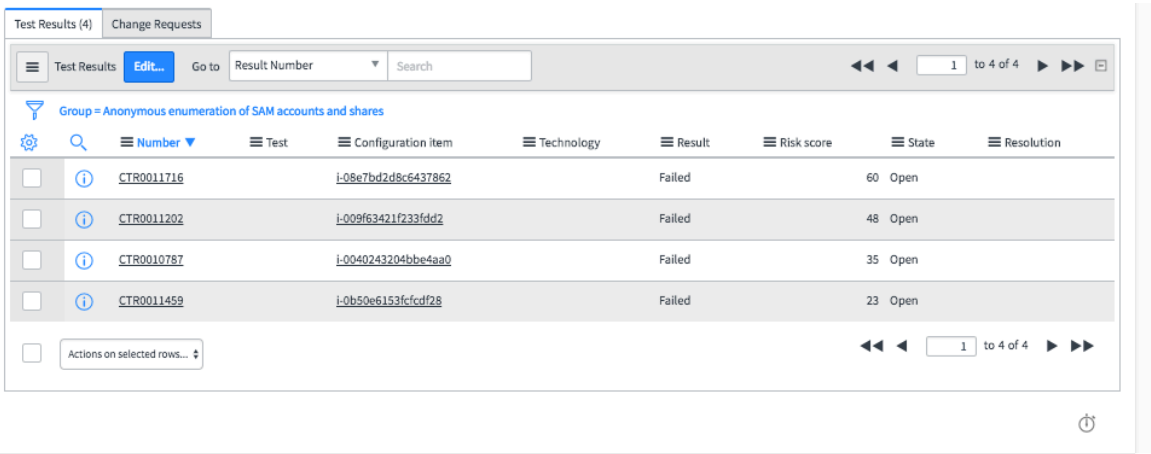
Remediation Task form

Field	Description
Number	Auto-assigned ID in the system.
Risk score	Auto-populated by risk score calculator. This is a rollup risk score. This risk score is weighted, with 85% of the score from the max risk score across all Test Results not 'Closed' (Open, Under Investigation, Awaiting Implementation, Deferred, Resolved), and 15% of the score from the number of test results that are not 'Closed'.
Risk rating	Auto-populated by risk score calculator. Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.
State	Initially **Open**, is the remediation state of the group. For more information, see Configuration Compliance states.
Assignment group	Assign the remediation task to a remediation group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Assigned to	Assign personnel to remediate the remediation task.
Created	Date you created this group.
Updated	Date you updated this group.
Short Description	Name of the remediation task.
Description	Description of this remediation task.
Test	Select a Configuration Test for this Remediation Task.
Related tabs	
Group Configuration	Grouping Methods to use: ○ Manual (default): ○ Filter or Group Rule: Table: preselected as Test Result [sn_vulc_result] Test result condition: Choose the filters to use. **Note:** The records match condition link above the filter conditions displays the test result records you have chosen in a new window. Click **Preview** to see how many results your filter criteria returns before you save the new group. The Test Results related list must be created manually by clicking the **Edit** button in the **Test Results** related tab.
Notes	Work notes related to this remediation task.

5. Right click in the header to **Save** or click **Submit** to save and return to the list of remediation tasks.
   Displays the **Test Results** and **Change Request** related lists.



Manually create a Configuration Compliance remediation task from the Test Results list

You can manually create a remediation task from the **Test Result** list and perform remediation from the resulting remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vulc.admin

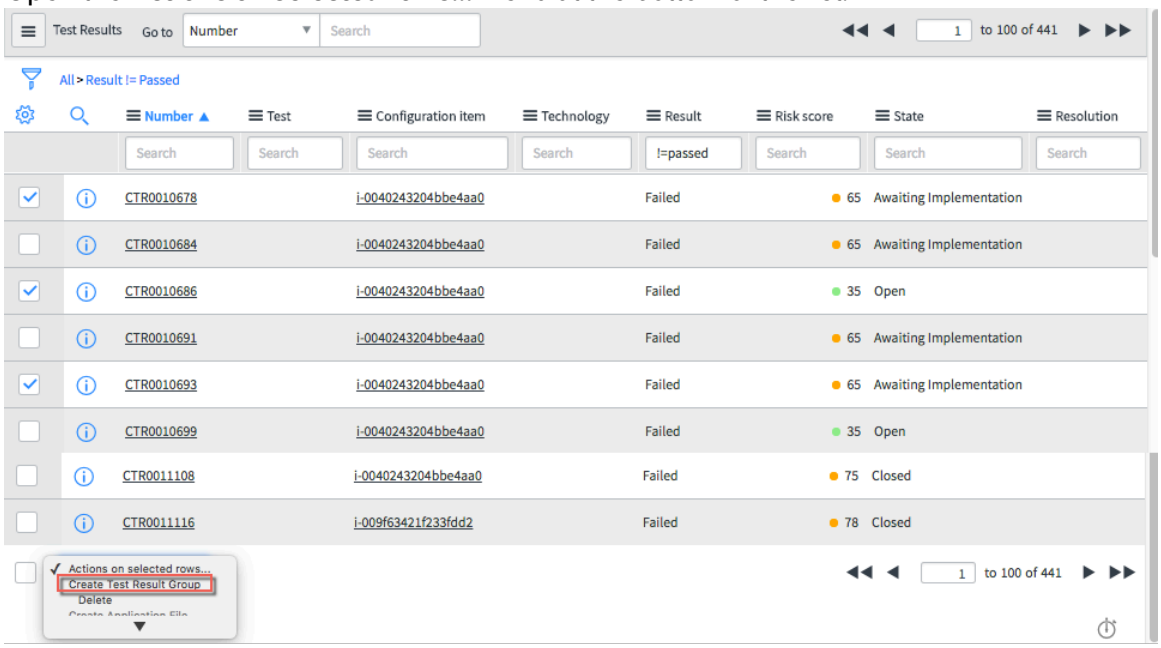
About this task
This method requires selecting test results to include and creating the group from the **Actions on selected rows...** menu. This method is good for results that are not easily filtered or situations where you want to specify test results for remediation.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

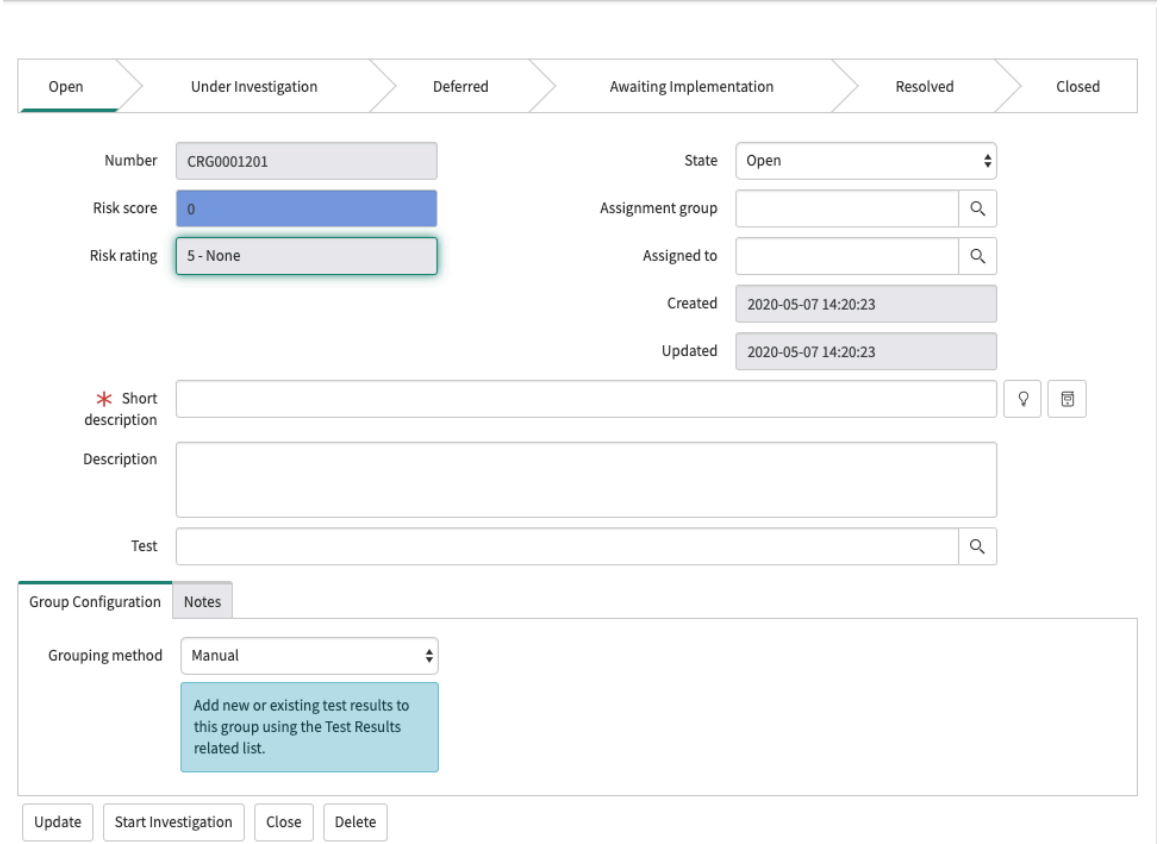
Procedure
1. Navigate to **All** > **Configuration Compliance** > **Test Results**.
2. In the navigation panel, select a Test Result module to open a list.
3. Select the test results to include in the group by checking the box next to each one.
4. Open the **Actions on selected rows...** menu at the bottom of the list.



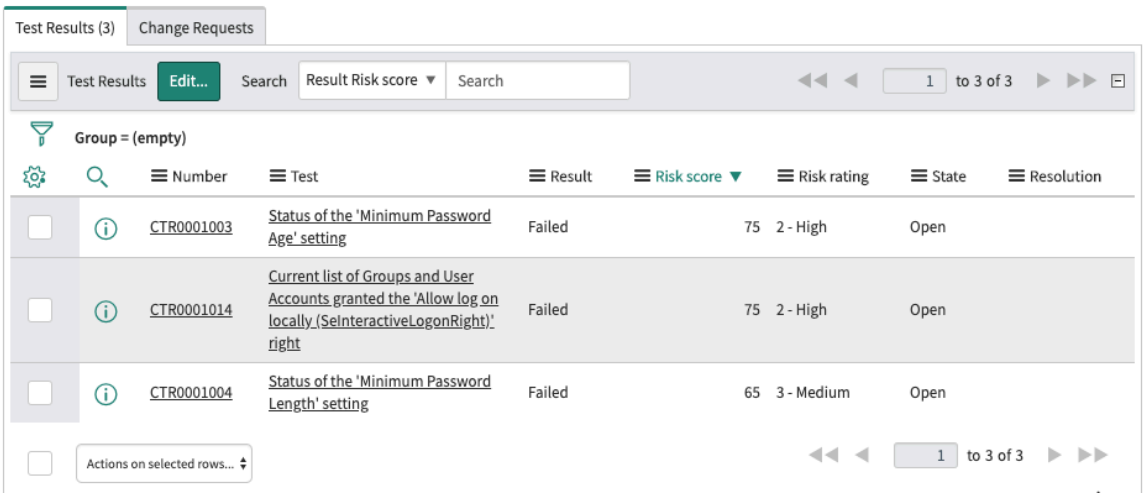
5. Choose **Create Remediation Task**.
   The remediation task is created and opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Test Result Group form



The test results you selected for the group are displayed on the Test Results related list along with any associated change requests.



6. Fill in the fields on the form, as appropriate.

Field	Description
Number	Auto-assigned ID in the system.
Score	Auto-populated by risk score rollup calculator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	This is a rollup risk score. This risk score is weighted, with 85% of the score from the max risk score across all Test Results not 'Closed' (Open, Under Investigation, Awaiting Implementation, Deferred, Resolved), and 15% of the score from the number of test results that are not 'Closed'.
Rating	Auto-populated by risk score rollup calculator. Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.
Historical risk score	Auto-populated by risk score rollup calculator. The inherent risk score across all the passed test results in a remediation task. This field displays the amount of risk that was remediated by a test group and is only displayed after a test group is in the 'Closed' state and the risk score is zero.
State	Initially **Open**, is the remediation state of the group. For more information, see Configuration Compliance states.
Assignment group	Assign the remediation task to a remediation group.
Assigned to	Assign personnel to remediate the group.
Created	Date you created this group.
Updated	Date you updated this group.
Short Description	Name of the remediation task.
Description	Text description of this remediation task.
	Select a Configuration Test for this Remediation Task.
Related tabs	
Group Configuration	Grouping Methods to use: ○ Manual (default) ○ Filter Table: preselected as Test Result Test result condition: Choose the filters to use. **Note:** The records match condition link above the filter conditions displays the test result records you have chosen in a new window. Click **Preview** to see how many results your filter criteria returns before you save the new group.
Notes	Work notes related to this remediation task.
Related lists	
Test results	Test results included in this group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Change requests	Change requests associated with this group.

7. Right click on the header to **Save** or click **Submit** to save and return to the list of remediation tasks.

Create a change request in Configuration Compliance

You can create a change request from a remediation task in the Configuration Compliance application.

Before you begin

Role required: user with the itil role

About this task

As an IT or remediation specialist, create a change request (CHG) directly from a remediation task for all the test results in the group. Create a change request with pre-populated information to expedite your investigation for vulnerabilities that require manual intervention.

You can create, approve, implement, review, and close change requests directly from remediation tasks that are assigned to you. You can create three types of change requests with pre-populated information from a remediation task:

Standard

A pre-authorized change that is low risk, relatively common, and follows a specified procedure or work instruction.

Normal

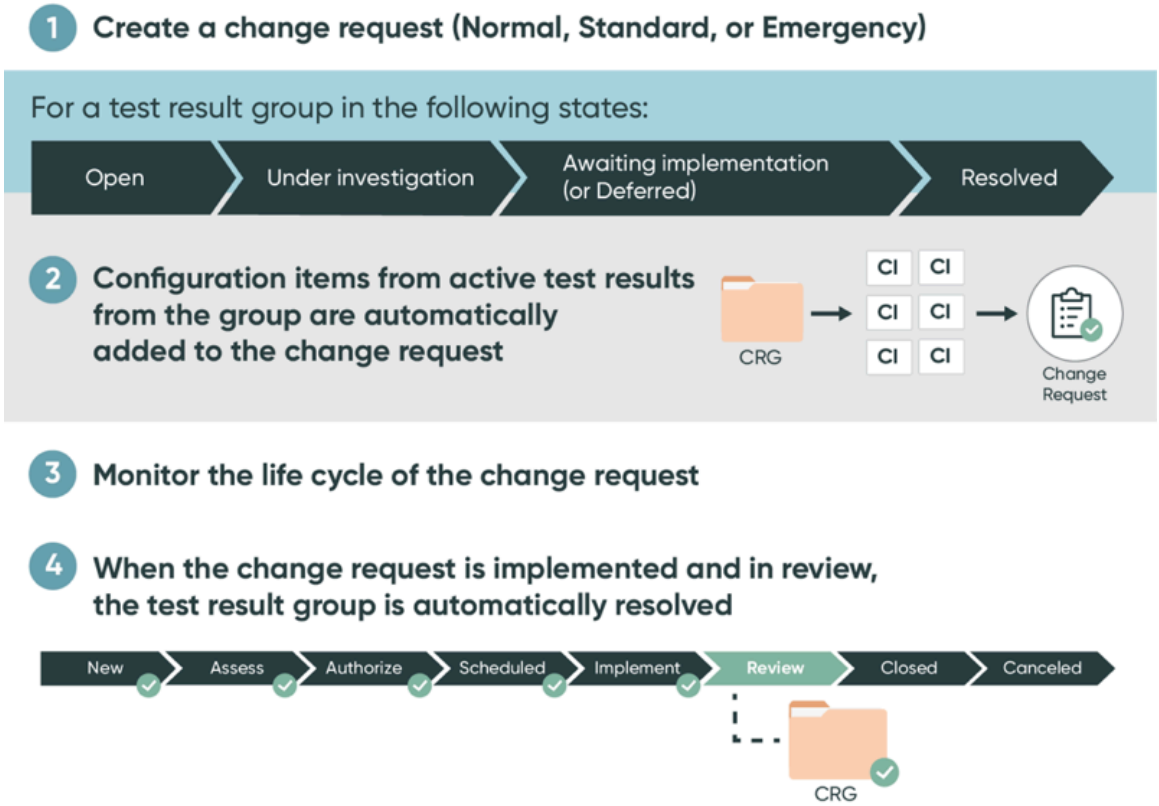
Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed.

Emergency

A change to resolve a major incident.

The following image illustrates the basic flow for creating a change request from a remediation task. The detailed steps for this flow follow the image.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Starting with version 19.0 of Vulnerability Response, you can create change requests for Remediation Tasks from the IT Remediation Workspace. For more information, see Create a change request in the IT Remediation Workspace.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Remediation Tasks** > **My Open Groups**.
   The list of remediation tasks assigned to your groups is displayed.
2. In the Number column, click the remediation task you want to create a change request for.
   You can create change requests from remediation tasks in any states other than **Closed** or **In review**.

   The remediation task record is displayed.
3. In the upper right of the record, click **Create Change**.
   The change request form is displayed.
4. Fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. From the list of the **Applies to** field, choose one to continue.

Option	Description
All active test results in this group	If selected, all active test results from this re mediation task with a state other than **Closed** are added automatically to the change re quest after you click **Create Change**.
All active test results in this group matching a set of conditions	If selected, the condition builder is displayed. Enter filter criteria to identify the test results that you want for the new change request. An example of a filter you might create would locate only test results from the group that match a specific state and risk score: State is **Open** and Risk Score is greater than **50**.

5. For the **Add CIs to CR** check box, choose one to continue.

Option	Description
Check box selected	Default is selected. If the check box is select ed, any configuration items (CIs) that belong to active test results from this remediation task are added to this change request. The test result transitions to **Awaiting Implemen tation**.
Check box cleared	Clear the check box if you do not want the CIs from the active test results from this remedia tion task added to the new change request. The remediation task remains in its current state.

6. From the list for the **Change type** field, choose one to continue.

Option	Description
Emergency	A change to resolve a major incident.
Normal	A change type that is used to implement any change to a service that is not a standard or emergency change.
Standard	A pre-authorized, low-risk change request that is frequently implemented. Approved standard change requests can be predefined in a catalog of templates to make accessing and requesting a standard change more ef ficient. If selected, two fields are displayed. Select one from each list to fill in these fields:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ **Change category**: Select a category for the change from your existing catalog, for example, `Hardware`, `Server Standard Changes`, `Software`. ○ **Change template**: Select one available template for change requests with pre-defined supporting tasks from your catalog. For more information on ITSM change request categories, templates, and change types, see Change types.

The feature automatically reads the types of change requests that you set up in your catalog in ITSM Change Management. For example, if you change the name for your Standard change requests in ITSM from `Standard` to `Pre-approved`, your new name is automatically displayed in the Change type list on the Create change request form.

7. The fields in the Change Request Preview section of the form are pre-populated with information from the remediation task.
   If required, edit these fields.
8. Click **Create Change**.
   The change request is displayed. On the Affected CIs related list, the CIs from the test results that matched your criteria are displayed. If the change request requires approval, the **Request Approval** button is displayed.

   After the change request is created, the test result group moves to the **Awaiting Implementation** state. After the change request for this remediation task is resolved, if there are no other open change requests associated with this remediation task, the remediation task is also moved to the **Resolved** state.

   See State synchronization between change requests and remediation tasks for more information.

   Note: You can still manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the remediation task from the `Closed` or `Deferred` states.

Associate a remediation task to an existing change request

Associate a remediation task in Configuration Compliance application to an existing change request.

Before you begin
Role required: a user with the itil role

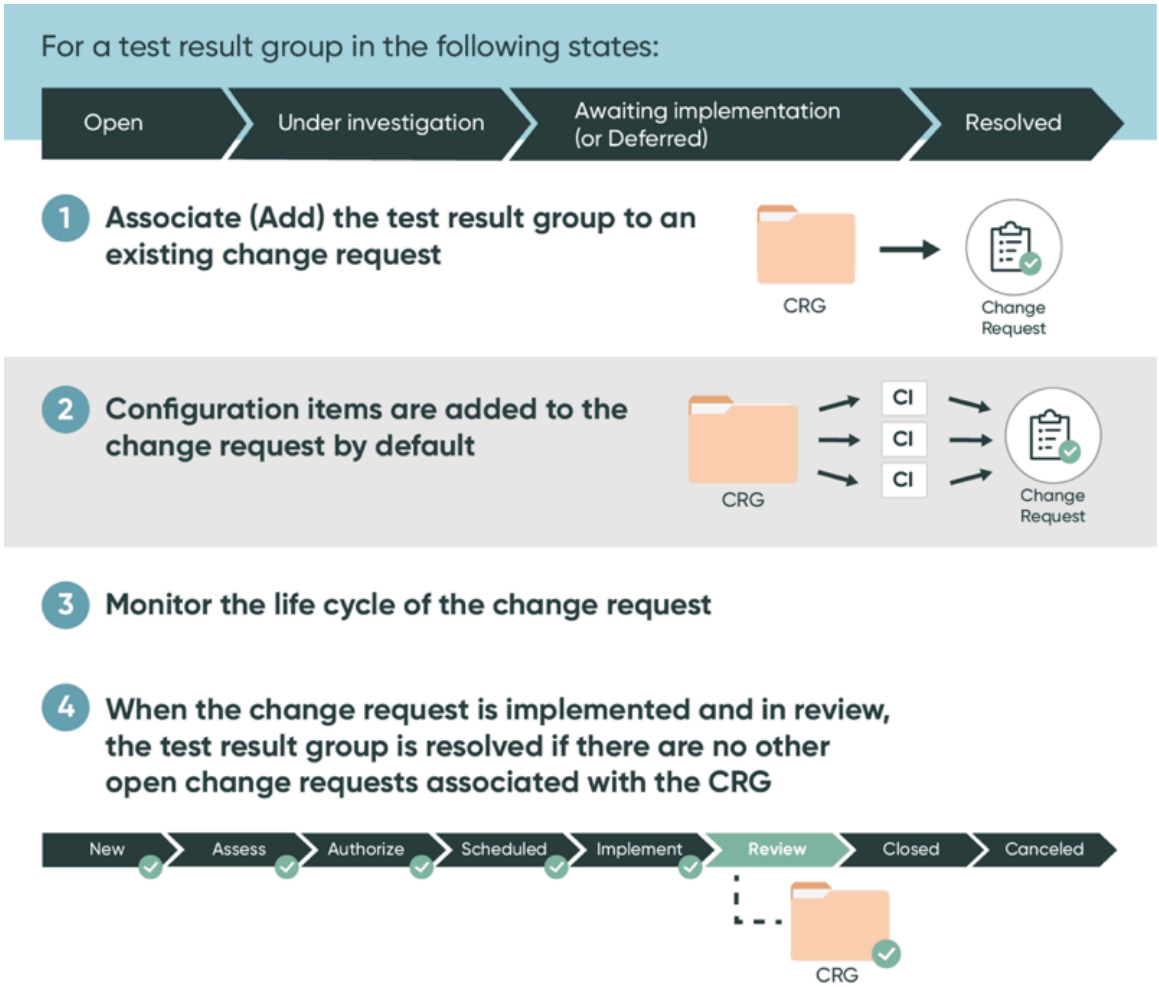
About this task
As an IT or remediation specialist, avoid creating duplicate change requests (CHG) as you work to resolve your remediation tasks by associating a remediation task (RT) to a change request that is already available in your instance.

You can associate remediation tasks that are assigned to you or your assignment group to existing change requests directly from the remediation task records. The following image

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

illustrates the basic flow for associating an existing change request to a remediation task. The detailed steps for this flow follow the image.

Note: You can associate an existing change request to a remediation task in any state other than **Canceled** (**Open**, **Under Investigation**, **Awaiting Implementation**, **Closed**, and **Deferred**). Change requests, including those closed within the last 90 days, are available to associate from the form. When you associate a change request to an existing remediation task, only the active test results and their configuration items are added to the change request.



Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Remediation Tasks** > **My Open Tasks**.
   The list of remediation tasks assigned to your groups is displayed.
2. In the Number column, click the remediation task you want to create a change request for.

   The remediation task record is displayed.
3. In the upper right of the record, click **Create Change**.
   The change request form is displayed.
4. Scroll to the Change Requests related list and select it.
   Any change requests associated with the remediation task are displayed along with the **Add** button.
5. Click **Add**.
   The Add Existing Change Request to Test Result Group dialog is displayed.
6. Click the search icon and select an item from the list.
   You can filter the list that is displayed to narrow your search.
7. Click **Submit**.
   The TRG is displayed along with a message that indicates the change request was successfully associated to the remediation task. Under the change requests related list, the new change request is displayed. The CIs from the remediation task are by default added to the change request and are displayed on the Affected CIs related list. You can also add CIs to the change request from this related list. A message indicates the number of test results that have moved to the new group, and the new TRG is displayed.

   Note: For under 200 test results, the split operation is done synchronously, and the test results are displayed in the new group.

   For over 200 test results, the split operation is done asynchronously in the background, and it may take a few seconds for the test results to appear in the new group. The following message is also displayed: `n test results will be moved from TRGxxxxxxx to new test result group GRCxxxxx shortly.`

   You can associate any change requests to the remediation task, with the following exceptions:

   - Change requests in the **Canceled** state.
   - Change requests in the **Closed** state older than 90 days.
   - Change requests already associated with the TRG. The system will not permit you to associate a change request that is already associated with the TRG.

   After the change request for this remediation task is resolved, if there are no other open change requests associated with this remediation task, the remediation task is also moved to the**Resolved** state.

   Note: You can still manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the remediation task from the `Closed` or `Deferred` states.

   For more information, see State synchronization between change requests and remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Split a remediation task

From an existing remediation task in the Configuration Compliance application, identify a subset of test results that you want to move to a new Remediation Task.

Before you begin

Role required: a user with the itil role

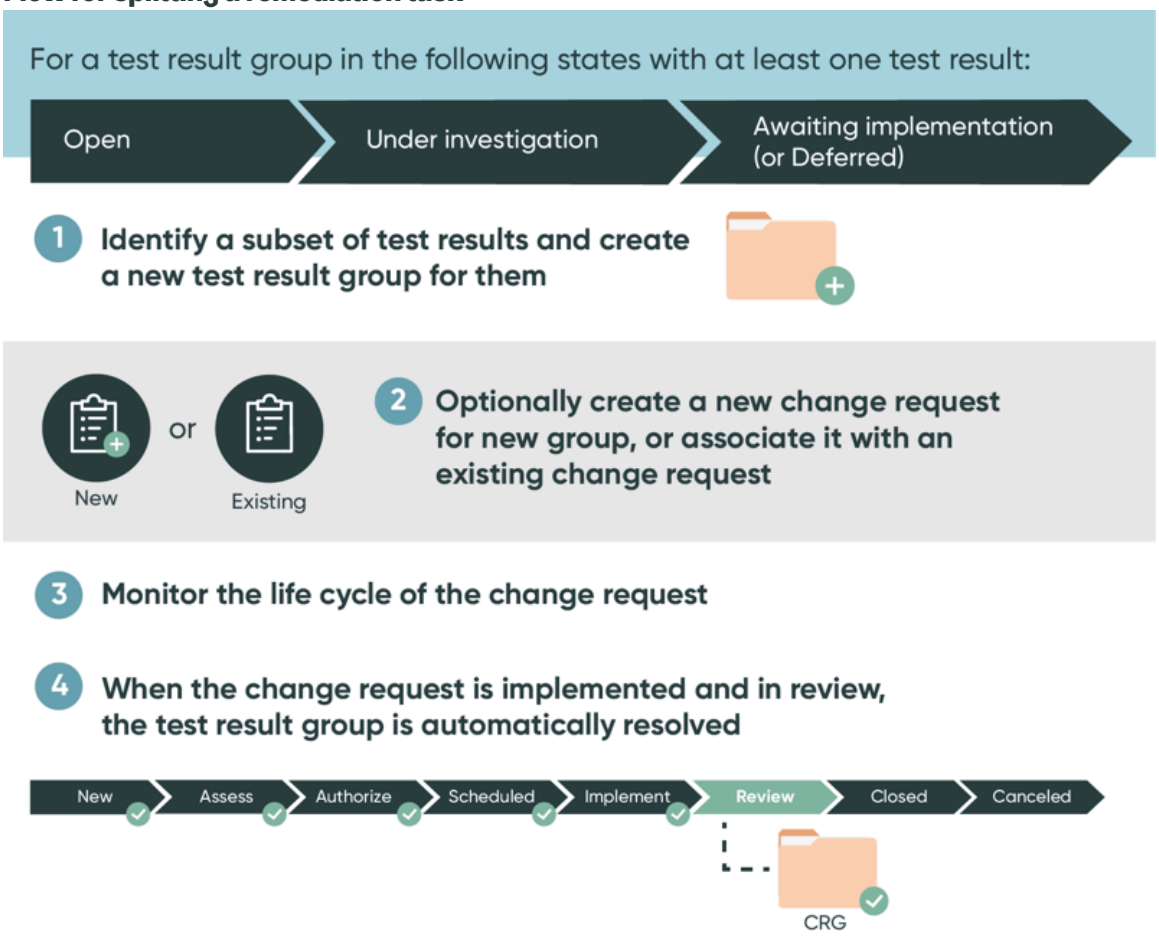
About this task

As an IT or remediation specialist, you can split existing remediation tasks in the **Open**, **Under Investigation**, or **Awaiting Implementation** states with more than one test result. By creating a new Remediation Task with test results that match specific criteria, you can work with a specific group of test results without impacting the original remediation task.

When you specify the conditions for the test results that you want to move to a new remediation task with the condition builder, only the active test results that match your criteria are moved to the new task. You are not required to create change requests (CHGs) when you split a remediation task. You have the option to split a remediation task at the same time you create a change request, or, you can split a remediation task without creating a change request.

The following image illustrates the basic flow for splitting a remediation task. The detailed steps for this flow follow the image.

Flow for splitting a remediation task



Use cases for splitting test results from existing Remediation Tasks into new tasks might include the following examples:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- When you want to create a change request or change requests for a split group.
- When you reassign a split task to another user in your assignment group.
- When you request a deferral or exception for a split task because you know that some test results on specific configuration items (CI) cannot be remediated in a given time frame.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Tests** > **Remediation Tasks** > **My Open Tasks**.
   The list of Remediation Tasks assigned to your groups is displayed.
2. In the Number column, click the remediation task that you want to split.

   The Remediation Task record is displayed.
3. To create a subset of test results for a new task that matches specific criteria, follow these steps.

   On the upper right of the record, click **Split Group**.

   You might prefer this method of creating a new group if you are working from a large group with multiple test results.

   The Split remediation task form is displayed.
4. With the condition builder displayed, specify the conditions for the test results that you want to move to a new remediation task.

   For example, you may prefer to filter out only test results that match the following conditions:

   - In the **Open** state.
   - Risk scores greater than 75.
   - Result is **Failed**.

   If test results match your filter after you enter the conditions, a message is displayed with the number of test results that match.

   If a message is displayed that no test results match your filter, or, that all your test results match your criteria, adjust the conditions so at least one test result matches your filter criteria.
5. Click **Preview items** to view the matched test results.
   A new window, Remediation Tasks, displays the items.
6. To preview details about the test results that match your filter criteria, follow these steps before you click **Split Group** to create the new group.
   These details include the assignment group and who the test result is assigned to. Viewing this information on the preview may help ensure that the new task is properly assigned.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. With the Remediations list displayed in the preview, click an item in the Result column. The Test Result record is displayed.

b. Verify the **Assignment group** and **Assigned to** fields are correct.

c. Click **Update**.

7. When you are ready to create the new group, click **Split Group**.
   A message indicates the number of test results that are moved to the new group, and the new remediation task is displayed. To help you identify the new task, you might prefer to edit the text in the **Short description** field and edit the Assignment group or Assigned to fields again, if required.

   Note: For under 200 test results, the split operation is done synchronously, and the test results are displayed in the new task.

   For over 200 test results, the split operation is done asynchronously in the background, and it may take a few seconds for the test results to appear in the new task. The following message is also displayed: `n test results will be moved from TRGxxxxxxx to new test result group GRCxxxxx shortly.`

8. Alternatively, you can create a new remediation task by selecting test results directly from the Test Results related list on a remediation task.

   You might prefer this method if you have only a few test results in a group, or you know exactly which tests you want to move to a new task.

   a. With the remediation task record displayed, scroll to the Test Results related list.

   b. In the far left column, select check boxes for the test results you want to create a new remediation task for.

   c. From the Actions on selected rows list in the lower left of the record, click **Split Group**.

   d. In the Split remediation task form that is displayed, to help you identify the new group, you might prefer to edit the text in the **Short description** field.

   e. Click **Split Group**.
      A message indicates the number of test results that have moved to the new task, and the new remediation task is displayed.

      After the change request for this remediation task is resolved, if there are no other open change requests associated with this remediation task, the remediation task is also moved to the **Resolved** state.

      Note: You can still manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change requests states do not automatically move the remediation task from the `Closed` or `Deferred` states.

      For more information, see State synchronization between change requests and remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

You can create or associate change requests for your new remediation tasks. For more information, see Associate a remediation task to an existing change request and Create a change request in Configuration Compliance.

Remove assignments from remediation tasks for you or your groups

Reassign the test result records in the Configuration Compliance application if the records have been incorrectly assigned to you or your group.

Before you begin

Role required: sn_vulc.remediation_owner

About this task

Starting with v14.3 of the Configuration Compliance application,If you determine that remediation tasks (RTs) and their associated test results aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups, you can remove yourself or your groups from the Assigned to and Assignment group fields on RT records.

The **Unassign** button is displayed on remediation task records in any state other than the Closed or Resolved states.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to a remediation task record that is assigned to you that is in any state other than Closed or Resolved.
2. To clear the **Assigned to** and **Assignment group** fields, at the top of the record, select **Unassign**.
3. In the **Unassign** dialog, provide work notes and select **Submit**.
   - The work notes that you provided are displayed in the Notes section.
   - On the **State Change Approval** tab, the state change approval record (CA#) displays the In Review state, which helps you to track the approval workflow.
   - On the **Requested Approvals** tab, your request for the removal of you or your assignment group is displayed as the Requested state.

Result

The request is approved by using a default, one-level approval workflow. For more information, see Approve an unassign request in Configuration Compliance.

- If your request is approved, the state change approval record and the requested approval record transition to **Approved**. You and your groups are removed from the **Assigned to** and **Assignment group** fields. `Unassigned` is displayed in the **Assignment type** field, and the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

remediation task is displayed on the list of the Unassigned module for the Configuration Compliance application.

Notifications that records are unassigned are sent automatically to vulnerability managers or analysts in the Unassign notification group. For more information about the notifications and the properties for this feature, see Removing assignments from Configuration Compliance test result groups.

- If your request is rejected, the state change approval record and the requested approval record transition to Rejected.

Note: As a vulnerability administrator, you can set the *sn_vulc.unassign_test_result_group.approval_required* system property to **false** to disable the approval process.

What to do next

Navigate to the Unassigned module for the Configuration Compliance application monitor any unassigned records for items that might fall under your scope, and then reassign them to yourself.

Approve an unassign request in Configuration Compliance

Approve requests for the removal of remediation tasks from an assignment group or an individual user in the Configuration Compliance application.

Before you begin

Role required: sn_vulc.unassign_approver

About this task

By default, an approval configuration is provided. For unassign approvals, one approver is required in the Approver – Level 1 approval group. By default, the unassign approval group (`Unassign Approver CC - Level 1`) is created and users that are part of this group can approve the request. By default, this group contains the unassign approver role, sn_vulc.unassign_approver. You can modify or create a group and update the approval configuration by navigating to **All** > **Configuration Compliance** > **My Approvals** > **Approval Rules** > **Test Result Group Field Change Request** > **Unassign Test Result Group**.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request by adding the appropriate comments.

Automatic closing of test results

You can automatically close test results (TRs) associated with retired configuration items (CIs).

To configure the auto-close option, navigate to the system property **sn_vulc.auto_close_test_results_linked_to_retired_CIs** and set it to true. To automatically close TRs related to retired CIs, see Automatically close test results related to retired CIs.

For information on working with retired configuration items, see Working with retired configuration items in Configuration Compliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Working with retired configuration items in Configuration Compliance

Decommissioned configuration items (CIs) are moved to retired, archived, or deleted state in the Configuration Management Database (CMDB). Configuration Compliance contains test results (TRs) that are made up of CIs. When the state of a CI is updated to retired, the associated TRs are closed with the substate 'CI decommissioned'.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

If the CMDB changes the life cycle stage status of a CI to retired, you can choose to automatically close the associated TRs. For more information on automatically closing the associated TRs, see Automatically close test results related to retired CIs.

The retired CI is eventually archived or permanently deleted from the CMDB.

Impact of retiring the CIs:

- **Impact on discovered items:** When the CI is retired, the related DI is marked as 'CI decommissioned'.
- **Impact on test results:** When the state of a DI is updated to 'CI decommissioned', the associated TR is closed and the Notes section is automatically updated.

  Note: The state of a DI is automatically updated to 'CI decommissioned' whenever the life cycle state of a CI is updated. On the other hand, the state of a TR is updated to Closed only when the **sn_vulc.auto_close_test_results_linked_to_retired_CIs** property is set to true. For more information on automatically closing the associated TRs, see Automatically close test results related to retired CIs.

The scheduled job *`Close Test Results for decommissioned CIs`* is run daily for the updated DIs. If the auto-close configuration option is enabled for retired CIs, it identifies the DI containing a decommissioned CI, and closes the related TR with the substate 'CI decommissioned'. If all the TRs in a remediation task are closed and their substate is CI decommissioned, the remediation task is also closed with the substate 'Canceled'.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If a CI moves back to the original state from the 'Retired' state, the 'Discovered Items' entry is updated as well. TRs are automatically opened when data is ingested again from the scanner.

Automatically close test results related to retired CIs

If the Configuration Management Database (CMDB) changes the life cycle stage status of a configuration item (CI) to retired, you can choose to automatically close the associated test results (TRs).

Before you begin

Role required: sn_vulc.admin

About this task

To automatically close the associated TRs, you must enable the system property **sn_vulc.auto_close_test_results_linked_to_retired_CIs** to auto-close TRs that are associated with retired CIs. If this option is enabled, new and existing TRs reported for the same CI, are automatically created or updated in the 'Closed' state. These are based on the Asset ID in the scanner payload and Discovered Items entry status. For more information on the impact of retired CIs, see Working with retired configuration items in Configuration Compliance.

Note: The state of a DI is updated to 'CI decommissioned' whenever the life cycle state of a CI is updated. On the other hand, the state of a TR is updated to Closed only when the **sn_vulc.auto_close_test_results_linked_to_retired_CIs** system property is enabled.

Procedure

1. Navigate to **System properties** > **All properties** and filter by *sn_vulc.auto_close_test_results_linked_to_retired_CIs* in the Name column.
2. Select the property.
3. To automatically close test results associated with the retired CIs, set the value of the property to true.

Automatically closing stale test results in Configuration Compliance

You can activate the Auto-Close Stale Test Results feature to automatically close older test results not recently found by your third-party integrations. Moving these test results to **Closed-Stale** reduces the number of active test results and remediation tasks in your instance and helps you reconcile assets in your Configuration Management Database (CMDB).

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview

The Auto Close Stale Test Results module helps you automatically close older, stale test results not recently found by your third-party integrations. Test results are moved to **Closed-Stale** based on the conditions you set in the condition builder.

Key terms

Test result

Tests results are imported results from libraries of configuration tests that are mapped to frameworks, policies, and authoritative sources that define how a class of technology assets should be governed. The Configuration Compliance application does not calculate the test results but imports them with third-party integrations.

Asset last scanned date

Refers to the value of Last configuration compliance scan date column of the Discovered Item table that is related to the test result. This date refers the most current date and time an asset was last scanned by a third-party scanner.

Last failed date

Refers to the Last seen column date of the Test Results table when the **Result** field value is [failed].

Stale test results

Refers to test results in your instance that are aged and have not been found, updated, or detected by third-party integration scans for a significant amount of time.

Test Results last found

This search option uses a date and time provided by the third-party scanner. This term refers to the most current, or latest date (days ago) that test results were found again by the scanner. This parameter can be configured.

Use case

At times, assets (configuration items) might be decommissioned in your environment or purged by third party-scanners. When this happens, the assets' associated configuration test results are not updated in the Configuration Compliance application by imported detections and they become inactive (stale).

To reduce the number of active test results (TRs) and remediation tasks (RTs) in your instance, activate the Auto-Close Stale Test Results feature. This feature closes aged test results automatically that have unchanged states or have not been recently imported by your integrations.

As an example, suppose a particular configuration item (CI) has multiple asset IDs, and one of these IDs has not been imported on detections from a third-party scanner in the last 90 days. If you set the condition builder in the Auto-Close Stale Test Results module to close tests results that have not been found or updated in the past 90 days or more, this feature automatically closes any test results that match this filtering.

Note: This feature only closes test result detections based on the filter conditions that you set in the condition builder and are detected by your third-party scanner integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Resolution field

To differentiate between the detections that are closed by third-party scanners such as the Qualys and Tenable.io products and the Auto-Close Stale Test Results feature in your instance, a new value for the **Resolution** field, [Closed-Stale], has been added. **Closed-Stale** indicates that a TR was closed by the auto-close feature. **Closed** or **Fixed-Closed** indicates that a TR was closed by a scanner.

Rollup of TR states to TRGs with the Auto-Close feature

The state progression and precedence for test results is: **Open** > **Closed** > **Fixed-Closed** > **Closed-Stale**.

1. If any TRs in a TRG are **Open**, the TRG state is not changed.
2. If at least one TR is **Closed - Fixed** and the rest are **Closed - Stale**, the TRG state transitions to **Closed - Fixed**.
3. If all the TRs in a TRG are **Closed - Stale**, the TRG state transitions to **Closed - Canceled**.

Supported integrations

For more information on the third-party integrations that support this feature, see Understanding the Qualys Vulnerability Integration and Tenable.io integrations with the Vulnerability Response and Configuration Compliance applications.

Use Auto-Close Stale Test Results in Configuration Compliance

Activate Auto-Close Stale Test Results (TRs) to automatically close older test results based on filter conditions that you set.

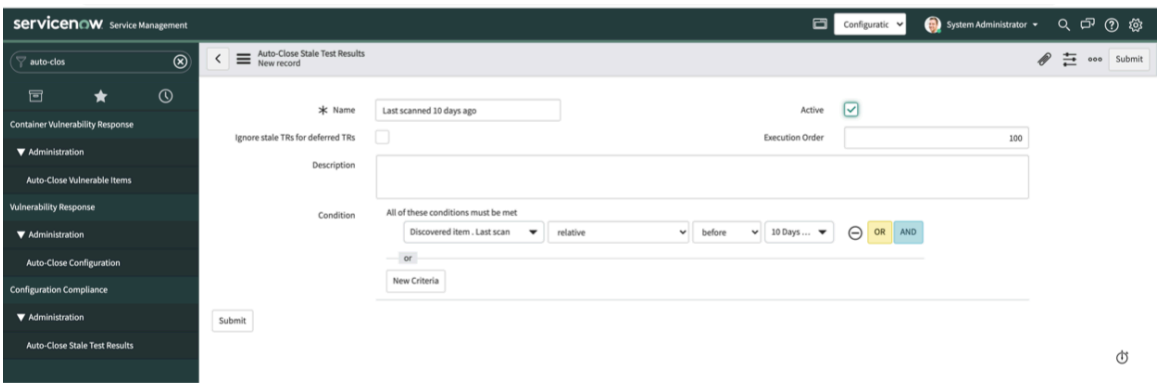
Before you begin

For more information about this feature, key terms, and any setup that may be required for your third-party integrations that import test result data, see Automatically closing stale test results in Configuration Compliance.

Role required: sn_vulc.admin

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Administration** > **Auto-Close Stale Test Results**.
2. Fill in the fields on the form.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Value
Name	Name for this configuration record.
Active	If selected, this record is active and it will automatically close any test results that match its filter criteria.
Ignore stale TRs for deferred TRs	If selected, any TRs that are mapped to the **In-review** or **Deferred** states are ignored and not closed. If you clear this option, any TRs that match your criteria will be closed.
Execution order	100 is the default value. This value determines the order of execution in ascending order for each configuration record used for locating and marking test results that are stale.
Description	A description for this record. This text might help you easily find it again if you create a larger number of records.
Condition	The filtering conditions used for finding TRs that you want closed. The default filter is **Discovered Item** > **Last scan**.

3. Click **Submit**.

   The scheduled job, *Auto-Close Stale Test Results*, runs daily. This job identifies the TRs based on the conditions that you provided and transitions the ones that match to **Closed-Stale**.

   After TRs are marked as **Closed-Stale**, if the scanner finds these TRs again, the test results are reopened and the states transition to**Open**.

   If a TR is marked as **Closed-Stale**, and the scanner finds that it has been fixed, the TR transitions to**Closed-Fixed**. States also roll up to remediation tasks as described in the following list:

   a. If any TRs in a remediation task are **Open**, the remediation task state is not changed.

   b. If at least one TR is **Closed - Fixed** and the rest are **Closed - Stale**, the remediation task state transitions to **Closed - Fixed**.

   c. If all the TRs in a remediation task are **Closed - Stale**, the TRG state transitions to **Closed - Canceled**.

Close a remediation task

If you determine that the issue associated with a remediation task can be immediately closed without further analysis, you can use the **Close** feature.

Before you begin

Role required:

- sn_vulc.admin
- sn_vulc.remediation_owner

Note: With the sn_vulc.remediation_owner role, you can reassign or close remediation tasks that are assigned to you or to your assignment groups.

About this task

Starting with v15.0 of Configuration Compliance, the **Close** button has been removed for a remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you resolve a remediation task, the resolution notes reflects in the work notes of all its test results.

Procedure

1. Open the remediation task record.
2. Select the **Close** button.
3. Describe why the issue is being closed in the pop-up window.
4. Select **Close**.

Related topics

Configuration Compliance states

Requesting and approving an exception for a remediation task

You can request to defer the remediation of a remediation task for a specified period. Users who are a part of the approver group can approve exception requests.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

To request or approve exception requests, see:

- Request an exception for a remediation task in Configuration Compliance
- Approve an exception request in Configuration Compliance

Note:

Email notifications are sent at every stage of exception management, providing the status and other details of a request. For example, when an exception is requested, the requester receives an email confirming that the request is raised. The approver also receives an email stating that an exception has been requested.

Starting from v14.11 of Configuration Compliance, you can configure the time frames for approving exceptions, along with email notifications for both the approver and requester after a set number of days. When a request is raised, the test result changes to In-Review status and a state change record is created. If the approver doesn't respond within the configured time frame, the test result reverts to Open status. The previous state is stored in the **backup_state** field. For more information, see Configure approval rules for Exception Management.

Request an exception for a remediation task in Configuration Compliance

Request an exception to defer the remediation of a remediation task for a specified period if it can’t be remediated immediately.

Before you begin

Role required: sn_vulc.remediation_owner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Important: You can request an exception for:

- remediation tasks in the Vulnerability Manager Workspace and IT Remediation Workspace. For more information, see Request an exception in the IT Remediation Workspace.
- multiple test results simultaneously from the Vulnerability Manager Workspace. For more information, see Request bulk exception in the Vulnerability Manager Workspace.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Remediation Tasks** > **All Tasks**.
2. Select the remediation task that you want to request an exception for.
   The selected task must be in the Open, Under Investigation, or Awaiting Implementation state.
3. On the Remediation Task form, click **Request Exception**.

   Note: Depending on whether Vulnerability Response or GRC: Policy and Compliance Management is selected in the **Configuration Compliance** > **Exception Management** screen, the Request Exception form changes. See Configure Exception Management for Configuration Compliance

4. If Vulnerability Response is selected in the Exception Management screen, then do the following:

   a. On the form, fill in the fields.

Request Exception form

Field	Description
Until	Date on which the exception request expires. This date must be within the duration selected in the **All** > **Configuration Compliance** > **Administration** > **Exception Management** screen. When the exception request expires, the group reverts to its Open state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: Starting with version 14.7 of Configuration Compliance (CC), if a deferred remediation task is reopened by a scanner before the exception window expires, then the state of the remediation task changes from Open to Deferred. This functionality is disabled by default. To enable this functionality, set the value of the system property *sn_vulc.auto_defer_test_result_in_activ* to true. Also, the deferred until date persists even after the remediation task reopens after the expiration date.
Reason	Reason for the exception. Choices are as follows: ▪ Risk Accepted ▪ Awaiting Maintenance Window ▪ Fix Unavailable ▪ Mitigating Control in Place ▪ Other To see how to add new reason choices, see Define policy reason mappings.
Additional information	Details that are related to the reason why this request is being made. This field is to be updated by the remediation owner.

b. Submit the exception request by clicking **Request Approval**.

Result

The state of the remediation task changes to In Review. Use the **State Change Approval** tab to track the status of the exception request.

Request an extension for an exception rule in Configuration Compliance

Request an extension for a deferred exception rule before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin

Role required: sn_vul.exception_approver

About this task

You can also request an extension from the Vulnerability Response Workspaces. For more information, see Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Exception Rules**.
2. Select an approved exception rule.
3. Select **Request Extension**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the exception rule must be extended.
Reason	Enter the reason for deferring the exception rule. Choices include: ○ Risk accepted ○ Awaiting maintenance window ○ Fix unavailable ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

5. Select **Request Approval**.
   On approval of the request, the Deferred until, Reason and Additional information fields get updated on the exception rule and the associated remediation tasks. An email is also triggered on submission of the request and subsequent action by the approver.

Note:

- The request goes through two levels of approval.
- If a deferred exception rule is extended again, the extend deferral count increases in the backend.

Request an exception for remediation tasks using GRC: Policy and Compliance Management

Request policy exceptions using the GRC policy exception management capability in the Policy and Compliance Management application from within Configuration Compliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Before you can use the Policy Exception Integration to request policy exceptions, you must download the GRC: Policy and Compliance Management application from the ServiceNow Store.

Role required: sn_vulc.remediation_owner

You can also request exceptions in the classic UI.

About this task

Starting with version 19.0 of Vulnerability Response, you can request policy exceptions for Remediation Tasks (RTs) in the IT Remediation Workspace. For more information, see Request an exception using GRC: Policy and Compliance Management in the IT Remediation Workspace.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Application Vulnerability Response** > **Application Vulnerable Items** (or **Remediation Tasks**)>**All**, and open the item or group for which you want to request an exception.
   The selected item or group must be in Open, Under investigation, or Awaiting implementation state.
2. On the selected form, click **Request Exception**.
3. If GRC: Policy and Compliance Management is selected in the Exception Management screen, do the following.

   a. On the form, fill in the fields.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you're requesting an exception for.
Control objective	Control objectives that are associated with the policy you selected. If a policy isn't selected, all the control objectives are listed.
Valid from	Date when the exception will start. The default value is the current date. This date can't be in the past.
Valid until	Date when the policy exception expires and when the state of the vulnerable item or group changes from Deferred to Open.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The number of days that the policy exception is valid can't exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This field must be filled in by the remediation owner.

b. Submit the exception request by clicking **Request Approval**.
The state of the remediation task changes to In Review and a policy exception is created. Use the **State Change Approval** tab to track the status of the exception request.

c. View the policy exception by clicking the Policy Exceptions related list.

d. Click the policy exception number.

e. In the **Approver** field, select the name of the approver.

f. Click the Source tab and select a control objective from the **Control objective** field.

g. Click the Risk assessment tab and select the risk rating from the **Risk rating** field.

h. Save the form.

i. Click the **Impacted Controls** tab.

j. Add the controls by clicking **Add**.

k. Save the form.

Note: You can raise a compliance review by clicking **Request compliance review**.

The approval form is sent to the approver.

The approver can either approve the request by clicking **Approve** or request additional approval by clicking **Request Additional Approval**.

The record state changes to Deferred. The reason stated is the one you selected when raising the exception request. The **Deferral** tab provides additional notes on the record.

Note: If the request gets rejected, the record moves to its previous state.

4. Click **Submit**.
For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approve an exception request in Configuration Compliance

Approve exception requests for remediation tasks that can't be remediated immediately. You must assess these requests for risk and then approve them for deferral until they can be remediated.

Important: As an admin or analyst, you can approve or reject an exception request from the Vulnerability Manager Worksapce.

Before you begin

Role required: sn_vulc.exception_approver

Procedure

1. Navigate to **All** > **Configuration Compliance** > **My Approvals**.
2. Select a request from your queue.
3. Approve or reject the request with appropriate comments.

Note: In case of a two-level approval workflow, after the first-level approval, the request is submitted to the second level for further approval. If there are no users in the second level, the request is automatically approved after the first-level approval.

After the request is approved, the remediation task moves to a Deferred state. In case of rejection, the remediation task reverts to its earlier state.

Define policy reason mappings

You can define the reason choices to be available to any user who requests an exception.

Before you begin

Role required: sn_vul.compliance.manager and sn_vulc.admin

Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Integration Registry**.

Note: You can either select a reason from the reason choices available in the Reason Choices table or add a new reason.

2. Click the Container Vulnerability Response - CVIT integration registry.
3. To add an existing reason choice, perform the following steps:
   a. In the Reason Choices list, click **New**.
   b. Click the magnifying glass icon to select a reason.
4. To add new reason choices to the Reason Choices table, perform the following steps:
   a. In Reason Choices list, click **New**.
   b. Click the magnifying glass icon.
   c. Click **New**.
   d. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reason Choice List form

Field	Description
Label	Unique label for this choice.
Value	Unique value for this choice. This value is mapped in the Policy Exception Reason Mappings table for the respective applications. To navigate to this table, enter sn_sec_cmn_policy_reason_mapping.LIST in the filter navigator.
Order	Order for this choice. Reasons are ordered based on this number.
Default	Option to indicate that this reason choice will be available whenever an on demand policy exception is requested. If the integration registry doesn't contain any application-specific choices, then all reason choices that have the **Default** field selected will be available.
Active	Option to display the choice in the list of reason choices.

5. Click **Submit**.

Analytics and reporting for Configuration Compliance

The following reports are provided for monitoring.

View policies, CIs, tests, and test results on the Configuration Compliance Overview reports.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Configuration Compliance reporting

The Configuration Compliance homepage provides an executive view into policies, CIs, tests, and test results, helping security staff pinpoint areas of concern quickly. Configuration Compliance significance charts can be added, as needed. You can also return Configuration Compliance -related information using the global search feature.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

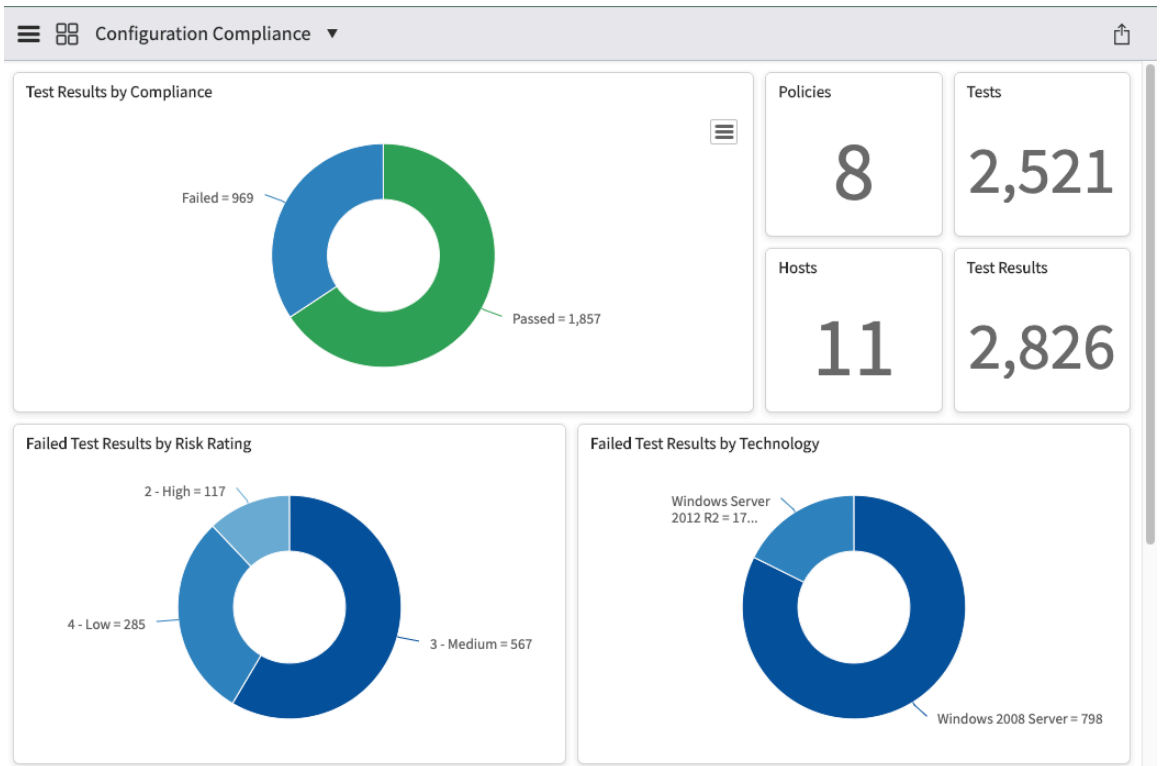
Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

In each chart, you can point to any part of a chart (bar, pie, data point) to view general data specific to that part of the chart. If you click any part of a report, a list opens to provide detailed information.

Note:

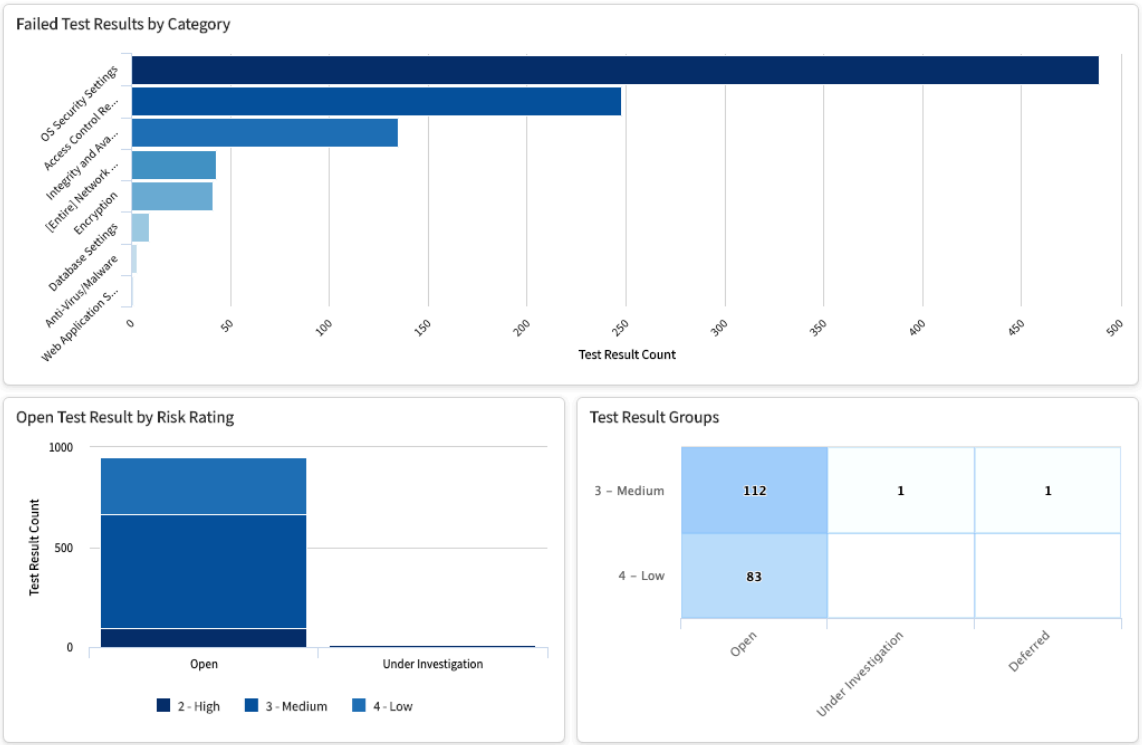
- Dashboards on the Configuration Compliance homepage are available only when the Performance Analytics for Configuration Compliance application is activated. For steps to activate this application, see Activate Performance Analytics for Configuration Compliance.
- Anyone with the sn_vulc.read role can view the dashboard. Anyone in the sn_vulc.write or sn_vulc.admin role can create and edit a dashboard. Only sn_vulc.admin can delete a dashboard.

Vulnerability Overview reports



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance report



Vulnerability Overview reports

Name	Visual	Description
Test Results by Compliance	Donut	Displays the number of open tests that have passed or failed.
Polices	Number	Number of policies with failed test results.
Tests	Number	Number of tests with failed test results.
Hosts	Number	Number of hosts with failed test results.
Test Results	Number	Displays the number of test results.
Failed Test Results by Risk Rating	Donut	Displays the number of failed tests by risk rating.
Failed Test Results by Technology	Donut	Displays models with failed tests.
Failed Test Results by Category	Bar	Displays categories with the most failed test results.
Open Test Result by Risk Rating	Bar	Displays the number of open test results by risk rating.
Remediation Tasks	Chart	Displays remediation tasks by state and risk rating.

Configuration Compliance dashboard

This Platform Analytics Solution contains prepackaged Performance Analytics and Reporting content for use with other ServiceNow AI Platform products. This Platform Analytics Solution provides visibility into non-compliant host level and cloud control plane configurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This Platform Analytics Solution contains prepackaged Performance Analytics and Reporting content for use with other ServiceNow AI Platform products. This Platform Analytics Solution provides visibility into non-compliant host level and cloud control plane configurations.

The Performance Analytics for Configuration Compliance dashboard contains multiple widgets that present data for different dimensions. It provides a comprehensive view of compliance trends, configuration issues, remediation trends, and exception management.

Note: The Performance Analytics for Configuration Compliance plugin must be installed to view the Configuration Compliance [PA] dashboard in the Next Experience framework. If not installed, you can view the existing dashboard, which is built using the reporting framework.

Activate Performance Analytics for Configuration Compliance

Activate the content pack ServiceNow Store application for the Platform Analytics Solution.

Before you begin

Activate the full, subscription version of Performance Analytics on the instance where you are activating this Platform Analytics Solution. You can activate Performance Analytics on a non-production instance without purchasing a subscription. For more information, see Activate your Performance Analytics subscription.

You need a Now Support account and permission to request applications for the instances under consideration. The Now Support account and the instance must be part of the same company. For more information, see Install a ServiceNow Product on the ServiceNow Store.

Role required: admin

About this task

Use Performance Analytics for the Configuration Compliance dashboard to generate reports on the remediation tasks, the compliance status, the remediation actions, and the exception requests.

Procedure

1. Navigate to **All** > **System Applications** > **All Applications** > **ServiceNow Store**.
2. Browse for Performance Analytics for Configuration Compliance and verify that you have the valid entitlements.
3. Search for `Performance Analytics for Configuration Compliance`.
4. Install the application.

   When you install this application, you also activate the Configuration Compliance application.

Viewing the Performance Analytics for Configuration Compliance dashboard

You can manage your most important configuration issues and remediate them quickly by viewing the reports on the Configuration Compliance Performance Analytics (PA) dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Required ServiceNow AI Platform roles

The following roles are required for the Configuration Compliance Performance Analytics dashboard:

- admin: An admin can install and activate the Performance Analytics for Configuration Compliance and make changes to the system properties.
- pa_admin: A performance analytics administrator can create and review the background jobs, indicators, breakdowns, widgets, and dashboards. This admin can also set up and start the data collection.
- sn_vulc.read: A user with the read role can review the dashboard data.

Access the Configuration Compliance dashboard

To open the dashboard, navigate to **All** > **Configuration Compliance** > **Overview**.

Starting with version 14.9 of Configuration Compliance, this dashboard can also be viewed in the New Experience UI. To view the dashboard in the new UI, navigate to **Workspaces** > **Vulnerability Manager Workspace** and click the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view other dashboards, click the drop-down next to the dashboard name. For more information, see the Dashboards in the Vulnerability Manager Workspace and Dashboards in the IT Remediation Workspace.

Note: If you are on Tokyo, you can view the dashboards in the Next Experience UI but with some functional loss.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance [PA] dashboard tabs

Overview tab

The **Overview** tab provides five filters. These filters are the Asset category, Cloud resource type, Cloud service provider, Cloud account, and Cloud region, which you can apply to visualize the reports for the filters applied. If you select a category and apply the changes, all the widgets that support the category get refreshed. Each widget displays the applied filter at the bottom and the number of filters applied on the filter icon of the widget. Click the report in a widget to view the additional information on the **KPI Details** tab. On the **KPI Details** tab, you can:

- Show the records.
- Compare the records.
- Change the chart type.
- Select the date range.
- View the trends that are based on the duration.
- Apply the additional filters including the filters that are unavailable on the **Overview** tab. An example is the Host tag.

The following example shows how you can apply the filters in the **Overview** tab and perform the actions in the **KPI Details** tab.

Compliance tab

The **Compliance** tab displays the compliance percentage for the various authoritative sources, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Data Interchange Standards Association (DISA). You can refine this list by using the column header filters and selecting a category.

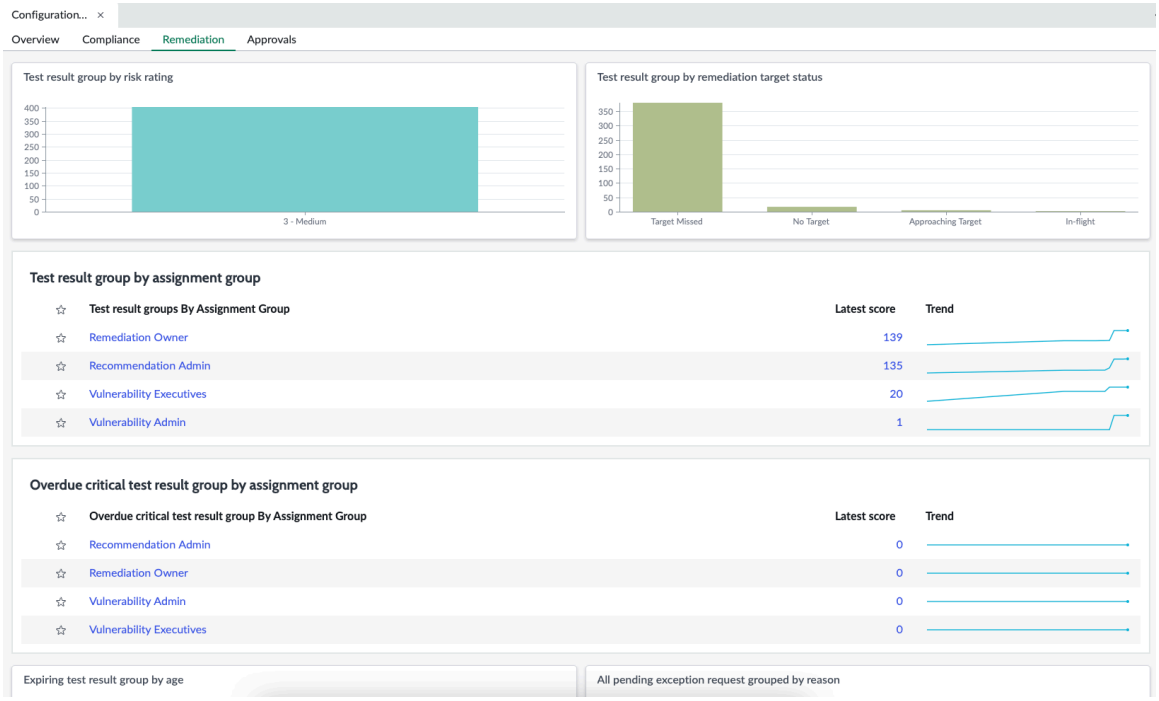
The following example shows how you can filter the data in the **Compliance** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tab

The **Remediation** tab displays the information about the progress of how remediation is going. You can use this tab to see into the misconfiguration remediation hygiene.

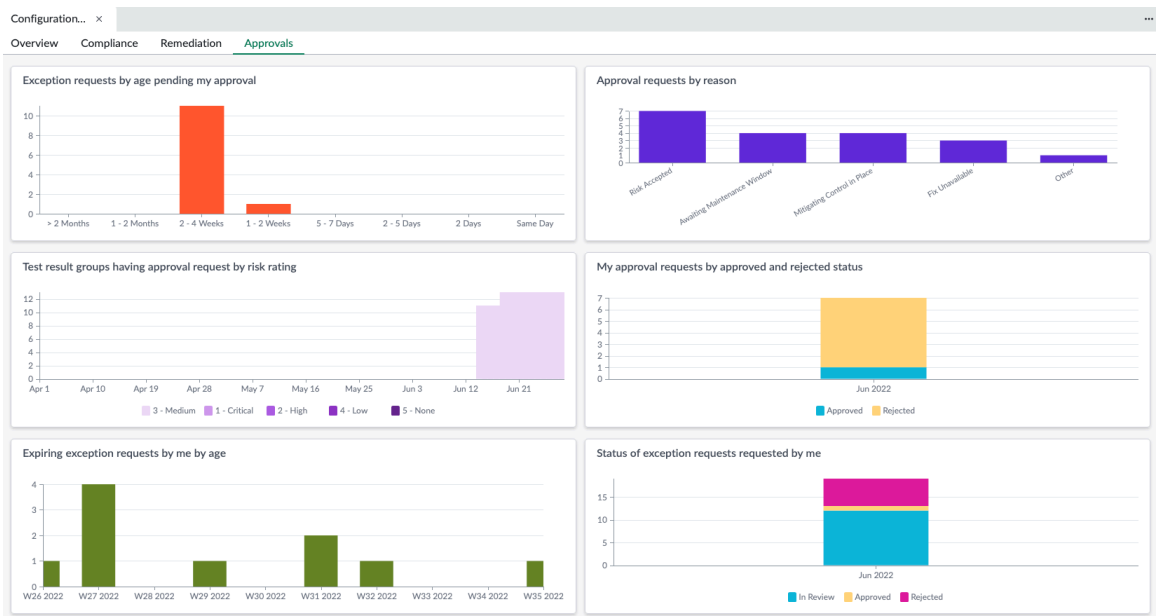
The following example shows the **Remediation** tab.



Approvals tab

The reports on the **Approvals** tab display the information about the exception requests and their approval status.

The following example shows the **Approvals** tab.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Breakdowns

The breakdowns that are used by the indicators are as follows:

- Deferred Reason
- Age
- Assignment group
- Remediation status
- Result
- Risk rating
- Asset category
- Host tag
- Configuration test
- Cloud service provider
- Cloud region
- Cloud account
- Cloud resource type

Filters

In the **Overview** tab, you can apply the following filters to the widgets to visualize the filtered data.

Name	Type	Description
Asset category	Choice	Type of asset. The four options are: • Cloud • Container • Infra • OT
Cloud resource type	Choice	Type of resource. An example is a virtual machine. The data in the filter is filled in when you run the integration.
Cloud service provider	Choice	Service provider for the cloud. The three options are:

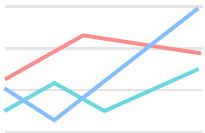
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Type	Description
		• Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Cloud account	Choice	Account ID that is created when an account is created in a cloud service. For example, AWS. The account ID data is filled into the filter when you run the integration.
Cloud region	Choice	Location where the resource is hosted.

Note: You can select multiple options from the filters and select **Apply**. Each widget shows the filters that are applied and the filters that aren't applied. Depending on the data available, the report is generated. The widget also shows the count of the filter that is supported.

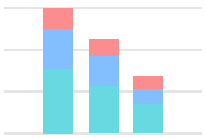
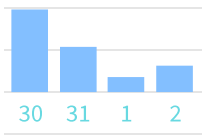
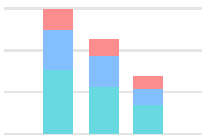
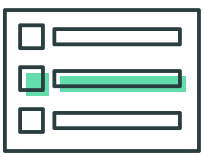
Data visualizations

Overview tab visualizations

Report name	Type	Source table	Description
Compliance Trend	Line chart 	Test Results	Information about the compliance trend: • Resources: Total number of resources that are available in the system. • Fail: Number of resources with at least one failed test result. • Pass: Number of resources with all the test results in the passed state.
Remediation Task	Single score 	Test Results	Number of remediation tasks, which are present in the system and are in an active state.
Critical remediation tasks near due	Single score	Test Results	Number of remediation tasks where the risk rating

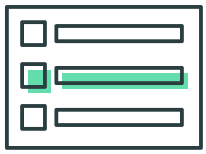
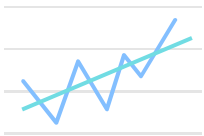
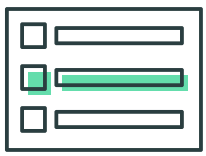
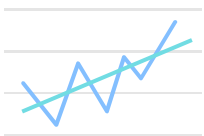
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab visualizations (continued)

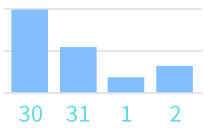
Report name	Type	Source table	Description
			is "critical" and the remediation status is "approaching target."
Test results by risk rating	Bar 	Test Results	Test results in the failed state, which are grouped according to the risk rating.
Test results by age	Bar 	Test Results	Test results in the failed state, which are grouped according to when the test results were created.
Closed test results by remediation target adherence	Bar 	Test Results	Test results in the passed state, which indicates that this test is closed.
Overdue critical test results by assignment group	List and Score 	Test Results	Number of test results where the risk rating is "critical" and the remediation status is "target missed". The report indicates that the test results are in an Open state. If the test results cross the remediation target date, it's considered as overdue.
Overdue test results-services	List, Score, and Trend	PA dashboards database view for Services	Number of test results for services where the remediation status is "target missed". This report also displays the name of the services or departments with the highest test results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab visualizations (continued)

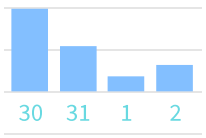
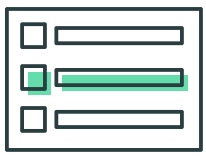
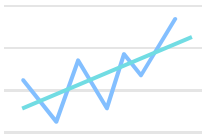
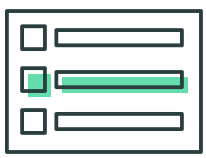
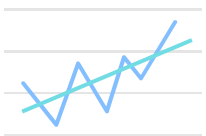
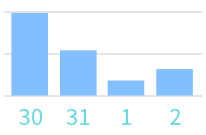
Report name	Type	Source table	Description
	 		
Overdue test results-service owners	List, Score, and Trend  	PA dashboards database view for Services	Number of test results for service owners whose remediation status is "target missed". This report also displays the name of the services or departments with the highest test results.

Remediation tab visualizations

Title	Type	Source table	Description
Remediation task by risk rating	Bar 	Remediation task	Breakdown of the risk ratings of all the test results groups that are in the active state.
Remediation task by remediation target status	Bar	Remediation task	Breakdown of the remediation targets of all the test results groups that missed the target, have no target, and are

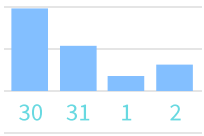
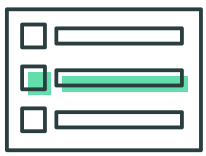
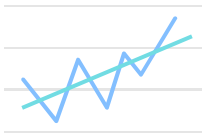
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tab visualizations (continued)

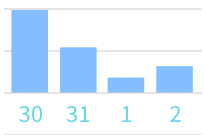
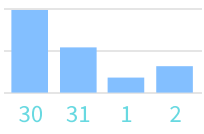
Title	Type	Source table	Description
			approaching the target.
Remediation task by assignment group	List, Score, and Trend  	Remediation task	Breakdown of the remediation tasks that are based on an assignment group.
Overdue critical remediation task by assignment group	List, Score, and Trend  	Remediation task	Breakdown of the remediation tasks that are based on an assignment group. These remediation tasks have a risk rating as "critical", and their remediation target hasn't been met.
Expiring remediation task by age	Bar 	Remediation Task	Remediation tasks that are going to expire within a certain duration. A maximum of 10 duration buckets can be created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tab visualizations (continued)

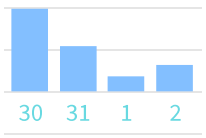
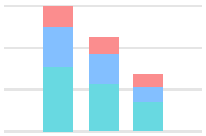
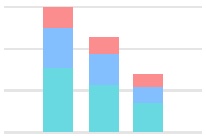
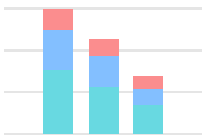
Title	Type	Source table	Description
All pending exception requests grouped by reason	Bar 	State change approval	State change approval requests that are grouped by the reason for the exception.
Critical exceptions on test results by assignment group	List, Score, and Trend  	Test Results	Test results that are in a deferred and critical state and are grouped based on the assignment group.

Approvals tab visualizations

Reports	Type	Source table	Description
Exception requests by age pending my approval	Bar 	Approval	Exception requests that are created by you and that are pending approval. The requests are grouped according to the duration of the request.
Approval requests by reason	Bar 	State change approval	State change approval requests for creating an exception and include the reason for the exception.
Remediation tasks having approval request by risk rating	Bar	Remediation task	Remediation tasks that have an approval

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approvals tab visualizations (continued)

Reports	Type	Source table	Description
			request that is based on the criticality.
My approval requests by approved and rejected status	Bar 	State change approval	Exception requests that are grouped by the approved and rejected statuses.
Expiring exception requests by me by age	Bar 	State change approval	Exception requests that are going to expire in the coming weeks. The exception requests are grouped based on weeks. Whenever an exception request is created, a date is selected for the validity of the exception request. The calculation for the age of the request is based on this date.
Status of exception requests requested by me	Bar 	State change approval	Exception requests that are created by you and that are grouped according to the following statuses: • In review • Approved • Rejected

Aggregated reports framework for Configuration Compliance

Using aggregated reports framework, you can create reports for the data that involves complex and long-running on-the-fly queries for better performance.

The aggregated reports framework improves the performance by:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- using lesser resources and rendering reports faster,
- aggregating the data and reusing aggregations and breakdowns (Group By) and
- reducing the queries to the database

When you have more than one million configuration test results, use the aggreated reports framework alongside the standard reports.

Required roles

The following roles and tasks are associated with this solution:

- ServiceNow AI Platform administrator (admin): Install and activate this Platform Analytics Solution and make any necessary changes to system properties.
- Performance Analytics administrator (pa_admin): Review the aggregations, widgets, and dashboards. Set up and start data collection. Share the dashboards with appropriate stakeholders.
- Admin (sn_vul_cmn.admin): Create aggregations.
- VR write(sn_vul_cmn.write): Edit the data in the Aggregations and Aggregated Results.
- VR read (sn_vul_cmn.read): Review the data in the Aggregations and Aggregated Results.
- Vulnerability analyst (sn_vul.vulnerability_analyst): Review Aggregated Results.

Related topics

Configure an aggregation for source data

Run multiple aggregations simultaneously

Configure the number of aggregations that can run simultaneously

Create a report using an aggregation

Configuration Compliance reference information

Several types of components are installed with activation of the Configuration Compliance application, including tables, scheduled jobs, and user roles.

The following topics provide you with reference information, troubleshooting, in addition to field data on the forms and records found in Configuration Compliance.

- Components installed with Configuration Compliance
- Test Results fields
- Resolving Configuration Compliance import issues
- Modify Qualys PC Results start date

View Configuration Compliance test groups

Once you have imported the results of a third-party scan into your instance, you can see your test compliance at the test group level. Use this view before an audit of that test group and any associated test records.

Before you begin

Role required: sn_vulc.read and sn_vulc.remediation_owner to view

About this task

Test groups are imported records and uneditable inside Configuration Compliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Test Groups**.
   The list of Test results display. Starting with v15.0 of Configuration Compliance, the **% Test Result Compliance** column displays the percentage of test results that are compliant with the tests in a test group.

   % Test Result Compliance = (No. of Test results closed in a test group/Total no. of test results associated with a test group) * 100

2. Click the **Short description** of the Test Group you want to view.

Configuration Compliance Test Group form fields

Field	Description
Source	System name of the third-party scanner, or the name entered in the ServiceNow plugin for the API that is used to communicate with Configuration Compliance.
Technologies	List of technologies associated with the test group in the third-party scanner application.
Source ID	Identifier assigned to this test group by the third-party scanner.
Source created	Date and time the test group was defined in the third-party scanner application.
Source updated	Date and time the test group was last modified in the third-policy scanner application.
Short description	Summary description or title assigned to the test group in the third-party scanner application.
Description	Detailed description of the test group as defined in the third-party scanner application.
Tests	List of tests that reference this test group. Imported from the third-party scanner. You can navigate the list to detailed information about a specific test, if necessary.
Remediation Status (Version 12.0)	
Excludes Deferred	These values do not include CIs from deferred test results. ○ **Remaining CIs**: The number (count) of configuration items (CIs) with active test results (any state other than **Closed**) for this policy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **% CIs remediated**: Percent of compliant CIs for this test group. This number excludes CIs with deferred test results. ○ **Total CIs**: The total number of CIs impacted by this test group. This count excludes deferred test results.
Includes Deferred	The values represent CIs from all active test results (any state other than **Closed**). ○ **Remaining CIs**: The number of unique CIs associated with one or more test results not closed to which this test group has been applied. ○ **% CIs remediated**: The percent of compliant CIs for this test group. ○ **Total CIs**: Total number of CIs impacted by this test group.

Starting with version 12.0, to update these values on-demand, below the Remediation status tab, click the **Update Status** related link. A message is displayed that indicates the data is being refreshed. Click the **View status** link to view progress on the update. After a few moments, any data that has changed or been updated since the last scheduled job are refreshed on the record. Updated field values are refreshed.

3. **Optional:** Disable the import of test results for a test group by selecting the **Disable import** button.

   (Optional) The value in the **Is import disabled** column changes to *true*. The test results for the test group are not imported from the upcoming ingestion.

   Note: The **Disable import** button is available for the test results obtained from the Qualys scanner only.

   Starting with v23.0 of Vulnerability Response:

   ○ You can enable or disable the import of test results for a Qualys test group in the Vulnerability Manager Workspace. For more information, see Enable or disable the import of test results for a Qualys test group.

   ○ The **Mark deprecated** button is renamed to **Disable import**.

   ○ The **Is deprecated** column is renamed to **Is import disabled**.

View Configuration Compliance authoritative sources

Use this module to view summary information about each authoritative source and to research the source publications that were used to create the record.

Before you begin

Role required:

- sn_vulc.admin to update
- sn_vulc.remediation_owner to view

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Supporting Data** > **Authoritative Sources**.
2. Click the **Short description** of the authoritative source you want to view.

Configuration Compliance authoritative sources form fields

Field	Description
Number	ID number assigned to the authoritative source by your instance during the import process.
Source	System name of the third-party scanner application, or the name entered in the scanner plugin for the API that communicates with Configuration Compliance.
Source ID	Identifier assigned to the authoritative source by the third-party scanner.
Short description	Name given to this authoritative source in the third-party scanner.
Publisher	Name of the organization or publication that was the original source of information for this authoritative source.
Citations	List of cited information about the test results. Imported from the third-party scanner. You can navigate this list to detailed information about a specific test, if necessary.

3. **Optional:** Add a **Publisher**.
4. Click **Update**.
5. You can delete this record by clicking **Delete**.
   Removes the record from your instance. If it is still in use in your third-party integration, it returns in the next import

View Configuration Compliance technologies

Use this module to view summary information about each authoritative sources and citation (also known, in Qualys, as a framework). You can research the source publications that were used to create the record.

Before you begin

Role required:

- sn_vulc.admin to update
- sn_vulc.remediation_owner to view

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Supporting Data** > **Technologies**.
2. Click the **Short description** of the authoritative source you want to view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance authoritative sources form fields

Field	Description
Number	ID number assigned to the authoritative source by your instance during the import process.
Source	System name of the third-party scanner, or the name entered in the third-party scanner plugin for the API that communicates with Configuration Compliance.
Source ID	Identifier assigned to the authoritative source by the third-party scanner.

3. You can delete this record by clicking **Delete**.
   Removes the record from your instance. If it is still in use in your third-party integration, it returns in the next import

View Configuration Compliance tests

Use this module to research detailed information about these tests. Included are the expert source citations that were used when creating them, the third-party configuration policies in which they are used, and the results obtained from the scan.

Before you begin

Role required:

- sn_vulc.admin to update
- sn_vulc.remediation_owner to view

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Controls**.
2. Navigate to **All** > **Configuration Compliance** > **Tests**
3. From the list, open the control (compliance test) you want to view.

   Starting with version 12.0, to update these values on-demand, below the Remediation status tab, click the **Update Status** Related link. A message is displayed that indicates the data is being refreshed. Click the **View status** link to view progress on the update. After a few moments, any data that has changed or been updated since the last scheduled job are refreshed on the record. Field values such as the**Risk Score**, **Risk Rating**, **Remediation target date**, **State**, and the fields on the **Remediation Status** tab are refreshed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance test form fields

Field	Description
Number	Number assigned to the control during the import process.
Result	Status of the scan. Pass or Fail. If this test belongs to multiple remediation tasks, then its state is determined following an order of precedence.
Source	System name of the third-party integration application, or the name entered in the plugin for the API that is used to communicate with Configuration Compliance.
Criticality	Severity of the configuration issue or issues associated with the control as defined in the third-party integration. The level of criticality is adjusted to match the granularity of similar vulnerability indicators available in Vulnerability Response. The possible levels are: **Critical** The configuration issue associated with the control is causing a disruption to one or more business-critical CIs. **High** The configuration issue associated with the control is a threat, but is not causing a shutdown of critical network resources. **Moderate** The configuration issue associated with the control is a risk, but is not an immediate threat. **Low** The configuration issue associated with the control is a low-level threat and can be ignored in favor of CIs that are at greater risk. **Minor** The configuration issue associated with the control is a minor risk and can be ignored if necessary.
Source ID	Identifier assigned to the control by the third-party integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Category	Major classification category given to this type of control by the third-party vendor.
Risk score	This is a rollup risk score. This risk score is weighted, with 85% of the score from the max risk score across all Test Results not 'Closed' (Open, Under Investigation, Awaiting Implementation, Deferred, Resolved), and 15% of the score from the number of test results that are not 'Closed'.Value calculated by risk score calculators that is based on the business criticality and test criticality values of test results.
Sub-category	Sub-category assigned to this class of test by the third-party vendor.
Risk rating	Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.
Technologies	List of technologies covered by this test.
Source created	Date the test was first defined in the third-party integration.
Source updated	Date the test was last updated in the third-party integration.
Short description	Summary description or title entered or assigned to the test in the third-party integration.
Remediation Status (v 12.0)	
Excludes Deferred	These values do not include deferred test results. ○ **Open test results**: The number (count) of active (any state other than **Closed**) test results for this configuration test. ○ **% Test results remediated**: The percent of remediated test results for this remediation task. ○ **Total test results**: The total number of test results for this remediation task.
Includes Deferred	These values include deferred test results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Open test results**: The number (count) of all active (any state other than **Closed**) test results for this remediation task. ○ **% Test results remediated**: The percent of remediated test results for this remediation task. ○ **Total test results**: The total number of test results for this remediation task.
Description	Long description of the test. For the Qualys Vulnerability Integration, this field defaults to the contents of the Qualys Cloud Platform cover page.
Remediation	Steps instructions describing how to remediate the non-compliance.
Related Tabs	
Citations	List of citations entered for each authoritative source associated with the test.
Test Groups	List of Configuration Compliance test groups that use this test.
Test Results	List of CIs affected by the configuration issue or issues associated with this test. You can access individual tests, ServiceNow configuration items, or the list of affected technologies, if necessary.
GRC Policy Statements	If the GRC Policy and Compliance Management plugin is installed, this tab contains the related GRC policy. You can edit this list to add or remove policy statements.

View Configuration Compliance test results

View Configuration Compliance test results for auditing and remediation. The test results are automatically created during third-party vulnerability integration imports.

Important: You can view the test results created during the third-party vulnerability integration imports in the Vulnerability Manager Workspace. For more information, see List page in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vulc.read to view
- sn_vulc.remediation_owner to view and update
- sn_vulc.delete to delete

About this task

Configuration Compliance does not create or update the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using **Test Result Groups**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Test Results**.
   Starting with v15.0 of Configuration Compliance, the following columns appear in the Test Results list.

Test Results list

Column	Description
Active	Indicates if a test result is active. A test result is marked: ○ True: If the State isn't Closed. ○ False: If the State is Closed.
Age	Time period for which a test result is active since it was last open. This field is empty for the closed test results. Format: Days HH:MM: SS
Age closed	Time period for which a test result was active before it transitioned to 'Closed'. When the test result transitions to 'Closed', the value from the Age column is displayed in the Aged closed field. This field is empty for an active test result. Format: Days HH:MM: SS For more information on how to customize the Age closed calculation, see the KB1703270 article.
Closed	Timestamp at which a test result is closed. Format: YYYY-MM-DD HH:MM: SS
Last opened	Timestamp at which a test result is opened, that is, when the **Active** field value changes to *true*.

2. Open the control that you want to view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance test result form fields

Field	Description
Number	The number assigned to the test during the import process.
Source	The system name of the third-party SCA application, or the name entered in the application plugin for the API that is used to communicate with Configuration Compliance.
Source ID	The identifier assigned to the control by the SCA application.
Result	Passed, Failed, Error, or Unknown. Imported from Qualys.
Risk score	Calculator result for this test. Prior to v15.0 of Configuration Compliance, the risk score of a passed test result is set to '0'. Starting with v15.0 of Configuration Compliance, the risk score of the passed test result isn't changed to '0' so that you can estimate the risk mitigated. The risk score of the passed test result isn't included in calculating the risk score of a remediation task.
Risk rating	Based on a range of risk scores on a 1-5 numeric scale that rates overall risk based on a range of risk scores as 1 - Critical to 5 - None. This field replaces the Priority field in previous versions.
State	Calculated from the remediation tasks that the test result belongs to. If the test result belongs to multiple groups, an order of precedence is applied to determine state.
Resolution	Calculated from the remediation tasks that the test result belongs to. If the test result belongs to multiple groups, an order of precedence is applied to determine resolution.
First seen	Date first imported into Configuration Compliance. Starting with v13.1.1, the **First seen** field displays the date provided by the scanner. Otherwise, it displays the date first imported into Configuration Compliance.
Last seen	Date last imported into Configuration Compliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Starting with v13.1.1, the **Last seen** field displays the date provided by the scanner. Otherwise, it displays the date last imported into Configuration Compliance.
Last pass	Latest date on which the test result is passed.
Test	Name of the test.
Configuration item	Name of the CI attached to the test.
Technology	Software version running on the CI.
Description	Description of the test
Expected Values	Expected values configured in Qualys and imported by Configuration Compliance. This value is a Boolean expression that when evaluated to true makes the test result **Passed**. The expression can be a combination of logical, set, or regular expression operators.
Actual Values	Values returned by the test. These values are plugged into the expected values Boolean expression to determine if the result should pass or fail. They're imported from Qualys. Starting with version 14.9 of Configuration Compliance, the Extended Evidence and Cause of Failure values are added in the Actual Values column.
Remediation	Remediation instructions.
Related Tabs	
Remediation Tasks	Remediation tasks associated with this test result.
Test Result History	Related list of test results that show the history of pass/fail results for the same CI/technology/test.

View a remediation task

You can view, or, alternatively, create a remediation task and perform remediation.

Important: You can view the remediation tasks in the Vulnerability Manager Workspace. For more information, see List page in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vulc.admin to update or create
- sn_vulc.remediation_owner to view

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Procedure

1. Navigate to **All** > **Configuration Compliance** > **Remediation Tasks**.
2. From the list, click the record you want to view.
3. Alternatively, click **New** to create a new remediation task and fill in the fields.

Configuration Compliance Remediation Task form fields

Field	Description
Number	The automatically generated number for this record.
State	Progress status of the group. ○ Open ○ Under investigation ○ Awaiting Implementation ○ Deferred ○ Resolved ○ Closed
Risk score	This score is the rolled-up value of the risk scores for all the active test results in a remediation task. This score changes as test results are remediated in the test result group.
Assignment group	Group selected to work on this remediation task.
Risk rating	The amount of risk a failed test result poses to your system. It is based on a range of risk scores on a 1-5 numeric scale that rates risks as Critical (1) to None (5).
Assigned to	Individual from the selected assignment group that works on this set of tasks.
Remediation target	Date by which the test results should be remediated, since first identified.
Created	The date and time this remediation task was created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Remediation status	Status of the remediation for the group. It is determined by the test result with the nearest due date. For open groups states include In-flight, Approaching Target and Target Missed. For closed groups states include No Target, Target Met and Target Missed. For calculated remediation target dates, if the remediation task is closed, the overall remediation status of all of the closed test results is shown in the remediation task. Those determine whether the group met its date or not. A closed remediation task remediation Status is **No Target** if none of its closed results had a remediation target date. It is **Target Missed** if any of its closed results missed their target date. It is **Target Met** if at least one closed result met its target and none of the others missed it.
Updated	The date and time this record was last modified.
Short description	Brief description of this test result group.
Description	Long description of the test result group that includes the list of software associated with this test result group.
Test	The configuration test associated with this test result group.
Remediation Status (Version 12.0)	
Excludes Deferred	These values do not include deferred test results. ○ **Open test results**: The number (count) of active (any state other than **Closed**) test results for this remediation task. ○ **% Test results remediated**: The percent of remediated (closed) test results for this test result group. ○ **Total test results**: The total number of test results for this remediation task.
Includes Deferred	The values represent all active test results (any state other than **Closed**).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Open test results**: The number (count) of active (any state other than **Closed**) test results for this test result group. ○ **% Test results remediated**: The percent of remediated (closed) test results for this remediation task. ○ **Total test results**: The total number of test results for this remediation task.
Group Configuration	The type of filtering used to select the test results for the remediation task.
Grouping method	Name of method used.
Group rule	Name of the group rule used.
Notes	System notes associated with the record.
Related Links	**Version 12.0: Update status link**. Update the values on the test result record on-demand. View any data that has changed or been updated since the last scheduled job.
Test Results	The test results in this remediation task.
Change requests (v 12.0)	The list of change requests associated with this test result group.
State Change Approvals (v 12.0)	Status and states of change request approvals associated with this remediation task.

Test result and remediation task state transitions in the Configuration Compliance application

The states of configuration test records and their associated remediation tasks (RTs) are impacted if test result records are deferred, resolved, reopened, and transferred to other remediation efforts (REs).

State transition scenarios between test results and remediation tasks

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

The following table details how states and sub-states transition between configuration test results and remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a remediation task state transitions from...	...to state/sub-states	Its associated test results states transition from...	...to state/sub-states	Description
Open	Under Investigation	Open	Under Investigation	States transition bi-directionally.
Open	In Review	Open	In Review	States transition bi-directionally.
Open	Deferred/with any reason selected for Resolution	Open	Deferred	Test results keep the same reason for Resolution as the remediation task.
Deferred/with any reason for Resolution	Open	Test results remain Deferred		Test results keep the same Resolution as the remediation task.
Open	Resolved/ Fixed	Open	Resolved	States/sub-states transition bi-directionally.
Open	Resolved and Resolved to Closed/Fixed	Open	Resolved	If a remediation task transitions to Closed/ Fixed, it can transition back to Open. If the task transitions to Open, its associated test results transition from Resolved back to Open.
Open	Resolved	Open	Resolved	States/sub-states transition bi-directionally.
Open	Resolved/ Cancelled	Open	Resolved	States/sub-states transition bi-directionally.
Open	Resolved and Resolved to Closed	Open	Resolved	If a remediation task transitions to Closed automatically, its associated test results can transition back to Open.
Open	Resolved and Resolved to Closed/Result Invalid	Open	Resolved and Resolved to Closed/Result Invalid	If a remediation task transitions to Resolved it can

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a remediation task state transitions from...	...to state/sub-states	Its associated test results states transition from...	...to state/sub-states	Description
				transition back to Open. If a remediation task transitions to Closed/Result Invalid, it and its associated test results cannot be reopened.
Open	Closed/Fixed	Test results remain Open		

Note:

- Starting with v14.12 of Configuration Compliance, the **Result invalid** option is removed in the **Resolution** filed in the Close modal.
- Starting with v14.12 of Configuration Compliance, the **Remediation Task State Approval** workflow is deprecated and replaced by the flow Remediation Task State Approval in the flow designer.

State synchronization between change requests and remediation tasks

There is a synchronized relationship between the State fields of remediation tasks and the State fields of change requests (CHGs) in the Configuration Compliance application.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

As a change request moves through its life cycle, it also moves the state of any related remediation tasks automatically. State synchronization is enabled by a system property (sn_vulc.cr_state_sync) by default in your instance when you download the Configuration Compliance application from the ServiceNow Store starting with v12.0.

When state synchronization is enabled, the CHG State field changes the remediation task State field automatically in the following cases:

- When a new change request is created for a remediation task, if it is not in **Awaiting Implementation**, the remediation task state moves forward to **Awaiting Implementation**.
- When an existing change request is associated to a remediation task, if it is not in **Awaiting Implementation**, the remediation task state moves forward to **Awaiting Implementation**.
- After the tasks on a change request are completed (`Implemented`), and the CHG is moved to the **Review** state, the remediation task moves forward to **Resolved**.

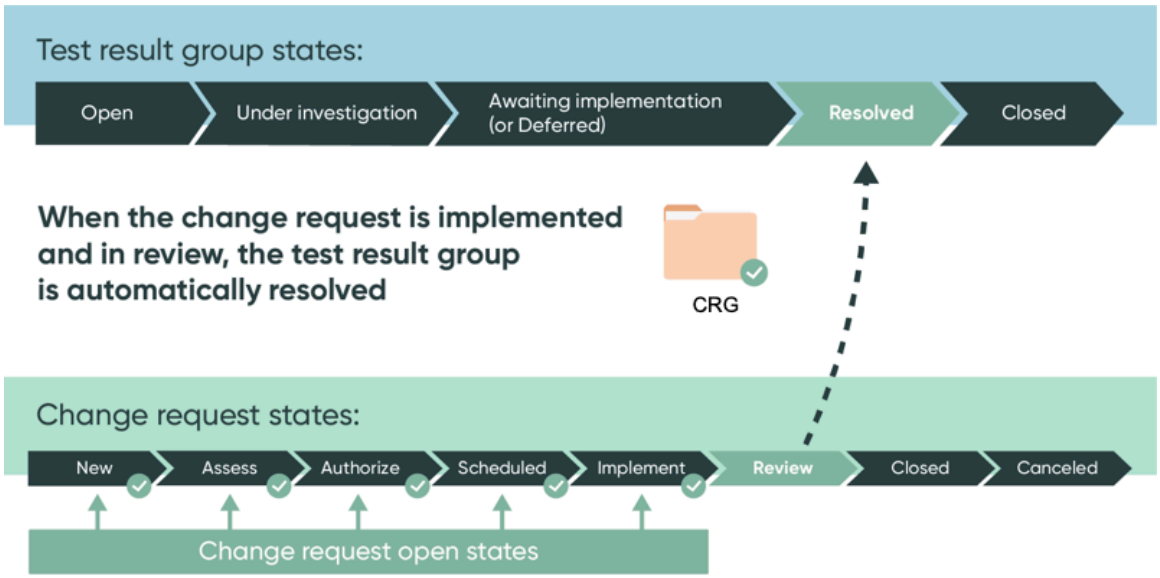
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information and examples of state synchronization, see the following sections.

Note: You can still manually move change requests and remediation tasks through the states of their life cycles on their respective records with state synchronization enabled, but when the system registers that a change request has changed its state, or you add a change request or remove it from a remediation task, state synchronization potentially can override your manual intervention. However, change request states do not automatically move the remediation task from the **Closed**.

Forward state synchronization

The following image illustrates how CHG states automatically move remediation task states in a forward life cycle, that is, from **Open** to **Resolved**.



You can create new change requests for any remediation task in a state other than **Resolved** or **Closed**. State synchronization automatically moves the TRG bi-directionally through the **Open**, **Under Investigation**, **Awaiting Implementation**, and **Resolved** states. This movement is based on certain values of the state field on the change request. State synchronization between the change request and the remediation task is invoked automatically unless the check box (**Add CIs to CR**) is displayed on a form and you choose to clear the check box.

The remediation task does not move forward to **Resolved** when a CHG is in its open states. Any CHG in states prior to **Review** in its life cycle such as, **New**, **Assess**, **Authorize**, **Scheduled** or **Implement**, as shown in the preceding figure, are considered open states for the CHG. Open states do not move the state field on the remediation task, because investigations or tasks on the CHG are not completed. State synchronization is invoked when a CHG is created for, or associated to, the remediation task, or when the state of an existing relationship changes on the CHG. The completed CHG states are **Review** and successfully **Closed**. When a CHG is closed successfully, its closed codes are: **Successful**, or **Successful with issues**, in which case the remediation task moves forward to **Resolved**.

Backward state synchronization

As a CHG is processed during its life cycle, it may be canceled at some point. In this case, if the CHG is **Canceled**, or **Closed** (with a close code of **Unsuccessful**), the remediation task automatically moves back to **Under Investigation**. The remediation task moves back to **Under Investigation**, because there is no active plan to remediate the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a remediation task is in a **Resolved** state, and you create a new CHG or associate it to an existing CHG in one of the initial open states, the remediation task automatically transitions back to **Awaiting Implementation**. The remediation task moves back to this state, because more work is now assigned to the CHG.

Remediation tasks with more than one CHG

If a remediation task in **Awaiting Implementation** has more than one CHG associated with it, state synchronization is based on the status of the CHG in the earliest state of its life cycle. For example, say a remediation task has four CHGs associated with it, CHG1, CHG2, CHG3, and CHG4 as shown in the following table.

CHG number	CHG state
1	**Implement**
2	**Canceled**
3	Closed (close code of **Unsuccessful**)
4	Closed (close code **Unsuccessful**)

State synchronization between the CHG and the remediation task in this case is based on CHG1, which is in the earliest state of the four CHGs, (**Implement**). In this case, the remediation task remains in **Awaiting Implementation**.

In another example, if a remediation task is in the **Resolved** state and has an existing CHG that has been implemented and is in the **Review** state, and a new CHG is created, the remediation task moves back from **Resolved** to **Awaiting Implementation**. State synchronization is based on the CHG in the **New** state, which is the CHG in the earliest state.

CHG number	CHG state
1	Review
2	New

Also, when remediation tasks have more than one CHG, the state of the remediation task transitions automatically in the following cases:

- When a CHG moves forward to **Review**, if all other CHGs associated with the remediation task are in **Review** or **Closed** states (with a successful close code), the remediation task automatically transitions to **Resolved**. Any other related CHGs that are canceled or closed unsuccessfully are ignored.
- When a CHG moves to **Canceled** or **Closed** (close code of **Unsuccessful**), if all other CHGs associated with the remediation task are in the same state, then the remediation task automatically transitions back to **Under Investigation**.

For more information about remediation task states and what you can do in each state, see Configuration Compliance states.

Domain separation and Configuration Compliance

Domain separation is supported in Configuration Compliance. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

How domain separation works in Configuration Compliance

With domain separation you can standardize (Configuration Compliance) procedures, across the customer base you serve, with lowered operational costs and a higher quality of service.

Separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

Domain separation support in Configuration Compliance by version releases

Release	Support level	Notes
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	

Domain separation for the Configuration Compliance application covers the following product functionality:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Ingests the test results from third-party scanners (Qualys) in the correct domain.

  The data ingests in the same domain as that of the integration user, whose credentials are used for integration.

- Re-scans specific hosts from Configuration Compliance in the domain from which it was requested.
- Uses the CMDB CI lookup process to ensure that the CI information from the scanners matches the CIs in CMDB of the integration user's domain.
- Calculates risk scores at the test result level as per the risk score calculator defined in the same domain as that of the integration user.
- Remediation Task rule(s) can be defined, assigned, and stay in, the same domain as the domain of the integration user.
- Remediation tasks created using the doc remediation task rules stay in the same domain as where the remediation task rules are created.
- Deferral workflow goes through the approval process in the same domain for which the deferral is requested.
- Reports and dashboards display the test result states such as age of test results, open test results by CI, test results by impact in the domain to which it belongs.
- Knowledge from third-party scanners (Qualys) can be ingested in the global domain and data can be shared across multiple clients.

Note: In all the above cases the overarching principles of visibility in separated domains separation in the ServiceNow AI Platform apply.

Use cases

The Configuration Compliance application manages the life cycle of a test result end to end. The following use cases are domain-separation aware:

- **Ingest** test results from Qualys
  - Ingest data from multiple instances
  - De-duplicate the test results
  - Match up with CMDB CI
- **Enrichment** of test results with risk scores
  - Asset enrichment (CMDB)
  - Risk score
- **Group** test results and assign the remediation task
  - Automatically group the test results
  - Automatically assign the remediation task
- **Remediate**
  - Remediation task assigned as a remediation task
  - Comprehensive remediation life cycle
  - Deferral workflow
- **Measure** the security posture of the organization and compliance management program

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Results trend, by compliance, category, criticality and technology
- Status and distribution on policies, tests, hosts, test results, and risk score

Setup

Setting up domain separation for Configuration Compliance does not require any additional steps. All Configuration Compliance tables acquire the Domain column after the instance is domain separated. You can direct test result integration import data to specific domains. For more information, see Create domain-separated imports for an integration. For more information on additional precautions and settings, see Additional settings for domain separation.

Domain-separated data

Data can be domain separated, which means:

- Test results ingested from third-party scanners stays in the same domain as the domain of the integration user, and is not accessible from any other domain.
- Test results or hosts in one domain cannot be viewed from other domains.
- The risk scoring algorithm and the remediation task rules cannot be viewed by anyone outside the domain.
- Deferral workflows created in one domain are not visible in another domain.
- All email notifications are contained within the domain they belong to.

How compliance analysts manage their own application data

- Analysts create their own application installation, multi-source application management, and CI lookup rules.
- Analysts can configure specific integrations exclusively for use within the domain.
- Analysts can create their own deferral and change management workflows.
- Analysts can create their own remediation task rules, risk-scoring logic to accurately prioritize results, auto-assign remediation tasks and assign to the correct assignment group.
- Domain users create a manual remediation task and then close it.

Business logic and processes that can be domain-separated by instance owner

- Configuration Compliance users and groups
- Configuration Compliance integrations (starting with the Madrid release)
- Complete setup configuration (user and group management, application installation, multi-source application management, CI lookup rules, remediation task rules, risk calculators, etc.)
- Complete remediation life cycle including deferral

Related topics

Domain separation for service providers

Test Results fields

Test results are automatically created during third-part vulnerability integration imports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Configuration Compliance does not create or update the test results, but imports them as part of a third-party integration. Once they are viewable in Configuration Compliance, they are remediated using **Test Result Groups**.

Test results fields

Field	Description
Number	Number assigned to the test result during the import process.
Source	System name of the third-party integration application, or the name entered in the application for the API that is used to communicate with Configuration Compliance.
Source ID	Identifier assigned to the test result by the third-party integration.
Risk Score	Score based on the *Criticality* value of the test. If you do not have installed and configured, a middle value of 50 is used.
Resolution	Resolution of the test result, calculated from associated groups.
Result	Status of the scan. Pass or Fail. If this test belongs to multiple remediation tasks, then its state is determined following an order of precedence.
State	State of the test result, calculated from associated groups.
Assignment group	Group selected to work on this test result.
Assigned to	Individual from the selected assignment group to work on this test result.
Assignment type	Type of assignment. Choices are: • Rule • Manual • None
Assignment rule	Which assignment rule was used with this test result, when applicable.
First seen	Time and date the test result was first seen.
Last seen	Time and date the test result was last seen.
Test	The control that this result belongs to.
Configuration item	Configuration item associated with this test result.
Technology	Technology associated with this test result.
Description	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Detailed description of the test result as defined in the third-party scanner application.
Expected Values	
Expected values	Description and expected values as defined in the third-party scanner application.
Actual Values	
Actual values	Description and actual values as defined in the third-party scanner application.
Remediation	
Remediation	Remediation action as defined in the third-party scanner application.

The following are the vulnerable items related lists.

Related List	Description
Remediation Tasks	Remediation tasks associated with this test result.
Test Result History	List of past records containing different results.

Configuration Compliance criticality maps

Configuration Compliance criticality mapping transforms criticality fields from the source to fields in Configuration Compliance.

The Configuration Compliance base system ships with a standard Qualys Cloud Platform to standard ServiceNow mapping. Creating or editing a criticality map is intended only for customized or non-standard third-party mappings in your environment.

Configuration Compliance states

With Configuration Compliance, you can see a state model to learn what the status of the remediation task is at any given time. The remediation task states control the test result states by precedence.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Remediation Task States

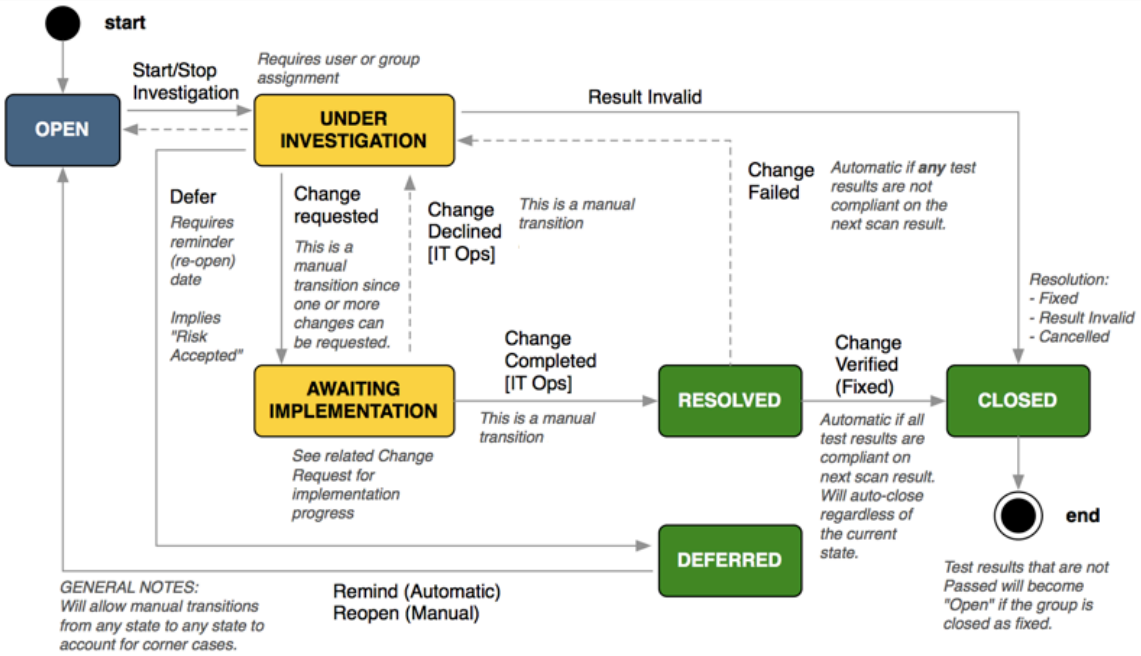
Remediation tasks (RTs) have many possible states. Automatic transition is available from the Resolved state based on the next scan results. If all test results pass on the next scan, the remediation task is closed. Otherwise, it transitions to the Under Investigation state. The system

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

verifies this closed state, but it re-evaluates the remediation task state if a test result is added to or deleted from the remediation task. The work notes are updated to reflect the transition.

The following figure shows how the state of a remediation task transitions from the Open state to the Closed state.

Configuration Compliance state flow (prior to v15.0)



Note:

- Each remediation task form contains **Follow** and **Update** buttons, which are standard for ServiceNow tasks.
- Starting with v15.0 of Configuration Compliance, the following have been removed:
  - **Close** button
  - the **Resolution** field in the Resolve modal.

The following table lists the Configuration Compliance states.

Configuration Compliance states

State	Description
Open	State upon creation.
Under Investigation	Triggered by the **Start Investigation** button. From this state, you can: **Create a Change Request** For more information, see Create a change request in Configuration Compliance. **Request exception** Provide a reason and select a reopen date. **Delete** Confirm the deletion. Removes the remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance states (continued)

State	Description
	Mark as false positive Provide a reason and notes. Marks the remediation task as false positive.
In Review	Triggered when the remediation task is being assessed for the next action. Typically used to validate investigation outcomes or approve proposed changes/exceptions before implementation. From this state, you can transition to any of the following based on your approval or rejections: **Awaiting Implementation** Transition to awaiting implementation if approved **Under Investigation** Transition back to under investigation if further analysis is required. **Delete** Confirm the deletion. Removes the remediation task.
Deferred	Triggered by the **Defer** button. From this state you can: **Reopen** Transition back to an Open state. **Delete** Confirm the deletion. Removes the group. Deferment information appears under the **Defer/Close** related tab. On the defer date, the group reopens for remediation.
Awaiting Implementation	Triggered by the **Awaiting Implementation** button. From this state you can: **Create a Security Incident** For more information, see Create a security incident. **Create a Change Request** For more information, see Create a change request in Configuration Compliance. **Resolve** In the **Resolution notes**, add the reason why you are resolving the Remediation Task. The state becomes Resolved. Notes appear under the **Resolution** related tab. **Delete** Confirm the deletion. Removes the remediation task.
Resolved	Triggered from the **Resolve** button. From this state you can: **Create a Security Incident** For more information, see Create a security incident. **Reopen**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Compliance states (continued)

State	Description
	Transition back to an Open state. **Delete** Confirm the deletion. Removes the remediation task. Notes appear under the **Notes** related tab. Resolution information appears under the **Resolution** related tab. The notes reflects in the **Work notes** of all the test results associated with the Remediation Task.
Closed	Triggered from the **Close** button or **Mark as false positive** button. Starting from v14.12 of Configuration Compliance, you can close a remediation task by marking it as false positive. From this state you can: **Reopen** Transition back to an Open state. **Delete** Confirm the deletion. Removes the group. Closure information appears under the **Defer/Close** related tab. The notes reflects in the **Work notes** of all the test results associated with the Remediation Task.

- If the Remediation Task is marked as Closed or Fixed and if the test result added is not itself Closed or Fixed, the test result state does not change, and the remediation task state is changed to Open.
- When you create a new remediation task or split a remediation task, the **Reason**, and **Until** fields are reevaluated for new and old remediation tasks. When the state of all test results is Deferred, the value in the **Reason** and **Until** fields are rolled up to the remediation task.
  - If all the test results in a remediation task are deferred, and have the same **Reason**, then the remediation task is assigned the same **Reason**. Otherwise, the **Reason** field is changed to **None**.
  - The date in the **Until** field is updated with the closest until date of all the remediation tasks to which the test results belong to.

  Note: This evaluation is done by the *`Rollup test result values to test result RT1nd configuration test`* scheduled job, which runs every one hour.

- If the **Last Seen** is greater than the **Resolution date** for a resolved test result, then the test result is reopened. In a resolved Remediation Task, if at least one test result is reopened during ingestion, then the remediation task moves to the Under investigation state.

Test Result States

The state of a remediation task also changes the state of its associated test results. This mechanism has two cases:

Test results that belong to only one remediation task

Results match the state of the remediation task with three exceptions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If the remediation task changes its state to Closed and its resolution (substate) to Fixed, the item ignores that change and then falls back to the Open state.
- If the remediation task changes its state to Closed and its resolution (substate) to Cancelled, the item ignores that change and then falls back to the Open state.
- If the test result source status is Fixed (updated by a scan or import), then when the remediation task changes its state, the test result changes its state to Closed (Fixed) no matter what state the remediation task is in.

Test results that belong to multiple remediation tasks

Test results do not match the state of the remediation task automatically. Instead, it searches among all the associated groups to find the state with the highest precedence to apply. This is the state of precedence:

Closed > **Closed (substate: False positive)** > **Deferred** > **Resolved** > **In Review** > **Awaiting Implementation** > **Under Investigation** > **Open** > **Closed (substate: Cancelled)** > **Closed (substate: Fixed)**

Note: **Closed (substate: Fixed)** and **Closed (substate: Cancelled)** are two special cases.

Note: Starting with v15.0 of Configuration Compliance, the **Result Invalid** substate has been deprecated.

Remediation Task state examples

For example:

Remediation Tasks State	Test result State
RT1: **Open** > **Under Investigation** RT2: **Open**	**Under Investigation** When RT1 is Under Investigation and RT2 is Open, the test result changes to Under Investigation, since after the search, between RT1 and RT2, RT1 has the state with the highest precedence.
RT1: **Under Investigation** RT2: **Open** > **Under Investigation**	**Under Investigation** When RT2 is Under Investigation and RT1 is Under Investigation, the test result stays as Under Investigation, since after the search, between RT1 and RT2, they have the state with the same precedence.
RT1: **Under Investigation** RT2: **Under Investigation** > **Awaiting Implementation**	**Awaiting Implementation** When RT2 is Awaiting Implementation and RT1 is Under Investigation, the test result changes to Awaiting Implementation, since after the search, between RT1 and RT2, RT2 has the state with the highest precedence.
RT1: **Under Investigation** > **Deferred** RT2: **Awaiting Implementation**	**Deferred**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation Tasks State	Test result State
	When RT1 is Deferred and RT2 is Awaiting Implementation, the test result changes to Deferred, since after the search, item 1 found out that between RT1 and RT2, RT1 has the state with the highest precedence
RT1: **Deferred** RT2: **Awaiting Implementation** > **Closed (Result Invalid)**	**Closed (Result Invalid)** > **Deferred** When RT2 is Closed and the resolution (substate) is Result Invalid, and RT1 is Deferred, the test result changes to Closed (Result Invalid), since after the search, between RT1 and RT2, RT2 has the state with the highest precedence.
RT1: **Deferred** RT2: **Closed (Result Invalid)** > **Open (via Reopen)**	**Deferred** When RT2 is re-opened and its state changes to Open, and RT1 is Deferred, the test result changes to Deferred, since after the search, between RT1 and RT2, RT1 has the state with the highest precedence.
RT1: **Deferred** RT2: **Awaiting Implementation** > **Closed (False Positive)**	**Closed (False Positive)** When RT2 is Closed and the resolution (substate) is False Positive and RT1 is Deferred, the test result changes to Closed (False Positive), since after the search, between RT1 and RT2, RT2 has the state with the highest precedence.

Test result state special cases

Remediation Task State	Test result state
RT1: **Under Investigation** RT2: **Awaiting Implementation** > **Closed (Fixed or Cancelled)**	**Under Investigation** When RT2 is Closed (substate Fixed or substate Cancelled), and RT1 is Under Investigation, the test result changes from Awaiting Implementation (previously, the highest precedence) to Under Investigation (currently, the highest precedence).
RT1: any state RT2: any state	If the test result source status is Fixed (updated by a scan or import), then when the remediation task changes its state, the test result changes its state to Closed (Fixed) no matter what states the other associated remediation tasks are in. The test result search for remediation task state does not occur.

State roll-up and roll-down scenarios

State roll-up and roll-down scenarios automatically sync the status of remediation tasks (RTs) and configuration test result (CTR), ensuring real-time updates across both. This dynamic interaction reduces manual tracking, enhances accuracy, and provides users with an up-to-

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

date view of progress, making configuration compliance more efficient and helping users make informed decisions quickly.

Roll-up behaviour

When configuration test result (CTR) state change, these changes may propagate up to the remediation task (RT) level.

The following table summarizes key roll-up scenarios where changes in configuration test result (CTR) state may influence the associated remediation task (RT) state, based on closure conditions, reassignments, and deferrals.

Roll-up scenarios

CTR State	RT State
Open > Closed-Fixed	Open > Closed-Fixed
Open > Closed-Stale	Open > Closed-Cancelled

Roll-down behaviour

When the state of a remediation task changes, the state is often propagated to the associated CTRs unless overridden by manual updates or exceptions.

The following table summarizes key roll-up scenarios where changes in remediation task (RT) state may affect the associated configuration test result (CTR) state, based on precedence rules and special conditions.

Roll-up scenarios

RT State	CTR State
Open > Under Investigation	Open > Under Investigation
Open > In Review	Open > In Review
Open > Deferred	Open > Deferred
Deferred > Open	Remains Deferred
Open > Resolved-Fixed	Open > Resolved-Fixed
Open > Resolved-Fixed > Closed-Fixed	Open > Resolved-Fixed > Closed-Fixed
Open > Resolved-Result Invalid	Open > Resolved-Result Invalid
Open > Resolved-Cancelled	Open > Resolved-Cancelled
Open > Resolved-Cancelled > Closed	Open > Resolved-Cancelled > Closed
Open > Resolved-Result Invalid > Closed-Result Invalid	Open > Resolved-Result Invalid > Closed-Result Invalid
Open > Closed-Fixed	Open > Closed-Fixed

Resolving Configuration Compliance import issues

Resolve issues with third-party integration import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Import issue resolution

Issue	Resolution
Test results are missing	Check the *Start Time* on the **Qualys PC Results** integration. It might not be set back far enough. See Modify Qualys PC Results start date.
The integration is failing	Check the **Vulnerability Integration Run** status. Individual integration process entries hold the imported XML, which can be examined for unexpected information. Navigate to **Qualys Vulnerability Integration** > **Primary Integrations** > **QualysPC Results** > **Vulnerability Integration Runs** related tab. Choose the latest run. Examine the status and notes of the entries in the related list **Vulnerabilty Integration Process** for anomalies. .

Modify Qualys PC Results start date

If data is missing for the start date in the Qualys PC Results import, it can be modified.

Before you begin

Role required: sn_vul_qualys.admin

Procedure

1. Navigate to **All** > **Qualys Vulnerability Integration** > **Administration** > **Primary Integrations**.
2. Click **Qualys PC Results** integration.
3. Click **Integration Details**.
4. Set the **Start time** field to a value in the past, so all scanned and detected test results, since that time, are detected.

   Note: If the date is left empty, no data is returned on the first run. Set the value to a maximum of a month in the past. This setting keeps large amount of data from exceeding the Qualys API rate limitations, as well as triggering execution timeouts.

5. Click **Submit** or **Update**.
6. **Optional:** Click **Execute Now** to run immediately.

CI lookup rules for Microsoft Defender for Cloud Integration for Security Operations and Palo Alto Prisma Cloud

You can use the configuration item (CI) lookup rules for the Microsoft Defender for Cloud Integration and Palo Alto Prisma Cloud integrations to find a correct match to commonly used resource types in the Configuration Management Database (CMDB).

Overview

The CI Lookup rules module contains the rules that help you to define the fields that have the matching data in the Configuration Management Database (CMDB). You can use these rules to identify the applications and application releases. All Microsoft Defender for Cloud Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and Palo Alto Prisma Cloud assets are uniquely identified by the combination of their object ID, cloud account, and logical datacenter in the ServiceNow platform. ServiceNow discovery populates the resource ID in the `Object_id` column of the CMDB in different formats for the different resource types. The following table shows the object ID formats of commonly used resource types that the discovery service uses to populate in the `Object_id` column of the CI. Any scanner that wants to look up an asset of a particular resource type must search by using the right object ID format. You can get the right object ID format by looking into the object ID column of corresponding CMDB CI class and then try to construct the object ID using the values that are received from scanner.

Object ID format for various resource types

Resource Type	Format
AWS::EC2::Instance	Object ID
AWS::ElasticLoadBalancing::LoadBalancer	Load balancer name
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

The CI match for a test result may not be found accurately in the Configuration Management Database (CMDB) unless the same format of the `object_id` is used in the lookup rule. Most of the times, the OOB CI lookup rules find a match for the most commonly used resource types for Microsoft Defender for Cloud Integration and Palo Alto Prisma Cloud. If the following CI lookup rules aren't finding the CIs in the CMDB for your test results, you can create a CI lookup rule for a resource type. For more information on how to create a CI lookup rule, see Create a CI lookup rule.

CI lookup rules

The following CI lookup rules are specific to the Microsoft Defender for Cloud Integration and Palo Alto Prisma Cloud.

S3 Bucket

This lookup rule attempts to find the CI in the CMDB by the value that was obtained by concatenating the `arn:aws:s3:::` and resource name. The obtained value is looked up in the `object_id` column of the `cmdb_ci_cloud_object_storage` table. This lookup rule applies only when the resource type is `AWS::S3::Bucket`.

Name

This lookup rule attempts to find the CI in the CMDB by name. The name, which is looked up in the `Object_id` column of the CI class, corresponds to a resource type in the `sn_capi_resource_type` table.

> **Note:** For the Palo Alto Prisma Cloud application, this CI lookup rule runs only for the `AWS::RDS::DBInstance`, `AWS::ElasticLoadBalancing::LoadBalancer`, and `AWS::CloudTrail::Trail` resource types. You can add the resource types that you want to execute this CI lookup rule for.

Resource Id

This lookup rule attempts to find the CI in the CMDB by the resource ID. The resource ID, which is looked up in the `Object_id` column of the CI class, corresponds to a resource type in the `sn_capi_resource_type` table.

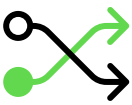
Note: You can set the priority for a CI lookup rule in the **Order** field. The CI lookup rule with the least order value is executed first.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response Workspaces

Vulnerability Response Workspaces offer a consolidated view of the features that enables you to multi-task from within the same pane by boosting productivity and saving time.

Vulnerability Response Workspaces

Vulnerability Manager Workspace  Learn about the Vulnerability Manager Workspace	**IT Remediation Workspace**  Learn about the IT Remediation Workspace	**Vulnerability Assessment Workspace**  Learn about the Vulnerability Assessment Workspace
Upgrade Vulnerability Response Workspace to USEM  Upgrade Vulnerability Response Workspace to Unified Security Exposure Management Workspace.		

Before you begin

Before you can use the workspaces:

- You need to perform a few configuration tasks. For more information, see Configure the Vulnerability Response Workspaces.
- Review important information about updates to remediation tasks, remediation task rules, and key terms and concepts about the workspaces, in Vulnerability Response Workspaces and updates to remediation tasks and remediation task rules.

Troubleshoot and get help

- Security Operations on ServiceNow Community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Patch orchestration with the Vulnerability Response Workspaces

You can manage patches and patch deployments for critical vulnerabilities for large groups of your assets with Patch orchestration with Vulnerability Response.

Patch orchestration in the Workspaces

Patch orchestration with the Vulnerability Response application uses scheduled imports from third-party solution integrations, patch vendors, and vulnerability scanners.

Patch orchestration with the Vulnerability Response application is supported in both the classic environment and the Vulnerability Response workspaces. Correlated data is rolled up and displayed in both the workspaces and the classic environment. For an overview about the features, requirements, and information about patch orchestration in the classic environment, see Patch orchestration with Vulnerability Response.

- For more information about the supported integrations with patch vendors, see Understanding the HCL BigFix patch orchestration integration with Vulnerability Response and Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM.
- For information about how to schedule patches form records in the workspaces, see Schedule patches with the Microsoft SCCM integration with Vulnerability Response and Schedule patches with the Vulnerability Response patch orchestration integration HCL BigFix.

Available versions of applications and dependencies required for the patch orchestration integration

To view patch Orchestration data and available updates (patches) in the workspaces in Vulnerability Response, the following applications are required. All applications listed are available in the ServiceNow® Store. Some applications require separate subscriptions. See Patch orchestration with Vulnerability Response.

Roles required

In addition to the sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin roles required for the Vulnerability Response Workspaces, users need roles that are specific to the patch orchestration integrations you are using to view data and schedule patches. See the following supported integrations for more information about these roles.

See Understanding the HCL BigFix patch orchestration integration with Vulnerability Response and Understanding the Vulnerability Response patch orchestration integration with Microsoft SCCM.

Patch data in the Vulnerability Response Workspaces

In the IT Remediation Workspace, you can view patch data in the workspaces:

- On the Home view, click scorecards to view records for Preferred solutions on VIs, Vulnerable CIs, and Preferred Patches on VIs.
- On the List view, view all the Patch Update records (VPUs) and the vulnerable items that are assigned to you that have patches from the available links.

You can schedule patches from the following records:

- Patch Update (VPU)
- Remediation task (RT)
- Discovered Item (SDI)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the Vulnerability Manager Workspace, you can view patches:

- From the Home view on watch topics on the Vulnerable Items tab, you can view preferred and potential patches, Patch scheduled dates, and other information.
- From the List view on remediation effort records, you can view patch data on VIT records on the Vulnerable Items tab.

Vulnerability Response Workspaces and updates to remediation tasks and remediation task rules

Remediation tasks bundle vulnerable items in the Vulnerability Response Workspaces.

Key terms for the Vulnerability Response Workspaces

Vulnerability Response Workspaces, or workspaces

Vulnerability Response supports the Vulnerability Response Workspaces. You can either use the classic Core UI experience or the workspaces.

Classic (legacy) UI

Refers to the Core UI experience. You still perform some actions and view a few lists in the classic environment.

Vulnerability Manager Workspace

In this workspace, managers monitor targeted vulnerabilities and select the VIs and test results that they care the most about to assign to IT.

IT Remediation Workspace

In this workspace, IT teams can focus on the most important vulnerabilities that are assigned to them by security. IT-centric information that includes impacted, distinct configuration items (CIs), Solutions, and remediation progress is easily available for remediation owners in this workspace.

Vulnerability Assessment Workspace

In this workspace, vulnerability analysts can perform vulnerability assessment during the zero-day vulnerability analysis. After a zero-day vulnerability is identified, they can assess the potential impact and risk associated with the vulnerability. The analysts can analyze the affected system,applications, or network components to understand the severity and possible attack vectors within the organization.

Watch topic

Watch Topics define a segment of the vulnerable items that vulnerability managers and analysts want to monitor in the Vulnerability Manager Workspace. Watch topics show a focused overview set of reports that pertain to a segment of VIs and test results with trending, CI, and vulnerability-related statistics. The dashboards on these topics can be used to monitor trends. The dashboards can also help managers:

- View remediation progress on critical items
- Determine the existence of vulnerabilities on critical systems
- See when a new exploit comes out
- Drive rapid response for resolving a particular set of vulnerabilities

Remediation effort (RE)

Remediation efforts are created by vulnerability managers when they determine it is time for IT to fix the vulnerabilities listed in a watch topic. Vulnerability managers and analysts can choose how they want to create remediation tasks, by assignment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

group and vulnerability, for example. Remediation tasks are contained in the remediation effort.

Remediation task (VUL)

IT teams use remediation tasks to remediate the vulnerabilities assigned to them by security. Remediation tasks are lists of the actions that are required to fix vulnerabilities. Remediation tasks are created automatically when security managers create remediation efforts.

Development of the Workspaces

In previous versions of Vulnerability Response, you had two options to monitor a set of vulnerable items (VIs) as a security and vulnerability analyst:

- The Overview dashboard, which summarizes all VIs
- Remediation tasks

Vulnerable items were sorted into remediation tasks automatically according to your pre-defined remediation task rules. Remediation tasks were designed to support IT teams with remediating manageable chunks of vulnerable items.

This automation made it possible to group very large numbers of VIs automatically for bulk assignment and remediation. However, vulnerability analysts and managers found monitoring the whole set of vulnerable items from remediation tasks challenging. In addition to performance problems with large groups, creating functional remediation task rules that filtered out only the vulnerabilities you that you found most critical can be difficult.

The Vulnerability Response Workspaces:

- Help security managers filter out, monitor active VIs and test results over time, and drive remediation for the vulnerabilities they determine are the most important.
- Provide IT teams with IT-centric information in one location that they can use to fix the vulnerabilities assigned to them by security.

Updates to remediation tasks in the workspaces

In the Vulnerability Manager workspace, vulnerability analysts and managers use Watch Topics and Remediation Efforts as two new methods for monitoring and assigning VIs for remediation.

Vulnerability groups are renamed, Remediation Tasks. This change applies to labels on lists, records, and rules in both the legacy UI and the workspaces. Remediation tasks are set up so that IT teams can work with them in the IT Remediation Workspace. The following list illustrates how as a vulnerability manager or vulnerability analyst, you might monitor vulnerabilities (VITs, AVITs, and CVITs) and test results (TRs), filter them, and assign them:

1. In the Vulnerability Manager Workspace, managers monitor imported vulnerabilities on watch topics. Managers and analysts use watch topics to monitor a dynamic set of filtered VIs over time that they think are the most critical.
2. With watch topics, security managers can determine when and what kind of VIs to hand off to IT teams in Remediation Efforts (REs). These REs are static lists of the VIs that security wants to IT teams to fix.

   From remediation efforts, managers have four options for how to bundle VIs into Remediation Tasks (VULs). Remediation tasks are automatically assigned to IT teams based on the assignment groups that are originally associated with the VIs.
3. IT teams work on remediation tasks in the IT Remediation Workspace without having to sort through all of the VIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A remediation task transitions through the same states as the remediation task does in previous versions of Vulnerability Response. When all the VIs in a remediation task are closed, the remediation task is closed and is set to **Inactive**.

Remediation progress is updated on data visualizations on the watch topics and on the IT remediation Home page.

Updates to remediation task rules in the workspaces

Vulnerability Group Rules are called Remediation Task Rules. This change applies to the labels on lists, records, and rules in both the legacy UI and the workspaces.

Table names, for example, [sn_vul_m2m_vul_group_item], are not changed.

If you have created vulnerability groups rules in a previous versions of Vulnerability Response, they are still available to you labeled as remediation task rules.

However, in the workspaces, vulnerability group rules are no longer used as the primary method of organizing a large volume of vulnerable items into vulnerability groups. You might prefer to leave your remediation task rules inactive as you get used to the workspaces.

You might prefer instead to incrementally start using the Vulnerability Response Workspaces.

1. If you are upgrading from a previous version of Vulnerability Response your existing VG rules are preserved. They are still available to you in the workspaces. The default group rule, Vulnerability, is inactive by default.
2. Configure assignment rules, and, perhaps if you want, risk rules, and then perform an import.
3. As a vulnerability manager or analyst, you can pick segments to monitor from the watch topics in the Vulnerability Manager Workspace. You can use watch topics as standalone features. Pick any subset of VIs and use the dashboard on them to monitor trends. With them, you can decide where and when to focus remediation efforts.
4. As a vulnerability managers or analyst, you create remediation efforts from watch topics when you decide it is time to remediate a subset of vulnerable items. A remediation task is also created automatically to hand off to IT when you create a remediation effort.
5. Over time, as a vulnerability manager or analyst, you might discover some routine patterns that you can handle with remediation tasks rules automatically.

To view your remediation task rules, navigate to **Vulnerability Response** > **Administration** > **Remediation Task Rules**.

More on assignment rules, remediation task rules, remediation efforts, and vulnerable items in the Vulnerability Response Workspaces

- Remediation Task records (VUL) are displayed on lists and records in both the classic environment and in the workspaces.
- A remediation task transitions through the same states as a vulnerability group. When all the VIs in a remediation task are closed, the remediation task transitions to the Inactive state.
- To help your teams with remediation, a vulnerable item can only be in one remediation effort. Once it is in a remediation effort, a vulnerable item won't be added to any other remediation efforts that you create.
- If you delete a remediation effort, the remediation effort becomes inactive and any active VIs are available for new remediation efforts.
- A vulnerable item can be in multiple remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Remediation tasks are assigned automatically to IT teams based on the assignment group that is associated with a vulnerable item in a remediation effort. If you create a remediation task on-demand, you select the assignment group.
- If you are an upgrading from a previous version of Vulnerability Response, your assignment rules have been preserved in the legacy UI.
- If you are an upgrading from a previous version of Vulnerability Response, your current users and groups are inherited and accessible to you in the workspaces.

For more information about the life cycles of remediation efforts, see Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces.

Configuration and setup for the Vulnerability Response Workspaces

For more information on assignment rules and remediation task rules, see Configure the Vulnerability Response Workspaces and Vulnerability Response assignment rules overview.

If you are a new customer and you've not already added them, you must set up users and groups so that vulnerable items and remediation tasks are assigned to the remediation groups that you want. Vulnerability Response assignment rules are used to assign work to groups.

Configure the Vulnerability Response Workspaces

Before you can use the workspaces, confirm you've completed the following setup tasks.

Before you begin

Role required: admin for assigning roles to users and groups and users to groups.

sn_vul.vulnerability_admin for editing, creating rules, and configuring the Vulnerability Response application.

Confirm you've completed the following setup tasks. See the steps following the list for more information about how to perform these tasks.

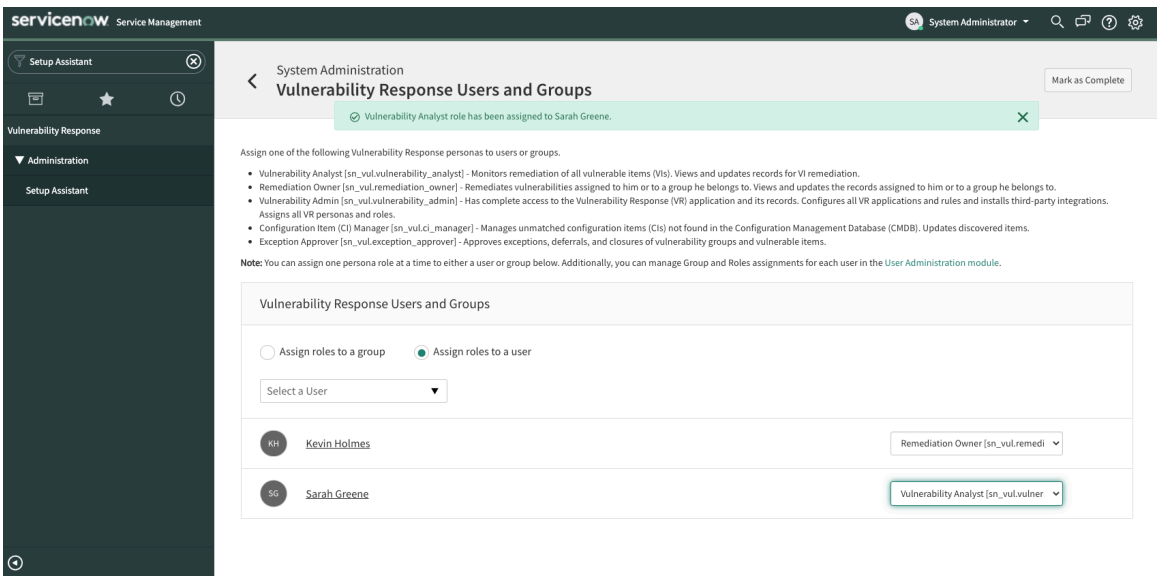
Task	Description
☐	If not already assigned, assign users and groups with the proper roles so that they have access to the workspaces. Role required: admin. See the steps below for more information.
☐	Set up assignment rules so vulnerable items are assigned to the proper groups for remediation. Role required: sn_vul.vulnerability_admin. For more information about assignment rules, see Vulnerability Response assignment rules overview. You create and edit assignment rules in the classic environment.
☐	(Optional): Edit or create your remediation task rules. Role required: sn_vul.vulnerability_admin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	Note: Functionally, remediation task rules work just like remediation task rules did in previous versions of Vulnerability Response. However, unlike the vulnerability groups that were created automatically from your remediation task rules, remediation tasks are created when you create remediation efforts. You have the following options for bundling the vulnerable items in a remediation effort into remediation tasks: • By Assignment group • By Assignment group and configuration item • By Assignment group and vulnerability • None - Use this option if you want to add VIs manually to a remediation task. See Create a remediation task on-demand in the Vulnerability Manager Workspace for more information. For more information about how VIs are automatically grouped and how the group rules are reapplied in the classic environment, see Vulnerability Response remediation tasks and remediation task rules overview.
☐	Edit remediation target rules. Role required: sn_vul.vulnerability_admin. Add remediation target rules in the classic environment. For more information about remediation target rules, see Create or edit a Vulnerability Response remediation target rule.

Procedure

1. After you install and activate the Vulnerability Response application, in the classic environment as a user with the admin role, navigate to **All** > **Vulnerability Response** > **Administration** > **Setup Assistant**.



2. In the Setup Assistant, assign users to the following groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: 1000 is the limit for the number of user groups a user can be assigned to in the Vulnerability Response Workspaces.

The following groups are provided with the Vulnerability Response application and are used in the workspaces. You can assign users to them in the Setup Assistant:

- Remediation Owner - This group is for IT remediation owners in the IT Remediation Workspace. Users with this role fix vulnerabilities assigned to them in remediation tasks.

  Note:

  If you want your remediation owners to create and view change requests and view vulnerable configuration item (CI) data in the IT Remediation Workspace and in the classic environment, assign them the itil role. You might prefer to assign the itil role to individual users instead of to all members in a group. The cmdb_read role is also an option for users to view CI data in the workspaces.

- Starting with v16.1, you can set up email reminders to your IT remediation owners. To set up email notifications to the workspaces, see Set up email notifications in the Vulnerability Response Workspaces.
- Vulnerability admin - This group is for vulnerability managers. This role configures the Vulnerability Response application in the Setup Assistant. This role also has permission to process exception and false positive requests.
- Vulnerability Analyst - This group is for security managers, vulnerability managers, and analysts in the Vulnerability Manager Workspace. This role monitors vulnerabilities, creates watch topics and remediation efforts, and monitors remediation progress.
- False Positive Approver - Users in this group process false positive requests for vulnerable items or remediation tasks. A false positive request requires a single-level approval process. You can manage assigning users to this group outside of the Setup Assistant in **User Administration**.
- Exception Approver - An exception request for a vulnerable item or remediation task is approved using a default, two-level approval workflow. The exception request requires two levels of approvers. Add users to both approval groups: Exception Approver - Level 1 and Exception Approver Level - 2. After the request is approved by the level 1 approver, it is sent on to the second level approver. You manage assigning users to this group outside of the Setup Assistant in **User Administration**.

  Note: Add users to the approval groups prior to submitting false positive and exception requests. If you create requests prior to assigning users with approval permission, the requests might not be visible to them.

Alternatively, click the **User Administration** link to manage and assign the following granular roles to your users and existing groups. These roles permit users to perform specific actions within the Vulnerability Response application and the workspaces.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- To create and view change requests in the IT Remediation Workspace and in the classic environment, assign them the itil role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Vulnerability Response personas and granular roles and Assign the Vulnerability Response persona roles using Setup Assistant for more information about assigning persona roles to users and users to groups.

3. Remediation tasks are automatically handed off to IT remediation assignment groups for processing when they are created.
   - By Assignment group
   - By Assignment group and configuration item
   - By Assignment group and vulnerability
   - None - Use this option if you want to add VIs manually to a remediation task.

   Note: For the version 18.0 of Vulnerability Response, the **None** option is not available.

   If you are upgrading from a previous version of Vulnerability Response, your assignment groups are preserved. However, you may prefer to edit these groups so that vulnerable items are associated with specific assignment groups until you get accustomed to how watch topics and remediation efforts work. For example, you can create assignment groups by product or region, but you can use any criteria that best suits your organization.

   You can also use assignment rules to assign remediation tasks to groups. You might prefer to run only high priority rules for the following items:
   - Items that need special handling
   - Items where risk is critical, or a VI requires handling by regulatory compliance

   The following assignment rules provided with the application are active by default:
   - Retired CI assignment rule
   - Assign to CI support group
   - Workstation Assignment Rule
   - Database Assignment Rule
   - Web Application Assignment Rule
   - Windows Server Assignment Rule
   - Non-windows Server Assignment Rule
   - Catch All Assignment Rule

   For more information about assignment rules, see Vulnerability Response assignment rules overview. You create and edit assignment rules in the classic environment.

4. **Optional:** Edit or create your remediation task rules.

   (Optional) In the workspaces, remediation tasks are created when you create remediation efforts. You have the following options for bundling the vulnerable items in a remediation effort into remediation tasks:

   - By Assignment group
   - By Assignment group and configuration item
   - By Assignment group and vulnerability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- None - Use this option if you want to add VIs manually to a remediation task. See Create a remediation task on-demand in the Vulnerability Manager Workspace for more information.

  Note: In the version 18.0 of Vulnerability Response, the **None** option is not available.

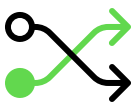
For more information about how VIs are automatically grouped and how the group rules are reapplied in the classic environment, see Vulnerability Response remediation tasks and remediation task rules overview.

Vulnerability Manager Workspace

The Vulnerability Manager Workspace enables vulnerability managers and analysts to monitor the vulnerabilities and misconfigurations that they care the most about and decide strategically which vulnerabilities they send to IT teams to fix.

Starting with v30.0 of Vulnerability Response, the Vulnerability Manager workspace is replaced with the Security Exposure Management workspace. The latter unifies Infrastructure Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance into a single workspace, eliminating silos and enabling cross-domain visibility. For detailed information, see Unified Security Exposure Management (USEM).

Get started

Explore  Learn about the features in the Vulnerability Manager Workspace	Monitor and manage  Learn how to monitor and manage vulnerable items (VITs, AVITs, and CVITs) and test results in the Vulnerability Manager Workspace	Remediate  Learn how to remediate vulnerable items (VITs, AVITs, and CVITs) and test results in the Vulnerability Manager Workspace
Reference  Learn more about the additional information required to use the Vulnerability Manager Workspace	**Upgrade Vulnerability Manager Workspace to USEM**  Upgrade Vulnerability Manager Workspace to Unified Security Exposure Management Workspace.	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Troubleshoot and get help

- Security Operations on ServiceNow Community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring the Vulnerability Manager Workspace

As a vulnerability manager and analyst, get a unified view of all the vulnerability types in the Vulnerability Manager Workspace. You can see host, application, and container vulnerabilities and configuration issues, create watch topics across these vulnerabilities and misconfigurations, create remediation efforts and create remediation tasks.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

You can view the Vulnerability Manager Workspace by navigating to **Workspaces** > **Vulnerability Manager Workspace**.

The Vulnerability Manager Workspace consists of the following pages:

Home page

Consists of predefined filters which are used for visualizing the summary of Host vulnerabilities, Application vulnerabilities, Container vulnerabilities, and Configuration test results.

For more information on the Home page, see Home page in the Vulnerability Manager Workspace.

Note: Starting from v21.0 of Vulnerability Response, the watch topics appear on the Watch Topics page.

Watch Topics page

Consists of a list of watch topics, which are categorized into four modules - Host vulnerabilities, Application vulnerabilities, Container vulnerabilities, and Configuration test results.

For more information on watch topics, see Watch Topics page in the Vulnerability Manager Workspace.

Dashboards page

Consists of the Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Overview, Application Vulnerability Management, Unified Vulnerability Response, and Health dashboards.

For more information, see Dashboards in the Vulnerability Manager Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Dashboards page appears from version 19.0 of Vulnerability Response.

List page

Consists of the default and customized list pages for remediation efforts, remediation tasks, host vulnerable items, application vulnerable items, container vulnerable items, configuration test results, exceptions, approvals, and libraries.

For more information, see List page in the Vulnerability Manager Workspace.

Home page in the Vulnerability Manager Workspace

The Home page in the Vulnerability Manager Workspace provides a summary of active records by showcasing visualizations of risk rating, remediation progress, assignments to assignment groups, records in remediation tasks, and vulnerabilities from cloud resources.

On the Home page, you can view the visualizations for the prefiltered host vulnerable items, container vulnerable items, application vulnerable items, and configuration test results. You can also view visualizations for a set of desired records by creating and applying filters. For more information on how to create, update, apply and delete filters, see Create and apply filters the summary of active records (VITs, AVITs, CVITs and CTRs).

Tip:

If the *sn_vul_cmn_ws.navigate_to_workspace* system property is set to `true` by the admin, upon selecting the predefined filter links in the Vulnerable Items, Application Vulnerable Items, Container Vulnerable Items and Test Results modules from the **All** menu, these links open in the Vulnerability Manager Workspace's Home page with auto-selection of the corresponding saved filter.

For example, if you select **High Risk** by navigating to **All** > **Vulnerability Response** > **Vulnerable items**, this link is redirected to the Home page of the Vulnerability Manager Workspace with auto-selection of the **High Risk** filter in the Host Vulnerabilities tab.

On the Home page, you can perform the following:

- Drill down into the data and view the list of records by clicking on the visualizations.
- Navigate to the list of active records in the classic UI by selecting the **View classic list** link.
- Open the list of active records in the Vulnerability Manager Workspace by selecting the active records count next to the **View by** drop-down.
- Update the visualizations by selecting the **Refresh Selected Saved Filter** icon.
- View the latest information by selecting the **Refresh** option in the three dots menu on a widget.

Host Vulnerabilities

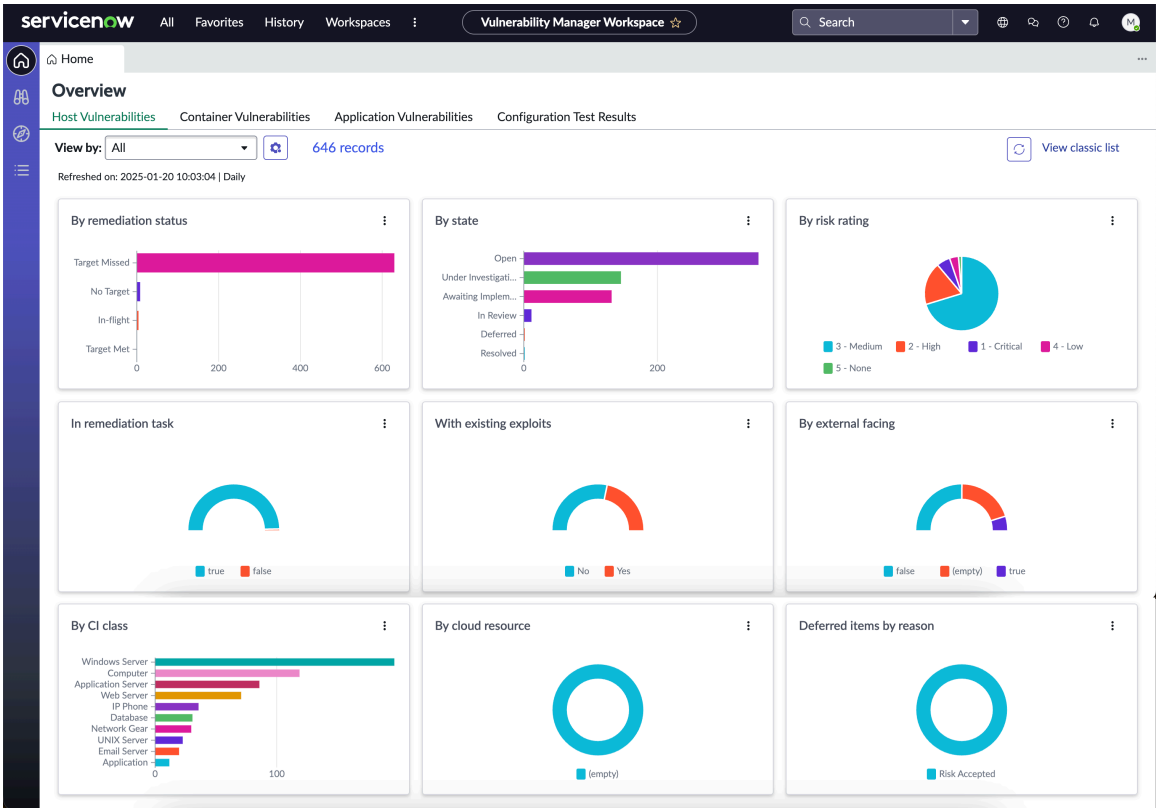
The **Host Vulnerabilities** tab contains visualizations that provide an overall summary of the active host vulnerabilities.

Roles required:

- sn_vul.vulnerability_analyst, and sn_vul.vulnerability_admin to view the visualizations by applying filters, and create filters.
- sn_vul.read_all granular role to view the visualizations by applying filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Host Vulnerabilities tab



The following table describes the visualizations on the Host vulnerabilities tab on the home page. Select these visualizations to get the list of corresponding records.

Visualizations in the Host Vulnerabilities tab on the Home page

Visualization	Type	Description
By assignment group & remediation status	Distribution bar	Active records assigned to various assignment groups that are grouped by remediation status.
By state	Bar	Active records categorized by various states (Open, Under Investigation, Awaiting Implementation, In Review, Resolved, and Deferred).
By risk rating	Pie chart	Active records categorized by risk rating (1 - Critical, 2- High, 3 - Medium, 4 - Low and 5 - None)
In remediation task	Semi circle donut	Active records that are and aren't part of the remediation task.
With existing exploits	Semi circle donut	Active records with and without known exploits.
By external facing	Semi circle donut	Active records categorized by the asset exposure to internet.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Visualizations in the Host Vulnerabilities tab on the Home page (continued)

Visualization	Type	Description
By CI class	Bar	Active records categorized by CI classes.
By cloud resource	Donut chart	Active records categorized by various cloud resources.
Deferred Items by reason	Donut chart	Active deferred records grouped by reason.

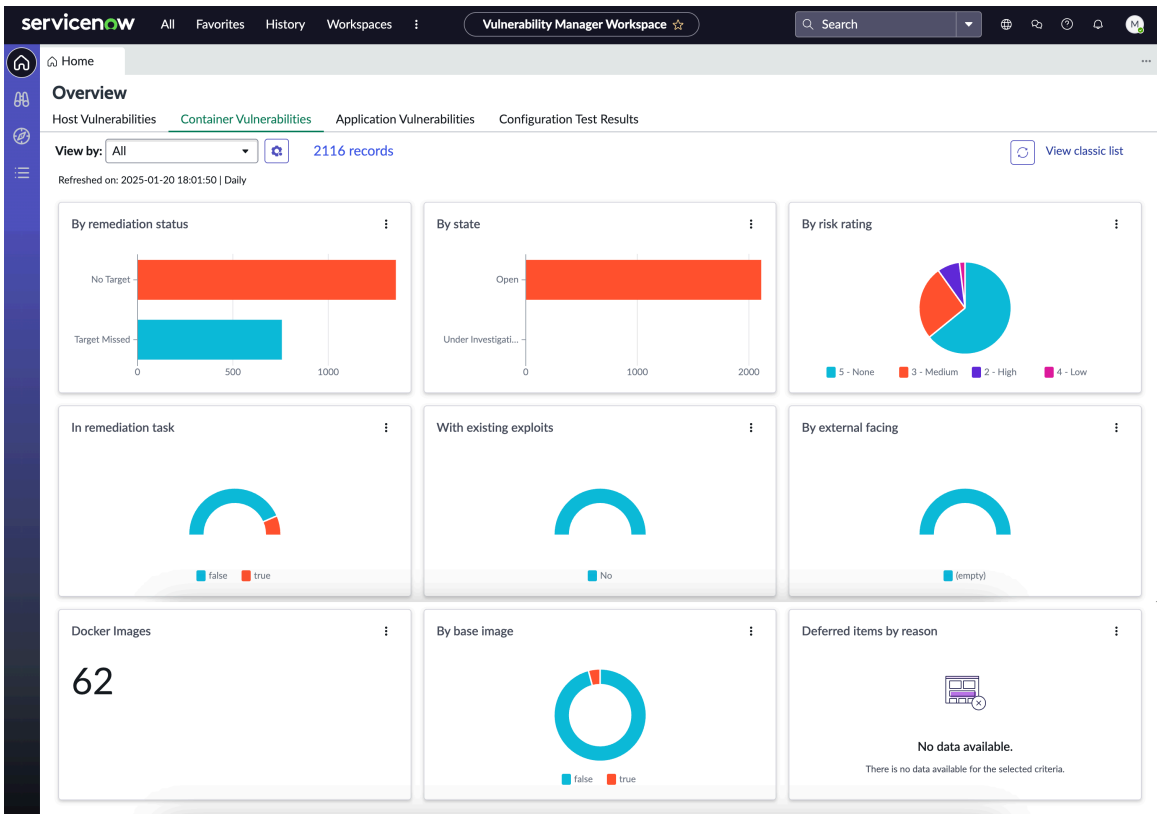
Container Vulnerabilities

The **Container Vulnerabilities** tab contains visualizations that provide an overall summary of the active container vulnerable items.

Roles required:

- sn_vul_container.vulnerability_analyst, or sn_vul_container.vulnerability_admin to view the visualizations by applying filters, and create filters.
- sn_vul_container.read_all granular role to view the visualizations by applying filters.

Container Vulnerabilities tab



The following table describes the visualizations on the Host vulnerabilities tab on the home page. Select these visualizations to get the list of corresponding records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Visualizations in the Container Vulnerabilities tab on the Home page

Visualization	Type	Description
By assignment group & remediation status	Distribution bar	Active records assigned to various assignment groups that are grouped by remediation status.
By state	Bar	Active records categorized by various states (Open, Under Investigation, Awaiting Implementation, In Review, Resolved, and Deferred).
By risk rating	Pie chart	Active records categorized by risk rating (1 - Critical, 2- High, 3 - Medium, 4 - Low and 5 - None)
In remediation task	Semi circle donut	Active records that are and aren't part of the remediation task.
With existing exploits	Semi circle donut	Active records with and without known exploits.
By external facing	Semi circle donut	Active records categorized by the asset exposure to the internet.
Docker Images	Count	Number of unique docker images.
By base image	Donut chart	Active records categorized by the type of the image.
Deferred Items by reason	Donut chart	Active deferred records grouped by reason.

Application Vulnerabilities

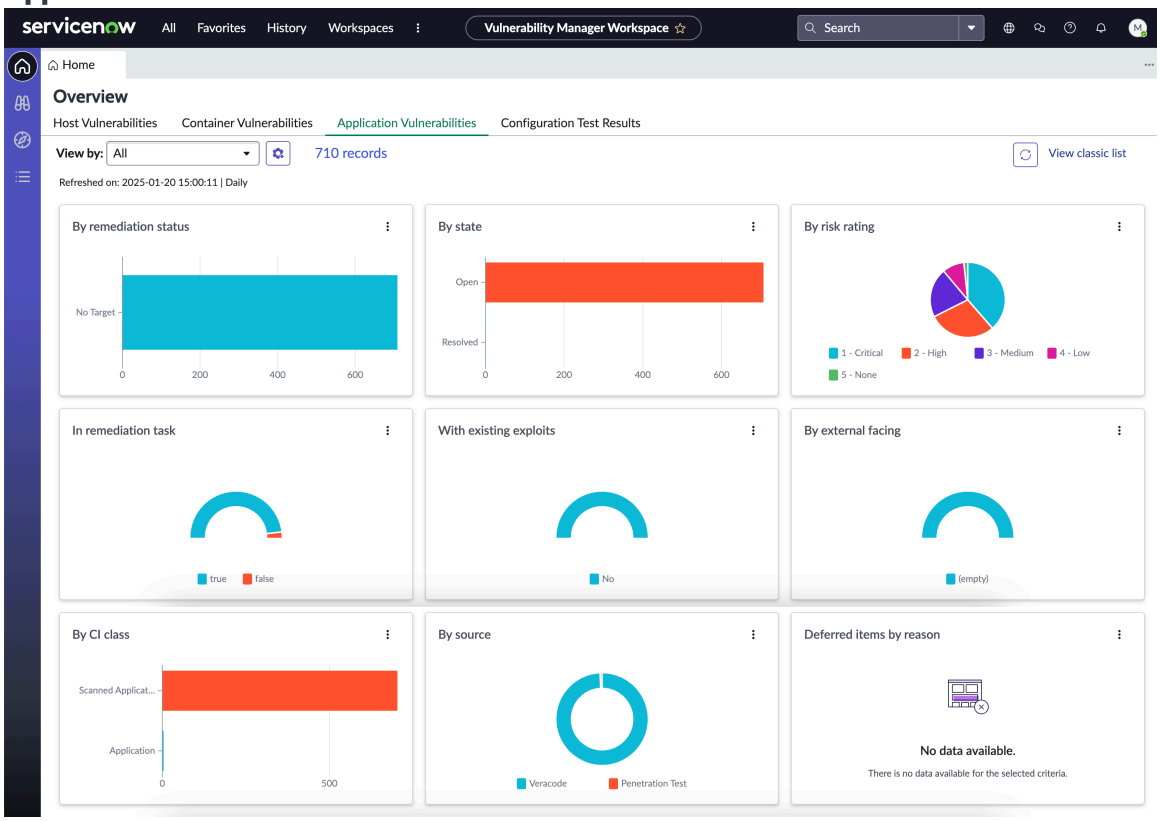
The **Application Vulnerabilities** tab contains visualizations that provide an overall summary of the application vulnerabilities.

Roles required:

- sn_vul.app_sec_manager to view the visualizations by applying filters, and create filters.
- sn_vul.app_read_all granular role to view the visualizations by applying filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerabilities tab



The following table describes the visualizations on the Host vulnerabilities tab on the home page. Select these visualizations to get the list of corresponding records.

Visualizations in the Application vulnerabilities tab on the Home page

Visualization	Type	Description
By assignment group & remediation status	Distribution bar	Active records assigned to various assignment groups that are grouped by remediation status.
By state	Bar	Active records categorized by various states (Open, Under Investigation, Awaiting Implementation, In Review, Resolved, and Deferred).
By risk rating	Pie chart	Active records categorized by risk rating (1 - Critical, 2- High, 3 - Medium, 4 - Low and 5 - None)
In remediation task	Semi circle donut	Active records that are and aren't part of the remediation task.
With existing exploits	Semi circle donut	Active records with and without known exploits.
By external facing	Semi circle donut	Active records categorized by the asset exposure to internet.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Visualizations in the Application vulnerabilities tab on the Home page (continued)

Visualization	Type	Description
By CI class	Bar	Active records categorized by CI classes.
By cloud resource	Donut chart	Active records categorized by various cloud resources.
Deferred Items by reason	Donut chart	Active deferred records grouped by reason.

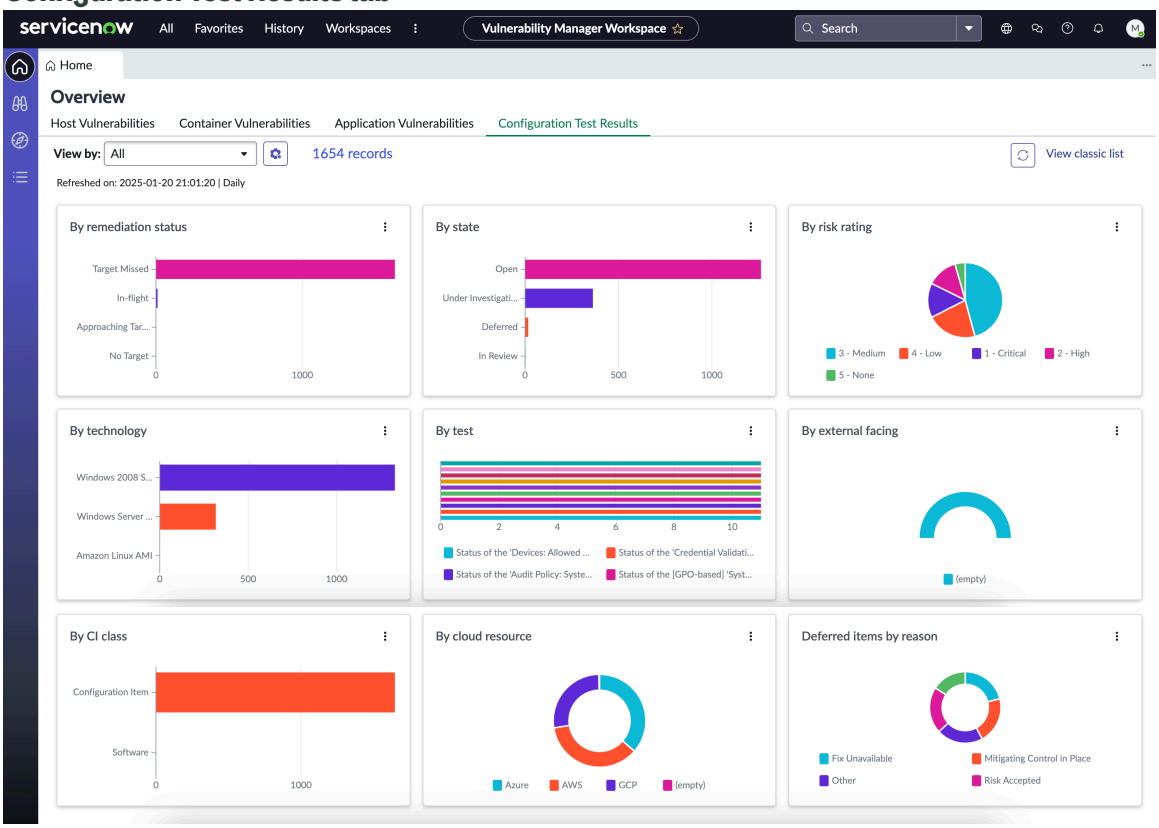
Configuration Test Results

The **Configuration Test Results** tab contains visualizations that provide an overall summary of the active misconfigurations of the assets in your organization.

Roles required:

- sn_vulc.admin to view the visualizations by applying filters, and create filters.
- sn_vulc.read granular role to view the visualizations by applying filters.

Configuration Test Results tab



The following table describes the visualizations on the Configuration test results tab on the home page. Select these visualizations to get the list of corresponding records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Visualizations in the Configuration Test Results tab on the Home page

Visualization		Description
By assignment group & remediation status	Distribution bar	Active records assigned to various assignment groups that are grouped by remediation status.
By state	Bar	Active records categorized by various states (Open, Under Investigation, Awaiting Implementation, In Review, Resolved, and Deferred).
By risk rating	Pie chart	Active records categorized by risk rating (1 - Critical, 2- High, 3 - Medium, 4 - Low and 5 - None)
By technology	Bar	Active records categorized by technology.
By test	Bar	Active records categorized by tests.
By external facing	Semi circle donut	Active records categorized by the asset exposure to internet.
By CI class	Bar	Active records categorized by CI classes.
By cloud resource	Donut chart	Active records categorized by various cloud resources.
Deferred Items by reason	Donut chart	Active deferred records grouped by reason.

Watch Topics page in the Vulnerability Manager Workspace

The Watch Topics page in the Vulnerability Manager Workspace enables you to create and edit a watch topic. A Watch topic is a set of data visualizations which enables you to monitor a filtered set of records (VITs, AVITs, CVITs and CTRs) over time on a dashboard that might be of a particular interest or priority to your organization.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

The data displayed on the data visualizations on the watch topics are dynamically updated as vulnerability data changes upon import. Use the dashboards to monitor the trends, scope, and types of vulnerabilities and your configuration items for the selected watch topic. This information helps you determine how the vulnerabilities in each watch topic impact your environment. The Watch Topics page consists of four modules - Host Vulnerabilities, Container Vulnerabilities, Application Vulnerabilities, Configuration Test Results, and Inactive. For more

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

information on the related items tabs and their visualizations in a watch topic, see Related items list and visualizations in a watch topic.

The following watch topics are provided with the base system in the Host Vulnerabilities module on the Watch Topics page:

- Vulnerabilities on External Facing Assets
- Vulnerabilities with Exploits Available
- Vulnerabilities on Windows Servers
- Vulnerabilities on LINUX Servers
- Critical Overdue Vulnerabilities
- Critical Vulnerabilities not in Remediation Tasks

Note: If a data visualization shows that there are no records for that category, but you can see a list of records when you click the graph icon, check the column with the watch topic name on the list that is displayed. Verify that the value for all the records listed in the column of the watch topic, for example, Internet-facing, is `false`. This value in this example indicates that there are no internet-facing records for this watch topic.

To start the remediation or when a critical need arises for the records that are in a watch topic, you can create a Remediation Effort from a watch topic. For more information, see Create a remediation effort in the Vulnerability Manager Workspace.

Related topics

Related items list and visualizations in a watch topic

Use watch topics in the Vulnerability Manager Workspace

Create a watch topic in the Vulnerability Manager Workspace

Edit or delete a watch topic in the Vulnerability Manager Workspace

Deactivate or activate a watch topic

Related items list and visualizations in a watch topic

You can create watch topics that are categorized into four modules, Host Vulnerabilities, Container Vulnerabilities, Application Vulnerabilities, and Configuration Test Results. The related items tabs in a watch topic differ for each module.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

The navigation pane on the landing page contains the following modules:

- Host Vulnerabilities: Displays the watch topics that include the host vulnerable items.
- Container Vulnerabilities: Displays the watch topics that include the container vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Application Vulnerabilities: Displays the watch topics that include the application vulnerable items.
- Configuration Test Results: Displays the watch topics that include the configuration items.
- Inactive: Displays the inactive watch topics from all four modules.

The following table shows the related items tabs that are available for different watch topic modules:

Watch topic and its related items

Watch topic	Related items tabs
Host Vulnerabilities	Overview, Impacted CIs, Distinct Vulnerabilities, and Vulnerable Items
Container Vulnerabilities	Overview, Impacted CIs, Distinct Vulnerabilities, and Vulnerable Items
Application Vulnerabilities	Overview and Vulnerable Items
Configuration Test Results	Overview, Impacted CIs, Distinct Configuration Tests, and Configuration Test Results

The following table provides a description of the related items tabs and the visualizations in a watch topic.

Related items tabs and visualization in a watch topic

Related items tab and visualization	Description
Overview	
Active Vulnerable Items over time	Number of active vulnerable items (VIs) over time. You can monitor the trends from this data for the past 30 days. You can also filter the data by using the Asset Category filters.
VIs in Remediation Efforts	Number of active VIs out of the total number of VIs that are already in the active remediation efforts.
Active Remediation Efforts	List of the active remediation efforts.
Impacted CIs	
Distinct CIs	Number of configuration items (CIs) (assets) impacted by these vulnerabilities.
VIs per CI class	Number of vulnerable items (VIs) for each Configuration Management Database (CMDB) CI class. **Note:** This widget appears only for the watch topics in host, application, and container vulnerabilities module.
Configuration Issues per CI class	Number of CIs for each Configuration Management Database (CMDB) CI class.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related items tabs and visualization in a watch topic (continued)

Related items tab and visualization	Description
	Note: This widget appears only for the watch topics in Configuration Issues module.
Internet facing VIs	Number of active VIs out of the total number of VIs for your assets that are exposed to the internet. **Note:** This widget appears only for the watch topics in host, application, and container vulnerabilities module.
Internet facing Configuration Issues	Number of active CIs out of the total number of CIs for your assets that are exposed to the internet. **Note:** This widget appears only for the watch topics in Configuration Issues module.
Distinct Vulnerabilities	
VIs with existing exploits	Active VIs with known exploits.
Distinct vulnerabilities	Number of individual, distinct vulnerabilities that are associated with your assets. The distinct vulnerabilities can be filtered based on the issue type.
VIs with PCI vulnerabilities	Number of individual, distinct assets that have active VIs with Payment Card Industry (PCI) vulnerabilities.
Vulnerable Items	
Host Vulnerable Items	List of all host vulnerable items. You can filter this list so that only the records that you want to see are displayed. **Note:** This list appears only for the watch topics in Host Vulnerabilities module.
Application Vulnerable Items	List of all application vulnerable items. You can filter this list so that only the records that you want to see are displayed. **Note:** This list appears only for the watch topics in Application Vulnerabilities module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related items tabs and visualization in a watch topic (continued)

Related items tab and visualization	Description
Container Vulnerable Items	List of all container vulnerable items. You can filter this list to display so that only the records that you want to see are displayed. **Note:** This list appears only for the watch topics in Container Vulnerabilities module.
Overview tab in a watch topic under Configuration Test Results module	
Active Configuration Test Results over time	Number of active configuration test results over time. You can monitor the trends from this data for the past 30 days.
Configuration Test Results in Remediation Efforts	Number of active configuration test results out of the total number of records that are already in the active remediation efforts.
Active Remediation Efforts	List of the active remediation efforts.
Distinct Configuration Tests tab in a watch topic under Configuration Test Results module	
Configuration Test Results via Test Criticality	Configuration test results that are based on the criticality of the issues.
Distinct Configuration Tests	Number of distinct configuration tests.
Configuration Test Results tab in a watch topic under Configuration Test Results module	List of configuration test results.

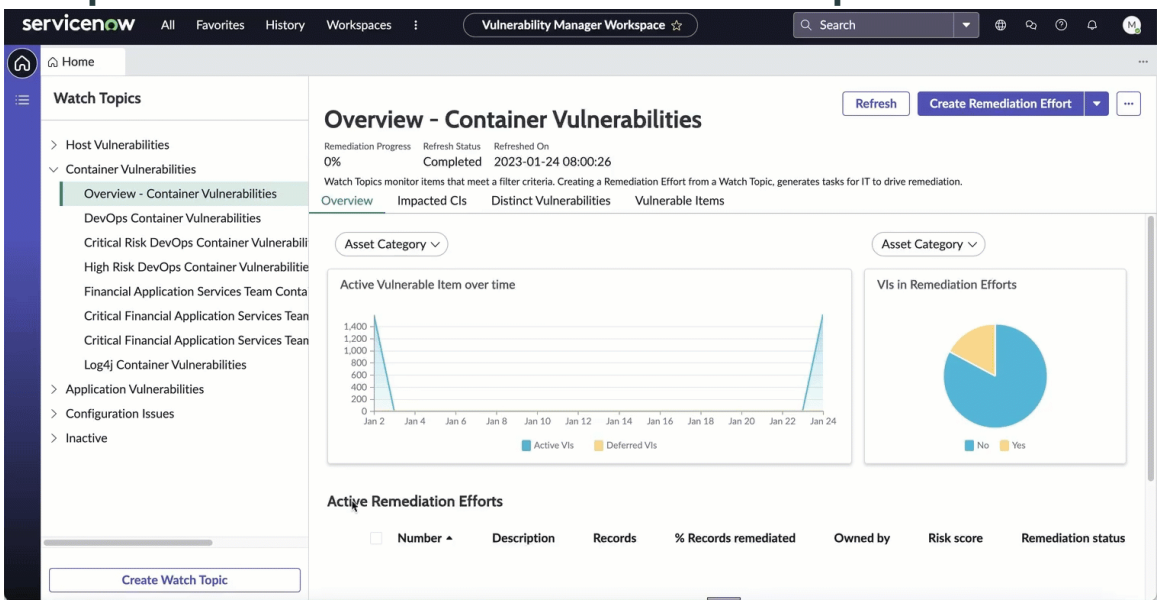
You can acquire the latest details of a watch topic by selecting the **Refresh** button. The latest refresh status and timestamp are displayed under the watch topic name. When you refresh a watch topic, all the details of the watch topic, including the charts and remediation efforts are updated. A watch topic is refreshed automatically when it is created or updated.

Note: Because you can't refresh an inactive watch topic, the **Refresh** button is inactive for an inactive watch topic.

Click a data plot on any of the widgets to view additional information about the records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example: Version 18.0 Data visualizations in a Watch Topic



Remediation efforts in the Vulnerability Manager Workspace

A Remediation Effort is a set of records that are associated with a watch topic. The records listed on a remediation effort are static. They are not updated by new import data or changes that you make to watch topics.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

With **Active** selected under the **Remediation efforts** list on the List page, click a remediation effort link to open it. To categorize the Remediation efforts into host vulnerable items (VITs), application vulnerable items (AVITs), container vulnerable items (CVITs), and configuration test results (CTRs), select the three dots menu on the **Record Type** column and then select **Group by Record type**.

The related list items on the remediation effort record permit you to view overall remediation progress and status on the records associated with it.

- On the **Overview** tab, monitor the records associated with this remediation effort that have been closed over time. To the right of the record, click the filter icon on the graph to see the filters applied to the data visualization.
- On the **Details** tab, view details about the remediation effort including its associated watch topic and status (Active or Inactive). You can deactivate a remediation effort from this page. If you deactivate the remediation effort before all the records are closed, any active records become available to add to new remediation efforts.
- On the **Remediation Tasks** tab, view the Remediation Tasks associated with this remediation effort. See the percentage of the records associated with this task that are remediated.
- On the **Vulnerable Items** tab, view the records associated with this remediation effort. When all the records in a remediation task are completed and closed, the remediation effort transitions

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

to Inactive. When a remediation effort is inactive, all the closed records associated with the remediation effort aren't available to add to new remediation efforts.

Note: The **Vulnerable Items** tab appears for the remediation efforts that are associated with watch topics in the Host Vulnerabilities, Application Vulnerabilities, and Container Vulnerabilities modules.

- On the **Configuration Test Results** tab, view the Configuration Test Results associated with the Remediation Effort. When all the records in a remediation task are completed and closed, the remediation effort transitions to Inactive. When a remediation effort is inactive, all the closed records associated with the remediation effort aren't available to add to new remediation efforts.

Note: The **Configuration Test Results** tab appears for the remediation efforts that are associated with the watch topics in the Configuration Test Results module.

For more details and UI actions you can perform from a remediation effort, see Use Remediation Effort records.

Related topics

Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces

Create a remediation effort in the Vulnerability Manager Workspace

Create a remediation task on-demand in the Vulnerability Manager Workspace

Create a recurring remediation effort in the Vulnerability Manager Workspace

Transfer records to remediation efforts in the Vulnerability Manager Workspace

Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces

The states of records and their associated remediation tasks (RTs) are impacted if records are deferred, resolved, reopened, and transferred to other remediation efforts (REs).

Roles required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Creating remediation efforts

How the states and life cycles of remediation efforts, remediation tasks, and records are impacted depends on how a remediation effort is created, when it's created, and if it's deactivated.

From the list in the upper right on a watch topic, you can create a remediation effort by clicking **Create a Remediation Effort** or **Create recurring effort**. You can create one recurring remediation effort per watch topic. If you create a recurring remediation effort, subsequent remediation efforts for the associated watch topic are created automatically based on the criteria you set. In either case:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To facilitate remediation, only Active records are added to the remediation efforts.
- All records in new remediation efforts are placed in new remediation tasks. Records can exist in multiple remediation tasks, but only one record can be associated with a remediation effort.

Note: A Remediation Effort is deactivated automatically when there are no active records.

Transferring records or record carry over

You can transfer records from one remediation effort to another when creating a remediation effort by selecting the **Transfer matching records from other active remediation efforts** check box. For more information on how to transfer the records, see Transfer records to remediation efforts in the Vulnerability Manager Workspace. If records are transferred from a remediation effort or carried over into recurring remediation efforts:

To a new remediation effort in the same watch topic

- All Remediation Tasks from the old Remediation Effort are moved to the new Remediation Effort.
- New Remediation Tasks are created based on the chosen grouping criteria for the records previously not part of any Remediation Task.
- The old Remediation Effort is deactivated.

To a new remediation effort in a different watch topic

All the records from the old Remediation Effort are moved to the new Remediation Effort and Remediation Tasks are created based on the chosen grouping criteria.

- If all records in the Remediation Tasks associated with the old Remediation Effort are transferred, these Remediation Tasks are closed-canceled.
- If only a subset of records are transferred, the Remediation Tasks associated with the old Remediation Effort are split and remain active.

The closed Remediation Tasks associated with old Remediation Effort are not affected.

Note: You can't transfer records from recurring remediation efforts into new remediation efforts. However, you can transfer records from existing, non-recurring remediation efforts into new remediation efforts. See Transfer records to remediation efforts in the Vulnerability Manager Workspace for more information about transferring records.

Dashboards in the Vulnerability Manager Workspace

In the Vulnerability Manager Workspace, you can view the dashboards in the Next Experience UI and use these dashboards to track and analyze the vulnerabilities.

Roles required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Access the dashboards in the Vulnerability Manager Workspace by navigating to **Workspaces** > **Vulnerability Manager Workspace** and selecting the **Dashboards** icon. The default dashboard is displayed based on your role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following table shows the default dashboard that is displayed for a specific role.

Default dashboard

Default Dashboard	Role
Unified Dashboard	sn_vul_cmn_vulnerability_admin or sn_vul_cmn_vulnerability_analyst
Vulnerability PA Dashboard	sn_vul_vulnerability_admin or sn_vul_vulnerability_analyst
Application overview	sn_vul_app_sec_manager
Container overview	sn_vul_container_vulnerability_admin or sn_vul_container_analyst

You can view the following dashboards for the tasks that you want to perform by selecting them from the drop-down on the Dashboards page.

Dashboards in the Vulnerability Manager Workspace

Dashboard	Description
Vulnerability Management (PA)	Track the volume, performance, and progress of the host vulnerabilities from the initial analysis and detection to the containment or remediation. For more information, see Vulnerability Management (PA) dashboard.
Vulnerability Approvals	View the number of approval requests approved, rejected, and pending for you. For more information, see Using the default Vulnerability Response dashboards.
CISO Dashboard	Reveals the overall security posture of your organization, including the security vulnerability and incidents. For more information, see Vulnerability Management CISO dashboard.
Container Vulnerability Management Overview	Track the volume, performance, and progress of the container vulnerabilities from the initial analysis and detection to the containment or remediation. For more information, see Container Vulnerability Response dashboard.
Application Vulnerability Management Dashboard	Track the volume, performance, and progress of the application vulnerabilities from the initial analysis and detection to the containment or remediation. For more information, see Application Vulnerability Management (PA) dashboard
Unified Vulnerability Response Dashboard	Provides visibility from multiple vulnerability scanners and security tools to provide a comprehensive view of an organization's vulnerabilities and risks. For more information, see Analytics and reporting solutions for the Unified Vulnerability Response Dashboard.

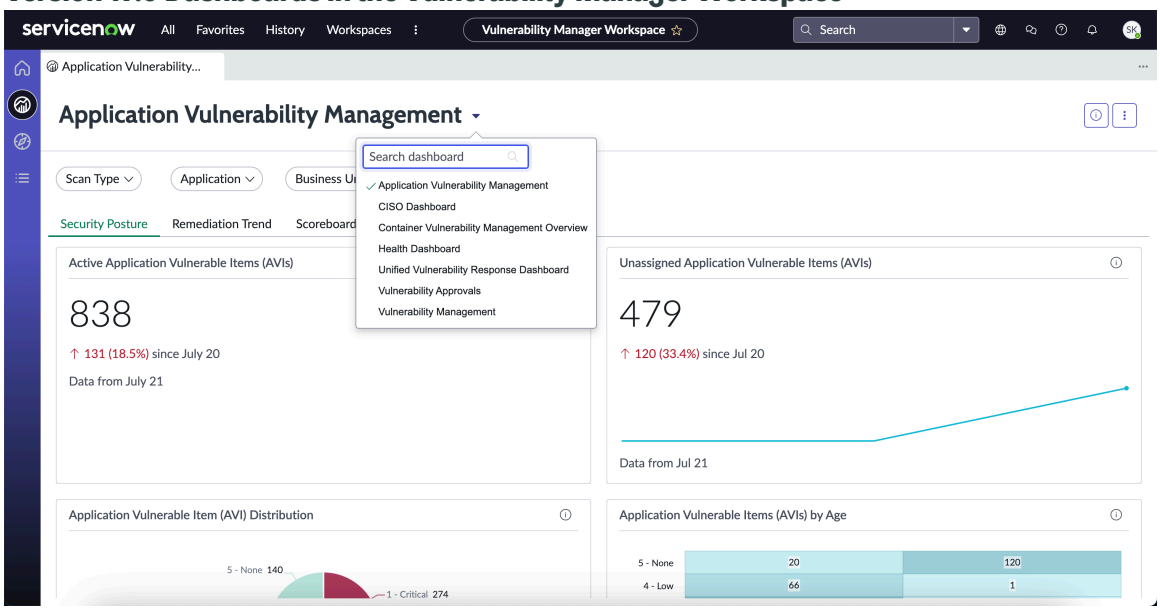
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Dashboards in the Vulnerability Manager Workspace (continued)

Dashboard	Description
Vulnerability Response Health Dashboard	Displays the overall health score of the Vulnerability Response application. For more information, see SecOps Vulnerability Response Health dashboard.

The following image shows the Dashboards page in the Vulnerability Manager Workspace.

Version 19.0 Dashboards in the Vulnerability Manager Workspace



You can also create a customized dashboard by selecting the More Options icon ⋮ and then selecting **Create new dashboard**.

List page in the Vulnerability Manager Workspace

The List page in the Vulnerability Manager workspace permits vulnerability and security managers and analysts to view remediation progress on records, drill down into Vulnerability Response records, and view the status of their approval requests and exceptions.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

These lists and links provide you with easy access to records and tasks. It contains two tabs:

- **Lists** tab: Displays the default lists for remediation efforts, remediation tasks, vulnerable items, configuration test results, solutions, exceptions, and libraries.
- **My Lists** tab: Displays any lists that you've renamed from the List tab and any lists that you create.

  You can also create your own list to monitor remediation progress. For more information, see Create a customized list of records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists tab

The following table shows the lists available in the Lists tab of the List page:

Tip:

If the *sn_vul_cmn_ws.navigate_to_workspace* system property is set to `true` by an admin, upon selecting the predefined filter links in the Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response and Configuration Compliance modules from the **All** menu, these links open in the List page in the Vulnerability Manager Workspace based on your role.

For example, if you select **Assigned to My Groups** by navigating to **All** > **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**, this link is redirected to the Vulnerability Manager Workspace. The **Assigned to My Groups** list in the **Remediation Tasks** module opens in the List page of the Vulnerability Manager Workspace if you have the vulnerability admin or analyst role. To view the host remediation tasks group the tasks by Record Type.

You can hide the record count on the lists using the *glide.ui.list.seismic.omit.count* system property. For more information on how to turn off/on the record count on a list, see the KBB0010402 KB article.

Lists

List item	Description	Modules	Roles Required
Remediation efforts (REs)	List of active REs and all the REs assigned to your assignment groups. Group the remediation efforts by **Record Type** to categorize them by host vulnerable items, application vulnerable items, container vulnerable items and configuration test results.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Remediation tasks	Contains the following lists: • Active: List of all the active host, application, container and Test result remediation tasks.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• All: List of both active and inactive host, application, container and Test result remediation tasks. • Assigned to me: List of Remediation tasks assigned to you for remediation. • Assigned to my group: Remediation tasks assigned to your assignment groups for remediation. Group the remediation tasks by **Record Type** to categorize them by host vulnerable items, application vulnerable items, container vulnerable items and configuration test results.		vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	Note: The Remediation tasks list includes tasks generated during the Remediation Effort creation in the Vulnerability Manager Workspace, as well as those created manually and by remediation task rules and other processes in the classic UI. The Remediation effort column will be empty for any remediation tasks that were not created as part of the Remediation Effort.		
Host Vulnerable items	Contains the following lists • Active: List of all the active host vulnerable items. • All: List of both active and inactive host vulnerable items. • Assigned to me: List of host vulnerable items assigned to you for remediation. • Assigned to my group: List of host vulnerable items assigned to your assignment groups for remediation.	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
Application Vulnerable items	Contains the following lists: • Active: List of all the active application vulnerable items. • All: List of both active and inactive application vulnerable items. • Assigned to me: List of application vulnerable items assigned to you for remediation. • Assigned to my group: List of application vulnerable items assigned to your assignment groups for remediation. You can create a new application vulnerable item by selecting the **New** button.	Application Vulnerability Response	sn_vul.app_sec_manager
Container Vulnerable items	Contains the following lists: • Active: List of all the active container vulnerable items. • All: List of both active and inactive container vulnerable items. • Assigned to me: List of container vulnerable items assigned to you for remediation. • Assigned to my group: List of container vulnerable items assigned to your assignment groups for remediation.	Container Vulnerability Response	sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
Configuration Test Results	Contains the following lists: • Active: List of all the active test results. • All: List of both active and inactive test results. • Assigned to me: List of test results assigned to you for remediation. • Assigned to my group: List of test results assigned to your assignment groups for remediation.	Configuration Compliance	sn_vulc.admin
Solutions	Contains the following lists: • All - Shows all the available solutions which you can use to remediate the host vulnerable items. • Highest Supersedence - Shows all the solutions which is used to populated Preferred Solutions. • With Vulnerable items - Shows the solutions which are being used as Preferred Solution on Vulnerable Items.	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin
Exceptions	Shows the approval states for all the exception and false positive requests associated with your assignment groups. • All: List of the exception, false positive, and	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	unassign approval requests related to VITs, AVITs, and CVITs and their remediation tasks (VUL, AVUL, and CVUL). • All (Configuration Compliance): List of the exceptions, false positive, and unassign approval requests related test results and remediation tasks (CTR#). Group the exceptions by **Record type** to categorize them by host vulnerable items, application vulnerable items, container vulnerable items and configuration test results.		vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Approvals	Assigned to me: Shows the approval requests assigned to you for processing. To process your approvals in the workspace, see Approve or reject requests in the Vulnerability Manager Workspace.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Libraries	Consists of the following lists:	Vulnerability Response, Application Vulnerability	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• CVEs (NVD) - List of all the Common Vulnerability and Exposures (CVEs) from Vulnerability Response, Application Vulnerability Response, and Container Vulnerability Response. • TPEs - List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs. • CWEs - List of all the Common Weakness Enumerations (CWEs) from Vulnerability Response, Application Vulnerability Response, and Container Vulnerability Response. • App vulnerabilities - List of all the third-party application vulnerability entries. • Test Groups - List of all the Configuration Compliance test groups. You can view the percentage of CI compliance and test results compliance for a Test Group in the record view. • Tests - List of all the tests from Configuration Compliance.	Response, Container Vulnerability Response, and Configuration Compliance	for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	You can view the percentage of test results compliance for a test in the record view. • Compensating Controls - List of all the compensating controls which can be used for risk reduction requests. You can add a compensating control by clicking **New**. For more information on how to add a compensating control, see Add a compensating control to the library.		
CMDB	Contains the following lists • **Discovered items**:List of all the discovered items. • **Discovered container images**: List of Container images. These container images provide information on the image ID, Docker image, and the image repository along with the layer information.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs) • sn_vul.app_sec_manager for application vulnerable items (AVITs) • sn_vul_container.vulnerability_analys or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs) • sn_vulc.admin for configuration test results (TRs)
Penetration Test Assessment Requests	Contains the following lists: • **Active**: List of active Penetration Test Assessment Requests.	Application Vulnerability Response	sn_vul.app_sec_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	• **All**: List of both active and inactive Penetration Test Assessment Requests • **Assigned to me**: List of Penetration Test Assessment Requests raised by you. • **Assigned to my group**: List of Penetration Test Assessment Requests raised by the users in your assignment groups. For information on how to create a penetration test assessment request, see Create a new penetration testing assessment request.		
Penetration Test Findings	Contains the following lists: • Active: List of all the active Penetration Test Findings. • All: List of both active and inactive Penetration Test Findings. • Assigned to me: List of Penetration Test Findings assigned to you for remediation. • Assigned to my group: List of Penetration Test Findings assigned to your assignment groups for remediation.	Application Vulnerability Response	sn_vul.app_sec_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Modules	Roles Required
	For information on how to create a penetration test findings, see Create penetration test findings based on an assessment questionnaire.		
Patches	All: List of all the available patches that can be used to remediation host vulnerable items.	Vulnerability Response	sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin
Supporting Data	Contains the following lists: • **Authoritative Sources**: List of authoritative sources that provide summary information which is useful to research the source publications. • **Technologies**: List of technologies that provide the summary information about each authoritative sources and citation (also known, in Qualys, as a framework).	Configuration Compliance	sn_vulc.admin

Related topics

Use the List view in the Vulnerability Manager Workspace

Bulk edit in the Vulnerability Manager Workspace

In the Vulnerability Manager Workspace, the bulk edit feature enables you to update multiple vulnerable items (VITs, AVITs, or CVITs) or configuration test results (TRs) simultaneously, streamlining the management and remediation process.

With bulk edit, you can select multiple vulnerabilities and apply consistent changes, such as assigning remediation owners, updating status, adding work notes, requesting exceptions, and requesting false positive. This saves time and effort by eliminating the need to edit vulnerable items individually, promoting efficient and consistent management of vulnerabilities.

The bulk edit feature is available for:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- host vulnerable items (VITs) starting from v21.0 of Vulnerability Response.
- application vulnerable items (AVITs) and container vulnerable items (CVITs) starting from v22.0 of Vulnerability Response.
- test results (TRs) starting from v23.0 of Vulnerability Response.

Roles required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

You can perform the following tasks using the bulk edit feature in the Vulnerability Manager Workspace:

- Assign records to an assignment group in bulk
- Request bulk exception in the Vulnerability Manager Workspace
- Remove assignments for host vulnerable items in bulk
- Bulk edit for false positive in the Vulnerability Manager Workspace
- Close records in bulk in the Vulnerability Manager Workspace

Understanding compensating controls for risk change

Compensating controls are the measures taken to reduce the risk posed by vulnerabilities that can't be patched immediately. They can be used to mitigate the likelihood or impact of a successful exploit.

Note: The compensating controls feature is available for host vulnerabilities only.

Applying compensating controls can help in reducing the risk of a vulnerability.

The following table shows the use cases for compensating controls:

Use cases for compensating controls

Use case	Compensating control
A vulnerability in a web server that enables attackers to execute arbitrary code.	Implement a Web application firewall (WAF) to block malicious requests to the web server.
A vulnerability in an operating system that enables attackers to escalate privileges to root.	Implement an application control to restrict the execution of applications on the host system.
A vulnerability in a database server that enables attackers to access sensitive data.	Implement network segmentation to isolate the database server from other hosts and critical systems.

For more information on the impact of compensating controls on the risk score of a vulnerable item and remediation task, see Impact of the compensating controls on risk score and expiration date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

- Add a compensating control to the library
- Associate compensating controls with CVEs or TPEs for risk change requests
- Disable or enable risk change for a CVE or TPE

Analytics and reporting solutions for the Unified Vulnerability Response Dashboard

The Unified Vulnerability Response Dashboard is a centralized aggregated dashboard that provides visibility from multiple vulnerability scanners and security tools to provide a comprehensive view of an organization's vulnerabilities and risks.

Required roles

The following roles and tasks are associated with this Solution. They're required for viewing and sharing the reports:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Related topics

- Analytics and Reporting Solutions

Unified Vulnerability Response Dashboard

The Unified Vulnerability Response dashboard provides a comprehensive view of an organization's vulnerabilities and risks. The vulnerabilities related to infrastructure, cloud, applications, and containers can be viewed in a centralized dashboard for better visibility and remediation.

Watch this four-minute video to learn about the Unified Vulnerability Response Dashboard.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

Required ServiceNow AI Platform roles

The following roles are associated with this solution. They're required for viewing, editing, and sharing the reports:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst

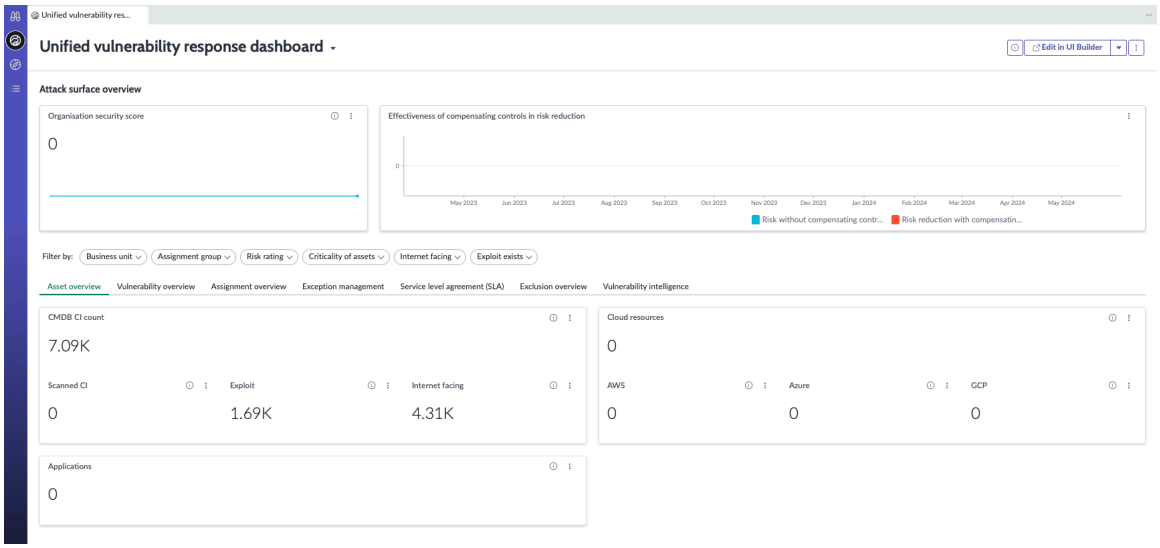
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Access the Unified Vulnerability Response Dashboard

To open the dashboard, navigate to either:

- **All** > **Vulnerability Response** > **Vulnerability Manager Workspace** and select the **Dashboards** icon. Depending on your role, the default dashboard is displayed. To view the Unified Vulnerability Response Dashboard, select the drop-down next to the dashboard name.
- **Workspaces** > **Platform Analytics Workspace** > **Dashboards** > **Unified Vulnerability Response Dashboard**.



Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

Users	Dashboard use
• Vulnerability Managers • Vulnerability Analysts	• Provides real-time visibility of the risks present in infrastructure, applications, configurations, and containers. Enables Vulnerability Managers and Vulnerability Analysts to prioritize and remediate the vulnerabilities in a timely way. • Provides an Attack Surface Overview of critical assets, which can be used to track the remediation progress and efforts. • Provides an overview of risks across business units (BUs). You can use filters to select BUs and compare the progress to reallocate resources, as necessary. Role-level access must be provided to the BU head.

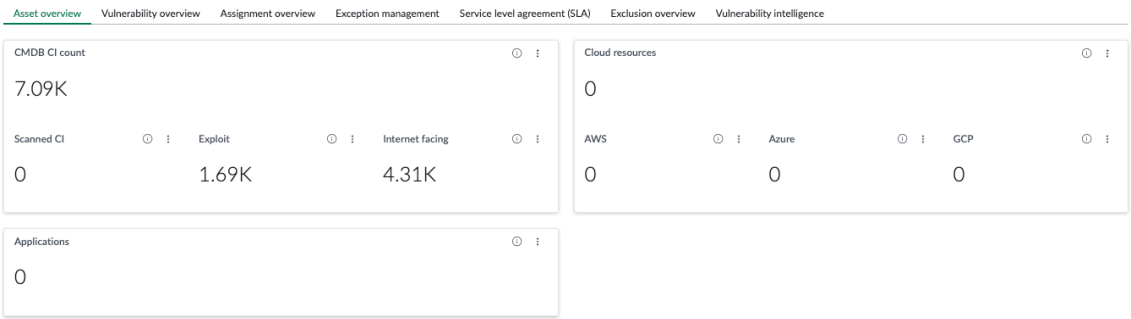
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Users	Dashboard use
	• Provides visibility into the potential impact by BUs. You can use the Common Vulnerability and Exposure (CVE) filter to identify exposures across the organization. • Provides visibility into the EPSS scores attained by vulnerable entries that exist in the CISA KEV catalog for Application, Host, and Container vulnerable items.

Unified Vulnerability Response Dashboard tabs

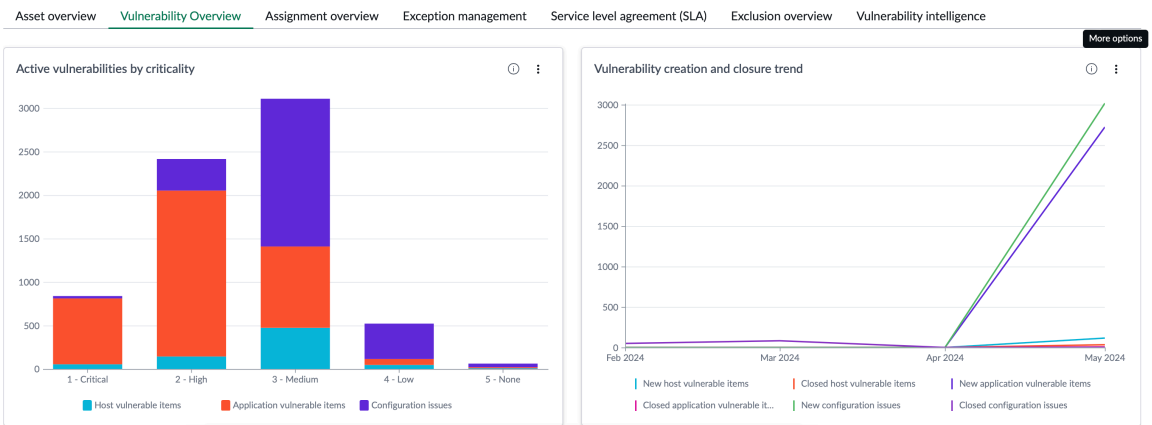
This dashboard lets you see the vulnerabilities or issues that are present in hosts, cloud, configurations, applications, and containers. You can view the vulnerabilities based on the business unit, assignment group, risk rating, criticality, and whether an exploit exists for the vulnerabilities.

The **Asset Overview** tab provides the overall status of configuration items (CIs) in the



system.

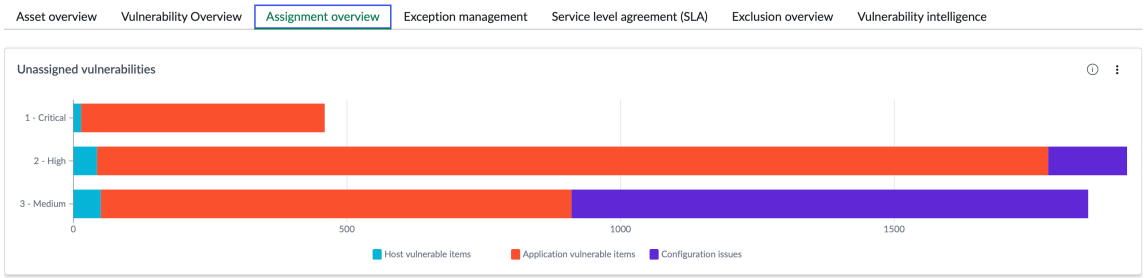
The **Vulnerability Overview** tab provides a status on the types of vulnerabilities such as host, application,



container.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Assignment Overview** tab provides a status on the assignment of the vulnerabilities.



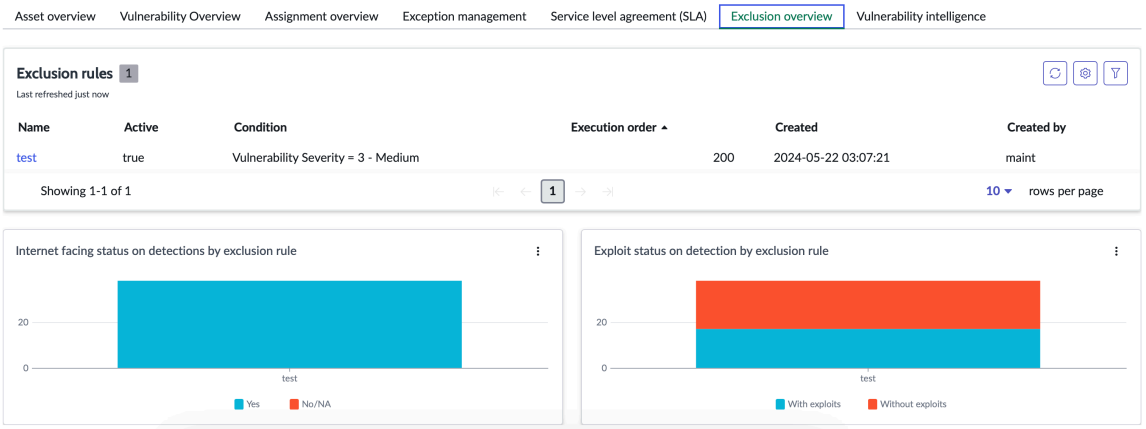
The **Exception Management** tab provides a status on the deferred vulnerabilities.



The **Service Level Agreement (SLA)** tab provides a status on the service level agreement attained by different assignment groups.



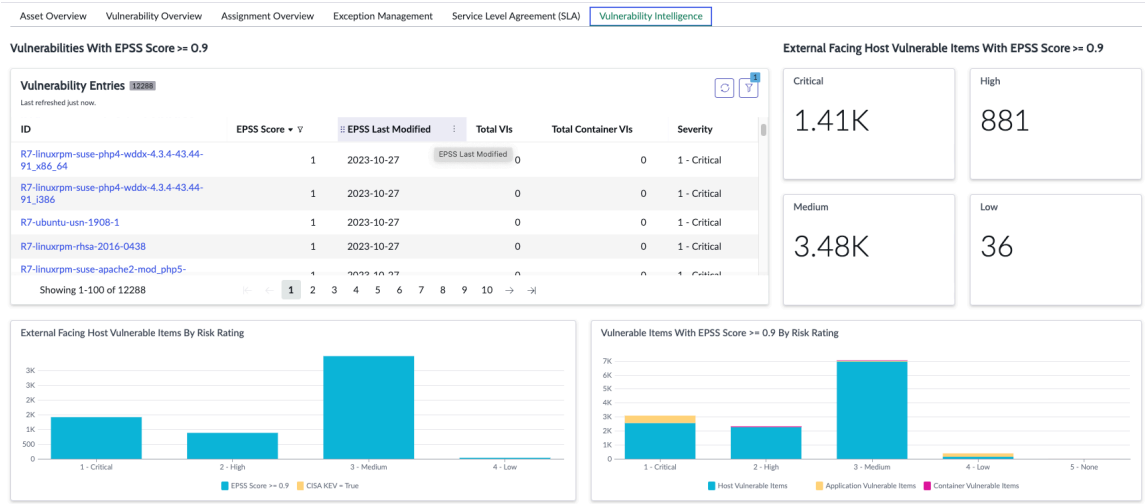
The **Exclusion overview** tab provides a status of exclusion rules you have created, as well as those affecting detections that are internet-facing and have available exploits.



The **Vulnerability Intelligence** tab provides a status on the EPSS scores attained by vulnerabilities having the CISA KEV flag true and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

EPSS Score >= 0.9 for Application, Host, and Container Vulnerable items.



Filters

You can filter the widgets based on the following:

- Business unit
- Assignment group
- Risk rating
- Criticality of assets
- Internet facing
- Exploit exists

When a filter is selected, the data in all widgets gets updated. However, if a filter is not applicable for a widget, a cross symbol is shown next to the filter name.

Note: Only Business unit and Assignment group filters are available in Tokyo. All the filters are available from Utah onwards.

Indicators

Scanned assets

Formula indicator for assets scanned in the last 60 days. Contains scanned discovered item assets, scanned application release assets, scanned discovered container image assets as contributing indicators.

Assets - Exploit exists

Formula indicator for assets where exploit exists in the vulnerabilities. Contains Host assets - Exploit exists, Application assets - Exploit exists, Container assets - Exploit exists as contributing indicators.

Infra Asset - Internet Facing

Indicator for fetching the count of assets, which are internet facing.

Discovered items based on Cloud Resource type

Indicator for fetching the count of assets having an asset category such as cloud.

Base Images

Indicator for fetching the count of base images.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CISA KEVs Asset Type

Formula indicator, which gives the count of container and host vulnerable items where the vulnerability has the CISA KEV (BOD 22-01) flag set to true. Contains CISA exists CVR, and CISA exists Vul Items as contributing indicators.

CISA Exists Vulnerable Items – Unassigned

Formula indicator, which gives the count of container and host vulnerable items where the vulnerability has the CISA KEV (BOD 22-01) flag set to true and the vulnerable items are unassigned. Contains Unassigned Container Vul Items, Unassigned Host Vul Item as contributing indicators.

CISA Exists Vulnerable Items - Target Missed

Formula indicator, which gives the count of container and host vulnerable items where the vulnerability has the CISA KEV (BOD 22-01) flag set to true and the vulnerable items have missed the target. Contains CISA exists Vul Items, CISA exists CVR as contributing indicators.

Active Host VITs

Count of active host vulnerable items (VITs).

Active Application VITs

Count of active application vulnerable items (AVITs).

Active Container VITs

Count of active container vulnerable items (CVITs).

New VITs

Count of VITs that opened on a day.

New AVITs

Count of AVITs that opened on a day.

New CVITs

Count of CVITs that opened on a day.

New Test Results

Count of test results (TRs) that were created on a day.

Closed AVITs

Count of VITs closed on a day.

Closed VITs

Count of AVITs closed on a day.

Closed CVITs

Count of CVITs closed on a day.

Closed Test Results

Count of TRs closed on a day.

Open Config Issues - Test results

Count of all open test results, which are in failed state.

Organization Risk Score

Risk score of an organization from the Rollup Application Risk Score table.

Unassigned Application Vul Item

AVITs with no assignment group or assigned to.

Unassigned Host Vul Item

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

VITs with no assignment group or assigned to.

Unassigned Container Vul Items

CVITs with no assignment group or assigned to.

Unassigned Config Issues

TRs with no assignment group or assigned to.

Deferred VITs

VITs in deferred state.

Deferred AVITs

AVITs in deferred state.

Deferred CVITs

CVITs in deferred state.

Host SLA - Closed

Average age closed of closed VITs.

Application SLA - Closed

Average age closed of closed AVITs.

Container SLA - Closed

Average age closed of closed CVITs.

Test Result SLA - Passed

Average age closed of passed TRs.

Host SLA - Closed (Critical & High)

Average age closed of closed critical and high VITs.

Application SLA - Closed (Critical & High)

Average age closed of critical and high AVITs.

Container SLA - Closed (Critical & High)

Average age closed of closed critical and high CVITs.

Test Result SLA - Passed (Critical & High)

Average age closed of passed critical and high TRs.

Aggregate MTTR

Average age closed of closed VITs, AVITs, CVITs, and TRs.

SLA Missed

Average age closed of closed and target missed VITs, AVITs, CVITs, and TRs.

Vulnerabilities With EPSS Scores >= 0.9

Count of vulnerability entries with EPSS scores greater than or equal to 0.9.

Breakdowns

- VIT type (unified)
- Internet Facing (unified)
- Risk Rating (unified)
- Exploit Exists (unified)
- Discovered Item Cloud Resource Type (unified)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- CISA Exists (unified)
- CMDB class (unified)
- Business Unit (unified)
- Business Criticality (unified)
- Deferred Reason (unified)
- Assignment group (unified)
- Remediation Status (unified)

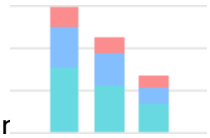
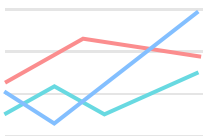
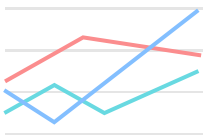
Data visualizations

Asset Overview tab

Title	Type	Description
Attack Surface Overview	 Single score	Number representing the aggregated score of an organization's security.
CMDB CI Count	 Single score	Number of CIs in the organization that are registered and tracked in the Configuration Management Database (CMDB). Provides a breakdown of the following CIs: • Scanned CIs: Number of scanned CIs • Exploit: Number of exploits available • Internet Facing: Number of internet facing CIs
Cloud Resource	 Single score	Number of CIs with asset category such as cloud. Provides a breakdown of the following cloud assets: • AWS • Azure • GCP
Docker Image	 Single score	Number of docker images including the number of base images.
Applications	 Single score	Number of applications in the organization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Overview tab

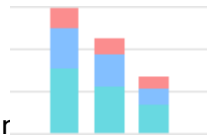
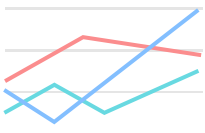
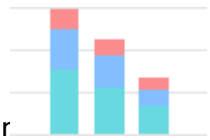
Title	Type	Description
CISA KEVs	Pie Chart	Number of vulnerabilities associated with the CISA catalog and CISA flag as true. Provides a breakdown based on the following: • CISA Vulnerability: Types of vulnerabilities with CISA flag as true • Host CIs - Internet Facing: Internet facing CIs • Unassigned VITs: Unassigned VITs with CISA flag as true • VITs missed target: VITs that missed target with CISA flag as true
Active Vulnerabilities by Criticality	Stacked Bar 	Number of active VITs, AVITs, and CVITs based on criticality.
Vulnerability creation and closure trend	Multiple Line 	Number of new and closed vulnerabilities for all applications. Provides a trend for the last three months.
Misconfiguration by cloud platform	Multiple Line 	Number of configuration issues based on risk rating for each cloud asset.
Cloud Compliance	Table	List of resources with the asset category as cloud along with the following details: • Resource name • Class • Vulnerability issues: Number of issues present in the resource that are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

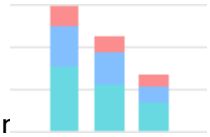
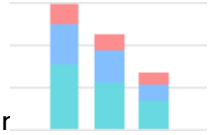
Vulnerability Overview tab (continued)

Title	Type	Description
		aggregated based on the risk rating. • Configuration issues: Number of resources with configuration issues along with the risk rating. • Cloud account: Cloud account ID. • Cloud region: Location of the cloud resources. • Cloud provider: Name of the cloud provider.

Assignment Overview tab

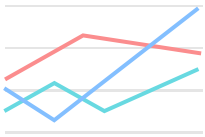
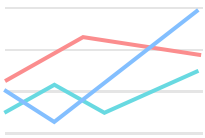
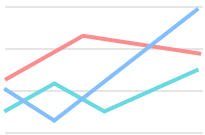
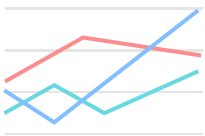
Title	Type	Description
Unassigned VITs	Stacked Bar 	Number of vulnerabilities that aren't assigned to any group or individual along with the risk rating.
MTTR by Assignment Group - Top 10	Multiple Line 	Mean time taken by an assignment group to identify and remediate the security vulnerabilities or issues. The top 10 assignment groups are displayed that have the highest mean time for remediation.
Top 10 Assignment Groups missing SLA (Critical & High Vulnerability)	Stacked Bar 	Top 10 assignment groups that missed the target date of remediation of critical and high vulnerabilities.

Exception Management tab

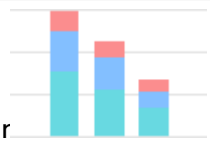
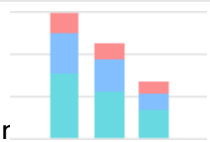
Title	Type	Description
Deferred VITs	Stacked Bar 	Number of vulnerabilities in the deferred state based on risk rating.
Critical and High Deferred VITs by Assignment Group	Stacked Bar 	Number of vulnerabilities with critical and high risk ratings in the deferred state that is categorized based on the assignment groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Service Level Agreement (SLA) tab

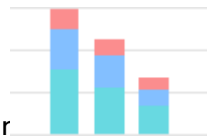
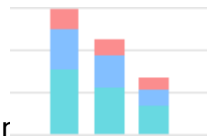
Title	Type	Description
Host Vulnerability: SLA attainment by assignment group	Multiple Line 	Time taken by an assignment group to remediate host vulnerabilities. Provides a trend for the last 10 months.
Compliance Issues: SLA attainment by assignment group	Multiple Line 	Time taken by an assignment group to remediate compliance issues. Provides a trend for the last 10 months.
Application Vulnerability: SLA attainment by assignment group	Multiple Line 	Time taken by an assignment group to remediate application vulnerabilities. Provides a trend for the last 10 months.
Container Vulnerability: SLA attainment by assignment group	Multiple Line 	Time taken by an assignment group to remediate container vulnerabilities. Provides a trend for the last 10 months.

Exclusion overview tab

Title	Type	Description
Exclusion rules	Table	List of all exclusion rules you have created.
Exclusion rules v/s Internet facing	Stacked Bar 	Exclusion rules impacting detections which belong to internet facing assets.
Exclusion rules v/s Exploit exists	Stacked Bar 	Exclusion rules impacting detections that are vulnerable to existing exploits.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Intelligence tab

Title	Type	Description
Vulnerabilities with EPSS Score>= 0.9	Table	Complete list view of all vulnerable entries (CVEs or TPEs) that have an EPSS score greater than or equal to 0.9 along with the following details. • ID: CVE ID of the vulnerability • EPSS Score • EPSS Last Modified • CISA KEV BOD 22-01: Indicates if the entry exists in the CISA KEV BOD (Binding Operational Directive 22-01) • Total VIs: Total count of VIs that exist for this vulnerability entry. • Total Container VIs: Total count of container VIs that exist for this vulnerability entry. • Severity
External Facing Host Vulnerable Items With EPSS Score >= 0.9	Single score 	Number indicating the aggregate count of external facing host vulnerable items with an EPSS score greater than or equal to 0.9. Provides single scores sorted by severity of risk rating.
External Facing Host Vulnerable Items By Risk Rating	Stacked Bar 	Number of external facing host vulnerable items by risk rating. The stack bars are categorized by EPSS Score >=0.9 and CISA KEV =True.
Vulnerable Items With EPSS Score >= 0.9 By Risk Rating	Stacked Bar 	Number of vulnerabilities with EPSS score greater than or equal to 0.9 sorted by risk rating. Provides a breakdown by host vulnerable items, application vulnerable items, and container vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled jobs for data collection

Data collection jobs automatically collect scores for automated indicators and breakdowns. The following scheduled jobs are run to collect scores on new data automatically.

Warning: By default, the following data collection jobs are deactivated in the base system:

- Unified Dashboard Daily Data Collection
- Unified Dashboard Weekly Data Collection
- Unified Dashboard Historical Data collection

Before enabling the jobs, refer to the KB.

Scheduled job	Frequency	Description
Unified Dashboard Historical Data collection	Once	Collects scores and snapshots for existing records.
Unified Dashboard Weekly Data Collection	Weekly	Collects data weekly.
Unified Dashboard Daily Data Collection	Daily	Collects data everyday.
Rollup Risk scores to Organization	Daily	Collects the aggregated risk score for an organization.
Populate cloud compliance daily counts	Daily	Collects data for cloud compliance.
EPSS Daily Job	Daily	Collects EPSS data from First.org.

A new table Rollup Application Risk Score [sn_vul_cmn_rollup_app_risk_score] is created in the Vulnerability Common Scope. This table is populated using the following rollup calculators via the scheduled jobs everyday.

Rollup calculator name	Description
Organization Risk Score Rollup	Rolls up the risk scores for all vulnerable items and configuration issues in an organization. It provides an overall risk score for an organization.
Vulnerable Item Rollup	Rolls up the risk scores for all vulnerable items in an organization, to contribute to the overall risk score of an organization.
Application Vulnerable Item Rollup	Rolls up the risk scores for all application vulnerable items in an organization, to contribute to the overall risk score of an organization.
Container Vulnerable Item Rollup	Rolls up the risk scores for all container vulnerable items in an organization, to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rollup calculator name	Description
	contribute to the overall risk score of an organization.
Test Result Rollup	Rolls up the risk scores for all test results in an organization, to contribute to the overall risk score of an organization.
Rollup EPSS Scores from NVDs to TPEs	Rolls up EPSS Scores from NVDs to TPEs, to contribute to the overall risk score of an organization.

Monitoring and managing vulnerable items and test results in the Vulnerability Manager Workspace

The Vulnerability Manager Workspace enables you to monitor vulnerable items (VITs, AVITs, and CVITs) and Test Results (TRs) using watch topics, and track and manage their remediation progress by creating remediation efforts.

Open search results in Vulnerability Manager Workspace

Open search results in Vulnerability Manager Workspace instead of classic UI by changing the application scope.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin or sn_vul.read_all for host vulnerable items (VITs)
- sn_vul.app_sec_manager or sn_vul.app_read_all for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin or sn_vul_container.read_all for container vulnerable items (CVITs)
- sn_vulc.admin or sn_vulc.read for configuration test results (TRs)

About this task

Example: If you search for a host vulnerable item with its number in the **Search** field by setting the application scope to Vulnerability Manager Workspace, the VIT opens in its record view in the Vulnerability Manager Workspace.

Procedure

1. In the unified navigation bar, select the Globe icon .
2. Select **Application Scope**.
3. Set the scope to **Vulnerability Manager Workspace**.

What to do next

When you search for records such as VITs, remediation tasks, state change approvals, and so on, in the **Search** field in the unified navigation bar, the records open in the Vulnerability Manager Workspace.

When the scope is not Global, the Globe icon displays with a red ring  . Select it again to change the scope.

Create and apply filters the summary of active records (VITs, AVITs, CVITs and CTRs)

As a vulnerability manager and analyst, you can filter the desired records to visualize their summary on the Home page of the Vulnerability Manager Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **Home page**.
2. Select the Gear icon , and then select **Create filter** in the Host Vulnerabilities, Container Vulnerabilities, Application Vulnerabilities or Configuration Test Results tabs.
3. On the Create Filter pop-up window, fill in the fields.

Create Filters pop-up window

Field	Description
Filter Name	Name for the filter.
Conditions	Condition to show only the records for which you want to see visualizations.
Refresh Daily	Update the visualization information every day.

4. Select **Save**.
5. View the visualizations for the filtered records by selecting the new filter in the **View by** field. For more information on the widgets, see Home page in the Vulnerability Manager Workspace.
6. To update or delete a filter:

   a. Select the Gear icon and then select **Edit filter**.

   b. On the Saved Filters pop-up window, select the filter you want to update or delete.

   c. Update or delete the filter.

Action	Steps
Delete the filter.	Select **Delete**.
Modify the filter name	Edit the filter name and select **Update**.
Change the filter conditions	Edit the condition to display information only for certain records and select **Update**.
Refresh Daily	Determine whether to refresh the visualization information every day and select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Home page in the Vulnerability Manager Workspace

Use watch topics in the Vulnerability Manager Workspace

Use watch topics in the Vulnerability Manager Workspace to view vulnerabilities and misconfigurations that are filtered from your imported data from the criteria that you set. Use this information to determine how the vulnerabilities and misconfigurations in each watch topic can impact your environment.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

From the Watch Topics page, you can do the following tasks:

- Monitor the number of remediation efforts and records (VITs, AVITs, CVITs and TRs) to see the progress of your vulnerability remediation.
- Edit or delete your existing watch topics and create watch topics.
- Create the remediation efforts and automatically hand off the remediation tasks to your IT teams for only the vulnerabilities that you want to fix.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

Procedure

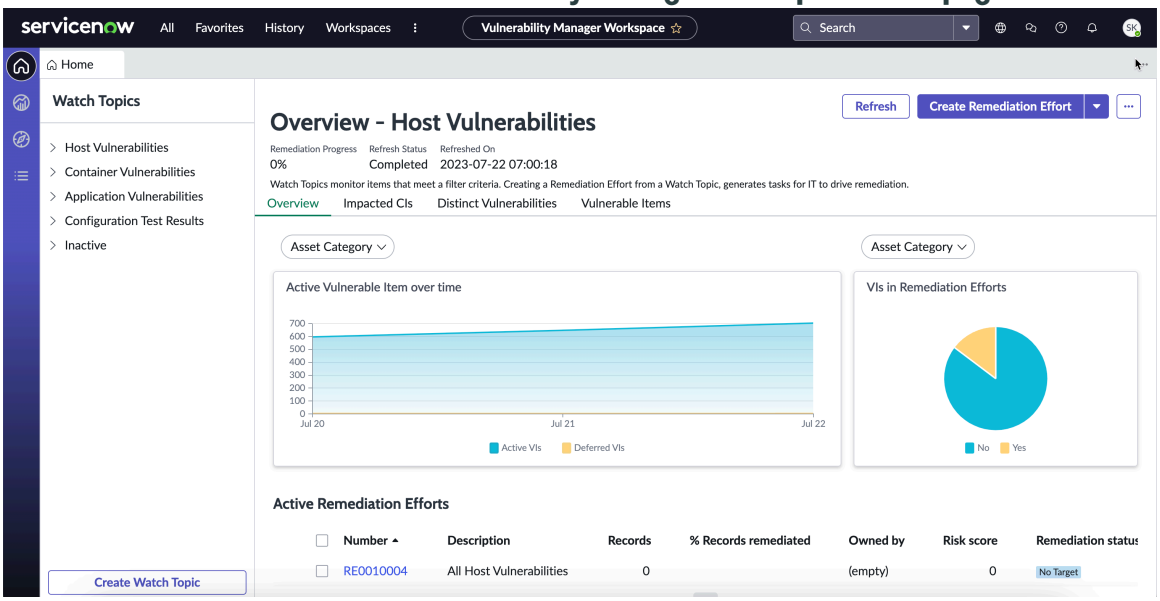
1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace**.
2. Select the watch topics icon.
3. Select a watch topic in the Host Vulnerabilities, Container Vulnerabilities, Application Vulnerabilities or Configuration Test Results tabs on the Watch Topics page.

   When you select a watch topic, the **Overview** tab is displayed by default.

   For more information on the watch topics, see Watch Topics page in the Vulnerability Manager Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Version 19.0 Overview tab in the Vulnerability Manager Workspace home page



The dashboards are dynamic and new vulnerability data updates upon import.

4. Select a **Related Items tab** to view more data.

   For more information on the related items list and visualizations in a watch topic, see Related items list and visualizations in a watch topic.

5. Do the UI actions on the Watch Topics page.

UI action	Description
Create a watch topic	Create your own watch topic by using your own set of conditions for the vulnerabilities that you feel are important. For more information on how to create a watch topic, see Create a watch topic in the Vulnerability Manager Workspace.
Edit or delete an existing Watch Topic	For more information on how to edit or delete a watch topic, see Edit or delete a watch topic in the Vulnerability Manager Workspace.
Deactivate or activate a watch topic	You can deactivate or activate a watch topic. For more information on how to deactivate or activate a watch topic, seeDeactivate or activate a watch topic.
Refresh a watch topic	You can acquire the latest details of a watch topic by selecting the **Refresh** button. The latest refresh status and timestamp are displayed under the watch topic name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
	○ A watch topic is refreshed automatically when it is created or updated. ○ When you refresh a watch topic, all the de tails of the watch topic, including the charts and remediation efforts are updated. **Note:** Because you can't refresh an in active watch topic, the **Refresh** button is inactive for an inactive watch topic.
Create a remediation effort	○ Create a remediation effort. A remediation effort contains the remediation tasks that are assigned to your IT teams. You can use this tool to drive and track the remediation progress from assignment through resolu tion. ○ When you create a remediation effort, all the active vulnerable items are automatical ly pulled in if they aren’t already part of an existing remediation effort for that watch top ic. ○ Remediation tasks are assigned to IT teams automatically based on the VI assignment group. ○ An example of a remediation effort from the Vulnerabilities on Windows Servers watch topic might be, Vulnerabilities on Windows Servers in Q2 2021. The remediation tasks in this effort are then assigned to the assign ment groups that are listed on the associat ed records.
Create a recurring effort	Create recurring remediation efforts on a schedule that helps you to track the vulnera bilities that might require your immediate and ongoing attention. For more information on the recurring effort creation, see Create a re curring remediation effort in the Vulnerability Manager Workspace. **Note:** You can't create a recurring effort for an inactive watch topic.
Refine filters for a column on a list	Roll over the title of a column and click the three vertical dots menu to set the filters for that column. For example, let's say that you want to do more filtering on your configuration items that are associated with the records. You can se lect the Configuration Item column to view the available filter conditions. You may want to set

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
	conditions to filter your assets so that you see only those assets that contain the PCI data.
Filter out items or match items from a row in a column	Filter out items or match items from a row in a column. For example, let's say that you want to view only the records that have a specific vul nerability. With the Vulnerable Items related item list tab selected, from the list of records, select the row of a record in the Summary col umn. Select the three vertical dots menu that is displayed and select one of the following op tions: ○ **Show Matching**: Shows all the other records that have this vulnerability. ○ **Filter Out**: Shows all the records that don't have this vulnerability.

6. **Optional:** Select a record to view more details.

Create a watch topic in the Vulnerability Manager Workspace

Vulnerability managers and analysts can create watch topics using a set of conditions to filter out subsets of records (VITs, AVITs, CVITs or CTRs) that they want to monitor.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

On the Overview tab of watch topics, a trending report that is updated nightly, along with other reports, show the current status of the records for that watch topic.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. **Optional:** Alternatively, to the right of the Create remediation effort button, click the three dots, followed by edit to modify an existing watch topic.

   Note: You might notice a delay before current data is displayed for a watch topic after you change the filtering.

3. In the lower left of the page, click **Create Watch Topic**.
4. In the modal that displays, fill in the fields.
   For more information on the Create watch topic modal fields, seeCreate Watch Topic form fields.
5. Define conditions for the selected record category.

Option in Category drop-down	Steps
Host Vulnerabilities	In the **Vulnerable Item Condition**, define con ditions to identify the host vulnerabilities. The host vulnerabilities are detected based on the set conditions.
Application Vulnerabilities	In the **Application Vulnerable Item Condi tion**, define conditions to identify the host vul nerabilities. The application vulnerabilities (or AVITs) are detected based on the set conditions.
Container Vulnerabilities	In the **Container Vulnerable Item Condition**, define conditions to identify the host vulnera bilities. The container vulnerabilities (CVITs) are de tected based on the set conditions.
Configuration Test Results	In the **Configuration Test Results Condition**, define conditions to identify the configuration issues. The configuration test results are detected based on the set conditions.

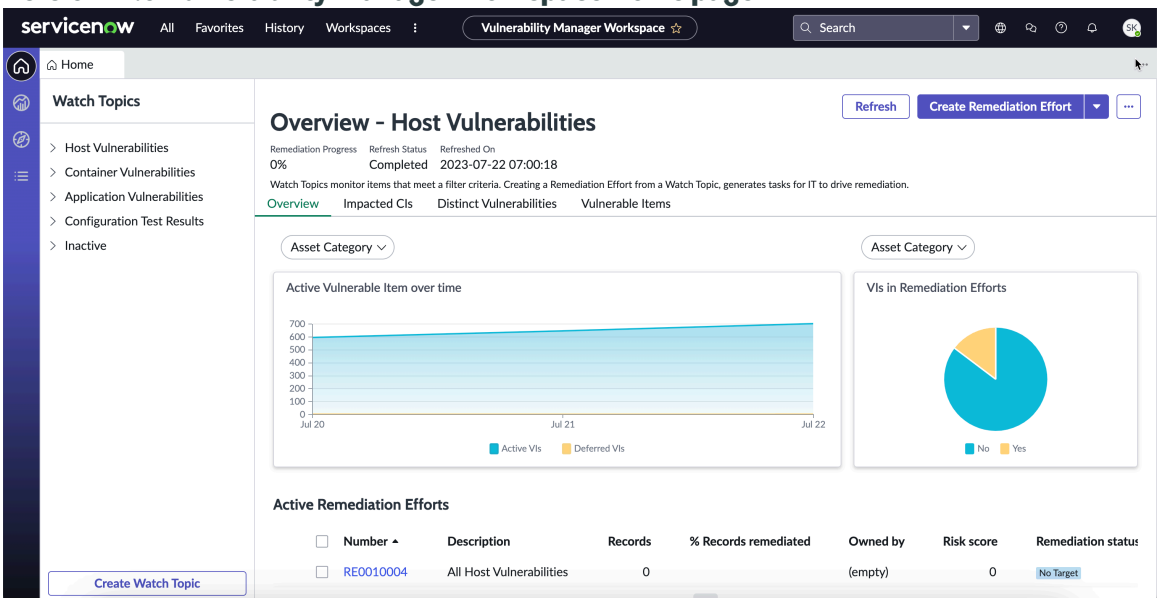
   Note: If you don't set any conditions in your watch topic, no data is pulled to the dashboard.

6. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your new watch topic is displayed on the Home landing page. The watch topics are categorized by record type in the navigation pane.

Version 19.0 Vulnerability Manager Workspace Home page



What to do next

Create a remediation effort.

Edit or delete a watch topic in the Vulnerability Manager Workspace

You can edit or delete an existing watch topic in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

If you edit an existing watch topic:

- The data on the dashboard is updated to reflect your changes.
- The records that are currently in the existing Remediation Efforts remain unchanged.
- The records that aren't currently in Remediation Efforts are displayed based on the criteria that you enter in the condition builder.

If you delete a watch topic before all its associated records are fixed, the records that are displayed with that watch topic aren’t affected.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. Open the watch topic that you want to edit.
3. Click the three dots ... and click **Edit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can't edit an inactive watch topic.

4. In the Edit watch topic modal, modify the fields.
5. Click **Submit**.

Note: You might notice a delay before current data is displayed for a watch topic after you change the filtering.

You can also edit existing recurring remediation efforts. If there's an existing recurring remediation effort for a watch topic, **Edit recurring effort** is available from the menu. Select this option to edit the recurring effort.

Any changes that you make and save to the remediation effort record don't affect any of the other remediation efforts that you have already created from the watch topic.

6. **Optional:** To delete a watch topic, select more icon ... on the watch topic and select **Delete**.

Deactivate or activate a watch topic

You can deactivate or activate a watch topic in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

- All the inactive watch topics are displayed in the **Inactive** module in the navigation pane.
- You can't create a remediation effort or a recurring remediation effort for an inactive watch topic.
- You can't refresh an inactive watch topic.
- The details of an inactive watch topic and its associated remediation efforts aren't updated.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. Open the watch topic that you want to deactivate.
3. Click the three dots and click **Deactivate**.
   The watch topic appears in the Inactive module.
4. To activate a watch topic, select a watch topic in the Inactive module, select the three dots menu and select **Activate**.
   The activated watch topic moves to the appropriate module in the navigation pane.

Use Remediation Effort records

When Vulnerability managers and analysts create remediation efforts (REs), remediation Tasks (VUL, AVUL, CVUL, and CRG) are automatically assigned to IT teams for remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

You have to create a remediation effort before you can use it to monitor remediation progress on Remediation Tasks.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. If not selected, in the upper left, click the List icon.

   The List view with active Remediation Effort records is displayed.

2. In the Record Type column, select the three dots menu and select **Group by Record type**.
   The remediation efforts categorize into host vulnerable items, application vulnerable items, container vulnerable items, and configuration test results.
3. From the List view landing page, with Active Remediation Efforts selected in the filtered lists, click a record to open it.
   The record displays. You can view the remediation tasks and records that are associated with the selected remediation effort.
4. Refer to the following table for the actions that you can perform on the remediation effort record.

   After you create a record, it may take a few minutes for the remediation tasks and large numbers of records to display.

UI action	Description
Add a tag	To the right of the header, click the small tag icon. You might want to add text that further helps you identify this record. For example, you might want to add a tag that this record has PCI or other critical data.
Add a work note to the record	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel.
Update the record	On the **Details** tab, for all fields that are editable, click a field to select it, make your changes, and click **Save** to update the record.
When displayed, click the filter icon to refine the data on the displayed page	With any one of the Remediation Tasks, Vulnerable Items, or Configuration Test Results tabs selected, on the far right, click the filter icon to show the filters that apply to the tab. In the panel that is displayed, click **Advanced view** to add or change filter conditions for the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
	items on the page. Click **Update** to save your changes. For example, on the **Vulnerable Items** tab, you might prefer to add the Age field and enter a range to display only records from a specific time period. Records that match the conditions that you set are displayed in the list.
Refine filters for items in a column	Select a column and click the three vertical dots menu expand it and enter conditions to refine and group the data in the column.
Filter out items or match items from a row in a column	Say, for example, you want to view only records that have a specific vulnerability. From the list of records, select the row of the record in the **Summary** column. Click the vertical dot menu that is displayed and choose one: ○ **Show matching** - show all the other records that have this vulnerability. ○ **Filter out** - show all records that don't have this vulnerability.

5. From the Remediation Tasks, Vulnerable Items and Configuration Test Results tabs, you can drill down into an individual Remediation Task (VUL, AVUL, CVUL, or CRG), Vulnerable item (VIT, AVIT, or CVIT) and Test Result (CTR) records respectively.

What to do next

If you want to create a remediation task on-demand from a remediation effort, see Create a remediation task on-demand in the Vulnerability Manager Workspace. You can also Create a customized list of records to help you monitor remediation progress.

Create a remediation effort in the Vulnerability Manager Workspace

A remediation effort record is a static list of records that you create from a watch topic in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

You use remediation efforts to hand off the tasks IT teams use to fix vulnerabilities and misconfigurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can edit existing remediation efforts.
- Create remediation efforts that are created automatically on the dates and times that you set.
- Transfer records from existing remediation efforts into a new remediation effort.

Starting with version 18.0, because you cannot create a remediation effort for an inactive watch topic, the **Create Remediation Effort** button is inactive.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. On the Watch Topics page, select a watch topic that you want to create a remediation effort for.
3. To view the records that are associated with the selected watch topic, under the record header, click **Vulnerable Items**, **Application Vulnerable Items**, **Container Vulnerable Items** or **Configuration Test Results** tab in their respective watch topics.

   The records display.

   For example, in the header under the Vulnerable Items tab, you can view the total number of records that this watch topic has.

   The following columns and data are displayed:

Columns in the Vulnerable Items tab

Column	Description
Number	The record number.
Summary	Description of the vulnerability.
Configuration item	The asset associated with the vulnerability.
Risk rating	Quantified Risk Score separating records into Critical, High, Medium, Low, and None.
State	Status of the record.
Remediation status	Status of remediation for a record.
Assignment group	Assignment groups responsible for remediation. Assignment of records to groups is based on the assignment rules that you create.
Remediation effort	If it is assigned to a remediation effort, each record lists its assigned remediation effort. After it is added to a remediation effort, a record won't be added to any other remediation efforts that you create.
Assignment group	Assignment groups responsible for remediation. Assignment of records to groups is based on the assignment rules that you create.
Remediation effort	If it is assigned to a remediation effort, each record lists its assigned remediation effort. After it is added to a remediation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Description
	effort, a record won't be added to any other remediation efforts that you create.
In remediation task	If `true`, this value indicates that a record is already in a remediation task. Records can be in multiple remediation tasks, but a record can be added only to one remediation effort.
Exploit exists	Indicates if a known exploit exists for a record.
Last opened	Date when the record was last opened in your ServiceNow AI Platform. If the record was closed and then reopened, this is the last time the record was reopened.

4. To create a remediation effort, click **Create Remediation Effort**.

   When you create remediation effort, records already in existing remediation efforts are not added to any new remediation efforts that you create from this watch topic.

   As records are updated or new records are created in watch topics, you can create remediation efforts.

5. Alternatively, you can Create a recurring remediation effort in the Vulnerability Manager Workspace.

   The **Edit** button is available in the menu for existing remediation efforts. You have the option to modify the fields and conditions from a modal that is displayed. Any changes you make and save to the remediation effort record do not affect any of the other remediation efforts you have already created from the watch topic.

6. In step 1 of the Create Remediation Effort modal, fill in the fields.

   In the Short description field, enter text that describes the recurring remediation effort and helps you locate and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts.

7. In step 2, Task generation, choose one method from the list to bundle the records in the remediation tasks that you generate from this remediation effort after it is created.

Option	Description
By Assignment group	Records with same assignment group are bun dled into one Remediation Task.
By Assignment group and configuration item	Records with same assignment group and Configuration Item are bundled into one Re mediation Task.
By Assignment group and (vulnerability or configuration test)	Records with same assignment group and Configuration Item are bundled into one Re mediation Task.
None (No remediation tasks are created).	Use this method if you want to add records manually to a remediation task for this effort.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	See Create a remediation task on-demand in the Vulnerability Manager Workspace.

8. To automatically refresh the duplicate host vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** check box.

   Note: This check box is available only for Host Vulnerabilities.

9. In step 3, Transfer, verify how many records you want to add to the remediation effort and see how many records are available for transfer from other active remediation efforts.

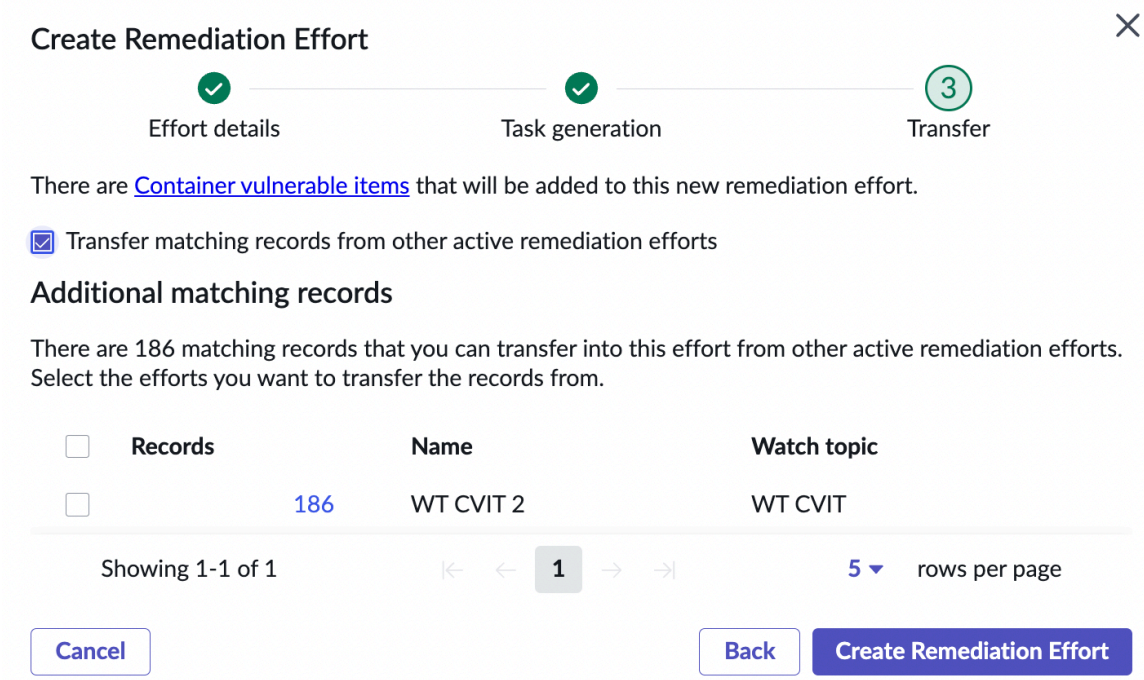
   If there are no new, active records to add, the following text is displayed:

   `There are no available active records that you can add to this new remediation effort.`

   Any additional records that are available for transfer to this effort are listed under `Additional matching records.`

   Select the **Transfer matching records from other active remediation efforts** check box and then select the check boxes for the records you want to transfer from other active remediation efforts.

   Version 18.0 Create Remediation Effort

   After you click **Create Remediation Effort**, in a few moments, the new remediation effort is displayed. Depending on the number of records, it may take some time to populate the new record. A message indicates if the record is still populating.

   The new remediation effort is created with any records that are available from the watch topic used to create it, in addition to any records that you selected for transfer from existing efforts.

   If you select records to transfer from an existing effort, and the existing effort transfers all of its records into your new effort, the remediation effort you moved the records from is closed. For

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by the records transfer, see Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces.

Note: If there are not any records available from the watch topic, or any records selected for transfer, the **Create Remediation Effort** button is deactivated.

The *Populate Efforts* scheduled job runs every 10 minutes to populate the data in the widgets based on the condition selected.

Click Remediation Progress tab to view the remediation progress. Click any item to view details including record type, risk score, risk rating, percentage of records remediated, records in deferred and non-deferred state and total number of records, conditions used in the watch topic, and remediation status. The Remediation Status information such as Remediation target and Remediation status is rolled up from the Vulnerable Items table. The highest record risk score is rolled-up from the Vulnerability Calculators table while risk score is rolled up from the **Vulnerability Rollup Calculators** > **Remediation Effort Rollup**.

The Remediation Tasks tab displays the tasks for all types of issues. The fields are populated when the following scheduled jobs run. They are executed automatically every 15 minutes:

- Rollup application vulnerable item values to vulnerability and group.
- Rollup container vulnerable item values to vulnerability and group.
- Rollup test result values to test result group and configuration test.
- Rollup vulnerable item values to vulnerability and group.

In the Lists view, you can view the Remediation efforts, Remediation Tasks, Vulnerable Items, Configurations Test Results and so on. You can open a remediation task or a vulnerable item and view the Details page. Click the More Actions ellipses and click **Start Investigation** to resolve a remediation task.

10. **Optional:** You can also edit existing recurring remediation efforts.

    (Optional) If there is an existing recurring remediation effort for a watch topic, **Edit recurring effort** is available from the menu in the upper right of a watch topic. Choose this option to edit the recurring effort.

    Any changes you make and save to the remediation effort record do not affect any of the other remediation efforts you have already created from the watch topic.

Create a remediation task on-demand in the Vulnerability Manager Workspace

Create a remediation task on-demand from a remediation effort. If you create a remediation task on-demand, you choose the records you want to add manually.

Before you begin

Role required: sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin

About this task

For version 18.0 of Vulnerability Response, you cannot create a Remediation Task from the record view of a Remediation Effort.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace**.
2. At the top left of the workspace with the Home page displayed, click the **List** view icon, to display the List landing page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Under Remediation Efforts, click either **Active** or **All**.
4. From the list that is displayed, click a record to open it.
   The overview tab of the record is displayed.
5. Click the **Vulnerable Items** tab.
   The list of records displays.
6. To create a new remediation task, in the Number column, select the records you want to add.
7. Click **Create remediation task**.
8. In the modal that is displayed, fill in the fields.

Field	Description
Short description	Enter text that can help you identify this remediation tasks easily from your existing remediation tasks.
Assignment group	Choose an assignment group for the tasks. Use the filter to help you locate the group you want.

9. Click **Create**.
10. The new remediation task is displayed with the active records you selected.

Create a recurring remediation effort in the Vulnerability Manager Workspace

You can create and schedule recurring remediation efforts that are generated automatically on the dates and times that you set.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

You can automatically create recurring remediation efforts on a schedule that helps you track vulnerabilities that might come up and require immediate and ongoing attention.

Starting with version 18.0, because you can't create a recurring remediation effort for an inactive watch topic, the **Create Recurring Effort** option is inactive. If you deactivate a watch topic that has a recurring effort already scheduled, then a new remediation effort is not created until the watch topic is activated. Also, the **Effort recurrence** and **Next recurrence date** details disappear on the upper right. After you activate the watch topic, a remediation effort is created at the upcoming schedule.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace** > **Watch Topics**.
2. On the Watch Topics page, select a watch topic that you want to create a recurring remediation effort for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can create one recurring remediation effort per watch topic.

Note: You cannot transfer records from recurring remediation efforts into new remediation efforts. However, you can transfer records from existing, non-recurring remediation efforts into new remediation efforts. See Transfer records to remediation efforts in the Vulnerability Manager Workspace for more information about transferring records.

3. On a watch topic, on the upper right from the Create Remediation Effort list, select **Create Recurring Effort**.

   The Create Recurring Effort modal is displayed.

4. In step 1, Effort details, fill in the required fields.

   In the Short description field, enter the text that describes the recurring remediation effort that helps you locate it and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts. For example, `Vulnerabilities on External Facing Assets`.

5. Click **Next**.
   Task generation details are displayed.
6. In step 2, Task generation, choose one method from the list to bundle the vulnerable items in the remediation tasks that you generate from this remediation effort after it is created.
   - By Assignment group
   - By Assignment group and configuration item
   - By Assignment group and vulnerability
   - None (No remediation tasks are created). Use this method if you want to add records manually to a remediation task for this effort. See Create a remediation task on-demand in the Vulnerability Manager Workspace.
7. To automatically refresh the duplicate host vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** option.

   Note: This check box is available only for Host Vulnerabilities.

8. Click **Next** to continue.
9. In step 3, Recurrence, select the frequency.

Option	Description
Quarterly (Every 3 months)	Schedules Remediation Effort once in every three month. **Note:** If the month you select has only 30 days, the remediation effort is created on that last date of the month.
Monthly	Schedules Remediation Effort once in every month.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Weekly	Schedules Remediation Effort once in every week. **Note:** This option is available starting from the version 19.0 of Vulnerability Response.
Daily	Schedules Remediation Effort everyday. **Note:** This option is available starting from the version 19.0 of Vulnerability Response.

a. Define the recurrence schedule.

   Use the lists to select the month/day/hour/minute you want the remediation effort created. The time zone for scheduling is by default your time zone.

   Note: If you have many vulnerabilities, you might prefer to set the creation for off-hours.

   If you want the job created on the last day of the month, the scheduled job creates the recurring remediation effort on the last day of the month. A message displays if the month does not have 31 days.

b. **Optional:** Select **Carry over vulnerabilities** to active vulnerabilities in this remediation effort to carry forward into each subsequent remediation effort that is created.

10. Click **Schedule recurrence**.
    A message is displayed that the recurring remediation record was created. The new remediation effort is not displayed immediately, it is created when you scheduled it. It is displayed on your lists after it is created by the scheduled job.

    The date the remediation effort will be created is shown on the corresponding watch topic. For more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by records transfer, see Life cycles of remediation efforts, remediation tasks, and records in the Vulnerability Response Workspaces.

Transfer records to remediation efforts in the Vulnerability Manager Workspace

You can transfer records from existing remediation efforts into new remediation efforts in the Vulnerability Manager Workspace.

Before you begin

If confronted by a zero-day threat or a very critical vulnerability that you want to resolve quickly, you might want to consolidate any active records that you already have for this vulnerability into one remediation effort. However, each record can only be in one effort, and records can overlap among watch topics. So, to gather them all, you need to transfer these records from multiple existing efforts into one remediation effort.

Say, for example, you created a remediation effort that has one, high-priority vulnerability in it. Because this vulnerability is widespread and potentially impacts the other areas in your environment, you might have records that are associated with this vulnerability already in

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

existing remediation efforts. To combine these records so they are all in one remediation effort, you can transfer any records from existing remediation efforts into a new remediation effort.

Note: You cannot transfer records from recurring remediation efforts into new remediation efforts. For more information, see Create a recurring remediation effort in the Vulnerability Manager Workspace.

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace**.
2. Select the watch topics icon.
3. On the Watch Topics page, select a watch topic that you want to create a recurring remediation effort for.
4. Click **Create Remediation Effort**.
   The Create Remediation Effort modal is displayed.
5. In step one, Effort details, fill in the required fields.

   In the Short description field enter text that describes the recurring remediation effort that helps you locate it and track it from the effort list.

   In the Description field, enter more text about the context of the effort that helps you locate it easily from the list of remediation efforts. For example, `Active Log4J Vulnerabilities`.

   a. In the Name field enter a name for your new remediation effort.
      By default the watch topic name is displayed.

   b. In the Description field, enter text that will help you locate this remediation effort easily from the list of remediation efforts.

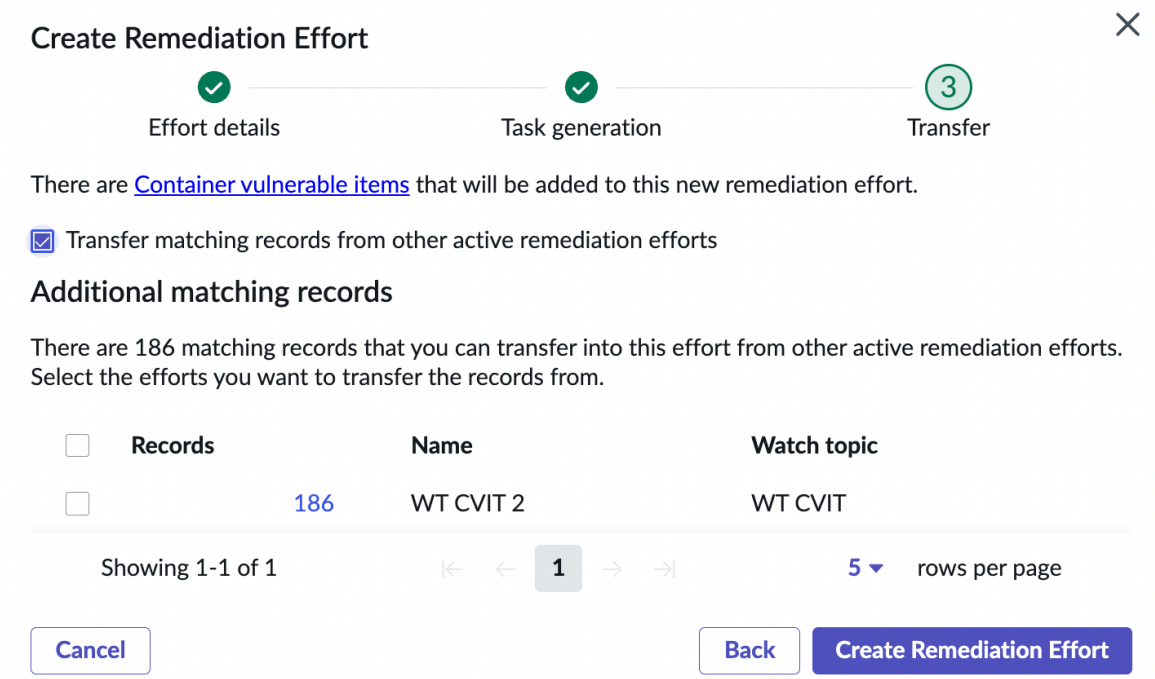
6. Click **Next**.
   Task generation details are displayed.
7. In step 2, Task generation, choose one method from the list to bundle the records in the remediation tasks that you generate from this remediation effort after it is created.
   - By Assignment group
   - By Assignment group and configuration item
   - By Assignment group and vulnerability
   - None (No remediation tasks are created). Use this method if you want to add records manually to a remediation task for this effort. See Create a remediation task on-demand in the Vulnerability Manager Workspace.
8. To automatically refresh the duplicate vulnerable items, you must select the **Automatically refresh duplicate vulnerable items for the created remediation tasks** option.
9. Click **Next**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. In step 3, Transfer, verify how many records will be added to the remediation effort and see how many records are available for transfer from other active remediation efforts.
11. To transfer records from other efforts, from the list, select the check boxes for the records you want.

    Select the **Transfer matching records from other active remediation efforts** check box and then select the check boxes for the records that you want to transfer from other active remediation efforts.

Version 18.0 Create Remediation Effort



12. Click **Create Remediation Effort**.

    After a few moments, the new remediation effort is displayed. Depending on the number of records, it may take some time. A message indicates that the record is populating.

    The new remediation effort is created with any records that are available from the watch topic used to create it, in addition to any records that you selected for transfer from existing efforts.

    If you select records to transfer from an existing effort, and the existing effort transfers all of its records into your new effort, the remediation effort you moved the records from is closed.

    Note: If there are neither any records available from the watch topic, nor any records selected for transfer, the **Create Remediation Effort** button is deactivated.

    For more information on how the Remediation Tasks associated with the Remediation Efforts are impacted by records transfer, see Transferring records or record carry over.

Add a compensating control to the library

As a Vulnerability Manager or Analyst, add a list of compensatory controls to the Compensating Controls library in the Vulnerability Manager Workspace, which can be applied for the risk change of vulnerable items, application vulnerable items, remediation tasks, and application remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

About this task
Some commonly used compensating controls are shipped with the base system. You can view these compensating controls by navigating to **Workspaces** > **Vulnerability Manager Workspace** > **Lists** > **Libraries** > **Compensating controls**. You can activate or deactivate these compensating controls as per your requirement.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure
1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page under Libraries, select **Compensating Controls**.
3. Click **New**.
4. On the Create Compensating Controls form, fill in the fields.

Create Compensating Controls form fields

Field	Description
Name	Name of the compensating control, which appears as an option in the **Compensating controls** drop-down of the Request exception modal.
Description	Brief information that provides details about the Compensating Control.
Active	Status of the compensating control. Only active controls appear in the **Compensating controls** drop-down of the Request exception modal.

5. Select **Save**.
6. On the Compensating Controls list under Libraries, select the desired compensating control and select **Edit**, activate or deactivate a compensating control and click **Save** to modify the compensating controls.
   All the active compensating controls appear as an option in the **Compensating controls** drop-down of the Request exception modal for risk change requests.

What to do next
Starting from v21.0 of Vulnerability Response, you can associate compensating controls with CVEs or TPEs after adding a compensating controls to the library. For more information on how to associate compensating controls, see Associate compensating controls with CVEs or TPEs for risk change requests.

Associate compensating controls with CVEs or TPEs for risk change requests

As a Vulnerability Manager or Analyst, you can associate relevant compensating controls with a CVE or TPE, which can be applied for risk change requests.

Disable or enable risk change for a CVE or TPE

As a Vulnerability Manager and Analyst, you can disable or enable the risk change requests for the host vulnerabilities from a Common Vulnerability Entry (CVE) or Third-party Entry (TPE).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

- Understanding compensating controls for risk change
- Disable or enable risk change for a CVE or TPE
- Associate compensating controls with CVEs or TPEs for risk change requests
- Impact of the compensating controls on risk score and expiration date

Associate compensating controls with CVEs or TPEs for risk change requests

As a Vulnerability Manager or Analyst, you can associate relevant compensating controls with a Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Vulnerability Manager Workspace, which can be applied for the risk change requests.

Before you begin

Role required: sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin

About this task

- If you don't associate compensating controls to a CVE or TPE, all the active controls appear in the Select Compensating Controls field of the Request Exception form.
- If you associate a compensating control to a CVE, this compensating control is automatically associated with the TPE, which is mapped to the CVE.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the Lists page, under Libraries, open one of the following for which you want to associate the controls:
   - **CVE** from the CVEs list.
   - **TPE** from the TPEs list.
3. Select **Associate controls**.

   Note: The **Associate controls** button appears only when the risk change is enabled for a CVE or TPE. In other words, you can associate compensating controls only when risk change is enabled for a CVE or TPE. If the **Associate controls** button isn't visible, select **Enable risk change**.

4. On the Associate controls modal, select the compensating controls that can be applied to vulnerabilities associated with the CVE or TPE for risk change.
5. Select **Submit**.
   - The associated compensating controls appear in the Applicable compensating controls tab in the record view of the CVE and TPE.
   - While a remediation owner requests risk change, these associated compensating controls appear in the Select Compensating Controls field on the Request Exception modal.

Related topics

- Understanding compensating controls for risk change
- Disable or enable risk change for a CVE or TPE

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Add a compensating control to the library
- Impact of the compensating controls on risk score and expiration date

Disable or enable risk change for a CVE or TPE

As a Vulnerability Manager and Analyst, you can disable or enable the risk change requests for the host vulnerabilities associated with a Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Vulnerability Manager Workspace.

Before you begin
Role required: admin

About this task
The risk change for a CVE and TPE is enabled by default.

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
   On the Lists page, under Libraries, open one of the following for which you want to disable the risk change requests:
   - **CVE** from the CVEs list.
   - **TPEs** from the TPEs list.
2. Select **Disable risk change**.
   The remediation owner can't request risk change for the host vulnerable items and application vulnerable items related to this CVE or TPE. In other words, the Request for Risk Reduction check box doesn't appear when the **Reason** is selected as `Mitigating Control in Place` on the Request Exception modal.
3. To enable the risk change requests for host vulnerable items and application vulnerable items, select **Enable risk change**.

Related topics

- Understanding compensating controls for risk change
- Add a compensating control to the library
- Associate compensating controls with CVEs or TPEs for risk change requests
- Impact of the compensating controls on risk score and expiration date

Rescan records and remediation tasks in the Vulnerability Manager Workspace

To verify that your remediation tasks and records have been resolved between scheduled scanning cycles, initiate rescans from your ServiceNow AI Platform on-demand.

Role required: sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

The Rapid7 and Qualys scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button is not available.

To activate these scanners, as a user with the sn_vul.vulnerability_admin role:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Locate the scanner product that you want to activate and click the record to open it.
3. Select the Active check box.
4. Click **Update**.

   The product you activated is displayed in the Source field on the vulnerable item and remediation task records after the next import, and **Rescan** is available as a UI action.

Rescan is supported for records and remediation tasks with the following integrations in the Vulnerability Manager Workspace. See the following topics for more information:

- Rescan Rapid7 vulnerable items from the Vulnerability Response workspaces
- Rescan Qualys vulnerable items from the Vulnerability Response workspaces
- Rescan Tenable.io and Tenable.sc vulnerable items from the Vulnerability Response workspaces

To initiate rescans in the Vulnerability Manager workspace from vulnerable item and remediation task records, the records require a supported scanner as a source.

You might prefer to create a filtered list that displays records by their source. See Create a customized list of records for an example of how to create a list.

Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace

Evaluate the assignments, remediation target date, remediation tasks, exceptions, and risk score for a set of records (VITs, AVITs, CVITs or TRs) in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

Prior to version 23.0 of Vulnerability Response, it was necessary to apply the rules to all records to obtain the latest assignments, remediation target dates, risk scores, and remediation tasks, which was a time-consuming process. Starting with version 23.0, you can selectively evaluate and update these properties for specific records, thereby reducing processing time. Additionally, you can refine the remediation process based on these updated properties. Starting with v24.0.6 of Vulnerability Response, you can evaluate the exception rules for selected records in the Vulnerability Manager Workspace.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable Items
   - Application Vulnerable Items

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Container Vulnerable Items
- Configuration Test Results

3. **Optional:** Select the check box of the desired records to updated only the selected records by selecting the Selected items option in the modal.
4. Select the **Re-evaluate** button.
5. In the Re-evaluate and update remediation properties modal, select the properties that you want to update for the selected records.

Field	Description
Record selection	○ **Selected items**: Updates the selected records only. ○ **All items**: Updates all the records in the list.
Assignments	Updates the assignments in the **Assignment Group** field according to the latest Assign ment Rules.
Risk score	Updates the risk score in the **Risk score** field as per the latest Risk Score Rules.
Remediation tasks	Updates the remediation tasks according to the latest Remediation task rules.
Exceptions	Updates the deferral status of the records ac cording to the latest Exception rules. For more information on how the deferral sta tus of the records is updated, see Re-evaluat ing the exceptions for selected records in the Vulnerability Manager Workspace.
Remediation target date	Updates the Remediation target date accord ing to the latest Remediation Target Rules.

Note: When you select a property, its dependent properties are selected automatically.

6. Select **Apply**.

Result
The properties are updated for the selected records. You can check the **Work notes** of the records for the previous and latest values of the updated remediation properties.

Use the List view in the Vulnerability Manager Workspace

The List view in the Vulnerability Manager Workspace permits vulnerability and security managers and analysts to view remediation progress on records, drill down into Vulnerability Response records, and view the status of their approval requests and exceptions.

Before you begin
Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Manager Workspace**.
2. At the top left of the workspace with the Home page displayed, click the **List** icon.
3. **Optional:** Click **My Lists** to create a list.
   For more information on how to create a list, see Create a customized list of records.
4. Refer to the following table for the actions that you can perform on the List page.

UI action	Description
Open a remediation effort	
To the left of the Number column with a list displayed, roll over a row and click the small information icon **(i)** for a record.	Details about the records are displayed in the right side panel of the page. Details include: ○ Assignment group ○ Vulnerability ○ Assigned to ○ Short description ○ Description You can edit the fields. If the Active check box is displayed, you can activate or deactivate the record. Click the **Update** to save your changes.
Refresh the list	With the refresh icon on the top right of the page, reload the current page.
Reset widths	Click the gear icon to adjust column widths on your lists. A copy of the original list is saved under **Your Lists**.
Copy the URL for the displayed page	Copy the URL for use elsewhere.
Export the page	In the modal, enter the file and delivery types and click **Export**.
Refine filters for the data on the page.	Select a column and expand the three vertical dots menu to view options that further filter the data in the column. For example, you might prefer to filter the Assignment group column from the active remediation tasks list by a specific assignment group.
Filter out items or match items from a row in a column	Select a cell in a column and refine the data displayed by choosing one:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

UI action	Description
	○ Show Matching - display only items that match the selected cell in the column. ○ Filter Out - Filter out the items from the column that match the selected cell in the column.
Reopened Count on Vulnerable Items/ Remediation Task	A “Reopened Count” field is added on the vulnerable items to track the number of times a Vulnerable item’s state is changed from Closed to Open or Active. You can now identify and remove the Row count for all the list/related list views in Workspace experience by configuring a system property “glide.ui.list.siesmic.omit.count”. You can select the on-demand button from the list to view the row counts.

5. Create an application vulnerable item from the **Active** or **All** list under *Application Vulnerable items* by clicking the **New** button on the upper right.

Create a customized list of records

You can create a customized list in the vulnerability manager workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. Select the **List** icon and click **My Lists**.
3. Select **New list**.
4. In the New List modal, click **Start from existing** and search in the List choice list for an existing list to use as a template.
5. Edit the List Name.
6. Add filters.
   For example, you might want to create a list of active records for a particular scanner that you want to monitor for rescans. You might use the filters: `Active is true`, and `Source contains (name of your scanner)`.
7. Edit the columns that you want displayed on your list.
8. Click **Create**.
   Your new list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Alternatively, click **Create your own**, enter a name, followed by **Select Source**.
10. Start typing in the field and select from the sources that display for your new list.
11. Click **Create**.
    Your new list is displayed.

    Note: If you leave the list module, the list displayed when you exit is the list you see when you return.

12. To delete a list, with the list displayed, click the gear icon on the upper right of the page.

Create a remediation task manually from the Vulnerability Manager Workspace

Starting with v25.0.4 of Vulnerability Response, you can create remediation tasks manually from the host vulnerable items, application vulnerable items, container vulnerable items, and configuration test results lists on the List page of Vulnerability Manager Workspace. You can also create remediation tasks from the drill-down lists that appear when you click on the visualizations on the Home page.

Before you begin

Role required:

- sn_vul.write_all, sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_write_all, or sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.write_all, sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.write, or sn_vulc.admin for configuration test results (TRs)

About this task

Manual creation of Remediation Tasks (RTs) in Vulnerability Manager Workspace offers granular control over remediation task management by enabling you to group records (VITs, CVITs, AVITs, or TRs) into remediation tasks dynamically in real time.

You can create a remediation task manually, when you want to:

- group vulnerable items by something other than the Remediation Task Rules criteria. For example, you can create remediation tasks for a particular manager, or for active, new exploits, such as ransomware that includes different vulnerabilities.
- group ungrouped records.
- remediation task rules are inactive.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **List**.
2. On the List page, open the **Active** or **All** list in one of the following lists:
   - Host Vulnerable Items
   - Application Vulnerable Items
   - Container Vulnerable Items
   - Configuration Test Results
3. **Optional:** Select the check box of the records you want to update and then select the Selected items option in the Record selection field on the Create Remediation Task modal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **Create Remediation Task**.
5. On the Create remediation task modal, fill in the following details.

Create remediation task modal

Field	Description
Record selection	○ **Selected items**: Updates the selected records only. ○ **All items**: Updates all the records in the list.
Short description	Brief note about the remediation tasks.
Grouping criteria	Choices are: ○ **Assignment group**: Records with same assignment group are grouped into one remediation task. ○ **Assignment group and configuration item**: Records with same assignment group and configuration item are grouped into one remediation task. ○ **Assignment group and vulnerability**: Records with same assignment group and vulnerability are grouped into one remediation task. ○ **Assignment group and risk rating**: Records with same assignment group and risk rating are grouped into one remediation task.
Managing records in other remediation tasks	Choices are: ○ **Skip records for new remediation tasks**: No action is taken on the records that are part of other remediation tasks. ○ **Move to new remediation tasks**: Records that are part of other remediation tasks are transferred to new remediation tasks. ○ **Keep in both current and new remediation tasks**: Records that are part of other remediation tasks are kept in both old and new remediation tasks.

6. Select **Create remediation task**.

Result

Remediation tasks are created based on the grouping criteria. An email notification is sent to the remediation owners in the assignment group, informing them that a remediation task has been created and assigned to their group. For examples on how remediation tasks are created based on the grouping criteria, see Examples for remediation task creation in the Vulnerability Manager Workspace and IT Remediation Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enable or disable the import of test results for a Qualys test group

Starting with v23.0 of Vulnerability Response, control the import of the test results for the tests in a Qualys test group by using the **Enable/Disable import** button, which is available in the test group's record view.

Before you begin

Role required: sn_vulc.admin

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **Lists**.
2. In the Libraries, under the Test Groups list, open a Qualys test group in the record view.
3. Disable the import of the test results associated with a Qualys test group by selecting the **Disable import** button.
   From the upcoming data ingestion, the test results aren't imported for the Qualys test group. The value in the **Is Import disabled** field changes to *true*.
4. **Optional:** Enable the import of the test results by selecting the **Enable import** button.

Modify the severity for a CVE or TPE

As a vulnerability manager or analyst, you can modify the severity level of Common Vulnerability Entry (CVE) or Third-party Entry (TPE) in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager, sn_vul.app_developer for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **Lists** > **Libraries**.
2. Open the appropriate entry:
   - **CVEs (NVD)**: To modify the severity of a CVE.
   - **TPEs**: To modify the severity of a TPE.
3. Select **Modify severity** from the **More Actions** icon 
4. Select the new severity level from the drop-down.
5. Provide a justification for your update.
6. Select **Submit**.

Note:

- You can revert to the original source severity using the **Reset Severity** option from the **More Actions** menu. This option appears only after you modify the severity.
- The **Modified severity** field appears only when you change the source severity. If you reset it to the original value, the field is removed.
- The system will use the **Modified severity** for risk calculations starting from the next scheduled job onwards. If the severity is reset, the original source severity will be applied instead.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approve or reject requests in the Vulnerability Manager Workspace

Approve or reject requests that are submitted by remediation owners.

Before you begin

Roles required:

Approver roles required for various approval requests

Approval type	Approval levels required	Approver roles	Additional information
False positive approvals	One	• sn_vul.false_positive_approver granular role for vulnerable items (VITs). • sn_vul.app_false_positive_approver role for application vulnerable items (AVITs) • sn_vul_container.false_positive_approver role for container vulnerable items (CVITs) • sn_vulc.false_positive_approver for configuration test results Or Approvers are required to be in the False Positive Approver user group.	
Exception approvals (deferrals)	Two	• One approver is required in the Approver - Level 1 group • One approver is required in the Approver - Level 2 group	An exception request for a record or remediation task is approved by using a default, two-level approval workflow. The exception request requires two levels of approvers. After the request is approved by the level 1 approver, it's sent on to the second-level approver and is then visible in approver 2's queue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver roles required for various approval requests (continued)

Approval type	Approval levels required	Approver roles	Additional information
Unassign approvals	One approver is required in the Approver – Level 1 group	• sn_vul.unassign_appr for AVITs and VITs • sn_vul_container.unas for CVITs • sn_vulc.unassign_app for configuration issues (CIs)	**Note:** By default, an approval configuration is provided and an unassign approval group is created. Users (Unassign Approver - Level 1) of this group can approve the request. This group contains an unassign approver role, sn_vul.unassign_approver, by default. You can modify or create a new group and update the approval configuration. To configure approval rules, navigate to the respective Approval Rules module, select any of the following approval rules, and navigate to the approval configuration in the **Approval Configurations** tab: • *Vulnerable item field change request* for a vulnerable item. • *Vulnerability field change request* for a remediation task. • *Application vulnerability field*

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver roles required for various approval requests (continued)

Approval type	Approval levels required	Approver roles	Additional information
Risk change approvals	Two	• One approver is required in the Approver - Level 1 group • One approver is required in the Approver - Level 2 group	The approval flow for risk change is same as the exception approvals (deferrals).

See Vulnerability Response personas and granular roles and Assign the Vulnerability Response persona roles using Setup Assistant for more information about assigning persona roles to users and users to groups.

Note: Add users to the approval groups before you submit approval requests. If you create requests before you add users to the approval groups, the requests might not be visible to those users that have the approval permission.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
   If an approver doesn't have access to the workspace, approvals can be processed at **Vulnerability Response** > **My Approvals** in the classic environment.
2. Select the List view icon ( ).
   The List page is displayed.
3. In the Approvals filtered list, select **Assigned to me**.
4. Locate a request that you want to process and then select the link in the State column.
   The Vulnerability State Change Approval record (VCA#) is displayed.
5. Choose one of the following options to approve or reject the request.

Option	Description
Click the Details tab, enter text in the Comments field, and click Reject	○ A message is displayed indicating that there's a rejected approval for the Vulnerability State Change Approval record. ○ The state on the Vulnerability State Change Approval record transitions to Rejected. ○ The state on the remediation task or the record remains the same. ○ The Vulnerability State Change Approval record is no longer displayed on your Approvals list view in the workspace.
From either the Request or Details tabs, click Approve	○ A message displays indicating that the Vulnerability State Change Approval record is approved. ○ The state on the remediation task or the record transitions to Deferred.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ Active records on the remediation tasks transition to Deferred. ○ The Vulnerability State Change Approval record is no longer displayed on your Ap provals list view.

Set up email notifications in the Vulnerability Response Workspaces

Identify users for automatic email reminders sent to users in the Remediation Owner user group.

Before you begin

Role required: admin

This feature automatically generates an email digest for users in the Remediation Owner user group. Add any users that you want to receive email notifications as described in Use the email digest in the Vulnerability Response Workspaces.

Verify that users have an active email address entered on their user record and that you have added them to the Remediation Owner user group.

If you want to change the delivery frequency, day, or time of the emails, or deactivate the feature, follow these steps.

Procedure

1. Navigate to **All** > **Scheduled Jobs**.
2. Locate the **Generate remediation digest** and click it to open it the record.

   You might prefer to leave the fields in their default settings until you verify that notifications are being sent. By default, emails are sent weekly on Monday mornings at 9:00 AM in the time zone of the instance that is running the job.

3. Modify the fields in the form.
   For more information on the form fields, seeGenerate remediation digest form fields.
4. Click **Update**.

What to do next

In the event you have verified all the information listed previously is correct, and you have users in the Remediation Owner user group but the emails are not sent as expected, check that there are channels activated to receive email notifications. See Create notification channels.

Remediating vulnerable items and test results in the Vulnerability Manager Workspace

In the Vulnerability Manager Workspace, you can remediate vulnerable items and test results by into a watch topic by defining a condition and you can track their remediation progress by creating remediation efforts.

Using bulk edit in the Vulnerability Manager Workspace

In the Vulnerability Manager Workspace, you can update the state of the records, request exceptions and false positives, and assign records to an assignment group multiple vulnerable items (VITs, AVITs, or CVITs) simultaneously using the bulk edit feature.

The bulk edit feature is available for:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- host vulnerable items (VITs) starting from v21.0 of Vulnerability Response.
- application vulnerable items (AVITs) and container vulnerable items (CVITs) starting from v22.0 of Vulnerability Response.
- test results starting from v23.0 of Vulnerability Response.

Update the state of records in bulk in the Vulnerability Manager Workspace

Update the state of multiple records (VITs, AVITs or CVITs) concurrently according to their remediation progress using the bulk edit feature in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items
- sn_vul.app_sec_manager for application vulnerable items
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **List**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the **Record Selection** field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the **Record Selection** field.
4. Select the **Bulk Edit** button.
5. On the Bulk Edit modal, fill in the following fields to update the state of the records.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: Records with invalid CI or CI decommissioned aren't updated.
State	Change for the **State** in the record. Choices are: ○ Do Not Update ○ Open ○ Under Investigation ○ Awaiting Implementation ○ DeferredRequest bulk exception in the Vulnerability Manager Workspace ○ ClosedBulk edit for false positive in the Vulnerability Manager Workspace ○ Resolved **Note:** Only the records for which the state transition is valid are updated.
Work notes	Text that you enter to describe the changes.

6. Select#**Edit**.

   A bulk edit asynchronous job updates the selected records.

Bulk edit host vulnerable items with patches and solutions

Recommend a patch or solution for multiple host vulnerable items concurrently using the bulk edit feature in the Vulnerability Manager Workspace.

Before you begin

Role required: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, and any role with sn_vul.bulk_edit granular role.

About this task

In the Bulk edit modal, while adding a preferred solution and patch, you can also unassign or assign multiple host vulnerable items (VITs) to an assignment group simultaneously.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.

   Note: The selected records must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the List page, under Host Vulnerable items, open the Active or All list.
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the **Record Selection** field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the **Record Selection** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Select the check box next to each item if you want to use the **Only Selected Items** option in the Record Selection field of Bulk Edit modal.
- Apply filters if you want to use the **All Vulnerable Items that match filter** option in the Record Selection field of Bulk Edit modal.

4. Select the **Bulk Edit** button.
5. On the Bulk Edit modal, fill in the fields to recommend a patch or solution for multiple host vulnerable items.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records (VITs) in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Change for the **State** of the host vulnerable items. You can add preferred solution and patch only when you choose the following states. ○ Do Not Update ○ Open ○ Under Investigation ○ Awaiting Implementation
Preferred Solution	Solution that is targeted for remediating all the vulnerable items selected for bulk edit. Select the change for the **Preferred Solution** field in the vulnerable item. Choices are from a lookup list of available preferred solutions for the VITs selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: ○ The set of available preferred solutions is an intersection of all potential solutions of the vulnerabilities across all selected VITs. ○ When selecting **Record selection** > **Vulnerability Entry** for a bulk edit, all VITs for the vulnerability will be set to the selected preferred solution. **Note:** This operation doesn't set the **Preferred solution** at the vulnerability entry level. Setting the **Preferred solution** at the vulnerability entry level would set the **Preferred solution** for all new VITs going forward. The bulk edit only modifies the current set of VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message is displayed asking you to select VITs with different criteria for setting the **Preferred solution**. ○ The total number of solutions that can be shown in the lookup list is limited to 170. If there are more than 170 solutions, a warning message is displayed. The updated value is shown in the Vulnerable item list view.
Preferred patch	Patch that is targeted for remediating all the vulnerability items selected for bulk edit. **Note:** ○ You must install Patch Orchestration to view the list preferred patches. ○ The set of available preferred patches is an intersection of all potential patches across all selected VITs. ○ Distinct vulnerabilities across the selection criteria are limited to 500. If there are more than 500 distinct vulnerabilities, a warning message displays asking you to select VITs with different criteria for setting the **Preferred patch**. ○ The total number of patches that can be shown in the lookup list is limited to 170. If there are more than 170 patches, a warning message is displayed.
Unassign	All the selected items are unassigned for assignment group and remediation owner. **Note:** ○ This field appears when you select the State as Do Not Update. ○ When you unassign records, a remediation task is created which is sent for approval. For more information, see Remove assignments for host vulnerable items in bulk

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Assignment group	Assignment group for the records. All the active assignment groups appear in this field. **Note:** This field is deactivated when you select the Unassign check box.
Work notes	Text that you enter to describe the changes.

6. Select **Edit**.

Result

A bulk edit asynchronous job updates the selected host vulnerable items (VITs). The preferred solution and patch are added to the relevant host vulnerable items (VITs). Open a host vulnerable item, and view the preferred solution and patch in the Remediation section of the Details tab.

Assign records to an assignment group in bulk

Assign multiple records (VITs, AVITs, CVITs, or TRs) concurrently to an assignment group using the bulk edit feature in the Vulnerability Manager Workspace.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the Record selection field.
   - Apply filters if you want to use the **All records that match filter** option in the Record selection field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to assign the records to an assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ *Only Selected Items*: Select this option if you want to update the records you selected using the check box. ○ *All records that match filter*: Select this option if you want to update the filtered records. ○ *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items. ○ *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, Awaiting Implementation or Deferred state are updated.
Assignment group	Assignment group for the records. All the active assignment groups appear in this field. **Note:** This field is deactivated when you select the Unassign check box for VITs.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.

Result

Open a record for which you updated the assignment group and navigate to the Overview tab, the user group to which the record is assigned appears in the **Assignment group** field.

Remove assignments for host vulnerable items in bulk

Remove yourself or your groups from the#**Assigned to** and#**Assignment group** fields on host vulnerable items (VITs) or remediation tasks (VUL) if you determine that the records aren't within your scope for remediation, or if you think that records have been incorrectly assigned to you or to your groups.

Before you begin

Role required: sn_vul.vulnerability_analyst, and sn_vul.vulnerability_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The #Unassign#feature is applicable for records in any state other than Closed or Resolved. When you remove assignments for host vulnerable items using the bulk edit feature, only relevant records are updated.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page, under Host Vulnerable items, open the Active or All list.
3. Perform one of the following:
   - Select the check box next to each item if you want to use the **Only Selected Items** option in the #unique_228_Connect_42_record-slection-field-unassign field.
   - Apply filters if you want to use the **All Vulnerable Items that match filter** option in the #unique_228_Connect_42_record-slection-field-unassign field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to remove assignments in bulk.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, Awaiting Implementation, or Deferred state are updated.
State	Select the state as Do Not Update.
Unassign	All the selected vulnerable items are unassigned from assignment group and remediation owner. **Note:** ○ This field appears when you select the State as Do Not Update. ○ When you unassign records, a remediation task is created which is sent for approval.
Work notes	Text that you enter to describe the changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click#**Edit**.
   A remediation task is created with the selected host vulnerable items (VITs).

   Your request is submitted for approval and the approver receives an email notification about your request.

   The state of the host vulnerable items (VITs) and remediation task (VUL) transitions to In Review. If a remediation task is updated with this feature, the **Assigned to** and **Assignment group** fields on all of its associated VITs are also cleared upon approval of your request.

Result

In the Vulnerability Manager Workspace, on the List page, navigate to **Exception Requests** > **All** and open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The **Assigned to** and#**Assignment group** fields of all the host vulnerable items are cleared.
Rejected	The **Assigned to** and#**Assignment group** fields of all the host vulnerable items are not updated.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Request bulk exception in the Vulnerability Manager Workspace

Request an exception for multiple records (VITs, AVITs, CVITs or TRs) concurrently using the bulk edit feature instead of manually selecting each record.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

When you request an exception for one or more records from the Bulk edit modal, a remediation task is created with the selected records.

Note: The Application Vulnerable Items (AVITs) from the scanners with the **Manage exceptions in ServiceNow** parameter set to false are not updated.

- If you select AVITs from various scanners, some with the **Manage exceptions in ServiceNow** parameter set to true and other set to false, the AVITs linked to the scanners with he **Manage exceptions in ServiceNow** parameter set to false are not updated.
- If you select AVITs from only the scanners with the **Manage exceptions in ServiceNow** parameter set to false, the *Defer* option does not appear in the **State** field in the Bulk Edit modal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:
   - Select the check box next to each item if you want to use the *Only Selected Items* option in the Record selection field.
   - Apply filters if you want to use the *All records that match filter* option in the Record selection field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the following fields to request an exception for multiple records (VITs, AVITs, CVITs, or TRs) simultaneously.

Bulk Edit modal fields

Field	Description
Record selection	Records to update. Choices are: ○ *Only Selected Items*: Select this option if you want to update the records you selected using the check box. ○ *All records that match filter*: Select this option if you want to update the filtered records. ○ *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items. ○ *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
State	Select the *Deferred* state to request an exception for the selected records. **Note:** ○ When you select this option, the Reason, Short description, Until, and Additional information fields appear. ○ When you defer records, a remediation task is created and this task is sent for approval.
Reason	Reason for deferring records: ○ Awaiting Maintenance Window ○ Fix Unavailable ○ Risk Accepted ○ Mitigating Control in Place ○ Other **Note:** The **Reason** field appears when you select the State as Deferred or Closed.
Short description	Brief note describing the reasons for deferral request. This information reflects in the **Description** field of the remediation task that is created for a deferral request. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Until	Date till which the record remains deferred. **Note:** This field appears when you select the State as Deferred.
Additional information	Any other necessary information. This information reflects in the Additional Information field in the Overview tab of the remediation task that is created for deferral and closed-false positive requests. If your deferral request is approved, this additional information appears as deferral notes for both VIT and remediation task. **Note:** This field appears when you select the State as Deferred and Closed-False positive.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.
7. On the Take Questionnaire modal, answer the questions and click#**Submit**.

   A remediation task is created containing the records that you selected. Your request is submitted for approval and the State of the records changes to#n Review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Take Questionnaire** modal appears only when the questionnaire is enabled for exception requests in the Exception Management form. For more information on configuring a questionnaire for exception requests, see Configure Exception Management for Vulnerability Response, Configure Exception Management for Application Vulnerability Response, and Configure Exception Management for Container Vulnerability Response.

The approver receives an email notification about your request.

Result

In the Vulnerability Manager Workspace, on the List page, navigate to **Exceptions** > **All**, open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The state of the Remediation task transitions to Deferred with the given Reason as sub-state. The state and reason are rolled down to the records.
Rejected	The state of the Remediation Task and its records doesn't change.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Bulk edit for false positive in the Vulnerability Manager Workspace

Mark one or more records (VITs, AVITs, CVITs, or TRs) as false positive concurrently using the bulk edit feature from the Vulnerability Manager Workspace instead of manually selecting each item.

Before you begin

Role required:

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items (VITs)
- sn_vul.app_sec_manager for application vulnerable items (AVITs)
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items (CVITs)
- sn_vulc.admin for configuration test results (TRs)

About this task

When you raise a false positive request for one or more records from the Bulk edit modal, a remediation task is created with the selected records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When you raise a false positive request for the Application Vulnerable Items (AVITs) using the bulk edit feature, the AVITs from the scanners with the **Manage False positive with Servicenow** parameter set to false are not updated.

- If you select AVITs from various scanners, some with the **Manage False positive with Servicenow** parameter set to true and other set to false, the AVITs linked to the scanners with the **Manage False positive with Servicenow** parameter set to false are not updated.
- If you select AVITs from only the scanners with the **Manage False positive with Servicenow** parameter set to false, the *False positive* option does not appear in the **Reason** field in the Bulk Edit modal.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace** > **List**.

   Note: The selected records must be in the Open, Under Investigation, or Awaiting Implementation state.

2. On the List page, open Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
   - Configuration Test Results
3. Perform one of the following:
   - Select the check box next to each item if you want to use the *Only Selected Items* option in the **Record selection** field.
   - Apply filters if you want to use the *All records that match filter* option in the **Record selection** field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to request false positive for multiple records.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ *Only Selected Items*: Select this option if you want to update the records you selected using the check box. ○ *All records that match filter*: Select this option if you want to update the filtered records. ○ *Remediation Task*: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ *Vulnerability Entry*: Select this option if you want to update the records specific to a vulnerability and then select a CVE or TPE in the **Vulnerability Entry** field. **Note:** This field appears for host vulnerable items, application vulnerable items, and container vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ *Configuration test*: Select this option if you want to update the test results specific to a test and then select a test in the **Configuration test** field. **Note:** This option appears for Configuration test results only. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Select the **Closed** state.
Reason	Select the Reason as False positive. **Note:** ○ When you select this option, the Short description, and Additional information fields appear. ○ A remediation task is created when you mark the records as False-positive and this task is sent for approval. **Note:** The **Reason** field appears when you select the State as Deferred or Closed.
Short description	Brief note describing the reasons for Closed-False positive request. This information reflects in the **Description** field of the remediation task that is created for a Closed-False positive request. **Note:** This field appears when you select the State as Deferred or Closed-False positive.
Additional information	Any other necessary information. This information reflects in the Additional Information field in the Overview tab of the remediation task that is created for Closed-False positive request. If your false positive request is approved, this additional information appears as notes for both VIT and remediation task. **Note:** This field appears when you select the State as Deferred or Closed-False positive.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.
7. On the Take Questionnaire modal, answer the questions and select **Submit**.
   A remediation task is created with the selected records. Your request is submitted for approval and the State of the remediation task changes to#n Review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The **Take Questionnaire** modal appears only when the questionnaire is enabled for false positive requests in the Exception Management form. For more information on configuring a questionnaire for false positive requests, see Configure Exception Management for Vulnerability Response, Configure Exception Management for Application Vulnerability Response, and Configure Exception Management for Container Vulnerability Response.

The approver receives an email notification about your request.

Result

In the Vulnerability Manager Workspace, on the List page, navigate to **Exceptions** > **All**, open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The state of the Remediation Task transitions to Closed with the Reason as False positive. The state and reason are rolled down to the records.
Rejected	The state of the Remediation Task and its records doesn't change.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of your request.

Close records in bulk in the Vulnerability Manager Workspace

Close multiple records (VITs, AVITs, or CVITs) concurrently using the bulk edit feature in the Vulnerability Manager Workspace.

Before you begin

Role required: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, or sn_vul_container.vulnerability_admin

Procedure

1. Navigate to **Workspaces** > **Vulnerability Manager Workspace**.
2. On the List page, open Active or All list in one of the following lists:
   - Host Vulnerable items
   - Container Vulnerable items
   - Application Vulnerable items
3. Perform one of the following:
   - Select the check box next to each item if you want to use the Only Selected Items option in the **Record Selection** field.
   - Apply filters if you want to use the All Vulnerable Items that match filter option in the **Record Selection** field.
4. Select the **Bulk Edit** button.
5. On the form, fill in the fields to close the selected records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Bulk Edit modal fields

Field	Description
Record Selection	Records to update. Choices are: ○ Only Selected Items: Select this option if you want to update the records you selected using the check box. ○ All Vulnerable Items that match filter: Select this option if you want to update the filtered records. ○ Remediation Task: Select this option if you want to update the records in a remediation task and then select the desired remediation task in the **Remediation task** field. ○ Vulnerability Entry: Select this option if you want to update the records specific to a common vulnerable entry (CVE) and then select the CVE in the **Vulnerability Entry** field. **Note:** ○ Records with invalid CI or CI decommissioned aren't updated. ○ Only the records in the Open, Under Investigation, or Awaiting Implementation state are updated.
State	Select the state as Closed.
Reason	Reason for closing records: ○ False Positive **Note:** When you select this option to mark the records as false- positive, the Reason, Short description, and Additional information fields appear. For more information on bulk edit for false positive, see Bulk edit for false positive in the Vulnerability Manager Workspace. ○ Cancelled ○ Fixed **Note:** The reasons, Cancelled and Fixed are not applicable to CVITs.
Work notes	Text that you enter to describe the changes.

6. Click#**Edit**.

A bulk edit asynchronous job updates the relevant records.

Request exceptions for remediation tasks and records from the Vulnerability Manager Workspace

From the Vulnerability Manager Workspace, vulnerability managers and analysts can request exceptions and false positives for a remediation task (VUL, AVUL, CVUL or CRG) and record (VIT, CVIT, AVIT or TR). You can also split a remediation task and create change requests.

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.vulnerability_analyst, or sn_vul.vulnerability_admin for host vulnerable items
- sn_vul.app_sec_manager for application vulnerable items
- sn_vul_container.vulnerability_analyst or sn_vul_container.vulnerability_admin for container vulnerable items
- sn_vulc.admin for configuration test results

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

In the Vulnerability Manager Workspace, you can perform the following on the records and remediation tasks:

- Split a remediation task (VUL, AVUL, CVUL, and CRG).
- Request an exception for a record (VIT, AVIT, CVIT, or CTR) or remediation task (VUL, AVUL, CVUL, or CRG).
- Request a policy exception for records (VIT, AVIT, or CVIT) or remediation task (VUL, AVUL, CVUL, or CRG).
- Create a change request for remediation task (VUL, CVUL, or CRG).
- Request a false positive for record (VIT, AVIT, or CVIT) or remediation task (VUL, AVUL, CVUL or CRG).

Note: You can raise false positive requests for a set of test results and remediation task (CRG) starting from v22.0 of Vulnerability Response.

You initiate these UI actions from records in the Vulnerability Manager Workspace, the same way remediation owners perform these tasks in the IT Remediation Workspace.

See the following topics for more information:

- Request a false positive in the IT Remediation Workspace
- Request an exception in the IT Remediation Workspace
- Request risk change in the IT Remediation Workspace
- Split a remediation task in the IT Remediation Workspace
- Create a change request in the IT Remediation Workspace
- Request an exception using GRC: Policy and Compliance Management in the IT Remediation Workspace
- Request false positive for a set of test results

Related topics

Exception Management overview

Configuration Compliance Exception Management overview

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request bulk exception in the Vulnerability Manager Workspace

Bulk edit for false positive in the Vulnerability Manager Workspace

Request an extension for a deferred vulnerable item in the Vulnerability Manager workspace

Request an extension for a deferred vulnerable item before it reaches its deferred until due date. As a remediation owner, you're no longer required to wait until the deferred due date to make this request.

Before you begin
Role required: sn_vul.vulnerability_admin or sn_vul.admin (deprecated)

About this task
You can also request an extension from the classic environment.

Use the same procedure to request an extension for an application vulnerable item, container vulnerable item, test result group, and a remediation task.

Procedure
1. Navigate to **Workspaces** > **Vulnerability Manager Workspaces**.
2. Select Lists.
3. Under Host Vulnerable Items, select **All**.
4. Filter the list by selecting deferred in the State column.
5. Select a deferred vulnerable item.

   Note: The Request Extension button is visible only when the state of the vulnerable item is Deferred.

6. Select the **Request Extension** button.
7. Fill in the fields on the form, as appropriate.

Field	Description
Extend Until	Select the date until when the deferred vulnerable item must be extended for remediation.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

8. Select **Request Extension**.
   An email is triggered on submission of the request and subsequent action by the approver.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The request goes through two levels of approval.
- If a deferred vulnerable item is extended again, the extend deferral count increases in the backend.

9. After the request is approved, the Until, Reason, and Deferral notes are updated.

Vulnerability Manager Workspace reference information

The following topics provide you with links, reference information, in addition to field data on the forms and records found in Vulnerability Manager Workspace.

- Create Watch Topic form fields
- GRC request exception form fields
- Generate remediation digest form fields
- Impact of the compensating controls on risk score and expiration date
- Examples for remediation task creation in the Vulnerability Manager Workspace and IT Remediation Workspace
- Re-evaluating the exceptions for selected records in the Vulnerability Manager Workspace

Create Watch Topic form fields

The following table describes the fields in the Create Watch Topic form in Vulnerability Manager Workspace.

Field	Description
Name	Name for your watch topic, for example, `Critical VIs`.
Owned by	The name of the user who owns the watch topic.
Display order	Enter a value between 100-1000. 100 is the default value. Lower values starting with 100 are displayed in ascending order on lists.
Owning group	The name of the group who owns the watch topic.
Active	Activate or deactivate the watch topic. Default is selected (Active).
Watch list	Add names of users who receive notifications and can view the watch topic.
Description	Text that describes your watch topic. This text is displayed in the Description field when you create a remediation effort from this watch topic.
Category	Type of record for which the watch topic is being created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The **Category** field appears starting from version 18.0.
Preview	Click **Preview** to see a list of how many records your filter conditions return. **Note:** Starting with version 18.0, the **Preview** button is not available.

Related topics

Create a watch topic in the Vulnerability Manager Workspace

GRC request exception form fields

The following table shows the field descriptions for the GRC request exception form.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you're requesting an exception for.
Control objective	Control objectives that are associated with the policy that you selected. If a policy isn't selected, all the control objectives are listed.
Valid from	Date when the exception starts. The default value is the current date. This date can't be in the past.
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid can't exceed the **Maximum exception duration (days)** that you set for the policy in Policy and Compliance. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details that are related to the reason why this request is being made. This field must be filled in by the remediation owner.

Generate remediation digest form fields

The following table shows the fields on the Generate remediation digest form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Generate remediation digest fields

Field	Description
Active check box	This check box is activated by default. If you don't want to send email notifications, deactivate this field.
Run	Weekly is the default. Choose an option from the list.
Day	Monday is the default. Choose an option from the list.
Time	Set a time to deliver the emails. Select a time zone if you want a time zone other than the one used by the instance running the job.

Impact of the compensating controls on risk score and expiration date

Starting from v20.0 of Vulnerability Response, as a Remediation Owner, you can request risk reduction for a host vulnerable item or remediation task. And the Vulnerability Manager or Analyst can approve these risk reduction requests.

For more information on how to request risk reduction and approve risk reduction approval, see Request risk change in the IT Remediation Workspace and Approve or reject requests in the Vulnerability Manager Workspace respectively.

When a risk reduction request is approved, the risk score is reduced according to the **Desired value** (risk rating) in the state change approval (VCA#) record. The highest risk score of the desired risk rating is assigned to the record when your risk reduction request is approved. The following example shows how the Risk score and Original risk score are updated when compensating controls are applied. The default highest risk scores of the risk ratings are used in the following example.

Impact of compensating controls on risk score and original risk score

Scenario	Risk rating	Risk score	Original risk score (Calculated risk score)
Data prior to v20.0	2 - High	80	The field is not available prior to v20.0.
After upgrading to v20.0	2 - High	80	Null
Calculated risk score changes to 90 during ingestion	1 - Critical	90	Null
When you apply compensating controls	3 - Medium	69	90
Calculated risk score changes to 70 during ingestion	3 - Medium	69	70

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Impact of compensating controls on risk score and original risk score (continued)

Scenario	Risk rating	Risk score	Original risk score (Calculated risk score)
Calculated risk score changes to 50 during ingestion	3 - Medium	50	50
Calculated risk score changes to 80 during ingestion	3 - Medium	50	80
When compensating controls expire on **Until date for risk reduction**	2 - High	80	Null

Impact of compensating controls on a remediation task

When your request for risk reduction is approved for a remediation task, the impact of compensating controls on its vulnerable items is as follows:

- The compensating controls applied on the remediation task are applied on its vulnerable items (other than those in Closed state) that have risk score greater than the risk score corresponding to the **Desired value** in the state change approval of a remediation task. And the risk score of these vulnerable items is reduced according to the **Desired value**.
- The **Until date for risk reduction** remains unchanged for the vulnerable items on which a compensating control is already applied. It is not updated with the **Until date for risk reduction** of the Remediation Task.
- The **Until date for risk reduction** is rolled down to the vulnerable items only when a compensatory control is not applied on any vulnerable item previously. If you apply the compensatory controls on the remediation task again, the **Until date for risk reduction** is not rolled down to the vulnerable items as the existing **Until date for risk reduction** of the vulnerable items is given priority.
- When a new vulnerable item is added to a remediation task on which compensatory controls are already applied, the risk is not rolled down to the vulnerable item.

Impact of a compensating control on a vulnerable item

When your request for risk reduction is approved for a vulnerable item:

- Its new risk score displays in the **Risk score** field and the old risk score (calculated risk score) moves to the **Original risk score** field. This change holds till the date specified in the **Until date for risk reduction** field.
- When a vulnerable item has compensating controls already applied, during ingestion:
  - If the calculated risk score is greater than the risk score then risk score remains same and original risk score is updated with the calculated risk score.
  - If the calculated risk score is less than the risk score then both risk score and original risk score are updated with the calculated risk score.
- If a Configuration Item (CI) is changed for a vulnerable item for which a compensating control is already applied:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The CI is updated for a vulnerable item by default as the *sn_sec_cmn.update_on_ci_change* system property is set to true.

  The compensating control is still applicable for the vulnerable item.

- The vulnerable item is closed and a new vulnerable item is created if the *sn_sec_cmn.update_on_ci_change* system property is set to false.

  The compensating control applied to the old vulnerable item is applied to the new vulnerable item and the **Until date for risk reduction**, **Original risk score** and **Risk score** remain the same.

- When a vulnerable item is reopened by the scanner and compensating control is already applied on it, the same compensating control is applied after it is reopened.

Related topics

Understanding compensating controls for risk change

Add a compensating control to the library

Associate compensating controls with CVEs or TPEs for risk change requests

Disable or enable risk change for a CVE or TPE

#unique_367_Connect_42_li-risk-reduction-vmws

Examples for remediation task creation in the Vulnerability Manager Workspace and IT Remediation Workspace

When you create remediation tasks manually in the Vulnerability Manager Workspace and IT Remediation Workspace, records are grouped into a remediation task based on the grouping criteria you select.

Consider the following example where 10 records are selected for remediation task creation. After providing the record selection details and a brief description, select the **Grouping criteria** according to your requirement and then select how you want to manage the records that are already part of existing remediation tasks.

Example: Remediation task creation based on the grouping criteria

Vulnerable items selected for remediation task creation

Vulnerable item id	Existing remediation tasks	Assignment group	Configuration item	Vulnerability	Risk rating
VIT10001	VUL10021, VUL10022	Remediation Manager	APSVR-NY-1672	CVE-2018-9020	4
VIT10002		Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	LDAP Admins	DEV-IBM-NY-682	CVE-2012-5357	1
VIT10004		Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable items selected for remediation task creation (continued)

Vulnerable item id	Existing remediation tasks	Assignment group	Configuration item	Vulnerability	Risk rating
VIT10006		Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10007		LDAP Admins	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008		LDAP Admins	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009		Remediation Manager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10010		LDAP Admins	DEV-SAP-SD-9388	CVE-2013-3906	4

The following list shows how the records are grouped into remediation tasks based on the grouping criteria selected when creating the remediation task.

Scenario1: Grouping criteria is selected as "Assignment group" and Managing records in other remediation tasks is selected as "Skip records for the new remediation tasks"

The records with the same assignment group are grouped into one remediation task. The records that are already part of existing remediation tasks are not added to the new remediation tasks. Here, three remediation tasks are created, each containing the records that are assigned to the **Remediation Manager**, **LDAP Admins**, and **Vulnerability Response** assignment groups.

Remediation task created in scenario 1

Remediation tasks created	Records in the remediation task
Remediation task 1 - VUL10001	This remediation task contains the records that are assigned to the **Remediation Manager** assignment group: • VIT10004 • VIT10006 • VIT10009 The VIT10001 record will not be moved to the VUL10001 remediation task.
Remediation task 2 - VUL10002	This remediation task contains the VIT10002 record that is assigned to the **Vulnerability Response** assignment group. The VIT10005 record will not be moved to the VUL10002 task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task created in scenario 1 (continued)

Remediation tasks created	Records in the remediation task
Remediation task 3 - VUL10003	This remediation task contains the records that are assigned to the **LDAP Admins** assignment group: • VIT10007 • VIT10008 • VIT10010 The VIT10003 record will not be moved to the VUL10003 remediation task.

Scenario 2: Grouping criteria is selected as "Assignment group and configuration item" and Managing records in other remediation tasks is selected as "Transfer records to the new remediation tasks"

The records with the same configuration item that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records are removed from their old remediation tasks and moved to the new remediation tasks. Here, five remediation tasks are created.

Remediation tasks created in scenario 2

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10004	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **APSVR-NY-1672** configuration item. • VIT10001 The VIT10001 record will be removed from the VUL10021, and VUL10022 remediation tasks.
Remediation task 2 - VUL10005	This remediation task contains the records that are assigned to **Vulnerability Response** assignment group and with **DEV-IBM-NY-682** configuration item. • VIT10002 • VIT10005 The VIT10005 record will be removed from the VUL10022 remediation task.
Remediation task 3 - VUL10006	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **DEV-IBM-NY-682** configuration item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tasks created in scenario 2 (continued)

Remediation tasks created	Records part of remediation task
	• VIT10003 • VIT10008 The VIT10003 record will be removed from the VUL10021 remediation task.
Remediation task 4 - VUL10007	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **CRMBK-SD-4210** configuration item. • VIT10004 • VIT10006 • VIT10009
Remediation task 5 - VUL10008	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **DEV-SAP-SD-9388** configuration item. • VIT10007 • VIT10010

Scenario 3: Grouping criteria is selected as "Assignment group and vulnerability" and Managing records in other remediation tasks is selected as "Keep records in both the current and new remediation tasks"

The records with the same vulnerability that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records will be added to their respective new remediation tasks without being removed from their old remediation tasks.Here, five remediation tasks are created.

Remediation tasks created in scenario 3

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10009	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **CVE-2018-9020** vulnerability. • VIT10001 The VIT10001 record will remain part of VUL10021, and VUL10022 remediation tasks as well.
Remediation task 2 - VUL10010	This remediation task contains the records that are assigned to **Vulnerability Response** assignment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tasks created in scenario 3 (continued)

Remediation tasks created	Records part of remediation task
	group and with **CVE-2018-9020** vulnerability. • VIT10002 • VIT10005 The VIT10005 record will remain part of VUL10022 remediation task as well.
Remediation task 3 - VUL10011	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **CVE-2012-5357** vulnerability. • VIT10003 The VIT10003 record will continue to be part of the VUL10021 remediation task also.
Remediation task 4 - VUL10012	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **CVE-2013-1710** vulnerability. • VIT10004 • VIT10006 • VIT10009
Remediation task 5 - VUL10013	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **CVE-2013-3906** vulnerability. • VIT10007 • VIT10008 • VIT10010

Scenario 4: Grouping criteria as "Assignment group and risk rating" and Managing records in other remediation tasks is selected as "Keep records in both the current and new remediation tasks"

The records with the same risk rating that are assigned to the same assignment group are grouped into a remediation task. The VIT10001, VIT10003, and VIT10005 records will be added to their respective new remediation tasks without being removed from their old remediation tasks. Here, five remediation tasks are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation task created in scenario 4

Remediation tasks created	Records part of remediation task
Remediation task 1 - VUL10014	This remediation task contains the records that are assigned to **Remediation owner** assignment group and with **4** risk rating. • VIT10001 • VIT10004 The VIT10001 record will continue to be part of VUL10021and VUL10022 remediation tasks.
Remediation task 2 - VUL10015	This remediation task contains the records that are assigned to **Vulnerability Response** assignment group and with **2** risk rating. • VIT10002 • VIT10005 The VIT10005 record will continue to be part of VUL10022 remediation task.
Remediation task 3 - VUL10016	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **1** risk rating. • VIT10003 • VIT10007 • VIT10008 The VIT10003 record will continue to be part of VUL10021 remediation task.
Remediation task 4 - VUL10017	This remediation task contains the records that are assigned to **Remediation Manager** assignment group and with **2** risk rating. • VIT10006 • VIT10009
Remediation task 5 - VUL10018	This remediation task contains the records that are assigned to **LDAP Admins** assignment group and with **4** risk rating. • VIT10010

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

- Create a remediation task manually from the Vulnerability Manager Workspace
- Create a remediation task manually in the IT Remediation Workspace

Re-evaluating the exceptions for selected records in the Vulnerability Manager Workspace

In the Vulnerability Manager Workspace, when you evaluate the exception rules for a set of records in the Re-evaluate and update the remediation properties modal, their deferral status and until date of deferral are updated as per the latest exception rules.

Scenarios

You may come across the following scenarios, when you evaluate the exceptions for a selected set of records in the Re-evaluate and update the remediation properties modal in the Vulnerability Manager Workspace:

Scenario 1: When the selected records are already deferred manually and they match the condition of an exception rule, these records remain in the Deferred state without any changes.

Scenario 2: When the selected records match the condition in the exception rules and these records are in a non-deferral state (such as open, In Review, Under Investigation), then these records are deferred until the date defined in the exception rule.

Scenario 3: When the selected records are already in the Deferred state (that are deferred using the exception rule A), they remain in the Deferred state in the following scenarios:

- the exception rule expires and the records do not match the condition
- the exception rule expires and the records match the condition
- the exception rule A expires and records match the condition of another exception rule B.

Scenario 4: Consider that the records are deferred using an exception rule. When you change the exception rule condition such that the Deferred state of the records is no longer valid and then reevaluate the exception rules for these records:

- the records move to the Open state
- the Until date, Deferral date, Deferral count and other fields are updated.

Example: Consider that you are evaluating the exceptions for following host vulnerable items (VITs)

Consider the exception rule with the following details:

Exception rule details

Field	Description	Value
Name	Name of the exception rule.	Deferring critical VITs
Valid from	Date from which this rule is active to defer the VIs.	20-08-2024
Valid to	Date from which the remediation task stops accepting new VIs.	30-11-2024
Reason	Reason to create this exception rule.	Risk Accepted

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception rule details (continued)

Field	Description	Value
Assignment group	Group that the remediation task that was created for tracking the deferred VIs is assigned to.	Remediation Group 1
Additional information	Additional information that the requester wants to provide to the approver. This information is populated in the description field of the remediation task.	This rule has been created to defer the critical VITs automatically.
Condition	Filter condition for the VIs that can be defined while processing the VIs.	Risk rating = 5 - Critical
Execute on existing data	Option that enables you to run this rule on existing data the first time that this rule is run.	Yes
State	State of the exception rule.	Approved
Execution order	Unique order for each exception rule.	100
Deferred until	Date until when the VULs and VIs are deferred. On this date, the created VUL is closed, all the VIs move out of the group, and group rules are reapplied.	2024-12-23 16:10:29

The following table shows how the state changes when the exception rules are reevaluated for multiple VITs simultaneously:

Records for which exceptions are reevaluated

VIT Number	State	Risk Rating	Updated state after reevaluating the exceptions -1	Until date - 1
VIT120067	Open	2 - Low	Open	-
VIT120068	In Review	3 - Medium	In Review	-
VIT120069	Under Investigation	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120070	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120071	Deferred	2 - Low	Deferred	2024-10-02 16:10:29 (Deferred manually)
VIT120072	Closed	5 - Critical	Closed	-

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the condition in the preceding exception rule is modified to `Risk rating = 2 - Low` and **Deferred until** is modified to `2024-12-31 14:10:23` the records are updated as follows:

Records for which exceptions are reevaluated

VIT Number	Updated state after reevaluating the exceptions -1	Risk-rating	Updated state after reevaluating the exceptions - 2	until date - 2
VIT120067	Open	2 - Low	Deferred	2024-12-31 14:10:23
VIT120068	In Review	3 - Medium	In Review	-
VIT120069	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120070	Deferred	5 - Critical	Deferred	2024-12-23 16:10:29
VIT120071	Deferred	2 - Low	Deferred (No change in the state)	2024-10-02 16:10:29 (No change in the until date)
VIT120072	Closed	5 - Critical	Closed	-

Related topics

- Re-evaluate the remediation properties of the records in the Vulnerability Manager Workspace
- Exception rules overview
- Configuration Compliance Exception Management overview

IT Remediation Workspace

IT teams view IT-centric tasks and information such as solutions and affected configuration items. IT teams can save time resolving vulnerabilities by easily creating change requests, rescanning vulnerable items, and submitting exception requests from the IT Remediation workspace.

Overview

Get started

Explore	Remediate	Reference
Learn about the IT Remediation Workspace	Learn how to remediate vulnerabilities and misconfigurations from the IT Remediation Workspace	Learn more about additional information required to use IT Remediation Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Troubleshoot and get help

- Security Operations on ServiceNow Community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring the IT Remediation Workspace

The IT Remediation Workspace is intended for IT remediation owners and IT groups. It is composed of home and list views as well as data visualizations that you can click that let you see the remediation tasks you've been assigned and how many records assigned to you have solutions.

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

The IT Remediation Workspace consists of the following pages, lists, and forms:

Landing (Home) page

The Home page consists of the Assigned remediation tasks card, Preferred solutions on VIs card, Impacted CIs card, Preferred patches on VIs card, and Remediation tasks list. For more information on the Home page, see Home page in the IT Remediation Workspace.

Dashboards page

The dashboards page consists of the Vulnerability Remediation dashboard. For more information on the Dashboards page, see Dashboards in the IT Remediation Workspace.

List page

This view consists of default and customized lists of Remediation Tasks, Host Vulnerable Items, Application Vulnerable items, Container Vulnerable items, Configuration Test Results assigned to you and Solutions, Exceptions Requests, etc. For more information on the List page, see List page in the IT Remediation Workspace. For more information about what you can do from this page, see Create a list in the IT Remediation Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View a workflow example in the IT Remediation Workspace

View an example of an end-to-end workflow in the IT Remediation Workspace. See how IT specialists might use the workspace to monitor critical vulnerable items and remediate the vulnerabilities assigned to them.

Before you begin

Role required: sn_vul.remediation_owner, sn_vul.app_security_champion, sn_vul_container.remediation_owner, or sn_vulc.remediation_owner

Procedure

Click the following image to view the steps of the workflow.

The image includes the following tasks:

- From the Home page (IT Remediation Owner landing page), view the remediation tasks that are assigned to you. Toggle between work that is assigned to you and your group. See the remediation tasks that have solutions.
- Click the **List** view to see the lists of your assigned work.
- From the List view with the **Assigned to my group** list selected, identify and assign work to yourself.
- On an open remediation task record:
  - Click the **Overview** tab to see the vulnerable items (VIs) and affected configuration items (CIs) that are associated with the record.
  - Click the **Solutions** tab to see preferred and potential solutions.
  - Click the **Details** tab to modify editable fields.
  - Click the UI actions: **Mark as False Positive**, **Create Change**, **Split Task**, **Request Exception**. Follow the prompts in the dialogs to help you with your remediation.

Home page in the IT Remediation Workspace

The Home page in the IT Remediation Workspace provides a consolidated list of host, application, container and test result remediation tasks that are assigned to you and your assignment groups.

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

The Home page consists of the following cards and list of remediation tasks assigned to you and your assignment groups, records assigned to you have solutions.

Assigned remediation tasks card

Number of active remediation tasks assigned to you. Select the tile to view the list of remediation tasks.

Preferred solutions on VIs card

Number of preferred solutions available to remediate the host vulnerable items. The Solutions list is displayed if the Vulnerability Solution Management application is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

installed. This card shows you solution data, potential and preferred solutions, from third-party vendors about your vulnerable items.

Impacted CIs card

The number of configuration items that have VIs that are assigned to you or your groups. For more information, see View configuration items with vulnerabilities in the IT Remediation Workspace.

Preferred patches on VIs card

Number of preferred patches available that can be used to remediate the host vulnerable items.

Remediation tasks list

The list of remediation tasks assigned to you and your assignment groups. You can filter the records by selecting the **Assigned to me** and **Assigned to my groups** options.

You can click a remediation task to view the details and start an investigation. In the Lists view, you can view the Remediation Tasks, Vulnerable Items, Configurations Test Results and so on. You can open a remediation task and click **Assign to me** to assign the task to yourself and start investigation.

Note: If you do not assign the task to yourself in the remediation task, you cannot view any UI actions at the record level.

Click the More Actions ellipses and click **Start Investigation** to resolve a remediation task.

For more information about what you can do on the home page, see Use remediation task records in the IT Remediation Workspace.

Dashboards in the IT Remediation Workspace

The Dashboards page in the IT Remediation Workspace provides the Vulnerability Remediation dashboard in the Next Experience UI which can be used to focus on the remediation tasks and vulnerable items.

As a remediation owner (sn_vul.remediation_owner), you can access the **Vulnerability Remediation** dashboard by navigating to **Workspaces** > **IT Remediation Workspace** and selecting the Dashboards icon. For more information on the Vulnerability Remediation dashboard, see Using the default Vulnerability Response dashboards.

You can create a customized dashboard by selecting the More options icon ⋮ and selecting **Create new dashboard**.

List page in the IT Remediation Workspace

The List view in the IT Remediation Workspace permits remediation owners to view the records (VITs, AVITs, CVITs, and TRs) assigned to them and their assignment groups, and remediate these vulnerabilities and misconfigurations. You can also view the list of preferred solutions that are recommended for remediating the host vulnerable items. Along with these lists, you can view the list of the exception requests and penetration test assessment requests raised by you, penetration test findings associated with your penetration test assessment requests, supported libraries and other supported data.

Roles required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

The lists and links on the List page provide you with easy access to records and tasks. It contains two tabs:

- **Lists** tab: Displays the default lists for remediation efforts, remediation tasks, vulnerable items (VITs, AVITs, and CVITs), solutions, exceptions, and configuration test results (TRs), etc. For more information, see the following table.
- **My Lists** tab: Displays any list that you've renamed from the List tab and any list that you create.

  You can also create your own list of records. For more information, see Create a list in the IT Remediation Workspace.

Tip:

If you set the *sn_vul_cmn_ws.navigate_to_workspace* system property to `true`, upon selecting the predefined filter links in the Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Test Results module in Configuration Compliance under the **All** menu, these links open in the List page in the IT Remediation Workspace.

For example, if you select **Assigned to My Groups** by navigating to **All** > **Vulnerability Response** > **Remediation Tasks** > **Assigned to My Groups**, this link is redirected to the IT Remediation Workspace. The Assigned to my group list in the Remediation Tasks module opens in the List page of the IT Remediation Workspace if you have a remediation owner role. To view the host remediation tasks, group the tasks by **Record Type**.

You can hide the record count on a list using the *glide.ui.list.seismic.omit.count* system property. For more information on how to turn off/on the record count display on a list, see the KBB0010402 KB article.

Lists tab

The following lists are displayed:

Lists

List item	Description	Applications required	Role Required
Remediation Tasks	View the list of remediation tasks and navigate to the desired task to start working on them. The following lists are available: • **Assigned to you**: Lists all the host, application, container and Test	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
	result remediation tasks that are assigned to you. • **Assigned to my group**: Lists all the host, application, container and Test result remediation tasks that are assigned to the assignment groups to which you belong to. Group the tasks by the Record type to categorize them into host, application, container and configuration test results remediation tasks. Remediation tasks that are created by the remediation task rules in the classic UI have an empty Remediation effort.		vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)
Impacted assets	View the list of assets that are impacted. The following lists are available: • **Assigned to you**: Lists all the host, application, container and Test result remediation tasks that are assigned to you. • **Assigned to my group**: Lists all the host, application, container and Test result remediation tasks that are assigned to the assignment groups that you belong to.	Vulnerability Response	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
Host Vulnerable items	View the list of host vulnerable items and navigate to the desired item to start working on them. This lists are available: • **Assigned to me**: List of host vulnerable items assigned to you for remediation. • **Assigned to my group**: List of host vulnerable items assigned to the assignment groups that you belong to.	Vulnerability Response	sn_vul.remediation_owner for host vulnerable items (VITs)
Application Vulnerable items	View the list of host vulnerable items and navigate to the desired item to start working on them. The following lists are available: • **Assigned to me**: List of application vulnerable items assigned to you for remediation. • **Assigned to my group**: List of application vulnerable items assigned to the assignment groups to which you belong to.	Application Vulnerability Response	sn_vul.app_security_champion
Container Vulnerable items	View the list of container vulnerable items and navigate to the desired item to start working on them. This list view contains: • **Assigned to me**: List of container vulnerable items assigned to you for remediation.	Container Vulnerability Response	sn_vul_container.remediation_owner View the list of assessments needed to perform post incident review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
	• **Assigned to my group**: List of container vulnerable items assigned to the assignment groups to which you belong to.		
Configuration Test Results	View the list of test results and navigate to the desired record to start working on them. This list view contains: • **Assigned to me**: List of configuration test results assigned to you for remediation. • **Assigned to my group**: List of configuration test results assigned to the assignment groups that you belong to.	Configuration Compliance	sn_vulc.remediation_owner
Solutions	Lists the solutions from the solution management application. The Solutions list is displayed if the Vulnerability Solution Management application is installed. • **All**: Shows all the available solutions which you use to remediate the host vulnerable items. • **Highest Supersedence**: Shows all the solutions which are used to populated Preferred Solutions.	Vulnerability Response	sn_vul.remediation_owner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
	• **With Vulnerable items**: Show the solutions which are being used as Preferred Solution on Vulnerable Items.		
Exception requests	• **My requests**: List of all the exception, false positive, and unassign approval requests raised by you for host, application, and container vulnerable items and their remediation tasks. • **My requests (configuration compliance)**: List of all the exception, false positive, and unassign approval requests raised by you for the test results and their remediation tasks that you are working on.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)
Libraries	• **NVDs**: A comprehensive library of vulnerability intelligence maintained by the National Institute of Standards and Technology (NIST). List of vulnerabilities found by NVD and includes security checklists, security-related software flaws, misconfigurations, product names,	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
	and impact metrics including exploits. • **CWEs**: List of community-developed software weakness types. Each CWE record also includes an associated knowledge article that describes the weakness. • **App Vulnerabilities**: • **TPEs**: List of imported third-party vulnerabilities in your instance. Contains a list of related references, vulnerable items, exploits, and CVEs. • **Tests**: Tests imported from the third party integrations with which the test results must comply. • **Test Groups**: List of test groups/ policies imported from the third party integrations. A test group contains a set of tests.		
CMDB	• **Discovered items**: List of all the discovered items. • **Discovered container images**:	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, and Configuration Compliance	• sn_vul.remediation_owner for host vulnerable items (VITs) • sn_vul.app_security_champion for application vulnerable items (AVITs) • sn_vul_container.remediation_owner for container

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
			vulnerable items (CVITs) • sn_vulc.remediation_owner for configuration test results (TRs)
Penetration Test Assessment Requests	Penetration testing assessment requests submitted to security team by you for performing a security assessment of any business application. This list contains: • **Assigned to Me**: List of Penetration Test Assessment Requests raised by you. • **Assigned to My Groups**: List of Penetration Test Assessment Requests raised by the users in your assignment groups.	Application Vulnerability Response	sn_vul.app_security_champion
Penetration Test Findings	List of vulnerabilities identified during the Pen Test Assessment performed by the security team: • **Assigned to Me**: List of Penetration Test Findings assigned to you for remediation. • **Assigned to My Groups**: List of Penetration Test Findings assigned to your assignment groups for remediation.	Application Vulnerability Response	sn_vul.app_security_champion
Supporting Data	This list view contains:	Configuration Compliance	sn_vulc.remediation_owner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Applications required	Role Required
	• **Authoritative Sources**: List of authoritative sources that provide the summary information which is useful to research the source publications that were used to create the record. • **Technologies**: List of technologies that provide the summary information about each authoritative sources and citation (also known, in Qualys, as a framework).		

Related topics

Use the List view in the Vulnerability Manager Workspace

Using the IT Remediation Workspace

The IT Remediation Workspace provides a consolidated list of host vulnerabilities, application vulnerabilities, container vulnerabilities, and misconfigurations that are assigned to you and your group. You can use this workspace to remediate, and request exceptions for vulnerabilities and misconfigurations.

Use the email digest in the Vulnerability Response Workspaces

Use email notifications to view your remediation progress and remind you when tasks are nearing, or are past SLA.

Before you begin

Role required: sn_vul.remediation_owner, sn_vul.app_security_champion, sn_vul_container.remediation_owner, or sn_vulc.remediation_owner

About this task

As a remediation owner, come into your work area and see your email notification as a summary of your work. See what you accomplished, what's approaching, and what's past due. Use the notification to help you organize and prioritize your critical remediation actions. Click a link in the email to bring you into directly into to your workspace. Notifications can help IT specialists with at-glance status of their work. As a vulnerability manager, help your IT specialists to get into the Platform directly from their email service for remediation tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Set up email notifications in the Vulnerability Response Workspaces for more information about how to configure this feature.

The email by default shows the tasks you've closed, the total active tasks assigned to you and your groups, newly assigned, VITs closed, along with other information.

Procedure

1. Navigate to your email, locate a notification, and click to open it.
   The notification is displayed with information about your work status.
2. Click **Go to workspace** to navigate to your work area.

Open search results in IT Remediation Workspace

Set the application scope to IT Remediation Workspace to open your search results in the IT Remediation Workspace instead of classic UI by changing the application scope.

Before you begin
Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

About this task
For example, if you search for a host vulnerable item with its number in the **Search** field by setting the application scope to IT Remediation Workspace, the VIT opens in its record view in the IT Remediation Workspace.

Procedure

1. In the unified navigation bar, select the globe icon  .
2. Select **Application Scope**, and then set the scope to **IT Remediation Workspace**.

Result
When you search for records such as VITs, remediation tasks, state change approvals, and so on, in the **Search** field in the unified navigation bar, the records open in the IT Remediation Workspace.

When the scope is not Global, the globe icon displays with a red ring  . Select it again to change the scope.

Create a list in the IT Remediation Workspace

With the List view in the IT Remediation Workspace, you can view remediation tasks and records assigned to you and your groups. You can also track your exception and false positive requests for remediation tasks (VUL, AVUL, CVUL, and CRG), vulnerable items (VIT, AVIT, and CVIT), and test results (TRs) and view solutions.

Before you begin
Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Procedure

1. Navigate to **All** > **Vulnerability Response** > **IT Remediation Workspace**.
2. Select the List icon.
   The List view displays.
   - Click a filtered list to view the total number of active remediation tasks or records assigned to you or your group. See Use remediation task records in the IT Remediation Workspace for more information about what you can do from these records.
   - View the total number of VIs assigned to you or your groups that have solutions. Click the **Preferred solutions on VIs** card to display the list.
   - See the vulnerable CIs assigned to you and your groups that have vulnerabilities on them on the **Vulnerable CIs** tab or on the Vulnerable CIs assigned to you and your group list on the List view.
3. Select the **My Lists** tab.
4. Select **Add new list**.
5. Create the list either based on an existing list or your own setup.

Creation type	Actions
List based on an existing list	**a.** Select the **Start from existing** tab. **b.** In the **List** field, select the existing list to use as a template fro the drop-down list. **c.** Provide the name for the list in the**List Name** field.
Newly created list	**a.** Select **Create your own** **b.** Provide the name for the list in the**List Name** field. **c.** Select the source whose data you want to fil ter in the list.

6. **Optional:** Create a filtered list.

   a. In the **Select columns** field, determine which columns will appear in the list by deleting any fields that you don't want to appear.

   b. Provide conditions to filter the list.

   (Optional) To add more than one condition, select **New condition set**.

   For example, if you wanted to create a list of active vulnerable items for a scanner you want to monitor, you might enter the conditions **[Active][is][true]** and **[Source][contains][scanner-name]**.

   c. Select **Create**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your new list is displayed.

Note: If you leave the list module, the list displayed when you exit is the list you see when you return. To delete the custom lists you create, with the list displayed, on the right of the pane, select the gear icon and then select **Delete**.

7. Refer to the following table for what you can do from the list view.

Task	Description
Click My Lists	Create new lists and view the lists you have created. In the modal that displays, create another ver sion of an existing list or a new one. The lists you create are displayed on the My List tab. To delete a list, with the list displayed, on the far right of the page click the gear icon.
Assign remediation task records to yourself	On the Lists tab with **Assigned to my group** selected, click a remediation task record (VUL) to open it. On the record that displays, click **Assign to me**. This option is only avail able if a remediation task is not already as signed to you.
Open a remediation task (VUL)	With a remediation task record displayed, click a related list item to open and view the following details: ○ Overview - View remediation progress and other remediation task details. ○ Solutions - View both preferred and poten tial solutions you can use to fix the vulnera bility. On the Solutions tab, child related list items show Preferred solutions and Poten tial solutions. ○ Details - More overview information includ ing the associated vulnerability. You can ed it these fields. ○ Change Requests - View the change re quests associated with the record. ○ Requested Approvals - View the requested approvals. If there are no change request approvals, this related list item is not dis played. ○ State Change Approvals - View the false positive and exception requests associat ed with this record. If there are no requests, this related list item is not displayed. Opened records remain displayed as tabs un til you close them. See Use remediation task

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	records in the IT Remediation Workspace for what you can do from the remediation task record.
Open a vulnerable item (VIT) record	With a vulnerable item record displayed, click a related list item to open and view the follow ing details: ○ Overview - The affected asset, associated vulnerability, initial detection, and other de tails about the state and target date. ○ Details - More overview information includ ing the preferred solution if available. You can edit these fields. ○ Detections - First found, last found, IP ad dress, Port, Protocol and Proof information, if available. ○ Impacted services - Business criticality, sup port group and service ○ Remediation Tasks - The remediation tasks this VI is associated with. Opened VIT records remain displayed as tabs until you close them. See Use remedia tion task records in the IT Remediation Work space for what you can do from the remedia tion task record.
Set filters for a column on a list	Select a column and expand the vertical dots menu to view options that further filter the da ta in the column. For example, from a list of vulnerable items selected, you might prefer to sort the Risk rat ing column so that only critical items are dis played.
Filter out items or match items from a row in a column	Select a cell in a column and refine the data displayed by choosing one: ○ Show Matching - Display only items that match the selected cell in the column. ○ Filter Out - Filter out the items from the col umn that match the selected cell in the col umn.
On the List view, to the left of the Number column with a list displayed, roll over a row and click the small information icon (i) for a record.	Details about the records are displayed in the right side panel of the page.

Use records in the IT Remediation Workspace

Use records to help you view your remediation progress and the impact of vulnerable items on your assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Procedure

1. In your ServiceNow AI Platform instance, navigate to **Workspaces** > **IT Remediation Workspace**.
   The Home landing page is displayed.
2. Navigate to a vulnerable item record and open it from either the Home landing page or the List view.

   The details tab includes information in the form header at the top that relates to the nature of the vulnerability, for example, `CVE-2013-5014 detected on LINUX-DAL-4331`. Under the form header, values for the State, Risk rating, Remediation target date are displayed.
3. Refer to the following table for the UI actions you can perform on the remediation task record.

Task	Description
Click a Related Items link	○ Overview - View details such as the state, Risk rating, Risk score, source, last found, remediation status, associated vulnerability, affected configuration item, and initial detection information. ○ Details - More overview information including the Preferred solution. You can edit these fields. ○ Detections - View detection information imported from your scanners. ○ Impacted Services - View the services impacted by the vulnerability. ○ Remediation tasks - View the other remediation tasks associated with this vulnerable item. Opened records from the VIT remain displayed as tabs under the record tabs until you close them.
Click a link to open a record	From list displayed on opened records from the related items links, view more details about the remediation tasks, detections, and impacted services.
Click a UI action	○ Assign to Me - This option is only displayed if the remediation task is not already assigned to you. ○ Mark as False Positive - Report when a scanner finds a vulnerability but you deter

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	mine that no vulnerability exists. Submit a request. ○ If the vulnerable item is assigned to you, you can rescan the VI. ○ Resolve - Resolve this vulnerable item. The associated remediation tasks transition to Resolved when all its VIs are Resolved. ○ Request Exception - If a target date is passed and you know you need some more time to resolve the vulnerability, submit a re quest. ○ Save - Save any changes and uppdate the record.
Add a work note or attach a file	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel. You can also upload a file.
Set filters for a column on a list	Select a column and expand the vertical dots menu to view options that further filter the da ta in the column. For example, with the Detections related item selected, you might prefer to sort the column so that only detections last found from a cer tain date are displayed.
Filter out items or match items from a row in a column	Select a cell in a column and refine the data displayed by choosing one: ○ Show Matching - display only items that match the selected cell in the column. ○ Filter Out - Filter out the items from the col umn that match the selected cell in the col umn.

Use remediation task records in the IT Remediation Workspace

Remediation tasks are created and assigned automatically from remediation efforts. IT teams and remediation owners can view remediation tasks in the IT Remediation Workspace.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

When vulnerability managers and analysts create remediation efforts to drive remediation, remediation tasks are created automatically and assigned to IT teams based on the group that is associated with the records in a remediation effort.

See the vulnerable CIs assigned to you and your groups that have vulnerabilities on them on the **Vulnerable CIs** tab or on the Vulnerable CIs assigned to you and your group list on the List view.

Procedure

1. In your ServiceNow AI Platform instance, navigate to **Vulnerability Response** > **IT Remediation Workspace**.
   The Home landing page is displayed.
2. In the Remediation Tasks section, click a remediation task to open it.
3. **Optional:** Alternatively, you can click the List icon in the upper left on the home page to see all the remediation tasks (VULs, AVULs, CVULs and CRGs) and records (VITs, AVITs, CVITs and TRs) assigned to you and your groups.
   For more information about how to use the list view, see Create a list in the IT Remediation Workspace.
4. From either the Home page or the List view, click a remediation task to open it.

   In the **Details** tab, you can update some of the information on the record, such as assignment group, state, short description, and so on. Click **Save** to apply your changes.

   The details tab includes information in the form header at the top that relates to the nature of the task, for example, `Vulnerabilities on XYZ Servers (San Diego)`. Under the form header, values for the State, Risk rating, Assignment group, Remediation status, and the percent of active records you've remediated are displayed.
5. Refer to the following table for the UI actions you can perform from the remediation task record.

Task	Description
Click a related items link	○ Overview - View your remediation progress with % of VIs remediated, the state, Risk rating, Assignment group, affected CIs and other task details. To see the Affected CIs, see the image following the table. ○ Solutions - View both preferred and potential solutions you can use to fix the vulnerability. On the record this that is displayed, child related list items show Preferred solutions and Potential solutions. See the images below the table. ○ Details - More overview information including the associated vulnerability. You can edit these fields. ○ Change Requests - View the change requests associated with the record. ○ Requested Approvals - View the submissions for change requests. If there are no change request approval requests, this related list item is not displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	○ State Change Approvals - View the false positive and exception requests associat ed with this record. If there are no requests, this related list item is not displayed. Opened records remain displayed as tabs un til you close them.
Click a link to open a record	From list displayed on opened records from the related items links, view more details about the records, the associated vulnerabili ties, affected CIs (assets), detection data, im pacted services, and associated records.
Click a UI action	○ Assign to Me - This option is only displayed if the remediation task is not already as signed to you. ○ Mark as False Positive - Submit a request if, for example, a scanner finds a vulnerability but you determine that no vulnerability ex ists. ○ Create Change - You can create a new change request or add this remediation task to an existing change request. ○ Split Task - Identify a subset of VIs you want to include in a new remediation task ○ Request Exception - Submit a request if a target date is passed and you know you need some more time to resolve the vulner ability. ○ Resolve - Resolve this RT. The remediation task transitions to Resolved and all its VIs transition to Resolved. ○ Save - Save any changes and update the record.
Add a work note or attach a file	In the far right of the screen, click the **Activity** icon (lightening icon) and enter a work note. Click the icon to toggle the panel. You can also upload a file.
Set filters for a column on a list	Select a column and expand the vertical three dots menu to view options that further fil ter the data in the column. For example, with the Overview-related item selected, you might prefer to sort the Risk rat ing column so that only critical items display.
Filter a column by a selected row	Select a cell in a column and refine the data displayed by choosing one:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	○ Show Matching - display only items that match the selected cell in the column. ○ Filter Out - filter out the items from the col umn that match the selected cell in the col umn.

The Solutions tab in a host remediation task shows you both Preferred and Potential solutions information that best matches the vulnerability associated with the remediation task. Solutions are patches that your IT teams apply to resolve vulnerabilities.

If the Vulnerability Solution Management application is installed, Preferred Solutions are the highest-superseding solutions that are applied to vulnerable items. The list of solutions is based on the vulnerable items in the host remediation task.

Potential solutions are the list of all solutions that are available for VITs in a host remediation task.

You can view the CIs (assets) that are affected by this vulnerability on the remediation task by navigating to **Overview** > **Affected CIs**.

Assign a remediation task or record to yourself in the IT Remediation Workspace

Assign a remediation task (VUL, AVUL, CVUL, or CRG) or record (VIT, AVIT, CVIT, or TR) to yourself from the List page in the IT Remediation Workspace workspace.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace** > **List** > **Remediation tasks** > **Assigned to my group**.
2. Open a remediation task (VUL, AVUL, CVUL or CRG) from the Remediation tasks list.
3. In the UI action buttons on the right, click **Assign to me**.

   The **Assign to me** button is only available if the record is not already assigned to you.

   The remediation task displays on the Assigned to me list under Remediation Tasks.
4. You can also assign a record (VIT, AVIT, CVIT, or TR) to yourself following the same steps from an open record.
   The **Assign to me** button is only available if the record is not already assigned to you.

View configuration items with vulnerabilities in the IT Remediation Workspace

The following enhancements were added to remediation tasks with version 16.1 of the Vulnerability Response application.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

The itil or cmdb_read role is also required if you want to view CI data in the workspaces.

About this task

See the configuration items (CI)s that are assigned to you that have vulnerabilities on them. Click **Impacted CIs** scorecard. Click the Filter list in the upper left to toggle between **Assigned to me** and **Assigned to my groups**. From the List view, click the links.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **IT Remediation Workspace**.
   The Home landing page is displayed.
2. Alternatively, you can view these lists from the links on the List view, or by navigating to their modules, for example, **All** > **Vulnerability Response** > **Remediation Tasks**.
3. Choose one to continue.
   Depending on what is selected in the filter toggle, view the lists of the following records that are assigned to you or to you and your groups.

Option	Description
Assigned remediation tasks	Remediation tasks (RT). For more information about the actions you can take from an RT, see Use remediation task records in the IT Remediation Workspace.
Preferred solution on VIs	Records (VITs) that have preferred solutions mapped to them. If the Vulnerability Solution Management application is installed, Preferred Solutions are the highest-superseding solutions that are applied to records. The list of solutions is based on the records in the remediation task record. To see what you can do from solution records, see Use remediation task records in the IT Remediation Workspace.
Impacted CIs	(CI)s with vulnerabilities. After its initial population, this scorecard shows updated counts of your vulnerable CIs after new VIs that have vulnerabilities are added, or when there are state changes to existing VIs. See the following steps for how to view this record and what you can do from this list.

4. Click the **Impacted CIs** scorecard.

   The list of CI records is displayed.

5. Click a configuration item to open its record.
   The record is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The related lists permit you to view details and various associated records. New available data on this record with this release includes:

- A time line that shows the recent activity on this record.
- Any change requests that are associated with this CI.
- Easily navigate to scorecards and view the remediation tasks, vulnerable items, and preferred solutions associated with this CI.
- You can navigate to the scorecards and view the preferred patches associated with this CI. Preferred patches are the patches associated with the vulnerable items. The Patches tab in the Related list displays the installed and missing patches for the CIs.
- Information about the CI that includes Class, Location, Internet-facing, Environment, and Maintenance schedule.

Create a change request in the IT Remediation Workspace

From a remediation task (VUL, AVUL, CVUL, or CRG), create a change request. Alternatively, add a remediation task to an existing change request.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Note: The itli role is required if you want to submit change requests from the IT Remediation Workspace.

About this task

There might be various reasons that you want to create a change request for a remediation task. Usually, it is because your investigation requires manual intervention to fix the vulnerabilities.

For more information about the change requests and creating change requests from the classic environment, see Change management for Vulnerability Response.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. Select the List icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the List page, in the Remediation tasks list, locate a remediation task (VUL, AVUL, CVUL, or CRG) that you want to create a change request for.
4. In the UI action buttons on the right, expand the list and choose one:
   - Click **Create Change**
   - **Add to existing change**
5. To create a new change request, in the modal that displays, fill in the fields.
   For information on the form fields, see Create change request form fields.
6. Select **Create Change Request**.
   The remediation task record displays and a message indicates that the change request is successfully created.

   Click the Change Requests related link on a record to view all the change requests associated with the record.
7. Alternatively, to add this remediation task to an existing change request, follow these steps.

   a. Click the down arrow to expand the list on the **Create Change** button.

   b. Select **Add to existing change**.

   c. In the modal that displays, click the search icon to view the list of existing change requests.

   d. To add conditions to the list to focus the list of change requests, in the upper right of the modal, click the filter icon (funnel).

   e. In the new pane that is displayed, click **Advanced view**.

   f. Use the condition builder to create your conditions.

   g. Select **Update**.

   h. From the list, click a change request to select it.
   An updated modal is displayed with your choice.

   i. **Optional:** In the modal, select the Add CIs to CR check box to add configuration items from all the active vulnerable items to the change request.

   j. Select **Add change**.
   The remediation record displays, and a message indicates that the change request is successfully created and submitted for approval.
      - Click the **View change** link in the message to open the change request (CHG) record.
      - Select the **Change Requests** related item menu link on the remediation task record to view all the change requests associated with the record.

   Alternatively, in the classic environment, navigate to **Self-service** > **My Requests**. After you submit the change and it is implemented, if state synchronization is enabled, the remediation task automatically moves to `Resolved`. For more information about states and state synchronization in change requests, see Create a change request from a remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a remediation task manually in the IT Remediation Workspace

Starting with v25.0.4 of Vulnerability Response, you can create remediation tasks manually from the Host vulnerable items, Application Vulnerable items, Container vulnerable items, and Configuration test results lists on the List page of IT Remediation Workspace.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace** > **List**.
2. On the List page, open the Active or All list in one of the following lists:
   - Host Vulnerable Items
   - Application Vulnerable Items
   - Container Vulnerable Items
   - Configuration Test Results
3. Select the check box of the records you want to update and then select the Selected items option in the Record selection field on the Create Remediation Task modal.
4. Select **Create Remediation Task**.
5. On the Create remediation task modal, fill in the following details.

Create remediation task modal

Field	Description
Record selection	**Selected items**: Updates the selected records only.
Short description	Brief note about the remediation tasks.
Grouping criteria	Choices are: ○ **Assignment group**: Records with same assignment group are grouped into one remediation task. ○ **Assignment group and configuration item**: Records with same assignment group and configuration item are grouped into one remediation task. ○ **Assignment group and vulnerability**: Records with same assignment group and vulnerability are grouped into one remediation task. ○ **Assignment group and risk rating**: Records with same assignment group and risk rating are grouped into one remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Managing records in other remediation tasks	Choices are: ○ **Skip records for new remediation tasks**: No action is taken on the records that are part of other remediation tasks. ○ **Move to new remediation tasks**: Records that are part of other remediation tasks are transferred to new remediation tasks. ○ **Keep in both current and new remediation tasks**: Records that are part of other remediation tasks are kept in both old and new remediation tasks.

6. Select **Create remediation task**.

Result

Remediation tasks are created based on the grouping criteria. An email notification is sent to the remediation owners in the assignment group, informing them that a remediation task has been created and assigned to their group. For examples on how remediation tasks are created based on the grouping criteria and record management criteria, see Examples for remediation task creation in the Vulnerability Manager Workspace and IT Remediation Workspace.

Split a remediation task in the IT Remediation Workspace

From a remediation task (VUL, AVUL, CVUL, or CRG), identify a subset of records and create a new remediation task for them.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

About this task

You can select individual records in the Overview tab of a remediation task and move them to a new remediation task.

Use cases for splitting records (VITs, AVITs, CVITs or CTRs) from existing remediation tasks into new tasks might include the following examples:

- You want to create a change request or change requests for a split task.
- You want to reassign a split task to another user in your assignment group.
- You request a deferral or exception for a split task, because you know that some vulnerabilities on specific configuration items (CIs) cannot be remediated by the target date.

For more information about change requests and splitting a remediation task in the classic environment and for versions of Vulnerability Response prior to v15.0, see Split a remediation task.

Starting with v19.0 of Vulnerability Response, you can split tasks for test result groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

Starting with version 18.0, you can split tasks for application vulnerability items and container vulnerability items.

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. Open a remediation task (VUL, AVUL, CVUL, or CRG) from Home page or List page.
3. In the Overview tab, select the records (VITs, AVITs, CVITs, or CTRs) that you want to move to a new remediation task.
4. Click **Split Task**.
5. In the dialog that is displayed, the number of records (VITs, AVITs, CVITs, or CTRs) you selected from the list is displayed.
6. Click **Split Task** again.
   A confirmation message is displayed with a link to the new remediation task.

   Alternatively, you can use the condition builder to filter records (VITs, AVITs, CVITs, or CTRs).
7. Locate a remediation task that you want to split.
8. In the UI action buttons on the right, click **Split Task**.
   After a few moments, the condition builder displays.
9. In the modal that is displayed, use the condition builder to identify the subset of records (VITs, AVITs, CVITs, or CTRs) that you want to add into a new remediation task.
10. Click **Split Task**.
    If a message displays that no records match your conditions, you must adjust your criteria and click **Split Task** again. Edit the short description field as required. This field can help you find your new remediation task after it is created.

    If records match your conditions, the number of matching records is displayed in a message.
11. **Optional:** Click the **Preview items** link to view the records that match your filter conditions.
    The new remediation task is displayed as a new tab.

Request a false positive in the IT Remediation Workspace

Raise a false positive request for host vulnerable item (VIT), application vulnerable item (AVIT), container vulnerable item (CVIT), or remediation task (VUL, AVUL, CVUL or CRG) in the IT Remediation Workspace.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

About this task

A false positive is a condition wherein the scanner reports that a vulnerability exists in the system, but in reality, there is no vulnerability. There can be multiple reasons, such as incorrect classification, improper logic or algorithm in the scanner.

For more information on how to request a false positive for a set of test results, see Request false positive for a set of test results.

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. Locate a remediation task (VUL, AVUL, CVUL or CRG) or vulnerable item (VIT, AVIT, or CVIT) that you want to mark as false positive.
3. In the UI action buttons on the right, select **Mark as False Positive**.
4. In the dialog that is displayed, enter information about the request and select **Request Approval**.
5. On the Take Questionnaire modal, answer the questions to provide additional information about your request to the approver and select **Submit**.

   Note: The Take Questionnaire modal appears only when the **Enable questionnaire to mark false positive** check box is selected in the Exception Management Configuration form. For more information, see Configure Exception Management for Vulnerability Response,Configure Exception Management for Application Vulnerability Response, Configure Exception Management for Container Vulnerability Response, and Configure Exception Management for Configuration Compliance.

   The state of the vulnerable item (VIT, AVIT, or CVIT) or remediation task (VUL, AVUL, or CVUL) transitions to In Review.

   Your request is submitted for approval and the approver receives an email notification about your request.

Result

You will receive an email notification upon approval or rejection of your request.

What to do next

In the IT Remediation Workspace, on the List page, navigate to **Exception Requests** > **My requests** and open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Record (VIT, AVIT, or CVIT)	Remediation task (VUL, AVUL, CVUL, or CRG)
Approved	The State of the record transitions to Closed with Reason as False positive.	The State of the remediation task transitions to Closed with Reason as False positive. The state is rolled down to the records in the remediation task accordingly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approval state	Record (VIT, AVIT, or CVIT)	Remediation task (VUL, AVUL, CVUL, or CRG)
		Navigate to the Details tab of a Remediation task and set the expiry date for false positive in the **Until** field if required. The remediation task reverts to the Open state after the specified date and the state is rolled down to the test results.
Rejected	The state of the record does not change.	The state of the remediation task and its records reverts to previous state.

In the **Activity stream** of a record or remediation task, you can view the entire workflow of the false positive request.

Related topics

False Positive overview

Request false positive for a set of test results

Starting with v22.0 of Vulnerability Response, you can raise a false positive request for a set of test results within a remediation task, in the IT Remediation Workspace.

Before you begin

Role required: sn_vulc.remediation_owner

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. On the List page, open a Configuration Compliance Remediation Task.
3. In the Overview related item, under the Test Results tab, select the test results that you want to mark as false positive.

   Note: You can request a false positive for a set of test results within a Remediation Task only when:

   - At least one selected test result is in the Active state.
   - Remediation Task has at least two test results.
   - All the test results aren't selected.

4. Select the **Mark as False Positive** button on the Configuration Test Results tab.
5. In the dialog that is displayed, enter information about the request and select **Request Approval**.
6. On the Take Questionnaire modal, answer the questions to provide additional information about your request to the approver and select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Take Questionnaire modal appears only when the **Enable questionnaire to mark false positive** check box is selected in the Exception Management Configuration form. For more information on how a questionnaire is configured, see Configure Exception Management for Configuration Compliance.

The selected test results are moved to a new remediation task and your request is submitted for approval. The task number appears in the **Activity stream** of the old Remediation Task. The approver receives an email notification about your request.

Result

You will receive an email notification on the approval or rejection of your request.

In the **Activity stream** of a test result or remediation task, you can view the entire workflow of the false positive request.

What to do next

1. In the IT Remediation Workspace, on the List page, navigate to **Exception Requests** > **My requests**.
2. Open the corresponding state change approval record (VCA#) and check the status of your request in the Approval state column:

Approval state	Result
Approved	The State of the new remediation task transitions to Closed with Reason as False positive.
Rejected	The state of the new remediation task changes to Open.

3. After the request is approved, navigate to the Details tab of the new Remediation Task, and set the expiry date for false positive in the **Until** field if necessary.

   The remediation task will revert to the Open state after the specified date and the State is rolled down to the test results.

Request an exception in the IT Remediation Workspace

Request an exception for the host vulnerable item (VIT), application vulnerability item (AVIT), container vulnerable item (CVIT) and remediation task (VUL, AVUL, CVUL, or CRG) from the IT Remediation Workspace.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

About this task

Some vulnerabilities might not have an existing patch, fix, or solution. Or, you might determine that a remediation task cannot be resolved by its target date. When your remediation can't

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

comply with a published vulnerability management or security policy, standard, or guideline, you can request an exception.

You can request exceptions for remediation tasks (VUL, AVUL, CVUL, or CRG) and vulnerable items (VITs, AVITs, or CVITs) from the IT Remediation Workspace that are assigned to you.

Starting with version 19.0 of Vulnerability Response, you can request exceptions for test results.

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

Starting with version 18.0, you can request exceptions for application vulnerability items and container vulnerability items.

For more information about requesting exceptions in the classic environment, see Request an exception for a remediation task.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **IT Remediation Workspace**.
2. Select the List icon.
3. In the Remediation tasks list, open a remediation task (VUL, AVUL, CVUL, or CRG) or record (VITs, AVITs, or CVITs) that you want to request an exception for.
4. In the UI action buttons on the right, click **Request Exception**.
5. In the dialog that displays, fill in the end date for the exception, select a reason from the list, and add any other required information.
6. Click **Request Exception**.
7. On the **Take Questionnaire** modal, answer the questions and click **Submit**.

   Note: Starting with version 18.0, you can answer the questionnaire to provide additional information about your request for the approver. The **Take Questionnaire** modal appears only when the **Enable questionnaire to request exception** check box is selected in the **Exception Management Configuration** form.

   A message displays that your request is successfully submitted for approval.

   An exception request for a remediation task is approved using a default, two-level approval workflow. After the request is approved by the level 1 approver, it is sent on to the level 2 approver.

   - The remediation task or record transitions to In Review while the exception request is open.
   - The remediation task or record transitions to Deferred if the request is approved.
   - The exception request record (VCA#) is closed after your exception request is approved.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To view the status of your approval requests, under Exception Requests on the List page, click **My requests**. The number for the request (VCA#) displays when you open the record or remediation task from the list.

- If the request is rejected, the request record (VCA#) displays **Rejected** in the Approval state column in your List view under My requests.
- You are required to submit a new exception request if you still want to defer this item.

Request an exception using GRC: Policy and Compliance Management in the IT Remediation Workspace

Request a policy exception for the host vulnerable item (VIT), application vulnerability item (AVIT), container vulnerable item (CVIT) or remediation task (VUL, AVUL, CVUL, or CRG) from the IT Remediation Workspace.

Before you begin

Role required:

- sn_vul.remediation_owner for host vulnerable items (VITs)
- sn_vul.app_security_champion for application vulnerable items (AVITs)
- sn_vul_container.remediation_owner for container vulnerable items (CVITs)
- sn_vulc.remediation_owner for configuration test results (TRs)

About this task

Note: Starting with v19.0 of Vulnerability Response, the following terms have been renamed:

Changes in terminology

Terminology prior to v19.0	Terminology v19.0 onwards
Test Result Groups	Remediation Tasks
Configuration Issues	Configuration Test Results
Policy	Test group

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. In the application navigator, select the list icon ( ).
3. On the List page, under Host Vulnerable items, Application Vulnerable items, Container Vulnerable items, or Remediation tasks, select the record that you want to request an exception for.
   The record that you select must be in the Open, Under investigation, or Awaiting implementation state.
4. Select the **Request Exception** button.
5. On the form, fill in the fields.
   For more information on the form fields, see Request exception form fields for policy exceptions.
6. Select **Request Exception**.
7. On the Take Questionnaire modal, answer the questions to provide additional information about your request and select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Take Questionnaire modal appears only when the questionnaire details are added to the respective integration registry.

A message appears that your request is successfully submitted for approval.

For more information on the Policy Exception Integration and the hand-off between the remediation owner and the compliance manager, see Policy and Compliance Management optional setup.

Request risk change in the IT Remediation Workspace

Starting from v20.0 of Vulnerability Response, you can request for the change in risk for a host vulnerable item or a remediation task in the IT Remediation Workspace.

Before you begin

Role required: sn_vul.remediation_owner

About this task

Starting from v21.0 of Vulnerability Response:

- You can request risk change for a remediation task if its vulnerability items are associated to a same Common Vulnerability Entry (CVE) or Third-party Entry (TPE) for which risk change is enabled.
- You can request risk change for a remediation task with vulnerable items and also application remediation task with application vulnerable items associated to different CVEs if the risk change is enabled for CVEs. With the following message “Select relevant compensating controls for the vulnerabilities managed in the remediation task”

Note: The compensating controls feature is available for host vulnerabilities only.

Procedure

1. Navigate to **Workspaces** > **IT Remediation Workspace**.
2. On the List page, open a host vulnerable item or a remediation task.
3. Select the three dots menu and select **Request Exception**.
4. On the Request Exception pop-up, fill in the fields.

Request Exception modal

Field	Description
Reason	Reason for your exception request. Select *Mitigating Control in Place* for risk change request. To see how to add new reason choices, see Define policy reason mapping.
Request for Deferral	Differ the record. This field is selected by default. **Note:** This field appears only when the *Mitigating Control in Place* option is selected in the **Reason** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Request for Risk Change	Enables you to request for the risk score change. **Note:** This check box appears only when the *Mitigating Control in Place* option is selected in the **Reason** field.
Current Risk Rating	Current severity of the risk. **Note:** This field appears only when the **Request for Risk Change** check box is selected.
Desired Risk Rating	New risk rating that you want to assign to the record. The highest risk score in this risk rating range is applied to the record when your request is approved. **Note:** This field appears only when the **Request for Risk Change** check box is selected.
Select Compensating Controls	Reason for your request to reduce the risk rating.
Until	Date on which the deferral or risk reduction request expires. When the exception request expires: ○ The record reverts to the Open state. ○ The compensating controls expire. ○ The calculated score will be in place of a reduced score.
Justification notes	Details that are related to the reason why this request is being made.

5. Select **Request Exception**.
6. On the Take Questionnaire modal, answer the questions to provide additional information about your request and select **Submit**.

   Note: The Take Questionnaire modal appears only when the questionnaire is enabled for exception management. For more information, see Configure Exception Management for Vulnerability Response.

   A message appears stating that your request is successfully submitted for approval. A notification is sent to the approver about your request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If you request for a deferral and risk change:
  - Two state change approvals (VCA#) are created for deferral and risk reduction.
  - The state of the record changes to In Review.
- If you request for risk change only:
  - A state change approval (VCA#) is created.
  - The state doesn't change.

On approval or rejection of your request, you'll receive a notification.

For more information on how the **Until date for risk change** is updated for a remediation task and vulnerable item when a risk change request is approved, see Impact of the compensating controls on risk score and expiration date.

What to do next

You will receive a notification when your request is approved or rejected by the approver. For more information on the approval process, see Approve or reject requests in the Vulnerability Manager Workspace.

Related topics

Understanding compensating controls for risk change

Disable or enable risk change for a CVE or TPE

Add a compensating control to the library

Impact of the compensating controls on risk score and expiration date

Rescan vulnerable items and remediation tasks in the IT Remediation Workspace

Verify that your vulnerable items have been remediated between scheduled scanning cycles. Initiate rescans from the IT Remediation Workspace in your ServiceNow AI Platform on-demand.

Rescans permit you to verify that your remediation activities, patches, and other actions have successfully fixed specific vulnerabilities on your configuration items (CIs).

Rescan is supported for the following integrations in the IT Remediation Workspace. See the following topics for more information:

- Rescan Qualys vulnerable items from the Vulnerability Response workspaces
- Rescan Rapid7 vulnerable items from the Vulnerability Response workspaces
- Rescan Tenable.io and Tenable.sc vulnerable items from the Vulnerability Response workspaces

Roles required: sn_vul.remediation_owner for the IT Remediation Workspace.

Rescan Qualys vulnerable items from the Vulnerability Response workspaces

Verify that your vulnerable items have been remediated between scheduled scanning cycles. Initiate rescans in the Qualys product on-demand from the IT Remediation Workspace in your ServiceNow AI Platform instance.

Before you begin

To initiate a rescan for the Qualys product from the classic environment, see Initiate rescan for the Qualys Vulnerability Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Qualys scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have these applications as a source, the **Rescan** button is not available.

To activate these scanners, as a user with the sn_vul.vulnerability_admin role:

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Locate the scanner product you want to activate and click the record to open it.
3. Select the Active check box.
4. Click **Update**.

   The product you activated is displayed in the Source field on vulnerable item and remediation task records after the next import, and **Rescan** is available as a UI action.

For more information about setting up your Qualys scanner, see Set up scanner appliances and Advanced Qualys configurations and modifications.

- You can initiate rescans on-demand for vulnerable items and remediation tasks that have the Qualys product as the source from the IT Remediation Workspace in your ServiceNow AI Platform.
- On a remediation task record, the record can be in any state other than **Closed**, and all the associated VIs must be from the Qualys product.
- To initiate rescans in the IT Remediation workspace from vulnerable item and remediation task records, these records must be assigned to you.

Roles required:

- sn_vul.remediation_owner for the IT Remediation Workspace.
- sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin from the Vulnerability Manager Workspace.

Procedure

1. Navigate to a vulnerable item or a remediation task that has been assigned to you and open it.

   Note: If you choose a remediation effort to initiate a rescan, all the VIs associated with that record are scanned.

2. In the upper right of the record, click **Rescan**.
3. In the Rescan modal, choose an option profile.
   An option profile is required when you initiate a Qualys scan from your ServiceNow AI Platform®. Option profiles contain Qualys scan settings.

Option	Description
Use default option profile	This is the option profile that is set as the de fault for the integration instance. You select this profile when you set up your Qualys scan ner. See Set up scanner appliances for more information.
Specify option profile	From the Option profile list, choose a profile to use for the scan.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	You can select the option profile you want to use for scans for matching configuration items.

4. In the Rescan modal, click **Request rescan**.
   The message, `The scan request is being processed` is displayed.
5. Click the **View status** link in the message to view the progress of the scan.

   The scan record (VSCAN#) displays. Below the record header with the scan number, the related item lists display the following information:

   - The Details list displays the scan number of the parent scan, the scanner source, and the state. View completed and failed scans under the Scan Summary section.
   - The Scans list displays any child scans and their states. When all the child scans are completed, the state of the parent scan transitions to Complete.
   - The Source list displays the vulnerable item used for the scan, the associated configuration item and vulnerability, the state of the VI, and its remediation status.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first.

   The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped.

   All VIs that have transitioned, or will transition, to Closed/Fixed are imported with the next scheduled import of the Qualys integrations.

Rescan Rapid7 vulnerable items from the Vulnerability Response workspaces

Verify your vulnerable items have been remediated between scheduled scanning cycles. Initiate rescans in the Rapid7 product on-demand from the IT Remediation Workspace in your ServiceNow AI Platform instance.

Before you begin

To initiate a rescan for the product from the classic environment, see Initiate rescan for the Rapid7 Vulnerability Integration. This topic also includes information about how to schedule scans with the integration parameters on the Rapid7 integration instance.

The Rapid7 scanners are deactivated by default in the Vulnerability Response application. If you try to perform a rescan from the vulnerable items or remediation tasks that have Rapid7 application as a source, the **Rescan** button is not available.

To activate these scanners, as a user with the sn_vul.vulnerability_admin role:

1. Navigate to **All** > **Vulnerability Response** > **Vulnerability Scanning** > **Scanners**.
2. Locate the scanner product you want to activate and click the record to open it.
3. Select the Active check box.
4. Click **Update**.

   The product you activated is displayed in the Source field on vulnerable item and remediation task records after the next import, and **Rescan** is available as a UI action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can initiate rescans on-demand for vulnerable items and remediation tasks that have the Rapid7 InsightVM product as the source from the IT Remediation Workspace in your ServiceNow AI Platform.
- On a remediation task record, the record can be in any state other than **Closed**, and all the associated VIs must be from the Rapid7 product.
- To initiate rescans in the IT Remediation workspace from vulnerable item and remediation task records, these records need to be assigned to you.

Roles required:

- sn_vul.remediation_owner for the IT Remediation workspace
- sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin from the Vulnerability Manager Workspace

Procedure

1. Navigate to a vulnerable item or a remediation task that has been assigned to you and open it.

   Note: If you choose a remediation effort to initiate a rescan, all the VIs associated with that record are scanned.

2. In the upper right of the record, click **Rescan**.
3. In the Confirm rescan modal, click **Request rescan**.
   The message, `The scan request is being processed` is displayed.
4. Click the **View status** link in the message to view the progress of the scan.

   The scan record (VSCAN#) is displayed. Below the record header with the scan number, the related item lists display the following information:

   - The Details list displays the scan number of the parent scan, the scanner source, and the state. View completed and failed scans under the Scan Summary section.
   - The Scans list displays any child scans and their states. When all the child scans are completed, the state of the parent scan transitions to Complete.
   - The Source list displays the vulnerable item used for the scan, the associated configuration item and vulnerability, the state of the VI, and its remediation status.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first.

   The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped.

   All VIs that have transitioned, or will transition, to Closed/Fixed are imported with the next scheduled import of the Rapid7 integrations.

Rescan Tenable.io and Tenable.sc vulnerable items from the Vulnerability Response workspaces

Verify your vulnerable items have been remediated between scheduled scanning cycles. Initiate rescans in the Tenable.io and Tenable.sc products on-demand from the IT Remediation Workspace in your ServiceNow AI Platform instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

To initiate a rescan for the Tenable.io and Tenable.sc products from the classic environment of Vulnerability Response, see Initiate rescan for the Tenable.sc integration and Initiate rescan for the Tenable.io integration.

To perform rescans from your ServiceNow AI Platform, you need your Tenable credentials. For more information about setting up your Tenable.io and Tenable.sc scanners and importing your credentials from Tenable, see Configure the Tenable Vulnerability Integration using Setup Assistant.

- You can initiate rescans on-demand for vulnerable items and remediation tasks that have the Tenable.io or Tenable.sc product as the source from the IT Remediation Workspace in your ServiceNow AI Platform.
- On a remediation task record, the record can be in any state other than **Closed**, and all the associated VIs must be from the Tenable.io or the Tenable.sc product.
- To initiate rescans in the IT Remediation Workspace from vulnerable item and remediation task records, these records must be assigned to you.

Roles required:

- sn_vul.remediation_owner for the IT Remediation Workspace
- sn_vul.vulnerability_analyst or sn_vul.vulnerability_admin from the Vulnerability Manager Workspace

Procedure

1. Navigate to a vulnerable item or a remediation task that has been assigned to you and open it.

   Note: If you choose a remediation effort to initiate a rescan, all the VIs associated with that record are scanned.

2. In the upper right of a record, click **Rescan**.
   You are prompted to choose the instance or instances for the rescan and the scanner credentials you want to use to access the scanner. The displayed credentials are those imported by the Tenable.io and Tenable.sc Scan Credential Integrations.
3. In the modal, click the search icon.

   In the Select a scan credential modal that displays, use the filters in the column headings to select the name, instance and or instances, and the credential types that you want to use.

   See the following table for more information.

Column	Description
Name	Choose the name of the credential(s) you want. Roll over the column title. Use the verti cal three dots menu in the column title to filter the names of your credentials.
Integration instance	Choose a Tenable.io or, if for Tenable.sc, the Tenable.sc integration instance that you want to initiate the rescan from. All your integration instances for Tenable.io or Tenable.sc are displayed. If a VI exists in more than one integration instance, you can

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Description
	use this filter to limit or expand the instances you want to scan. **Note:** If you choose to rescan VIs from a remediation task record for a single in tegration instance, only the active VIs that are associated with that remedia tion task, for that instance, using the cre dential(s) that you select are scanned.
Type	These are the available scanner credentials imported from the Tenable.io or Tenable.sc products. Roll over the column title. Use the vertical three dots menu in the column title to open the modal and select the credential types you want.

4. In the updated Rescan modal, click **Request rescan**.
   The message, `The scan request is being processed` is displayed.
5. Click the **View status** link in the message to view the progress of the scan.

   The scan record (VSCAN#) is displayed. Below the record header with the scan number, the related item lists display the following information:

   - The Details list displays the scan number of the parent scan, the scanner source, and the state. View completed and failed scans under the Scan Summary section.
   - The Scans list displays any child scans and their states. When all the child scans complete, the state of the parent scan transitions to Complete.
   - The Source list displays the vulnerable item used for the scan, the associated configuration item and vulnerability, the state of the VI, and its remediation status.

   Your ServiceNow AI Platform® instance tracks the rescan status until it successfully completes, or, until the set tracking period times out, whichever happens first.

   The time-out does not stop the scan. The time-out refers to when the ServiceNow AI Platform® stopped tracking your rescan status, not when the actual rescan stopped.

   All VIs that have transitioned, or will transition, to Closed/Fixed are imported with the next scheduled import of the Tenable.io or Tenable.sc integrations.

IT Remediation Workspace reference information

The following topics provide you with links, reference information, in addition to field data on the forms and records found in IT Remediation Workspace.

Create change request form fields

The following table shows the fields and their description in the Create change request form.

Field	Description
Change type	Normal – Normal is the default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Standard- two additional fields are displayed: Standard change category - Select a category from the list Standard change template – Select a template from the choice list to use for this change request Emergency - Critical priority
Add CIs to change request	Default is enabled. If enabled, the change request adds any configuration items (CI) that belong to active vulnerable items in this remediation effort are added to this change request.
Priority	High is the default. Select a priority from the list.
Assignment group	The assignment group is by default taken from the watch topic. Click the search icon, and from the modal choose another assignment group.
Planned end date	Click the calendar icon to select a planned end date.
Assigned to	The current user is by default assigned to the remediation task. Click the search icon, and from the modal choose another user.
Short description	The short description is taken from the remediation task. Click the text to edit it.
Description	The description is taken from the remediation task. Click the text to edit it.
Justification	The Justification taken from the remediation task. Click the text to edit it.
Implementation plan	Pre-populated with preferred solution information if it is available. View the solution or enter a justification plan.

Related topics

Create a change request in the IT Remediation Workspace

Request exception form fields for policy exceptions

The following table shows the fields that you must fill on the Request exception form for policy exceptions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request Exception form

Field	Description
Policy	Vulnerability Management policy that you're requesting an exception for.
Control objective	Control objectives associated with the policy that you selected. If a policy isn't selected, all the control objectives are listed.
Valid from	Date when the exception starts. The default value is the current date. This date can't be in the past.
Valid until	Date that the policy exception expires and the state of the vulnerable item or group changes from Deferred to Open. **Note:** The number of days that the policy exception is valid can't exceed the value in the **Maximum exception duration (days)** field that you set for the policy. For more information, see Create a policy.
Reason	Reason for requesting an exception.
Justification	Details related to the reason this exception is being requested. This field must be filled in by the remediation owner.

Related topics

Request an exception using GRC: Policy and Compliance Management in the IT Remediation Workspace

Request exception form fields for risk reduction

The following table shows the fields that you must fill on the Request exception form for risk reduction requests.

Request Exception form

Field	Description
Reason	Reason for your exception request. Select *Mitigating Control in Place* for risk reduction request. To see how to add new reason choices, see Define policy reason mapping.
Request for Deferral	Differ the record. This field is selected by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request Exception form (continued)

Field	Description
	Note: This field appears only when the *Mitigating Control in Place* option is selected in the **Reason** field.
Request for Risk Reduction	Enables you to request for the risk score reduction. **Note:** This check box appears only when the *Mitigating Control in Place* option is selected in the **Reason** field.
Current Risk Rating	Current severity of the risk. **Note:** This field appears only when the **Request for Risk Reduction** check box is selected.
Desired Risk Rating	New risk rating that you want to assign to the record. The highest risk score in this risk rating range is applied to the record when your request is approved. **Note:** This field appears only when the **Request for Risk Reduction** check box is selected.
Select Compensating Controls	Reason for your request to reduce the risk rating.
Until	Date on which the deferral or risk reduction request expires. When the exception request expires: • The record reverts to the Open state. • The compensating controls expire. • The calculated score will be in place of a reduced score.
Justification notes	Details that are related to the reason why this request is being made.

Explore the Vulnerability Assessment workspace

The Vulnerability Assessment Workspace is designed for the Vulnerability event manager to perform exposure assessment, and proactively manage critical vulnerability events especially during the critical vulnerability events such as a zero-day event.

After a critical vulnerability is identified, vulnerability event managers can assess the potential impact and risk associated with the vulnerability. The analysts can analyze the affected system,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

applications, or network components to understand the severity and possible attack vectors within the organization.

The Vulnerability Assessment Workspace contains:

Exposure Assessment page

Provides detailed visibility into the assets exposed to vulnerabilities and vulnerable software. The Exposure assessment functionality provides:

- Visibility into impacted assets for vulnerability and affected software
- Ability to perform standalone assessments for a single CVE or vulnerable software
- Visibility to impacted assets for CISA known exploited vulnerability CVEs
- Visibility to exposure from additional discovery model and assets.
- Ability to create vulnerable items

Vulnerability Assessment page

The Vulnerability Assessment page where you can handle vulnerability crisis events from assessment to resolution using the Vulnerability Crisis Management workflow. The workflow lets you track vulnerability events of interest, analyse risk associated with them, perform exposure assessment across multiple inventories (For e.g. Software Installations inventory) and declare it as a crisis for elevated response engagement. You can then associate the vulnerability assessment record to a major security incident and enable the security incident response team to respond to the crisis.

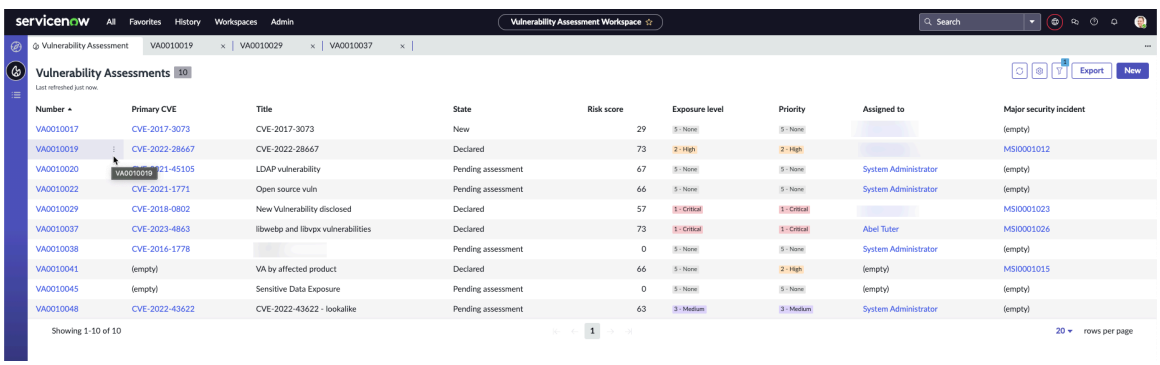
- Create and modify vulnerability assessments for critical vulnerability events
- Record key attributes of the vulnerability to calculate risk
- Perform vulnerability assessment to determine exposure level and priority
- Declare the vulnerability assessment as a critical event
- Associate the vulnerability assessment to a major security incident by linking, proposing or promoting the vulnerability assessment to a major security incident.

List page

The List page comprises a library containing:

- CVEs
- TPEs
- CWEs

The following image shows you the Vulnerability Assessment Workspace home page.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring exposure assessment

Exposure assessment uses the Common Platform Enumeration (CPE) framework, which is a part of the Common Vulnerabilities and Exposures (CVEs) system, to evaluate the vulnerability exposure of your assets to vulnerability software. This assessment is performed using a software discovery model.

By employing a matching algorithm, the relevant CPEs are associated and mapped to the software discovery model, enabling the identification of potential exposures.

You can use the exposure assessment by CVE or software to identify exposure to potential vulnerabilities for the following scenarios:

- Vulnerabilities that may not be identified by traditional scanners
- Zero-day vulnerabilities before the scanner provide the signature for vulnerability detection

Exposure assessment provides an early warning to remediate these vulnerabilities, and improve the maturity of the vulnerability management program.

Prerequisites for exposure assessment

Available versions

Application	Version
Vulnerability Crisis Management plugin	1.0
Vulnerability Response	20.0
Vulnerability Response with NVD	1.3
Vulnerability Response Integration with CISA	1.2
Vulnerability Response Integration with NVD **Note:** For more information, see Understanding the NVD integrations.	1.3
Software Asset Management	Software Asset Management Foundation plugin or Software Asset Management Professional plugin

Use cases

For examples of how Vulnerability Analysts organization would use the Vulnerability Exposure Assessment workspace, see these use cases.

Assessment type	Use
Assess by CVE	Assess vulnerabilities by CVE to gain a full understanding of the impact and exposure of the affected systems using Software Asset Management (SAM) and Discovery data. Take prompt remediation actions by creating manual VITs and assigning them to remediation owners. Assessing by CVEs is beneficial because scanners may not detect

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assessment type	Use
	all the affected systems, whereas Discovery typically identifies most of the software on the attack surface.
Assess by Software	Assess the impact by software when CVE is unavailable to identify the number of CIs where the software is installed. By assessing by software, you can proactively act on zero-day or critical vulnerabilities by creating a manual VIT and assigning it to the remediation owner before they're officially published or before scanners identify them.
Assess by Publisher	Assess vulnerabilities by a software vendor to understand the impact and exposure of affected systems for the CVEs published by the vendor within a time frame. Assessing by publisher helps you evaluate the vendor risk and critical vulnerabilities, enabling proactive remediation.

Compatibility and system requirements

The Vulnerability Response application is available on the ServiceNow Store. The ITSM Software Asset Management application (com.snc.asset_management) is required for the Exposure Assessment module. This application manages all your assets and software licenses, and the SAM Foundation version of this application is part of the Vulnerability Response application that you download from the ServiceNow Store.

Important: The Exposure Assessment application works with the following plugins:

- Software Asset Management Foundation plugin (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Software Asset Management plugin (com.snc.software_asset_management)

To verify the SAM Foundation application is installed on your instance, navigate to **System Applications** > **All Available Applications** > **All** and search for com.snc.asset_management. If the application isn't installed, select **Install**. As the Vulnerability Exposure Assessment application requires access to the asset data on your ServiceNow AI Platform® instance, the asset management applications must have data to reference. The Software Discovery Models table (cmdb_sam_sw_discovery_model) and the Software installations (cmdb_sam_sw_install) require data.

Matching algorithm fields for software discovery models

The Software Asset Management Professional application enables you to edit a software discovery model to manually normalize discovered software that hasn't been fully normalized (partially normalized, publisher normalized, or match not found) on the Software Discovery Models form so that it can be reconciled. Starting with version 20.0 of Vulnerability Response supports normalized discovery model that comes from Software Asset Management Professional. The following fields are used for the matching algorithm for software discovery models.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CPE (Software model)	SAM Foundations	SAM Professional
Vendor	Primary Key	Primary Key
Product	Display Name	Display Name
Version	Discovered Publisher	Discovered Publisher
Edition	Discovered Product	Discovered Product
	Discovered Version	Discovered Version
		Normalized Publisher
		Normalized Product
		Normalized Version

Note: The SAM Professional application isn't part of the core Vulnerability Response product from the ServiceNow Store and requires a separate subscription.

System property

To process the CISA-exploited vulnerabilities automatically for exposure assessment, set the system property *sn_vul_analyst.enable_exposure_for_cisa* to *true*. The default value is *false*.

Scheduled jobs

Following are the scheduled jobs.

Scheduled job name	Description
Check potential vulnerability exposure	Processes the delta CVEs, software, and installations to get the exposure. **Note:** This scheduled job runs every 12 hours. It runs for a longer period than the other scheduled jobs.
Insert CISA exploited CVE to exposure config	On-demand. Inserts the CISA CVEs into the Exposure Configuration table to calculate the exposure.
Run exposure assessment for configured CVEs	On-demand. Calculates the exposure for all the CVE records in the Exposure Configuration table.
Run software exposure	On-demand. Calculates the exposure for all the software records in the Exposure Configuration table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key terms

- **Confidence score:** A confidence score is a measurement of the reliability in providing a recommendation for a field. The higher the score, the more reliable the recommendation. For sample calculations, see Confidence score calculation example.
- **Software installation count:** Number of software assets impacted by the vulnerability.
- **Software model:** Software model associated with the product. Drill-down on the software model to see the software model result. For more information, see Software Asset Management Foundation plugin discovery models and software installations.

The **Software installation count** field provides the total number of software installs, regardless of their active or inactive status on the discovery model. Starting with v22.0 of Vulnerability Response, a new system property, *sn_vul.filter_inactive_sw_installs*, has been introduced to determine whether inactive software installations should be filtered out for exposure assessment. By default, the property is enabled in the base system. When the filter is enabled, only active installations are displayed.

The **Discovery model** field specifically shows the count of active software installations, as the inactive ones are filtered out based on the default active=true filter on the Software Discovery Model table. The count in this field should match the filtered count displayed in the **Software installation count** field. The count in the **Software installation** field persists even if you update the system property. To obtain the updated count, you must run the scheduled jobs *Run exposure assessment for configured CVEs* and *Run software exposure that updates the count*.

Exposure assessment by CVE

Exposure assessment uses Common Vulnerabilities and Exposures (CVEs) to assess the exposure of your assets using the software discovery model. You can use the exposure assessment by CVE to identify exposure to potential vulnerabilities.

For information on assessing exposure by CVE, see:

- Add CVEs to assess exposure
- Create VIs for CVEs for exposure assessment
- Activate or deactivate CVEs for exposure assessment
- Export impacted CIs for exposure assessment
- Confidence score calculation example

Add CVEs to assess exposure

Add Common Vulnerabilities and Exposures (CVEs) to the exposure configuration list of CVEs in Exposure Assessment to assess the impact of a new vulnerability or zero-day vulnerability.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by CVE**.
2. Select **Add**.
3. In the Add CVE dialog box, select the CVEs you want to add to the list and select the **Add** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CVEs that are already in the list are not added again. The rest are added to the list of CVEs.

Note: Select the filter icon to navigate to the **Advanced view** and specify the CVEs you want to view.

4. To assess the impact of the CVEs that are already in the list:

   a. Select the check box of the CVEs that you want to reassess.

   b. Select the **Reassess** button.
   The updated details appear in respective columns.

Create VIs for CVEs for exposure assessment

Create vulnerable items (VIs) from the Exposure Assessment page. Vulnerability event managers then analyze this list of VIs and recommend solutions and patches that help the IT team to patch these vulnerabilities.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

About this task
After the exposure is assessed, the list for the potential assessment is displayed on the exposure assessment record with the configuration items (CIs) count. You can select the records and in the list action, select **Create Vulnerable items** to create vulnerable items (VIs) for the CIs where the vulnerable software is present and on the Common Vulnerabilities and Exposures (CVEs). VIs are created in the background. This process might take some time. After the items are created, you can navigate to the VI table to view the records created.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by CVE**.
2. Select the required CVEs and select the **Create Vulnerable Items** option.
3. In the Create vulnerable items dialog box, select the **Create vulnerable items** option.
4. Select the **View status** link to view the status of the background job used to create the VIs.

Activate or deactivate CVEs for exposure assessment

For delta processing of a CVE, you can activate it, thus adding it to the active list of CVEs.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

Note: Starting with version 4.0.1 of Vulnerability Exposure Assessment, if a Common Vulnerability Entry (CVE) has not been updated or had vulnerable items (VITs) created in the past 30 days, the exposure assessment record for that CVE is automatically marked as inactive. However, you can manually activate or deactivate these records. Additionally, the scheduled job *`Check potential vulnerability exposure`* runs continually to scan for such CVEs to designate them as inactive.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by CVE**.
2. Select the required active CVEs and select the **Deactivate** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The CVEs are deactivated.

Note: To activate software, follow the same process and select the **Activate** option.

3. Refresh the page to view the updated status (false) in the Active column.

Export impacted CIs for exposure assessment

You can track the impacted assets list for a new CVE by exporting the configuration items (CIs) related to an exposure assessment record to an excel sheet. This sheet can be used to share the assets details and owners to create incidents with the known impacted assets for the zero-day vulnerabilities.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by CVE**.
2. Select the Discovery model for the record whose CIs you want to export.
   The Software Installations tab contains the active CIs related to the software record. These CIs are stored in the **Installed on** column.
3. Select the **Export** option.
4. In the Export dialog box, select the File Type and Delivery Type to export the related CIs.
5. Select the **Export** option.

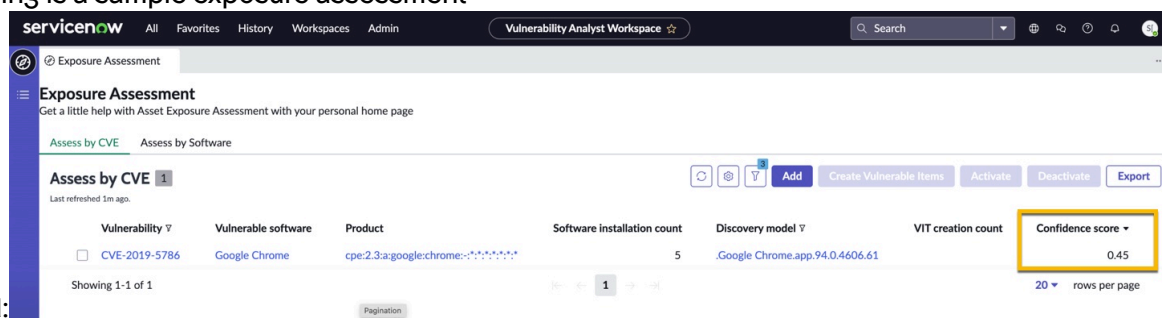
Confidence score calculation example

Example of calculating the confidence for a zero-day vulnerability based on its Common Vulnerabilities and Exposures (CVE) information.

Following is an example of calculating the confidence score from the Common Platform Enumeration (CPE) information of **CVE-2019-5786**.

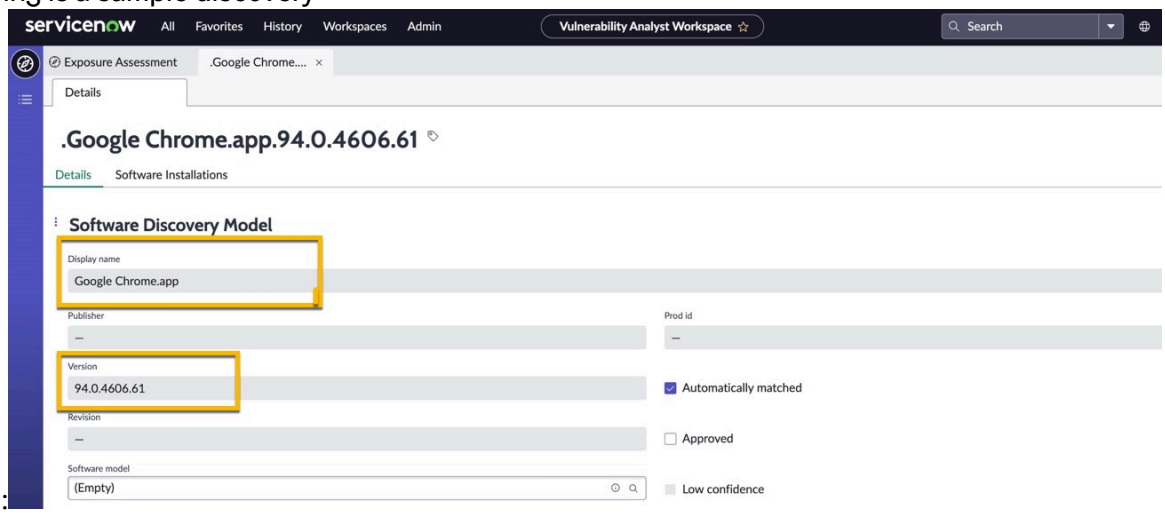
Note: To view the CPEs, you can group the Vulnerability column by vulnerability. For details on viewing the vulnerable software details, see View vulnerable software details.

Following is a sample exposure assessment record:



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Following is a sample discovery model:



How to calculate the confidence score

The confidence score range is 0–1. Based on the CPE information, the confidence score is calculated using the following formula:

```
((BASE SCORE) + (publisher score) +(product score) + (version
 score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

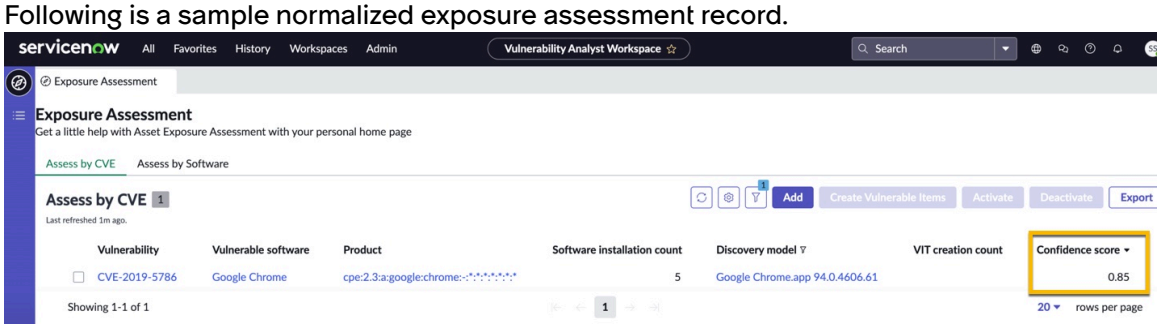
```
.45
```

Note: To refer to the values used to calculate the confidence score, see Confidence score reference tables for exposure assessment.

Calculating confidence score when the software model is matched with the normalized discovery model

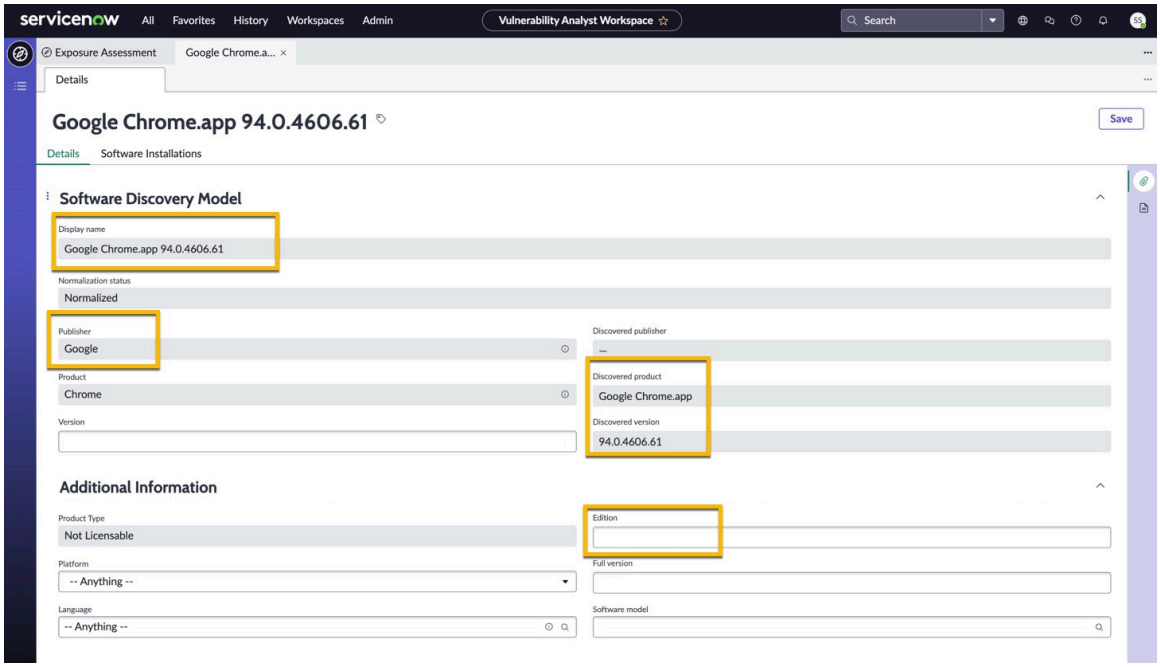
If you are using the normalized discovery model, the additional information available for the software discovery model provides an enhanced confidence score. Following is the sample calculation:

Following is a sample normalized exposure assessment record.



Following is a sample normalized discovery model.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




```
((BASE SCORE) + (publisher score) + (product score) + (version
 score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Note: To refer to the values used to calculate the confidence score, see Confidence score reference tables for exposure assessment.

View vulnerable software details

View the details of the vulnerable software, in this case, Google Chrome. It is matched against the discovery model and the Common Platform Enumeration (CPE). This CPE version impacts all the Google Chrome versions.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **All** and type in *sn_vul_software.LIST*.
2. In the list of vulnerable software, search for **cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*** to view the information.

Confidence score reference tables for exposure assessment

Reference values used to calculate the confidence score.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reference tables

Confidence score calculation reference table

Vulnerable software segment	Discovery model segment	Score	Discovery model exact match segment	Exact match score
Publisher	Display name	15	Publisher	5
Model	Display name	15	Model	5
Version	Display name	10	Version	5
Edition	Display name	3	Normalized edition	2
Display name	Display name	10	Display name	5

Confidence score summary table

Score	Value
Sum of all scores	75
Base score **Note:** Minimum score given to all matched discovery models.	25
Total score	100

Exposure assessment by software

Exposure assessment for zero-day vulnerabilities, when Common Vulnerabilities and Exposures (CVEs) for the asset or configuration item is not available. It uses the software information to assess exposure, using the software discovery model.

For information on assessing exposure by software, see:

- Add software for exposure assessment
- Create VIs for software for exposure assessment
- Activate or deactivate software for exposure assessment
- Export impacted CIs for software in the Vulnerability Assessment workspace

Add software for exposure assessment

Add a new software to the Exposure Assessment module to assess the impact of a new vulnerability or zero-day vulnerability.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Software** > **Add**.
2. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Publisher	Publisher of the software.
Product	Product name of the software.
Version	Version of the software product.
Edition	Edition of the software.

Note: If you try to add exposure for software that exists in the table with the status 'false', a duplicate record is not created. The status of the existing software is updated to 'true'.

3. Select the **Add** option.
4. To assess the impact of the software that are already in the list:
   a. Select the check box of the software that you want to reassess.
   b. Select the **Reassess** button.
   The updated details appear in respective columns.

Create VIs for software for exposure assessment

Create vulnerable items (VIs) from the Exposure Assessment page. Vulnerability event managers then analyze this list of VIs and recommend solutions and patches that help the IT team to patch these vulnerabilities.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Software**.
2. Select the records for which you want to create VIs.
3. Select the **Create Vulnerable Items** option.
4. In the Create vulnerable items dialog box, select from:
   - Existing vulnerability
   - New vulnerability
5. Select the **Create Vulnerable Items** option.

Activate or deactivate software for exposure assessment

To stop further delta processing of software, you can choose to deactivate it, thus removing it from the active list of software.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Software**.
2. To deactivate, select the required active software and select the **Deactivate** option.
   The software is deactivated.

   Note: To activate software, follow the same process and select the **Activate** option.

3. Refresh the page to view the updated status (false) in the Active column.

Export impacted CIs for software in the Vulnerability Assessment workspace

You can track the impacted assets list for new software by exporting the configuration items (CIs) related to an exposure assessment record to an excel sheet. This sheet can be used to share the assets details and owners to create incidents with the known impacted assets for the zero-day vulnerabilities.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Software**.
2. Select the discovery model for the record whose CIs you want to export.
   The Software Installations tab contains the active CIs related to the software record. These CIs are stored in the **Installed on** column.
3. Select the **Export** option.
4. In the Export dialog box, select the **File Type** and **Delivery Type** to export the related CIs.
5. Select the **Export** option.

Exposure assessment by publisher software

Assess exposure for zero-day vulnerabilities, when Common Vulnerabilities and Exposures (CVEs) for the asset or configuration item is unavailable. It uses the software information to assess exposure, using the software discovery model.

For information on assessing exposure by software, see:

- Add software by a publisher for exposure assessment
- Create VIs for software by a publisher for exposure assessment
- Activate or deactivate software by a publisher for exposure assessment
- Export impacted CIs for software by a publisher in the Vulnerability Assessment workspace

Add software by a publisher for exposure assessment

Add software by a publisher to the Exposure Assessment module to assess the impact of a new vulnerability or zero-day vulnerability.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Publisher** > **New**.
2. In the New assessment window, select the publisher for which you want to perform the assessment.
3. Select a date in the **CVE published from** field.
   If any of the Common Vulnerability Entries (CVEs) associated with the software is modified after the selected date, then that software is considered for exposure assessment.
4. Select the severity level of the CVE in the **CVE Severity** section.
5. Select **Start assessment**.
   Once the job is completed, the selected records are created.

Create VIs for software by a publisher for exposure assessment

Create vulnerable items (VIs) from the Exposure Assessment page to analyze the list of VIs and recommend solutions and patches that can help the IT team to patch the vulnerabilities.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Publisher**.
2. Select the records for which you want to create VIs.
3. Select the **Create Vulnerable Items** option.
4. In the Create vulnerable items dialog box, select from:
   - Existing vulnerability
   - New vulnerability
5. Select the **Create Vulnerable Items** option.

Activate or deactivate software by a publisher for exposure assessment

Activate or deactivate software by a publisher to stop delta processing of the software and remove it from the active list of software.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Publisher**.
2. To deactivate, select the required active software by a publisher and select the **Deactivate** option under the **Reassess** button.
   The publisher is deactivated.

   Note: To activate the software by a publisher, follow the same process and select the **Activate** option.

3. Refresh the page to view the updated status (false) in the Active column.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Export impacted CIs for software by a publisher in the Vulnerability Assessment workspace

You can track the impacted assets list for new software by exporting the configuration items (CIs) related to an exposure assessment record to an excel sheet. This sheet can be used to share the assets details and owners to create incidents with the known impacted assets for the zero-day vulnerabilities.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Exposure Assessment** > **Assess by Publisher**.
2. Select the discovery model for the record whose CIs you want to export.
   The Software Installations tab contains the active CIs related to the software record. These CIs are stored in the **Installed on** column.
3. Select the **Export** option.
4. In the Export dialog box, select the **File Type** and **Delivery Type** to export the related CIs.
5. Select the **Export** option.

Exploring vulnerability assessment

The Vulnerability Assessment Workspace is designed for the Vulnerability Event Manager to create a vulnerability event and to perform vulnerability assessment, especially during the zero-day vulnerability analysis.

You can use the vulnerability assessment workspace to manage critical vulnerabilities, such as:

- Zero-day vulnerabilities of critical or high severity
- New threat intel identified for a vulnerability
- Rapid exploitation of a vulnerability of critical or high severity.

Vulnerability Assessment Workspace and Vulnerability Crisis Management

As a vulnerability event manager, identify and create a vulnerability event record for vulnerabilities of interest. Once you create the vulnerable event, you can perform risk assessment, manually update the risk attributes, and calculate the risk score automatically. Using the Vulnerability Assessment Workspace, you can perform the following actions to handle vulnerability crisis event from inception to resolution.

- Create a vulnerability assessment record
- Modify the vulnerability assessment record
- Perform a vulnerability assessment
- Review the Assessment details
- Assign a priority and exposure level to the vulnerability assessment record
- Add affected CIs to the assessment record
- Create vulnerable items for the affected CI or affected software component
- Link the vulnerability assessment record to major security incident in Major Security Incident Management

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prerequisites for vulnerability assessment

Available versions

Application	Version
Vulnerability Crisis Management plugin	1.0
Vulnerability Response	20.0
Vulnerability Response with NVD **Note:** For more information, see Understanding the NVD integrations.	1.4.2
Vulnerability Response Integration with CISA	1.2
Data Model for SBOM	1.1.2
Software Bill of Materials Core	2.0.2
Software Asset Management	Software Asset Management Foundation plugin or Software Asset Management Professional plugin
Major Security Incident Management	2.2.5

Scheduled jobs

The following are the scheduled jobs.

Scheduled job name	Description
Vulnerability Assessment	Updates the affected configuration items table and the source of the CI if vulnerable items (VITs or AVITs) are created after the assessment. **Note:** This scheduled job runs daily. It runs for a longer period than the other scheduled jobs.

Related topics

Vulnerability Crisis Management

Create a vulnerability assessment record

Create assessment records for vulnerabilities of interest. After you create the assessment, you can initiate initial risk assessment, manually update the record, and calculate the risk score automatically.

Before you begin

You need to be part of the base system Vulnerability Assessment Event Manager assignment group to be able to perform the tasks associated with vulnerability assessment.

Role required: sn_vul_analyst.vul_event_manager, sn_vul_analyst.emergency_response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can create a vulnerability assessment record for vulnerabilities of interest either by associating the event record to a primary CVE or to an affected product.

Procedure

1. Navigate to **All** > **Workspaces** > **Vulnerability Assessment Workspace**.
2. Select the **Vulnerability Assessment** icon.
3. Select **New**.
4. Enter an appropriate title in the **Title** field.
5. **Optional:** Select a primary CVE to associate with the new assessment record from the **Primary CVE** field.

   Note: All the preliminary details on the assessment record are populated based on the product that you select or create or the primary CVE that you associate with the record.

6. Select **Submit**.
   The vulnerability assessment record with the title you had entered is created and displays in a new vulnerability assessment tab. By default, the vulnerability assessment record displays in the **Details** tab.

   Note: By default, the details of the primary CVE associated/ mapped are displayed.

   - If no primary CVE is selected during the vulnerability assessment event record creation, a default record is created.
   - If the primary CVE has associated CVEs then the related CVEs are populated in the **Vulnerability Entries** tab. You can add more associated CVEs from the **Vulnerability Entries** tab.

7. Navigate to the **Affected Products** tab.

   a. Select **New**.

   b. On the form, fill in the fields.

Field	Description
Publisher	Publisher of the software. This is a mandatory field.
Product	Product name of the software. This is a mandatory field.
Version	Version of the software product.
Edition	Edition of the software.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you try to add vulnerability for software that exists in the table with the status 'false', a duplicate record is not created. The status of the existing software is updated to 'true'.

c. Select **OK**.

8. Select **Save**.

Update the vulnerability assessment auto-flush record

Update the vulnerability assessment auto-flush record.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

About this task
In the base system, the vulnerability assessment records retention period is set to 6 months. If any vulnerability assessment record state is closed, then the vulnerability assessment records will be stored only till the defined retention period and the related records of that assessment will be removed after 6 months from all the related tables.

Procedure

1. Navigate to **All** > **Auto Flushes**.
2. Open the record with table, sn_vul_analyst_vulnerability_assessment.
3. Select the **Active** check box to activate the auto-flush option for the vulnerability assessment record.
4. Click **Update**.

Modify the vulnerability assessment record

Update the Vulnerability Assessment record, post it’s creation. Based on the field's values you can calculate the risk score.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

About this task
After the primary CVE is added to the vulnerability assessment, the record is moved to a Pending Assessment state. You can further add other related CVEs in the **Vulnerability Entries**tab or add the products affected by this vulnerability from the **Affected Products** tab. You can make further modifications to the **Risk Assessment** fields and the **Risk Score** for the assessment record is automatically updated accordingly.

Procedure

1. Navigate to **All** > **Vulnerability Assessment Workspace** > **Vulnerability Assessment**.
2. On the **Details** tab, update the fields.

Field	Description
Title	Title describing the vulnerability event record.
Primary CVE	Primary CVE which you associated with the event record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
State	Current state of the event record.
Priority	Priority of the event record on a scale of 1-5.
Alert Source	Source of the potential vulnerability event.
Risk Score	Auto-calculated risk score. Not editable by default.
Exposure-level	The exposure level of the vulnerability event on a scale of 1-5.
Assignment Group	The assignnment group to whom the event record is assigned.
Assigned To	The user the event record is assigned to.
Description	Detailed description of the event record.

3. Navigate to the **Vulnerability Entries** tab to add associated or related CVEs.
   a. Select **New**.
   b. Search for the record in the **Vulnerability entry** field.
   c. Select the vulnerability record you want to associate with the assessment record.
   d. **Optional:** Select **Browse** to browse and attach a file.
   e. Select **Save**.
   The vulnerability records you selected are added to the assessment record and display in the **Vulnerabilities Entries** tab.
4. **Optional:** Add affected products.
5. Add related link to the assessment record.
6. Modify the **Risk Attributes** for the primary CVE associated with the vulnerability assessment event record.

Field	Description
Memory corruption	Indicates whether this event record can corrupt memory.
Remote code executable	Indicates if the remote code execution is possible.
Local privilege escalation	Indicates if local privilege escalation vulnerability exists.
Unauthorised access	Indicates if unauthorised access vulnerability exists.
DDOS	Indicates if the potential event could involve Distributed Denial of Service.
Attack Complexity	Indicates the complexity of the attach. Options are Low, Medium, or High.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Attack vector	Indicates the potential pathway or method of attack. Options are– Network, Adjacent network, Local, Physical, None.
Privileges required	Indicates the level of privileges an attacker required to exploit the vulnerability. Options are None, Low or High.
User interaction	Indicates whether or not user interaction is needed to exploit the vulnerability.
Confidentiality impact	Indicates the measure of the potential impact on confidentiality of the vulnerability. Options are None, Low, or High
Scope change	Indicates if the scope if the assessment has changed.
Availability impact	Indicates the potential impact to availability of a successfully exploited misuse vulnerability. Availability refers to the accessibility of information resources. Options are None, Low, or High
Integrity impact	Indicates the potential impact to integrity of a successfully exploited misuse vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. Options are None, Low, or High
Remediation level	Indicates the status or availability of remediation for the vulnerability. Options are Official Fix, Temporary Fix, Workaround, Unavailable, Not defined.
Exploit code maturity	Indicates the likelihood of the vulnerability being exploited based on the existing state of exploit techniques and code availability. Options are Unproven, Proof-of-concept, Functional, High, and Not defined.
Report confidence	Indicates how confident you are that the vulnerability exists.

7. Enter relevant comments in the **Compose** field.
   - Enter your work notes in the **Work notes (Private)** field.
   - Enter your comments (visible to everyone) in the **Comments** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. **Save** the assessment record.
   Based on the updates you made to the **Risk attribute** fields for the primary CVE or the affected product associated with the assessment record, the **Risk score** field is automatically updated.

   Note: To modify the base system risk score calculator rules or criteria, navigate to **All** > **Vulnerability Assessment Calculators** > **Vulnerability Assessment Risk Calculator** > **Vulnerability Assessment Risk Rule**. You can add criteria and modify the field level weightage to existing criteria as needed.

What to do next
Perform an initial assessment of the event record.

Delete associated CVEs or affected products from the vulnerability assessment record

Delete a vulnerability event record if it is no longer required.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

About this task
You can delete CVEs or affected products associated with the vulnerability assessment record. You can only delete vulnerability entries/associated CVEs or affected products if they are in **New** or **Pending assessment** states.

Procedure
1. Navigate to **All** > **Workspaces** > **Vulnerability Assessment**.
2. Select the vulnerability assessment record.
3. Select the **Vulnerability Entries** tab or the **Affected Products** tab.
4. Select the associated CVE or the affected product record.
5. Select **Delete**.

   Note: The **Delete** button displays only for an assessment record when they are in **New** or **Pending Assessment** states.

Add related link to the assessment record

Add additional links and information related to the assessment record.

Before you begin
Role required: sn_vul_analyst.vul_event_manager

Procedure
1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace**.
2. Select the assessment record entry.
3. Select the **Related Links** tab.
4. Enter a relevant description in the **Description** field.
5. Enter the URL in the **Link** field.
6. Select **OK**.
   The related link is added and listed on the Related Links tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Perform an assessment

After you've created the vulnerability assessment record and updated the risk attribute fields, run an assessment of the event record.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

About this task

Perform an initial assessment after an event for a vulnerability of interest has been created and determined to present risk to systems and data. The purpose of this activity is to further analyze the threat by updating the risk assessment with an in-depth exposure assessment.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Vulnerability Assessment**.
2. Select the relevant record from the list of vulnerability assessment event records.
3. Select **Assess** to run the vulnerability assessment.
   The Vulnerability Response - Process vulnerability assessment event background job is initiated and a relevant notification displays.
4. Select **View Status** on the notification to view the status of the running job.
5. Select **Save**.

   The **Assessments** tab displays assessment details. When the assessment is processed the VITs or AVITs associated with the vulnerable entries or CVEs display in the **Vulnerable Items** or the **Application Vulnerable Items** tab.

Result

- Vulnerable items or TPEs related to the associated CVEs are fetched during assessment. The CIs related to the vulnerable items are also identified and display in the Affected Configuration Items table.
- If the associated CIs do not exist in the affected CI table, the identified CIs are added to the table and the **Has vulnerable item** field value is set to **True**, and the **Source** field's value is set to Scanner.
- If the CI already exists in the affected CI table, only the **Has vulnerable item** field value is set to **True** and the **Source** fields value for the CI remains the same as when the assessment record was created.
- If vulnerable items are created after the assessment a Vulnerability Assessment scheduled job is run to update the affected CIs table and the source of the CI.

What to do next

- Assign a priority and exposure level to the vulnerability assessment record
- Add affected CIs to the assessment record
- Create vulnerable items for the affected CI or affected software component
- Add related link to the assessment record

Related topics

Assessment tab

Overview tab

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assessment tab

Review the assessment results in the assessment tab. After you perform an assessment of the vulnerability event, the record is correlated against the data from Software Bill of Materials and Software Asset Management and displayed with visualisations.

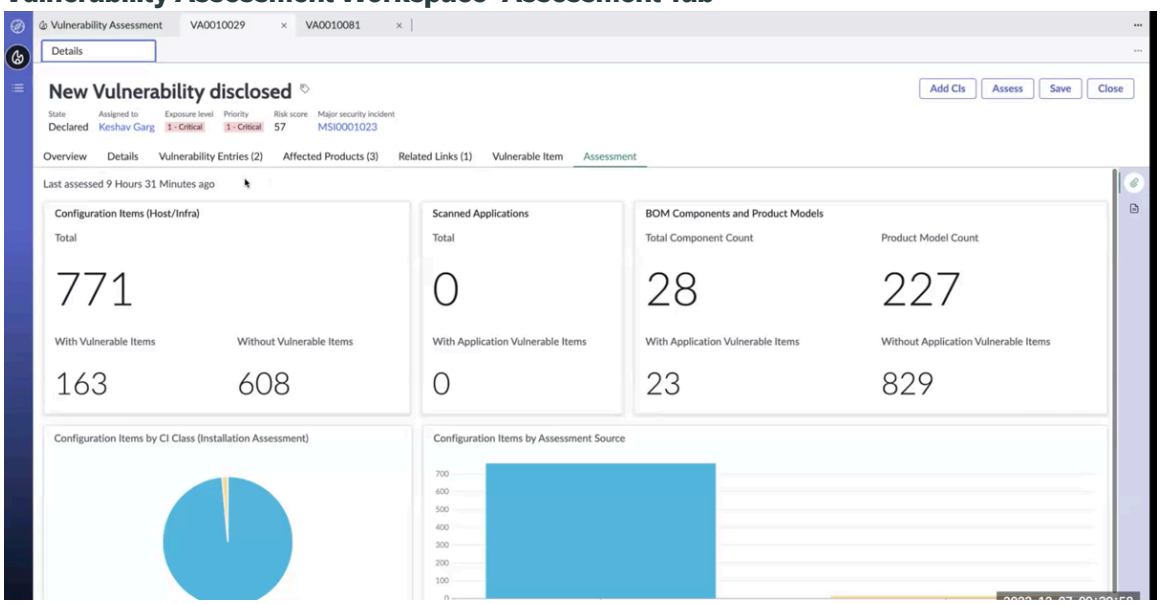
The assessment tab populates data (if available) based on the assessment record that you create and correlates the details against assessments from Software Asset Management and Software Bill of Materials component data in the CMDB.

How the assessment works

On selecting the **Assess** button, an assessment for all the related CVEs and affected products using both Software Asset Management and SBOM data is initiated. A background job is triggered and when the assessment is processed the VITs or AVITs associated with the vulnerable entries or CVEs display in the **Vulnerable Items** and **Application Vulnerable Items** tabs.

- All the vulnerable items or TPEs related to the CVE are identified.
- The Configuration Items (CIs) related to the vulnerable items are also identified and display in the affected configuration items table.
- If the CIs are not present in the affected CI table, the identified CIs are added to the table and the **Has vulnerable item** flag is turned to true, and the **Source** field's value is set to Scanner.
- If the CI already exists in the affected configuration items table, only the **Has vulnerable item** flag is set to true and the **Source** remains unchanged from when the assessment record was created.
- If vulnerable items are created after the assessment a Vulnerability Assessment scheduled job is run to update the affected CIs table and the source of the CI.
- On the Assessment workspace, you can view timestamps to see the last assessment of the events. The **Assessment** tab is visible only when the new assessments are created. If the assessment is in progress state, then the last assessment status will appear as the assessment is in progress. To view the updated assessment status, you need to refresh the page. Once the assessment is completed, the user will be able to see all the related tabs for that assessment.

Vulnerability Assessment Workspace- Assessment Tab



The assessment details displays for the following widgets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Configuration Items (Host/Infra)
- Scanned Applications
- BOM Components and Product Models
- Configuration Items by CI Class (Installation Assessment)
- Configuration Items by Assessment Source – Displays the Affected Configuration Items list.

Data visualizations

Name	Type	Description
Configuration Items (Host/Infra)	Single Score	Displays the count of CIs with and without VIs. The Configuration Items widget displays the total count of CIs that are found to be associated with the assessment record. The widget further displays the configuration items with vulnerable items and without vulnerable items.
Scanned Applications	Count	Total count of applications scanned with AVITs. **Note:** You can view the count of scanned applications for both primary and secondary CVEs.
BOM Components and Product Models	Single Score	Total Component count, Product model count, With Application Vulnerable Items, Without Application Vulnerable Items count.
Configuration Items by Assessment Source	Stacked bar	Affected Configuration Items stacked by the assessment source.
Configuration Items by CI Class (Installation Assessment)	Pie Chart	Configuration Items stacked by CI Class.

Overview tab

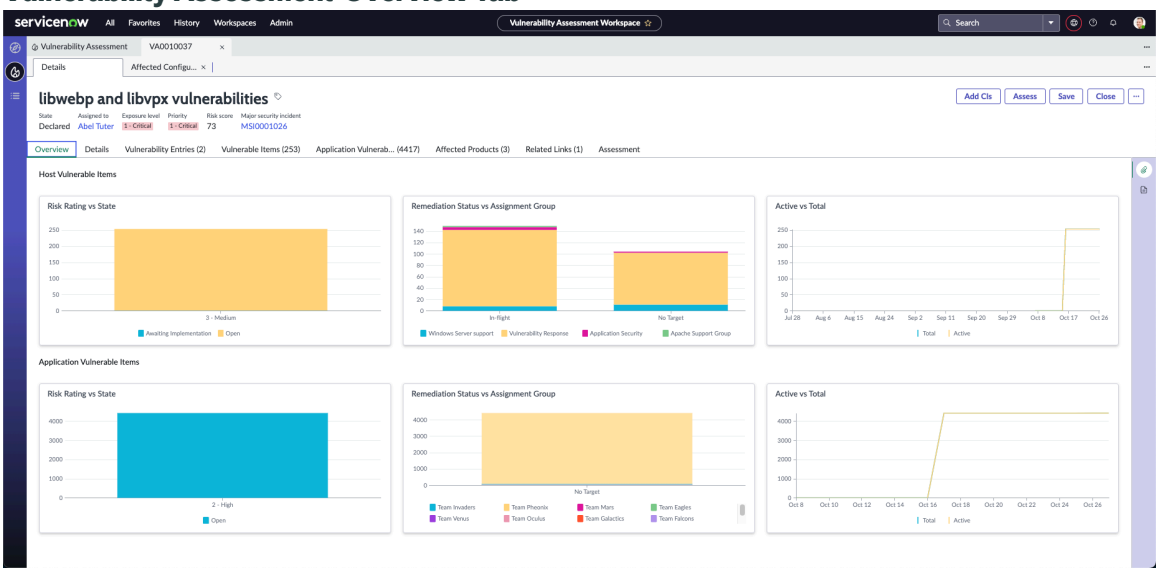
Overview of the assessment details display in the Overview tab. After you perform the initial assessment the record is correlated against the data from Software Bill of Materials and Software Asset Management and displayed with visualisations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab

The Overview tab populates data (if available) based on the assessment record that you create and correlates the details against assessments from Software Asset Management and Software Bill of Materials data in the CMDB. The

Vulnerability Assessment-Overview Tab



The assessment details displays for the following widgets.

- Host Vulnerable Items (Host/Infra)
  - Risk Rating vs State
  - Remediation Status vs Assignment Group
  - Active vs Total
- Application Vulnerable Items
  - Risk Rating vs State
  - Remediation Status vs Assignment Group
  - Active vs Total

Data visualizations

Host Vulnerable Items

Name	Type	Description
Risk Rating vs State	Stacked bar	State of the vulnerable items stacked by their risk rating.
Remediation Status vs Assignment Group	Stacked bar	Remediation status of the vulnerable item stacked by its assignment group.
Active vs Total	List and Line	Total vulnerable items associated with this entry versus active vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application Vulnerable Items

Name	Type	Description
Risk Rating vs State	Stacked bar	State of the application vulnerable items stacked by their risk rating.
Remediation Status vs Assignment Group	Stacked bar	Remediation status of the application vulnerable item stacked by its assignment group.
Active vs Total	List and Line	Total application vulnerable items associated with this entry versus active vulnerable items.

Assign a priority and exposure level to the vulnerability assessment record

Manually assign priority and exposure level to the vulnerability assessment record.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment workspace**.
2. Select a vulnerability assessment record.
3. Navigate to **Risk Attributes** in the **Details** tab.
4. Select a **Priority** from the list of options.
5. Select an **Exposure Level** from the list of options.
6. Select **Save**.

Add affected CIs to the assessment record

Manually add the CIs in your organization that you think should be associated with the vulnerability assessment record but do not display in the affected CIs after initial assessment.

Before you begin

Role required: sn_vul_analyst.vul_event_manager

About this task

Add CIs that you know may have been impacted but do not show up after the assessment is done. You can only add CIs when the assessment record is in **Declared** or **Pending assessment** state.

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace**.
2. Select the required assessment record from the list.
3. Select **Add CIs**.
4. Select the configuration items from the Configuration Items dialog box.
5. Select **Add CIs**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Vulnerability Response- Add Configuraton Items to Event background job initiates and a relevant notification displays.

6. Select **View Status** on the notification to view the status of the running job.

Result
Records are added to the Affected Configuration Items table with **Source** as *Manual*.

What to do next
Navigate to the **Assessment** tab, and refresh the **Configurations Items (Host/Infra)** widget to view the CIs that you added.

Create vulnerable items for the affected CI or affected software component

Create vulnerable items (VIs) or application vulnerable items (AVITs) from the Vulnerability Assessment Workspace. Vulnerability analysts analyze the list of VIs and recommend solutions and patches that help the IT team to patch these vulnerabilities.

The vulnerability event manager should be able to select one, many or all of the exposure search results to create Vulnerability Items.

- Application vulnerable item for SBOM assessment results that don't have AVITs associated
- Vulnerable Items for configuration items that don't have VITs associated
- Associate primary CVE to the vulnerability items.

Create VIs for configuration items without vulnerable items associated

Create vulnerable Items VITs for configuration items identified through the vulnerability assessment but don't have VITs associated with the record.

Before you begin
Role required: admin

Procedure

1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Assessments**.
2. Select the assessment record to which you need to create the VIT.
3. Select the **Assessment** tab.
4. Select **Without Configuration Items** count from the **Configuration Items (Host Infra)** widget.
5. Select the Configuration Items for which you want to create VITs from the **Affected Configuration Items** list.
6. Select **Create Vulnerable Item**.
   The Vulnerability Response - Create Manual VITs Vul Assessment background job is initiated and a relevant notification displays.
7. Select **View Status** on the notification to view the status of the running job.
   Vulnerable Items for the affected configuration items that you selected are created.

   The **Configuration Items (Host Infra)** widget will now display the same CI in the **With Vulnerable Items** count.

Create application vulnerable items (AVITs) for affected products models or components with no associated application vulnerable items

Create application vulnerable items (AVITs) for affected products or components items identified through the vulnerability assessment but don't have AVITs associated with the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

Procedure
1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace** > **Assessments**.
2. Select the assessment record to which you need to create the VIT.
3. Select the **Assessment** tab.
4. Select **Without Application Vulnerable Items** count from the **BOM Components and Product models** widget.
5. Select the affected product models for which you want to create AVITs from the **Affected Product Models** list.
6. Select **Create Application Vulnerable Item**.
   The Vulnerability Response - Create Manual VITs Vul Assessment background job is initiated and a relevant notification displays.
7. Select **View Status** on the notification to view the status of the running job.
   Application vulnerable Items for the affected product models items that you selected are created. for the primary CVE associated with the record.

   The **BOM Components and Product models** widget will now display the same product model or component in the **With Application Vulnerable Items** count.

Link the vulnerability assessment record to major security incident in Major Security Incident Management

You can link, propose or promote the assessment record to a Major Security Incident provided you have access to the Major Security Incident Management application.

Before you begin
Role required: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

About this task
You can move the assessment record to be associated with an existing major security incident, create a new MSI from the assessment record or promote the vulnerability assessment record to a major security incident. Leverage the Major Security Incident Management features such as the integrations with Microsoft Teams and Microsoft SharePoint.

You can also view the link to major security incidents on the Vulnerability Manager Workspace for vulnerable items. The MSIM link will be associated with the vulnerable assessment which will be shown on the vulnerability items and as well as on the other workspaces of Vulnerability Response.

Procedure
1. Navigate to **Workspaces** > **Vulnerability Assessment Workspace**.
2. Select the assessment record you want to link to a major security incident.
3. Select the **More Actions** icon, on the **Details** tab.
4. Select one of the following.

Option	Description
Link to Major Security Incident	Select the existing MSI record from the list of Major Security Incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	The vulnerability assessment record is linked to the existing major security incident.
Propose as Major Security Incident	Enter the following details and select **Propose**. ○ Detection Date ○ Justification ○ Potential Impact
Promote as Major Security Incident	Enter the following details and select **Promote**. ○ Detection Date ○ Estimated resolution date ○ Justification ○ Potential Impact

5. Select **Save**.

What to do next

Select the MSI record to open the record in the Major Security Incident Management view.

Related topics

- Link to Major Security Incident
- Propose as a Major Security Incident
- Promote to a Major Security Incident

Software Bill of Materials

View a list of the open source and third-party software components that you're using in your application development. Get insights into software licenses, version information, and the known vulnerabilities in your components in the Software Bill of Materials (SBOM) files that you upload into your instance.

Get started

Explore	Configure	Use
		
Learn about SBOM concepts and features.	Configure SBOM applications.	Learn how to import SBOM components and view data in the workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	Reference  Get details about SBOM forms, fields, tables, and properties.	

Troubleshoot and get help

- Security Operations community
- CycloneDX - Software bill of Materials (SBOM).
- SPDX.
- Search the Known Error Portal for known error articles.
- Contact Customer Service and Support.

Exploring Software Bill of Materials

Identify the components used in your organization's applications from Software Bill of Materials (SBOM) files you upload into your instance. Understand any risks associated with using open-source software to help you determine your potential exposure, view license compliance, and fix vulnerabilities.

Software Bill of Materials overview

Third-party and open-source components provide you with many advantages for the rapid creation and release of your software projects. However, in some cases, there are risks associated with using publicly accessible components, such as the following:

- Lack of visibility into component integrity
- Vulnerabilities in the open-source software
- Package Intelligence for open-source software
- Non-compliant software licenses

You can upload your software bill of material files via an API or manually. View the files that you import as entities, which are inventories of the third-party component libraries used in your software, including any transitive dependencies and available licensing information.

For more information about what is included in the software inventories in CycloneDX and SPDX SBOMs, see CycloneDX - Software Bill of Materials (SBOM) and SPDX.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Software Bill of Materials users

Users

User	Description
Vulnerability managers and analysts	View uploaded software bill of materials files in records, data visualizations, as well as enhanced vulnerability intelligence in the Software Bill of Materials (SBOM) Workspace. Vulnerability managers and analysts use this information to help them determine your software licensing compliance and the potential risk exposure with using open-source software.
Users that might include but are not limited to: • Technology or software lawyers • IT managers • Auditors • Software asset managers and teams	View uploaded proprietary and open-source software licenses for components of your uploaded SBOM files. Build a database of proprietary and open-source software licenses for the components. Review and classify licenses with missing information according to your internal or regulatory policies. Match your components to licenses and determine your overall license compliance and see your potential risk exposure to banned, restricted, or missing licenses.

Software Bill of Materials workflow

The SBOM applications enable you to upload files and view details for entities, component inventories, vulnerabilities, and software license information in the Software Bill of Materials (SBOM) Workspace.

- Upload SBOM files with an API or manually.
- Review the components in the SBOM file you uploaded in the SBOM Workspace.
- Review component license information from uploaded SBOM files and classify them to help you identify your exposure to restricted or banned licenses.
- Assess your risk exposure and create vulnerable items for components that have associated vulnerabilities.
- View reports and dashboards as well as your overall license compliance for uploaded SBOM components on the Home page in the SBOM Workspace.

Software Bill of Materials benefits

Three Software Bill of Materials applications enable you to view an accurate inventory of your software components and associated risks:

- Data Model for SBOM
- SBOM Core
- SBOM Response

For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SBOM benefits

Benefit	Application	Supported versions
This application provides the tables used to store SBOM data. This application is required. It includes the tables, ACLs, and roles that are required to read SBOM data.	Data Model for SBOM	v4.0, v3.0, v2.0
This application is required. It Includes the API required to upload SBOM documents and the business logic required to parse and import the data from those documents into your instance. You can view an inventory of your software components in the SBOM Workspace, but you cannot view the data visualizations on the landing page. Upload, parse, and process your software bill of materials files in CycloneDX and SPDX standards. Refer to the Supported versions column for the supported file formats and versions for these products. View bill of materials (BOM) entities and an inventory of your software components. A BOM entity is the root level component in an SBOM file. For example, for a CycloneDX SBOM, the component listed in the metadata is considered the BOM entity.	SBOM Core	v6.0, v5.0, v4.0 Starting with version 4.0, SBOM Core supports: • XML and JSON versions 1.0 through 1.6 of CycloneDX. • JSON versions 2.2 through 2.3 of SPDX.
• SBOM Response is required if you want access to the features and data visualizations on the landing page in the SBOM Workspace. • SBOM Response requires the Vulnerability Response application. • View your component inventory and assess your risk exposure in the SBOM Workspace. Set up rules to create application vulnerable items (AVITs) automatically and remediate them with the Application Vulnerability Response workflow. • View component license information that is uploaded with your SBOM files in the License administration module. Classify and resolve (match) the components you upload in your Application Vulnerability Response files to licenses so you can see the state of your over-all license compliance. • Starting with version 4.0 of Application Vulnerability Response Response, you can view components that are identified as stale or abandoned as 'Non-compliant' in the Policy as Code Engine (PaCE) interface that is available in the SBOM Workspace.	SBOM Response	v6.0, v5.0, v4.0

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SBOM benefits (continued)

Benefit	Application	Supported versions

• The OSV.dev and Deps.dev integrations are included when you install SBOM Response.
  ○ OSV.dev is an open-source API that provides vulnerability intelligence information for a given version of a package or library.
  ○ Deps.dev is an open-source API that provides a version list for a given package or library and identifies components that are in **Stale** and **Abandoned** states.
See Configuring the Deps.dev, OSV.dev, and PaCE integrations for Software Bill of Materials for more information.
See Integrating PaCE with other applications for more information about PaCE and PaCE policies.		

Generate and upload Software Bill of Materials (SBOM) files for software throughout its continuous integration and continuous deployment development cycles.	SBOM Response	• Data Model for SBOM: v1.4 and later. • SBOM Core: v3.0 and later. • SBOM Response: v4.0 and later.

Vulnerability Response applications and CSDM tables

The Vulnerability Response, Application Vulnerability Response, third-party vulnerability integrations and Software Bill of Materials applications manage (contribute data to) CSDM tables. These applications also use data from CSDM tables that other applications generate. Several ServiceNow products, therefore, benefit from and add value to these Security Operations applications. See Vulnerability Response applications and CSDM tables for more information.

What to explore next

To learn more about configuring and using Software Bill of Materials, see:

- Exploring supported applications for Software Bill of Materials
- Configuring Software Bill of Materials
- Uploading and viewing your SBOM files in the SBOM Workspace
- Viewing reports and dashboards in the Software Bill of Materials workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring supported applications for Software Bill of Materials

Third-party vulnerability intelligence and other integrations with the Software Bill of Materials applications can enhance the data of your uploaded files.

Supported applications benefits

Third-party vulnerability intelligence and other integrations with the Software Bill of Materials applications permit you to view counts for components that are considered stale and abandoned, as well as information about if you can fix any vulnerabilities associated with components.

The ServiceNow® applications and third-party integrations listed in the following table are supported by the SBOM applications. These applications provide you with enriched vulnerability data, vulnerability intelligence, and other key information that can help you view and prioritize the vulnerabilities associated with SBOM files. All these applications and integrations are available from the ServiceNow® Store.

Supported applications and third-party integrations

Benefit	Application	Supported versions	Users
Vulnerability Response is required if you install the SBOM Response application. Install The Vulnerability Response application prior to installing SBOM Response. Application Vulnerability Response features are installed with Vulnerability Response. These features enable access to the Vulnerability Manager Workspace in the Vulnerability Response application and the vulnerability workflow to help you remediate application vulnerable items (AVIT)s.	Vulnerability Response	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes.	
View enhanced NVD vulnerability and severity data. View imported data from the NVD and CWE integrations to enrich any vulnerability data	Vulnerability Response Integration with NVD and SBOM Response	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supported applications and third-party integrations (continued)

Benefit	Application	Supported versions	Users
you might find in your SBOM data. See Importing data with the NVD and CWE integrations and managing third-party libraries for more information.		and Release Schema Changes.	
Import software bills of material files with the Veracode Vulnerability Integration. The Veracode Vulnerability Integration includes the following enhancements with Veracode SBOM files: • If you have installed SBOM Response, you have the option to include vulnerabilities found by SBOM for the SBOM files you upload. • SBOM is mapped to the Source field for records in the Bill of Materials [sn_sbom_doc] table for the SBOM SBOM files that you upload. See Veracode Vulnerability Integration for more information.	Veracode Vulnerability Integration and SBOM Response	Starting with version 4.3 of the Veracode Vulnerability Integration. If you have the Veracode Vulnerability Integration already installed, you can also upload imported Veracode SBOM data in CycloneDX (JSON and XML) and SPDX (XML) formats starting with version v3.0 of SBOM Core. For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes.	
Upload SBOM files to the ServiceNow AI Platform from your GitHub repositories. Determine if SBOM files generated in your CI/CD (continuous integration and continuous delivery/	Obtain any required GitHub Actions for SBOM upload in the GitHub Marketplace.	Starting with version 4.0 of SBOM Core.	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supported applications and third-party integrations (continued)

Benefit	Application	Supported versions	Users
deployment) pipelines have been successfully queued in your ServiceNow AI Platform instance. Protect your environments from potentially harmful components during software development cycles with GitHub Actions that you initiate from your GitHub environment.			

Configuring Software Bill of Materials

Download and activate the required applications for the Software Bill of Materials (SBOM) application prior to uploading SBOM files.

Configuration overview

1. Download the required SBOM applications and any additional supported applications and integrations you want from the ServiceNow Store into your ServiceNow instance. See Exploring Software Bill of Materials and Download an application from the ServiceNow Store for the first time for more information about supported applications.

   The Vulnerability Response application is required for SBOM Response. Install The Vulnerability Response application prior to installing SBOM Response.

2. Locate the SBOM applications that you downloaded and select Install to activate them along with their dependencies in the following order. See Install the supported applications for Software Bill of Materials.

   - Vulnerability Response and its dependencies
   - Vulnerability Response Integration with NVD
   - Data Model for SBOM
   - SBOM Core
   - SBOM Response, which includes the OSV.dev and Deps.dev integrations and access to the capabilities of Policy as Code Engine (PaCE) in the SBOM Workspace.

3. Configure the Deps.dev and OSV.dev integrations. These integrations are included with the SBOM Response application and are installed and activated automatically. You must initiate the OSV.dev Integration - Comprehensive on-demand from its integration record. See Configuring the Deps.dev, OSV.dev, and PaCE integrations for Software Bill of Materials and Exploring Software Bill of Materials for more information.

   The Deps.dev Integration provides you with information about components that are in **Stale** and **Abandoned** states for a given version of a package or library that you upload in your SBOM files.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OSV.dev pulls vulnerability data from an open source database for a version of a package or library you upload in your SBOM files.

4. Refer to product documentation to configure any additional supported applications and integrations you installed. See Vulnerability Response integrations and Integrating Application Vulnerability Response with other applications.

Install the supported applications for Software Bill of Materials

Download and activate the required applications for the Software Bill of Materials (SBOM) application prior to uploading files.

Before you begin

Roles required: admin for download, installation, and activation of all applications and role assignments in your instance.

About this task

Procedure

1. Download the required SBOM applications from the ServiceNow Store into your ServiceNow instance.

   These applications enable you to upload and import SBOM files into your instance. You can view BOM entity and component data in the SBOM Workspace if you have SBOM Core installed.

   You can view BOM entity, component data, and data visualizations in the SBOM Workspace if you have SBOM Response installed.

   - Data Model for SBOM
   - SBOM Core

   For more information about downloading and activating applications, see the following:

   - Security Operations and the ServiceNow Store
   - Download an application from the ServiceNow Store for the first time

2. **Optional:** If you want to view your SBOM data in the SBOM Workspace, view imported third-party vulnerability intelligence, assess your risk exposure, and remediate vulnerabilities with the Application Vulnerability Response and Vulnerability Response workflows, download the following applications:

   - Vulnerability Response and its dependencies
   - Vulnerability Response Integration with NVD
   - SBOM Response

   For more information about these and other supported SBOM applications, see Exploring Software Bill of Materials.

3. After you have downloaded the applications, navigate to **All** > **System Applications** > **All Available Applications** > **All**.
4. Locate the SBOM applications that you downloaded and select **Install** to activate them along with their dependencies.

   A message is displayed after an application is successfully activated. Activate the applications in the following order:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Vulnerability Response and its dependencies
- Vulnerability Response Integration with NVD
- Data Model for SBOM
- SBOM Core
- SBOM Response, which includes the OSV.dev and Deps.dev integrations and supports the Policy as Code Engine (PaCE) interface in the SBOM Workspace.

See Configuring the Deps.dev, OSV.dev, and PaCE integrations for Software Bill of Materials for more information about configuring these integration applications after you have installed SBOM Response.

5. **Optional:** Activate integrations by navigating to **All** > **System Applications** > **All Available Applications** > **All** and selecting **Install**.

   (Optional) For more information about these integrations and the capabilities they provide, see Exploring Software Bill of Materials.

   - Vulnerability Response Integration with Veracode. See Install the ServiceNow Vulnerability Response Integration with Veracode for more information.
   - Vulnerability Response Integration with NVD, which is required if you want to view the enhanced data for vulnerabilities associated with uploaded components. See Understanding the NVD integrations for more information.
   - CWE Comprehensive 2000 Integration. See Configure and run the scheduled job for updating CWE records for more information about activating this scheduled job.

   A message is displayed after an application is successfully activated.

6. Assign the following roles to users.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolver
7. **Optional:** Assign users to the App-Sec Manager group if you are creating application vulnerable items for vulnerabilities in your imported SBOM data.

   (Optional) Users assigned to the App-Sec Manager group prioritize and manage application vulnerable items. Users in this group inherit many of the roles required for reading and editing records and configuring the applications supported by the Application Vulnerability Response application and its remediation workflows.

8. **Optional:** Deactivate the Reopen AVITs if detected (*sn_sbom_resp.reopen_avits_if_detected*) system property if you don't want **Closed** AVITs to transition back to the **Open** state automatically.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(Optional) A **Closed** application vulnerable item (AVIT) for a component with an associated vulnerability is re-opened (set to **Open**) automatically and visible in the SBOM Workspace if the following conditions exist:

- The AVIT with the associated vulnerability is detected again by a third-party integration's vulnerability scans or the component with the vulnerability is part of a subsequent SBOM upload.
- You have not deactivated the Reopen AVITs if detected (*sn_sbom_resp.reopen_avits_if_detected*) system property. This system property is activated by default.
- The substate of the **Closed** AVIT is not one of the following: **Mitigation Control in Place**, **Not Affected**, or **False Positive**. AVITs with these substates are not reopened by the system property.

What to do next

Upload your SBOM files. See Upload Software Bill of Materials files manually and Uploading Software Bill of Materials files using a REST API for more information.

Configuring the Deps.dev, OSV.dev, and PaCE integrations for Software Bill of Materials

You can edit some of the parameters for the Deps.dev and OSV.dev integrations. There are also two code trigger versions of these integrations that are used strictly for internal workflows, and you should not initiate these integrations on-demand. Additionally, you can activate a scheduled job to create policies using Policy as Code Engine (PaCE).

Code trigger integrations for internal workflows

Starting with v3.2 of SBOM Response, performance enhancements included the addition of two OSV.dev and Deps.dev code-trigger integrations:

- OSV Integration (on-demand code trigger)
- Deps.dev Integration (on-demand code trigger)

These integrations are initiated automatically by internal workflows and are for internal use only. Although you can locate them, you must not initiate these integrations on-demand with **Execute Now** button from their integration records.

Configuring the run schedule for the Deps.dev Integration

To modify the schedule, navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations** > **Deps.dev Integration**. The sn_vul.app_configure_integrations role is required to edit the schedule of this integration.

This Deps.dev integration is used to identify components that are in **Stale** and **Abandoned** states. A stale component's version is more than two major versions behind the latest version and two years behind the latest version. An abandoned component has not been updated for more than two years. The two year and two version thresholds can be edited with system properties. To edit these parameters, navigate to **All** > **System Properties** > **All Properties** and locate the following records:

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

The Deps.dev Integration is installed with SBOM Response. The integration is activated (Active check box selected on the integration record) by default and scheduled to run weekly. Note that

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

this is not the on-demand Deps.dev code trigger integration, and you can edit the schedule and initiate the scheduled job on-demand from its integration record. .

The threshold values for abandoned and stale are in months. The threshold value for version is numerical.

You can view imported data on the Home page of the workspace and in the BOM Queue module. Imported data is stored in the Package Groups [sn_sbom_pkg_group] table.

Configuring and initiating the OSV.dev Integration - Comprehensive

To configure and initiate this integration, navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations** > **OSV.dev Integration - Comprehensive**. The sn_vul.app_configure_integrations role is required.

You can view imported data on the Home page of the workspace on the Vulnerability tab on records from the entities list and in the Libraries module. Imported data is stored in the Application Vulnerable Entries [sn_vul_app_vul_entry] and the National Vulnerability Database Entries [sn_vul_nvd_entry] tables.

Note: You can configure the OSV.dev's *batchSize* integration parameter on the Integration Parameters tab on the **Open Source Vulnerabilities Instance** located at **All** > **Vulnerability Response** > **Administration** > **Integrations** > **Vulnerability Integrations** > **Open Source Vulnerabilities Instance**. The default is 75 Purls per API call.

You might prefer to leave this value in its default setting. Altering the value might impact performance.

The OSV.dev Integration - Comprehensive integration is installed with SBOM Response. The integration is activated (Active check box selected on the integration record) by default. Note that this is not the on-demand OSV.dev code trigger integration, and you must initiate this integration on-demand from its integration record.

Activating PaCE

Starting with version 4.0 of SBOM Response, you can view components that are identified as stale or abandoned as 'Non-compliant' in the Policy as Code Engine (PaCE) interface that is available in the SBOM Workspace.

- Determine if components are stale or abandoned with the *Run PaCE policies for SBOM Response* scheduled job. This scheduled job is deactivated by default.
- View components that are identified as stale or abandoned as Non-compliant in the PaCE interface that is available and viewed in the SBOM Workspace.

See Integrating PaCE with other applications for more information about PaCE and PaCE policies.

Uploading and viewing your SBOM files in the SBOM Workspace

The SBOM applications enable you to upload files and view details for entities, component inventories, license information and other details in the Software Bill of Materials Workspace.

Overview of uploading SBOM files

You can upload your software bill of material files via an API or manually. View the files that you import as entities, which are inventories of the third-party component libraries used in your software, including any transitive dependencies.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Uploading Software Bill of Materials files using a REST API.

  The Upload API is used for uploading and ingesting an SBOM file (CycloneDX/SPDX) into your instance.

- Upload Software Bill of Materials files manually.

  Upload software bill of materials files manually. The method you use to upload your files depends on whether you have the SBOM Core or SBOM Response applications installed.

- Uploading Software Bill of Materials for DevOps SBOM files.

  Generate and upload SBOM files for software throughout its continuous integration and continuous deployment development cycles.

- Classify and resolve component licenses in the License administration module.

  Review classify, and resolve (assign) license information for the components you upload in your SBOM files according to your internal or regulatory policies. You can match your components to licenses and determine your overall license compliance to see your potential risk exposure to banned, restricted, or missing licenses.

- Viewing reports and dashboards in the Software Bill of Materials workspace

  Vulnerability analysts and managers can view uploaded software bill of materials files and important data in records, data visualizations, as well as enhanced vulnerability intelligence and license information the Software Bill of Materials (SBOM) Workspace.

  Note: You must install SBOM Response if you want to view the data visualizations on the landing (Home) page of the workspace.

Uploading Software Bill of Materials files using a REST API

Review the following information prior to uploading Software Bill of Materials files using an API.

Using the REST API

To upload an SBOM file with an API, the sn_sbom_core.sbom_ingest role is required.

Upload API.

This API is used for uploading and ingesting an SBOM file (CycloneDX/SPDX) into your instance.

Version 4.0 of SBOM Core supports:

- XML and JSON in CycloneDx (versions 1.0 - 1.6).
- JSON in SPDX (versions 2.2-2.3)

- **Note:** Files over 32 MB might not load properly.

HTTP method: (POST)

API URL: `<host_name>/api/sbom/core/upload`

Note: `<host_name>` is your ServiceNow instance name.

All below request parameters are optional; the request body is the SBOM file content. If you are using DevOps as part of your development process, the value of 'requestedBy' should be 'devops'. See Uploading Software Bill of Materials for DevOps SBOM files for more general

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

information about DevOps. If the value for 'requestedby' is "devops" (devlopment operations), these parameters are mandatory:

- buildId
- lifecycleStage

In addition, if 'requestedBy' is 'devops', data for fetchVulenrabilityInfo, and fetchPackageInfo is included.

- buildId- string you send
- lifecycleStage- two values, production or pre_production
- fetchVulenrabilityInfo- t/f
- fetchPackageInfo-t/f

Request parameters	Possible values	Description
productModelId	Sys id	Sys id of product model to map with the root application of given SBOM.
businessApplicationId	Sys id	Sys id of business application to map with the root application of given SBOM.
businessApplicationName (deprecated)	Your business application name	Name of business application to map with the root application of given SBOM.
sbomSource	A product such as Veracode, for example	The source for your SBOM file.
requestedBy	A tool, or name of a methodology, Jenkins. If you use "devops", buildId and lifecycleStage are mandatory.	Upload requested by
buildId	A string requester sends.	Build ID of the SBOM build.
lifecycleStage	production or pre_production	Life cycle stage of the entity.
fetchVulenrabilityInfo	t/f	If true, triggers vulnerability intelligence integration.
fetchPackage Info	t/f	If true, triggers package intelligence integration.

Upload API Response: included 'status' success/fail, 'message' (string), 'bomRecordId' (this is the sys id of the SBOM that is returned through the upload API for a successful SBOM upload).

```
{
"result": {
"status": "success",
"message": "Queued for processing.",
"bomRecordId": "f207059b4393c290629aa597cbb8f247"
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
}

}
```

Status API

This API gets the status and summary of an SBOM that Is queued for ingestion.

- API URL: `/api/sbom/core/upload/status`
- HTTP method (GET)

Request parameters	Possible values	Description
bomRecordId	Sys id	SBOM record ID that is returned the through the upload API for a successful SBOM upload.

Status API default response example.

```
{
   "result": {
      "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
      "uploadStatus": "processed",
      "additionalInfoStatus": "not_requested",
      "uploadSummary": {
         "components": {
            "added": 0,
            "removed": 0,
            "total": 70
         }
       }
    }
}
```

Status API response with additional parameters example. If you requested fetchVulenrabilityInfo for that SBOM, you get the vulnerability breakdown as part of the response.

```
{
 "result": {

  "bomRecordId": "93af349b4393c290629aa597cbb8f258",

  "uploadStatus": "processed",

  "additionalInfoStatus": "complete",

  "uploadSummary": {

    "components": {

     "added": 0,

     "removed": 0,
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
    "total": 3
   },
   "vulnerabilityInfo": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "none": 0
   }
  },
  "buildId": "1"
 }
}
```


If you requested fetchPackageInfo for that SBOM, you get stale and abandoned counts as part of the response.

After an SBOM is successfully processed, where you view the uploaded records depends on the applications you're using.

- If you're using SBOM Response, the BOM Entity record is displayed on the SBOM Ingestion Status list in the BOM Queue module in the SBOM Workspace.
- If you're using SBOM Core, navigate to **SBOM Core** > **BOM Ingestion Status**.

Enhancements to supported SBOM standards and general usage information

Version 4.0 of SBOM Core supports:

- XML and JSON in CycloneDx (versions 1.0 - 1.6).
- JSON in SPDX (versions 2.2-2.3)

- **Note:** Files over 32 MB might not load properly.

Starting with v4.0 of SBOM Core, the following enhancements were made to support CycloneDx standards for versions 1.0 - 1.6:

- Import additional information in CycloneDX SBOM files with the (sn_sbom_core.collect_properties) property. This property is deactivated by default. Activate the property to import information that is generally not supported. Any information imported from these properties is uploaded to the SBOM Component Property [sn_sbom_comp_property] table for the following:
  - Uploaded SBOM files
  - Metadata

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Individual vulnerabilities
  - Components
- View imported component data for declared and concluded licenses for SBOM files in versions 1.4 and later of CycloneDX in two new license fields:
  - **Declared**
  - **Concluded**
- SBOM parsing support is extended for the following CycloneDX component types:
  - Version 1.5: Platform, Data, Device driver, Machine Learning model
  - Version 1.6: Cryptographic

Version 3.0 of SBOM Core supports:

- XML and JSON in CycloneDx (up to and including version 1.4).
- JSON in SPDX (up to and including v2.3).

If the calling user is successfully authenticated and has the sn_sbom_core.sbom_ingest role in your ServiceNow instance, you can access the API from outside of your instance to upload the SBOM data.

After data is uploaded, it is parsed. Before data is parsed, the following requirements are verified:

- Incoming data is checked that it is valid JSON or XML.
- The BOM format is supported. Starting with v2.1 of SBOM Core, CycloneDX (JSON and XML) and SPDX (XML) formats are supported.
- The minimum fields are available so that data can be parsed.

After these checks are verified, an entry is made into the Bill of Materials [sn_sbom_doc] table with incoming SBOM data as an attachment.

The *`Process BOM file`* business rule is triggered automatically as a result of the record insertion and data parsing.

Note: This business rule is activated during installation of SBOM Core by default.

All the components listed in an SBOM have a defined `type`.

- Components for which SBOM files were uploaded are considered BOM Entities.
- Components listed as `type=library` are considered third-party components.

Related topics

View upload status for Software Bill of Materials files

Viewing reports and dashboards in the Software Bill of Materials workspace

Upload Software Bill of Materials files manually

Upload Software Bill of Materials (SBOM) files manually.

Before you begin

Starting with version 4.0, SBOM Core supports:

- XML and JSON in versions 1.0 - 1.6 of CycloneDX.
- JSON in versions 2.2 - 2.3 of SPDX.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: sn_sbom_core.sbom_ingest

Procedure

1. Upload files manually.

   The method you use to upload your files depends on whether you have the SBOM Core or SBOM Response applications installed.

Option	Description
If you have installed SBOM Core	**a.** Navigate to **SBOM Core** > **BOM Ingestion Status**. **b.** On the Bill of Materials list select **New**. **c.** Select the **Click to add** link. You can upload one SBOM file at a time. **d.** Select **Choose file** and locate the file you want. The file name is displayed on the Choose an attachment file page. **e.** Select **OK**.
If you have installed SBOM Response starting with v4.0	**a.** Navigate to **All** > **Workspaces** > **SBOM Workspace** > **BOM Queue**. **b.** Select **Upload BOM**. The Upload SBOM file modal is displayed. **c.** Select the **Attach file** link. **d.** Locate the file you want and select **Open**. After your file uploads, a link for the file is displayed along with three icons that pro vide you with the following options: ▪ Download the file. ▪ Edit the file name. ▪ Delete the file from the upload. **e.** Select **Upload** to continue. You can upload one SBOM file at a time. **f.** (Optional) Select a Business application and a Product model from the lists. These values help you associate this SBOM to a business application or product model in your organization. This information is displayed on the BOM entity record after upload. **g.** Select **Upload**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	The BOM queue page is displayed and the file is listed on the SBOM ingestion section along with upload status other information about the file.

2. **Optional:** Upload SBOM files imported by the Veracode Vulnerability Integration.

> **Note:** You can upload Veracode files in CycloneDX (JSON and XML) and SPDX (XML) formats only if you have installed and activated the Veracode integration with Application Vulnerability Response. See the Veracode Vulnerability Integration for more information.

Result

After an SBOM is successfully processed, where you view the upload status depends on the applications you are using.

- If you are using SBOM Response, the BOM Entity record is displayed on the SBOM Ingestion Status list in the BOM Queue module in the SBOM Workspace.
- If you are using SBOM Core, navigate to **SBOM Core** > **BOM Ingestion Status**.

Related topics

Uploading Software Bill of Materials files using a REST API

Uploading Software Bill of Materials for DevOps SBOM files

Generate and upload Software Bill of Materials SBOM files for software throughout its continuous integration and continuous deployment development cycles.

DevOps and SBOM files

SBOM files can be generated at multiple stages throughout the software continuous integration and continuous deployment (CI/CD) development life cycle. Most software development operations (DevOps) in organizations use some type of CI/CD process to help them identify and prevent costly bugs that might surface after the release. Throughout the CI/CD pipeline, DevOps can generate SBOM files and pro-actively check for vulnerabilities and at-risk components. These checks can help organizations achieve better software quality and avoid costly maintenance later. Generating SBOM files is critical for successfully implementing and automating accurate build assessments during the CI/CD development.

Uploading SBOM files from development pipelines is supported starting with the following versions of the SBOM applications.

Supported versions

Application	Supported versions
Data Model for SBOM	v3.0, v2.0
SBOM Core	v5.0, v4.0, v3.0
SBOM Response	v5.0, v4.0, v3.2, 3.1

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use cases

Generating SBOM files and sending them via the SBOM Upload API as part of the DevOps build pipeline can provide counts for the following to determine whether the pipeline should succeed or fail:

- Added components
- removed components
- Vulnerabilities information
- Package information (abandoned/stale components)

DevOps policies and rules for the success or failure of a pipeline may be defined by the vulnerability counts and stale and abandoned component count thresholds that are received from the SBOM Status API.

For a failed pipeline, DevOps users can access information about the failed build in their ServiceNow® instance to help them better understand the root cause and origin of the vulnerabilities.

See Uploading Software Bill of Materials files using a REST API for more information about (POST) and (GET) parameters and URLs for the Upload and Status APIs.

Domain Separation

All the tables in the SBOM applications are domain separated.

Classifying licenses and resolving component licenses in the Software Bill of Materials workspace

Classify licenses and resolve (match) them to components, or create licenses in the License administration module in the SBOM workspace. Classifying and matching licenses to your components permits you determine your license compliance for the proprietary, open-source, and vendor-supplied software components you upload in your SBOM files.

License data and third-party software

As organizations build more of their own software applications, they are using open-source components and vendor-supplied software. Using third-party and open-source components provide you with many advantages for the rapid creation and release of your software projects, however, using these components comes with licensing risks:

- Open-source and vendor-supplied software components at times have dependencies on other components, and each component might have its own licensing requirements.
- If you’re not compliant with the terms of your licenses for the components and software in your applications, you might inadvertently ship code that violates your internal policies and regulatory licensing requirements.

The License administration module

The License administration module in the SBOM Workspace permits you to perform the following tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Classify licenses that require it for the components you upload with your SBOM files.
- Resolve each license you classify to a specific component.
- See what percentage of the components you are using are out of compliance on a data visualization on the Home page. You can use this information to help you determine your overall security posture and potential risk exposure.

If the SBOM files you upload include license information, the license database grows automatically as unique licenses are observed on each SBOM upload. With each SBOM upload, you can build a database of uploaded licenses and then classify them if necessary with the License administration module in the SBOM Workspace. You build an inventory of licenses so that you can assign them to components after you classify them in one of the following categories:

- Permitted
- Restricted
- Banned
- Unclassified

Legal personnel, license managers, compliance, and regulatory managers perform tasks in the License administration module.

Viewing uploaded license data

You have the following options to view any license information you've uploaded with your components in the SBOM Workspace.

- Navigate to **Workspaces** > **SBOM Workspace** > **Components**.

  On the Components page the License classification of components card displays a visualization of your overall license compliance with the following categories.

Category	Description
Banned	Licensed usage is not permitted.
Classification required	License is not yet classified and requires a review.
Permitted	Licensed usage is permitted without restriction.
Restricted	Licensed usage is not permitted in specific use cases.

  This snapshot uses the classifications and resolved license information you enter in the License administration module to calculate your over-all license compliance.

  If you select a component record from this list, you can view the component's license information along with other information in the State field.

- Alternatively, navigate to **Workspaces** > **SBOM Workspace** > **License administration** > **License classification**.

  This page tracks the total number of unique licenses that have been detected from the SBOM files you've uploaded. It also filters them in cards along the top of the page in the following categories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Unclassified - License requires review and classification.
- Banned - License usage is not permitted.
- Restricted - License is not permitted in specific use cases.
- Permitted - License usage is permitted without restriction.
- All licenses - Total count of licenses.

All the components in your organization are using one of the licenses that is listed on this page. When a new license is detected from an SBOM upload, a record is created and stored in the SBOM license [sn_sbom_license] table and added to this list. It's classification by default is, **Classification Required**. License records in this state must be reviewed and classified before you can resolve (match) them to components so your overall license compliance is accurately calculated.

For information on how to classify licenses, see Classify imported licenses in the Software Bill of Materials Workspace.

Roles

New licenses must be classified by a user with the sn_sbom_response.managelicense role. This user views uploaded license information and determines which licenses are permitted and which are banned. Users with this role cannot view the Component license resolution module unless they have the sn_sbom_response.licenseresolver role.

After classification, licenses must be resolved by a user with the sn_sbom_response.licenseresolver role so that your over-all license compliance can be determined. This user resolves licenses to components. Users with this role cannot view the License Classification module unless they have the sn_sbom_response.managelicense role.

Classifying new license information is an ongoing process. You might prefer to keep the total number displayed on the Unclassified card low. As a license manager, you might prefer to check for licenses that need classification every few days and after you upload SBOM files.

As a license resolver, you might prefer to check for updated classified licenses every few days.

Classify imported licenses in the Software Bill of Materials Workspace

Classify the component licenses you upload with your SBOM files with the License Classification feature.

Before you begin

Classifying new license information is an ongoing process. You might prefer to keep the total number displayed on the Unclassified card low. As a license manager, you might prefer to check for licenses that need classification every few days and after you upload SBOM files.

Role required: sn_sbom_response.managelicense

Procedure

1. Navigate to **Workspaces** > **SBOM Workspace** > **License administration** > **License Classification**.

   Note: Unless you also have the sn_sbom_response.licenseresolver role, only the License classification tab is visible.

2. **Optional:** Select a card to filter licenses by their classifications.
3. To classify licenses, choose one.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Bulk edit records or edit more than one record on the list.	**a.** Select multiple records. **b.** Double-click the Classification column header. **c.** Update the classification.
Edit and update the classification on the record.	**a.** Select a record from the list to open it. **b.** Add work notes and attachments, if re quired. **c.** Select **Save**.

4. After you classify licenses, you are ready to Resolve classified licenses to components.

Resolve licenses to components in the Software Bill of Materials Workspace

Resolve (assign) classified licenses to specific components with the Component License Resolution feature. Assign licenses to components with missing information or incorrect license information or create new licenses so your overall license compliance can be calculated.

Before you begin

Role required: sn_sbom_response.licenseresolver

Procedure

1. Navigate to **Workspaces** > **SBOM Workspace** > **License administration** > **Component License Resolution**.

   Note: Unless you also have the sn_sbom_response.managelicense role, only the Component License Resolution tab is visible.

   This page tracks the total number of unique licenses and an at-a-glance view of license totals that have been detected from the SBOM files you've uploaded. Licenses displayed on this page fall under two broad categories as they relate to components.

   - All instances of the component agree on a license.
   - There is a disagreement on a single license and there is more than one license for a component.

   In the second case, you must reconcile these licenses so a single license is resolved to a single component. License compliance is calculated based on one resolved license per component.

   The licenses on this page are filtered into the following categories to help you resolve them.

Value	Description
Components with unresolved licenses	No license is assigned to the component and it requires resolution. `(empty)` is displayed in the Resolved license column for these components. Both missing and multiple licenses totals are listed as part of this category.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Value	Description
Components with missing licenses.	Components with missing license information that require resolution.
Components with multiple licenses	Components that are visible across multiple entities which have different licenses and require resolution.
All components	Total list of components tracked in your organization. You can change licenses from this filtered list.

2. Select a card.
3. Choose one to resolve a license.

Option	Description
Assign an existing license to a component.	**a.** Double-click a field in the Resolved license column for a component. **b.** Select one license from the Resolved Li cense list. **c.** Your edit is saved and the associated card at the top is updated. **d.** Alternatively, select the record from the Name column to open it. It opens in a new tab. **e.** Click the **BOM entities** tab to see where the component is being used. **f.** Select one from the Resolved License list. **g.** Enter a justification. **h.** Select **Save**. **i.** Refresh the page to update it.
Change a license for a component that al ready has one.	You might choose this option if you determine a license has been incorrectly assigned to a component or needs to change. **a.** Select the **All components** card. **b.** Locate the component you want to modify. **c.** Select the record from the list to open it. **d.** Select one from the Resolved License list. **e.** Select **Save**. **f.** Refresh the page to update it.
Create a license.	You might use this option if you know a spe cific license is used in your organization, but a record was not detected from a previous SBOM upload and there is no record for it list ed in the License Classification module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	a. Select **New** on the License Classification tab and fill out the fields. **b.** Name- Unique name for this license. **Note:** The display name is based on the ID field. If the ID field is not de fined, the display name is based on the Name field. If the Name field is not defined, the display name is based on the Expression field. **c.** Classification. Select one: ▪ Unclassified - License requires review and classification. ▪ Banned - License usage is not permitted. ▪ Restricted - License is not permitted in specific use cases. ▪ Permitted - License usage is permitted without restriction. **d.** License type. This information is not used by the system or for a workflow. This infor mation is provided to help you store addi tional information and categorize your li censes. **e.** URL: Website for license source. This is not used by a workflow or a system. **f.** Expression: Arithmetically combine licens es. For example, `MIT AND Apache-2.0 WITH GPL-2.1-or-later` are com bined for an expression. License combina tions or expressions are treated as one li cense in the ServiceNow AI Platform. **g.** Attachments. Add attachment or wor knotes. **h.** Select **Save**. This license is added to your database, is displayed on the License Clas sification page, and can now be detected on components during SBOM uploads.
Upload multiple licenses and classifica tions.	You might choose this option if you have a file with multiple licenses and classifications that you want to create records for. You can upload files in the specified format and store it in the SBOM license [sn_sbom_license] ta ble.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	a. Navigate to the SBOM license [sn_sbom_license] table. **b.** Select the **More options** menu from any column. **c.** Select **Import**. On the page that is displayed, either upload an existing compatible template or download the template generated by the Platform (**Create Excel template**). You load the data into this template that is inserted into the table. **d. Choose file** and locate your file. **e.** Select **Upload**. Your file is uploaded, and the records are created in the SBOM license [sn_sbom_license] table and viewable in the SBOM Workspace on the License Classification page.

4. Navigate to the Home page in the SBOM Workspace to see what percentage of the components you are using are out of compliance in the License classification of components visualization.
   The data for this visualization is updated daily by the License breakdown of BOM components scheduled job. This job is part of the SBOM Reports Data Collector scheduled job that runs daily.

Viewing reports and dashboards in the Software Bill of Materials workspace

Vulnerability analysts view uploaded software bill of materials files in records, data visualizations, as well as enhanced vulnerability intelligence in the Software Bill of Materials (SBOM) Workspace.

SBOM Core

You can view BOM Entities and a list of components you've uploaded on the Home (landing) page and in the Components module in the SBOM Workspace.

SBOM Response

The SBOM Response application provides you with data visualizations with detailed information about BOM entities, entities with vulnerabilities, and active application vulnerable items on the Home (landing) page in the SBOM Workspace. The workspace with SBOM Response includes the following modules:

- Home page - Data visualizations and enhanced vulnerability details.
- Components - Version and fix information for components and license classification of components.
- AVIT (application vulnerable item) Creation Rules - Conditions for when application vulnerable items (AVITs) are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- BOM Queue - File upload status and history.
- List - AVIT records for your vulnerable components and Libraries (NVD, CWE, and application Vulnerabilities).

The following topics provide more information about how to locate details about your components in the Software Bill of Materials Workspace.

- Review the Home page in the Software Bill of Materials Workspace
- Reviewing the Components module in the Software Bill of Materials Workspace
- View upload status for Software Bill of Materials files
- Checking a Software Bill of Materials entity for vulnerabilities
- Classifying licenses and resolving component licenses in the Software Bill of Materials workspace

Review the Home page in the Software Bill of Materials Workspace

Uploaded data is rolled up to the visualizations on the landing (Home) page in the Software Bill of Materials (SBOM) Workspace. Data is modified after you upload files so vulnerability analysts can see trends and review current information about your components.

Before you begin

Roles required: sn_sbom_resp.sbom_analyst

Procedure

1. Navigate to **Workspaces** > **SBOM Workspace**.
   By default, the landing page (Home) is displayed.

   What you can see in the module depends on the applications you have installed.

   Imported data is not calculated and populated by live queries. Scores on the Home and Components pages are updated once daily with performance enhancements for reporting. This enhancement might provide you with faster load times for the scorecards on the Home and Components modules in the SBOM Workspace.

   These enhancements have no impact on how or where data is stored.

Installed application	Description
If you have installed SBOM Core	All BOM entities. The list includes the Name, Classifier (Application, Container, Library, and so on) and the component count for each entity. A BOM entity refers to the root level component in an SBOM file for which an SBOM document was generated and uploaded. Navigate to the Home page in the workspace to view the list of BOM entities.
If you have installed SBOM Response	The following data visualizations are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Installed application	Description
	○ All BOM Entities - A breakdown of BOM entities by type: Application, Container, Library, and Others. A BOM entity refers to the root level component in an SBOM file for which an SBOM document was generated and uploaded. ○ BOM Entities with Vulnerabilities - Entities that have a vulnerability associated with any component that they depend on. If an entity dependency has one **Critical** vulnerability, the entity's severity is considered critical. ○ Active AVIs - The trend for the number of application vulnerable items (AVI)s created each day. The data visualizations display data for the last 30 days. The 30-day range isn't editable. This data is available after you've reviewed and set up the creation rules for application vulnerable items. For more information, see Creating rules for application vulnerable items in the Software Bill of Materials Workspace.

2. Select a data visualization card to see its list of records.
3. Select the **Home** tab to return to the landing page.
4. Alternatively, select a record under the **BOM Entities** list.

   The entity name and version is displayed at the top of the record, for example, SNC - SECOPS - SIR2 . 0.

   Note: With the License administration module, the entity-license relationship is not displayed on this list. To view the entities where a component is used, navigate to the components module and open a component record. On the component record, you can view the State: Unresolved or Unclassified.

5. Select the tabs on the entity record to review the data.

   a. If not selected, select the **Overview** tab.

   Review the data. If a field isn't populated on this record, the data wasn't included with the SBOM files you uploaded.

Name	Description
Name	Entity name.
Classifier	Entity type, for example, an application, component, or library.
Version	Version number of the entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
Supplier	The product that supplied the entity.
Product model	If there's no existing product model or if you don't include one at the time of your SBOM upload via the API, one is created. The name of the entity is used for the product model record, for example `SNC - SECOPS - SIR2 . 0`.

b. Select the **Depends on** tab.

All the dependencies of this entity are listed as well as classifiers, for example, `Library`. The version number, `Licenses`, and other information are displayed.

Selecting a link on this list opens a record. Its tab is displayed below the Home and entity record tabs. The record you open might include the following related lists you can review: Overview, Hashes, BOM Entities, Vulnerabilities, and application vulnerable items (AVITs).

The BOM Entities related list displays all the entities that this displayed item is used in.

c. Select the **Vulnerabilities** tab to see the vulnerabilities associated with a dependency of this entity.

For more information about the vulnerabilities displayed for an entity, see View upload status for Software Bill of Materials files.

d. Select the **AVIs** tab to see if there are application vulnerable items for this entity.

6. **Optional:** After you review records, you can delete one or more BOM Entity records if you determine you no longer need them.

> **Note:** Deleting BOM entity records permanently removes them and their component relationships. Any application vulnerable items (AVIT)s that are associated with the BOM entities transition to **Closed**. If you decide later that you want the records and component relationships you delete back on the BOM entities list and available in the workspace, you must upload these BOM entities again.

a. If not on the Home page, select the **Home** tab to return to it.

b. Select the records(s) under the **BOM Entities** list that you want to delete.

c. Select **Delete**.

Reviewing the Components module in the Software Bill of Materials Workspace

The Components module in the Software Bill of Materials (SBOM) Workspace displays current information about vulnerable, stale, abandoned, and high-risk combinations for the components you import.

Viewing the Components module

Role required: sn_sbom_resp.sbom_analyst

Navigate to **Workspaces** > **SBOM Workspace** > **Components**.

What you can see in the module depends on the applications you have installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Imported data is not calculated and populated by live queries. Scores on the Home and Components pages are updated once daily with performance enhancements for reporting. This enhancement might provide you with faster load times for the scorecards on the Home and Components modules in the SBOM Workspace.

These enhancements have no impact on how or where data is stored.

Installed application	Description
If you have installed SBOM Core	An inventory of all uploaded components that includes the following information: • Name • Description • Version • BOM entity count
If you have installed SBOM Response	Select a graph or a number on the graph to view a list of associated records. **All Components** The list of **Stale** and **Abandoned** components, as well as those with at least one vulnerability in your total component count. These counts can help you identify components that require your attention. These subsets of components might not match your total component count because all of your components might not fit into these categories. • A stale component's version is more than two major versions behind the latest version and two years behind the latest version. • An abandoned component has not been updated for more than two years. • Vulnerable components are components that have any vulnerabilities with a severity of **High** or greater. **High-risk combinations** High-risk components might require your immediate attention. The Deps.dev integration, which is installed when you install the SBOM Response application, provides the packages intelligence for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Installed application	Description
	components in the **Stale** and **Abandoned** states. Imported, high-risk combinations are comprised of stale and abandoned components with at least one severe (**Critical** or **High**) vulnerability that you can fix with updates, replacement, or another type of repair. The **Completely fixable** status means that a component has an available version that can fix it. The percentage of the total number of high-risk components that have fixable versions is noted. **Fixibility of vulnerable components** Totals and breakdowns of the components with **Critical**, **High**, **Medium**, and **Low** vulnerabilities and if some or all of their vulnerabilities can be fixed. If a component has more than one vulnerability, the most critical vulnerability takes precedence. The fixability status: • Complete - There are fix versions for all the vulnerabilities associated with the current version of the component. • Partial - There is a fix version for at least one but not all of the vulnerabilities associated with the current version of the component. **License classification of components** Totals and breakdowns of components by their license classifications. The Component List under the visualizations enables you to see the name, description, version, and entity counts. In the right panel, you can view a version history. The current version is highlighted in the version history. The Common Vulnerabilities and Exposure (**CVE**) and **Fixability** columns are also displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assessing your risk with vulnerability intelligence

See Checking a Software Bill of Materials entity for vulnerabilities for more information about how to review vulnerability intelligence data in the workspace.

Assessing your risk with license compliance

See Classifying licenses and resolving component licenses in the Software Bill of Materials workspace for more information about how to license data your import with your components and viewing your over-all license compliance in the workspace.

Creating rules for application vulnerable items in the Software Bill of Materials Workspace

Before you can see application vulnerable items (AVITs) in the Software Bill of Materials (SBOM) Workspace, you must set up the conditions under which AVITs are created.

AVITs in the SBOM Workspace

If you've installed and activated the SBOM Response application, AVITs are created for SBOM files if any of the imported data matches the conditions of your existing AVIT creation rules.

The SBOM Response and Vulnerability Response applications are required to set up rules for creating application vulnerable items (AVITs) automatically and remediating them with the Application Vulnerability Response workflow. See Exploring Software Bill of Materials for more information.

As a user with the sn_sbom_resp.manage_avi_rule role, you must add AVIT creation rules in the SBOM Workspace before you can create AVITs for the vulnerabilities that are found in your ingested SBOM data. AVITs enable you to evaluate the integrity of the third-party components in your applications. An AVIT is created in your instance when an application is matched to a component that has an associated vulnerability.

In the SBOM Workspace, you can view only SBOM AVITs. However You can view SBOM AVITs along with other types of vulnerable items in the Vulnerability Manager Workspace in Vulnerability Response. You can view all the AVITs that have been created in the SBOM Workspace in the List Module. The list module also includes all the NVD and CWE entries and Application Vulnerabilities.

You can also assign AVITs for remediation based on recommendations from known vulnerability lists such as the National Vulnerability Database (NVD). A scheduled job is triggered, and if the conditions of your creation rules match the ingested data, AVITs are created.

You can track and remediate AVITs by setting up customized rules.

See Create an application vulnerable item rule in the Software Bill of Materials Workspace for information about how to create a rule.

SBOM AVITs in Vulnerability Manager Workspace in Vulnerability Response

You can view any SBOM AVITs that are created in the SBOM Workspace in the Vulnerability Manager Workspace if you have access to it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: To view only SBOM AVITs from the Application Vulnerable Items list in the Vulnerability Manager Workspace rather than all AVITs, set the condition **[Source] [is] [SBOM] AND [Scan type] [is] [SBOM-SCA]** on the Application Vulnerable Items [sn_vul_app_vulnerable_item] table. To view the table, navigate in your instance to **All** and enter **sn_vul_app_vulnerable_item.list** in the filter navigator.

For more information about the Vulnerability Manager Workspace, how to view watch topics, application remediation efforts, and application remediation task rules for AVITs that are configured from the Vulnerability Response application in the Vulnerability Manager Workspace, see Use watch topics in the Vulnerability Manager Workspace.

Remediation tasks (AVULs) are created from AVITs and assigned automatically to groups for remediation based on your assignment rules. For more information about how to create these rules, see the following topics:

- Create or edit Vulnerability Response assignment rules
- Create or edit Vulnerability Response remediation task rules and Create a remediation effort in the Vulnerability Manager Workspace.

Reopening application vulnerable items in SBOM Response

A **Closed** application vulnerable item (AVIT) for a component with an associated vulnerability is re-opened automatically and visible in the SBOM Workspace if the following conditions exist:

- The AVIT with the associated vulnerability is detected again by a third-party integration's vulnerability scans or the component with the vulnerability is part of a subsequent SBOM upload.
- You have not deactivated the Reopen AVITs if detected (*sn_sbom_resp.reopen_avits_if_detected*) system property. This system property is activated by default.
- The substate of the **Closed** AVIT is not one of the following: **Mitigation Control in Place**, **Not Affected**, or **False Positive**. AVITs with these substates are not reopened by the system property.

Deactivate this system property only if you do not want **Closed** AVITs to reopen automatically.

View upload status for Software Bill of Materials files

Check the upload status for the Software Bill of Materials (SBOM) files that you upload in the BOM Queue module in the Software Bill of Materials (SBOM) Workspace. Track the files that you upload successfully, your upload history, and errors.

Before you begin

Role required: sn_sbom_resp.sbom_analyst

Procedure

1. View your upload status.

   The method you use to view your upload status depends on the applications you have installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
SBOM Core	**a.** Navigate to **All** > **SBOM Core** > **BOM Ingestion Status**. **b.** On the Bill of Materials list, review the columns such **Status**, **BOM generation time**, and **Created** columns for details.
SBOM Response	**a.** Navigate to **All** > **SBOM Workspace** > **BOM Queue**. **b.** Select a visualization card to review the following details for the categories of your uploaded files: ▪ BOM updates in the last 30 days - Total BOM entities uploaded and parsed successfully over the past 30 days. ▪ Upload source - Total of successfully uploaded SBOM files and a breakdown of the methods used to ingest them (API or manual). ▪ Upload errors by category - Top five categories of upload errors. If no data appears on this visualization, all of your SBOM files uploaded successfully.

The status information in the Bill of Materials table [sn_sbom_doc_list] and the BOM Queue module both include BOM formats, ingestion Status, and BOM generation time. The Status column for BOM ingestion includes the following states:

- Queued - SBOM data has been uploaded.
- Processing - The component data is being processed as part of the import.
- Processed - Data ingestion has been successfully completed.
- Error - An error has occurred during processing.

In addition to the status of your uploaded files, you can view lists of components you've ingested by selecting a BOM entity record.

2. **Optional:** Access more information about errors and upload status by selecting the gear icon and adding fields such as **Error category** and **Error detail**.

Checking a Software Bill of Materials entity for vulnerabilities

Determine whether any vulnerabilities are associated with the components in an uploaded Software Bill of Materials (SBOM) file.

The following applications must be installed and activated before you can view the vulnerabilities and enhanced vulnerability data:

- SBOM Response
- Vulnerability Response Integration with NVD and CWE jobs
- Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Exploring Software Bill of Materials for more information.

Role required: sn_sbom_resp.sbom_analyst

1. Navigate to **All** > **SBOM Workspace** > **Components**.
2. you can view vulnerability information either through a visualization or a component record.

Method	Actions
BOM Entities with Vulnerabilities visualization	Select the **BOM Entities with Vulnerabilities** visualization graph. ○ If vulnerabilities are associated with this component, the totals are displayed in the CVE and CWE columns on the list. A component can have more than one vulnerability. If available, you can check the Fixability column on this list for entries. ○ If no vulnerabilities are associated with this component, these columns display 0 or no values for the component. If the CVE, CWE, and Fixibilty columns are not displayed, you can add them to the page by selecting the gear icon on the upper right of the page and **Edit columns**. Select them from the Available column list and select **OK**.
Component record	**a.** Select a record from the list below the visualizations. **b.** Select the **Vulnerabilities** tab on the record. **i.** If no data is displayed, no reported vulnerabilities are associated with the record. **ii.** If data is displayed, see Reviewing the Components module in the Software Bill of Materials Workspace and follow the steps in the remediation workflow for Application Vulnerability Response to address the vulnerability. For more information, see Remediating Application Vulnerability Response vulnerabilities.

Assessing your risk with vulnerability intelligence

View more enhanced vulnerability data with SBOM Response on component records. The SBOM Response application, Vulnerability Response, National Vulnerability Database (NVD) Integration and Common Weakness Enumeration (CWE) scheduled jobs described in Supported applications must be installed and activated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Select the **All Components** visualization to view its list of associated records.
2. Select a link in the **Name** column to open a record.

   The States, **Stale**, **Abandoned**, and **Vulnerable** are displayed under the component name. A component can have any combination of these states. If no state is displayed, the component is not stale, abandoned, or vulnerable.

   Review the current version and the latest published version. In the right panel, you can view a version history. The current version is highlighted in the version history and its location in the list may provide you with insight as to why a component is **Stale**, **Abandoned**, and **Vulnerable**. For example, you might be using an older version of a component.
3. Select the **Overview**, **Hashes**, **BOM Entities**, **Vulnerabilities**, and **AVIs** related tabs on the record.
   - Overview - A summary of the component details.
   - BOM Entities - A list of the entities associated with this component.
   - Hashes - If imported, hashes are displayed.
   - Vulnerabilities - Information about known vulnerabilities associated with this component. If this list is empty, there are no known vulnerabilities.

     If the list is populated, select the tab to view vulnerability IDs, summaries, and other vulnerability information for Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) data associated with this record. CVEs are broken down by severity, CWEs are broken down by how likely the component can be exploited. You can view the enhanced vulnerability records in the Vulnerability Response or Application Vulnerability Response applications by selecting the vulnerability ID link.
   - AVIs (AVITs) - Application vulnerable items associated with this component if you have created AVIT creation rules that match the component to a known vulnerability. The Application Vulnerability Response application (AVR) relates a vulnerability to an application to create an AVI record. For more information, see Creating rules for application vulnerable items in the Software Bill of Materials Workspace.

Components installed with Software Bill of Materials applications

Several types of components are installed with activation of the Software Bill of Materials applications, including tables, user roles, and scheduled jobs.

Roles installed

Role title [name]	Description	Contains roles
sn_sbom_response.managelicense	This role is installed with the SBOM Response application. This role permits you to resolve licenses to components.	None
sn_sbom_response.licenseresolver	This role is installed with the SBOM Response application.	None

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	This role permits you to view uploaded license information and determines which licenses are permitted and which are banned.	
SBOM write [sn_sbom_dm.app_write], SBOM create [sn_sbom_dm.app_create], SBOM read [sbom_dm.app_read]	These roles are installed with the Data Model for SBOM application. They permit you to read, create, and edit records in SBOM tables.	None
SBOM Cores ingests [sn_sbom_core.sbom_ingest] and SBOM Core admin [sn_sbom_core.admin]	These roles are installed with the SBOM Core application. The sn_sbom_core.sbom_ingest role permits you to upload SBOMs manually and via the REST API. The sn_sbom_core.admin role permits you to create, read, edit data, and upload SBOMs. This role also gives you access to the SBOM Core modules in your instance. It inherits the roles from the Data Model for SBOM application.	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read
SBOM Analyst [sn_sbom_resp.sbom_analyst]	This role is installed with the SBOM Response application. It inherits the sn_sbom_core.admin role and enables you to access the SBOM Workspace.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • sn_sbom_config_rule table

Tables installed with the SBOM applications

The tables listed in the following table are installed with the Data model for SBOM application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data model for SBOM tables

Table	Description
SBOM document [sn_sbom_doc]	Contains the BOM entities you've uploaded.
SBOM component [sn_sbom_component]	Contains imported SBOM components, classifiers, and versions that are included in the parent component.
SBOM component relationship [sn_sbom_comp_relationship]	Contains components and their dependencies.
SBOM m2m bom component [sn_sbom_m2m_bom_comp]	Contains the BOM component mappings.
SBOM license [sn_sbom_license]	Contains the open-source license IDs used for components.
SBOM supplier [sn_sbom_supplier]	Contains the organization that supplied the component, which might be a manufacturer, distributor, or repackager.
SBOM component ID [sn_sbom_comp_id]	Contains the component identifiers.
SBOM component properties [sn_sbom_comp_property]	Contains the component name-value properties.
SBOM hash [sn_sbom_hash]	Contains component hashing algorithms.
SBOM contact [sn_sbom_contact]	Contains contact information for the supplier.
SBOM external references [sn_sbom_comp_external_ref]	Contains components, component types, and external URLs that document systems, sites, and information that might be relevant but are not included with the SBOM.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data model for SBOM tables (continued)

Table	Description
SBOM package group [sn_sbom_pkg_group]	Contains the package group information for every component. Multiple version of libraries may be used across applications. Versions of the same components are grouped and added to this table to avoid pulling the same data multiple times.

The tables listred in the following table are installed with the SBOM Response application

SBOM Response tables

Table	Description
SBOM creation rule configuration [sn_sbom_config_rule]	Contains AVIT creation rules used in the SBOM Workspace.
SBOM m2m component vulnerabilities [sn_sbom_m2m_comp_vuln]	Contains the components and associated vulnerabilities.
Component vulnerability fix information [sn_sbom_comp_vuln_fix_info]	Contains the fix versions for each third-party vulnerability associated to a version of the component.
Component report insights [sn_sbom_comp_report_insight]	Contains insights about stale, abandoned, and fixability data for components.
Deps Integration Imports [sn_sbom_deps_integration_import]	Contains imported version list information for a given package or library.
OSV Integration Imports [sn_sbom_osv_integration_import]	Contains vulnerability intelligence information for a given version of a package or library.
Component Version Lists [sn_sbom_st_version_list]	Contains version information and published dates for components.

Scheduled jobs

Job	Description
Calculate Component Fixability and Vulnerability	Calculates information about how to fix components with vulnerabilities and how likely it is that you can fix components.
OSV Integration New Components	Retrieves all publicly known vulnerabilities associated with packages (libraries) that were imported after the last integration run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Job	Description
OSV Integration Comprehensive	Retrieves all publicly known vulnerabilities associated with all packages that have been imported.
Deps.dev Integration	Retrieves all publicly known versions for packages and used with to identify components in **Stale** and **Abandoned** states.
Update vuln_based_criticality on bom components	Updates criticality for components with vulnerabilities.

Create an application vulnerable item rule in the Software Bill of Materials Workspace

Set up the conditions under which application vulnerable items (AVITs) are created automatically in the AVI Creation Rules module in the Software Bill of Materials (SBOM) Workspace.

Before you begin

The SBOM Response application is required if you want to create application vulnerable items. See Exploring Software Bill of Materials for more information.

Role required: sn_sbom_resp.manage_avi_rule.

Procedure

1. Navigate to **SBOM Workspace** > **AVI Creation Rules**.
2. Select **New**.
3. Fill out the fields.

Field	Description
Name	Name of the rule.
Active	Indicates whether the creation rule is activated.
Execution order	Order in which the rules are evaluated. The rule with the lowest numerical value runs first. For example, you might create higher priority rules for items that need special handling, or where risk is critical, so they are run first. Next, create general rules for items that require no special handling. Finally, create a default rule to catch any components that have vulnerabilities.
Description	Description of the rule to help you distinguish it from other rules.
Conditions	Create the conditions under which application vulnerable items (AVIs) are created. For example, you might select **[Vulnerability > Severity][is][1-Critical]** to create AVITs for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	components that have vulnerabilities that are high-risk and might severely impact you. Note that you can add more conditions.

4. Select **Save**.
   Your creation rule runs automatically after the next upload and creates AVIs for components that match your conditions. You can also run the rule on-demand from the AVI Creation Rules module by selecting **Execute Now**.

Result

After they are created, you can verify that an AVIT was created specifically for SBOM data by checking the values in the **Source** and **Scan type** fields on an AVI record.

Field	Value
Source	SBOM
Scan type	SBOM-SCA

Enterprise security case management applications

Enterprise security case management applications include Security Incident Response, a security orchestration and automation response (SOAR) solution that helps you rapidly respond to evolving threats while optimizing and orchestrating enterprise security operations. It eliminates the errors and friction inherent in manual hand-offs across systems, teams, and responsibilities.

Overview

<Video to be added.>

Get started

The following Security Incident Response applications are available with separate subscriptions from the ServiceNow® Store. See Security Operations and the ServiceNow Store for more information about how to locate, get entitlement, and download apps onto your instance.

Security Incident Response	Major Security Incident Management	Threat Intelligence
		
Learn about the Security Incident Response application	Learn about the Major Security Incident Management application	Learn about the Threat Intelligence application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence Security Center



Learn about the Threat Intelligence Security Center application

Data Loss Prevention Incident Response



Learn about the Data Loss Prevention application

Shared features of Security Incident Response applications



Learn about the features that are shared among the Security Incident Response applications

Troubleshoot and get help

- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Security Incident Response

The ServiceNow® Security Incident Response application tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review, knowledge base article creation, and closure.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Security Incident Response

Explore



Learn about the features of Security Incident Response

Set up and Configure



Install and set up your Security Incident Response application

Administer



Manage and customize your security incidents

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response (continued)

Integrate	Use the Security Incident Response Workspace	Analytics and Reporting
		
Extend Security Incident Response by integrating it with other applications	Learn how to use the Security Incident Response and IT Remediation Workspaces	Monitor remediation progress
		
	Get additional information about Security Incident Response	

Request a Security Operations app on Store

If you are a new Security Operations customer on London Patch 6 or later, visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store.

Understanding Security Incident Response

With Security Incident Response (SIR), manage the life cycle of your security incidents from initial analysis to containment, eradication, and recovery. Security Incident Response enables you to get a comprehensive understanding of incident response procedures performed by your analysts, and understand trends and bottlenecks in those procedures with analytic-driven dashboards and reporting.

https://player.vimeo.com/video/1139195412?h=fa49bba693&badge=0&autopause=0&player_id=0&app_id=58479

Watch this video to learn about the SIR process, using Security Incident Response to thwart attacks and viewing security activity in the Security Incident Response Explorer.

Built in integrations with third-party cyber security solutions and partner-developed integrations from the ServiceNow Store enable security automation and orchestration for efficient and accurate incident response.

To protect your investigations and keep security incidents private, Security Incident Response provides the means to restrict access to the system to specific security-related roles and ACLs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

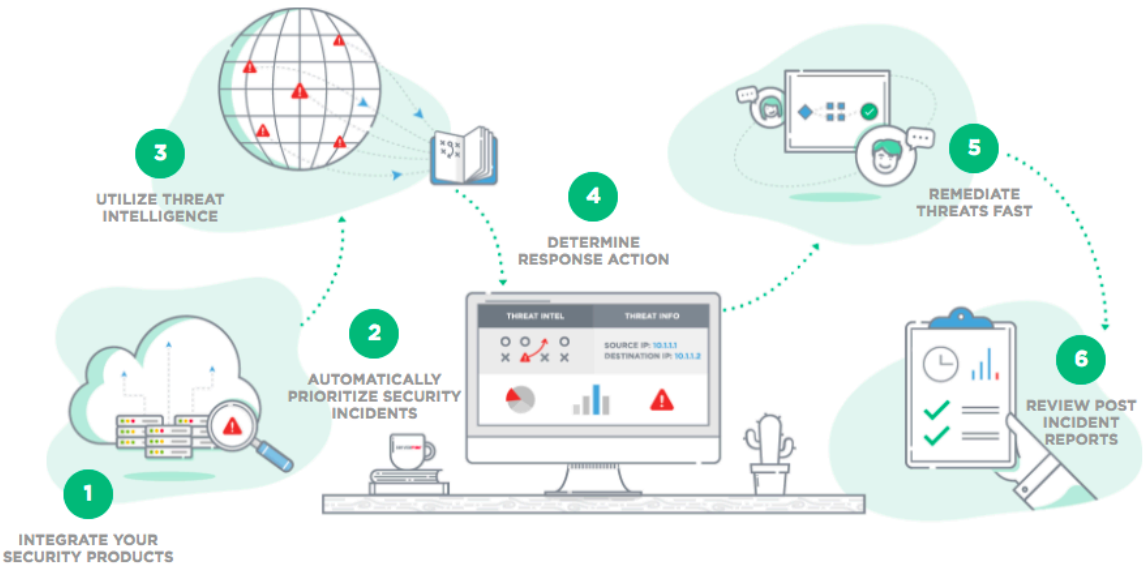
Non-security administrators can be restricted from access, unless you expressly allow them entry.

Note: IT System Administrators [admin] can impersonate ServiceNow users. However, when impersonating a user with an application admin role for Security Incident Response, an admin cannot access features granted by that role, including security incidents and profile information. Access to modules and applications in the navigation bar is also restricted. Also, admin cannot change the password of any user with an application admin role for Security Incident Response.

Security Incident Response information flow

Security Incident Response employs the following flow of information, from integration through investigation, and then on to resolution and review.

Note: This is an interactive infographic, so you can try clicking on any of the icons or steps in the image to learn about that process or task.



1. Click this image to learn about SIR integrations
2. Click this image to learn about Security Incident Creation
3. Click this image to learn about Threat Intelligence
4. Click this image to learn about SIR Workspace
5. Click this image to learn about MITRE Attack features
6. Click this image to learn about Post-incident review activities

Discovery

Security incidents can be logged or created in the following ways.

- From the Security Incident form
- From events that are spawned internally, or created by external monitoring or vulnerability tracking systems via alert rules, or manually
- From external monitoring or tracking systems
- From the service catalog

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Analysis

Depending on the selected view, you are using (default, Non-IT Security, Security ITIL, and so on), the Security Incident form can show any combination of vulnerabilities, incidents, changes, problems, tasks on the affected CI and affected CI groups. The system can identify malware, viruses, and other areas of vulnerability by cross-referencing the National Institute of Standards and Technology (NIST) database, or other third-party detection software. As security incidents are resolved, you can use any incident to create a security knowledge base article for future reference.

Perform further analysis using a business service map to locate other affected systems or business services that can be infected.

Containment, Eradication, and Recovery

As you monitor and analyze vulnerabilities, you can create and assign tasks to other departments. You can use a business service map to create tasks, problems, or changes for all affected systems, documents, activities, SMS messages, bridge calls, and so forth.

Review

After the incident is resolved, other steps can take place before closure. You can perform a post incident review. Creating knowledge base articles can help with future similar incidents. Significant incidents may require a post-incident resolution review. This review can take several forms. For example:

- Conduct a meeting to discuss the incident and gather responses.
- Write and distribute to those teams who worked on an incident a list of resolution review questions designed for each category or priority of incident.
- Incident managers can write the report and gather information on their own.

An incident resolution review report can be automatically generated that includes:

1. a summary of what was done
2. the time line
3. the type of security incident encountered
4. all related incidents, changes, problems, tasks, CI groups
5. the details of the resolution

In addition, an automated security incident resolution review survey system is available. It gathers the names of all users assigned to a security incident, and sends out a customized survey to gather data about the handling of the incident. This data can then be made available in a generated security incident review report, which you can edit into a final draft. Similar data can be added to a knowledge base article to contain lessons learned and the steps to take to resolve similar issues in the future.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Security Incident Response Terminology

The following terms are used in Security Incident Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Term	Definition
Active	Any security incident not in the closed or cancelled state.
Administrator lockdown	The ability to restrict Security Incident Response access to personnel with security-related roles and ACLs.
Inbound security requests	Requests submitted for low-impact security demands, such as requesting a new electronic badge.
Manage post incident activities	A review of the origins and handling of a security incident. The final product is a post incident report, which documents all actions performed and the reasons for doing them.
Response tasks	Tasks assigned to a security incident for tracking actions in response to the threat.
Understanding security incident calculators	Calculators used to update record values when pre-configured conditions are met.
Security incident treemaps	Chart type that hierarchically shows security incident data in the form of nested rectangles.
Threat lookup	A request submitted from the security incident catalog for scanning files, URLs, and IP addresses for malware.
Vulnerability scan	A request initiated from the Security Incident form for scanning affected resources (servers, computers, and other configuration items) for vulnerabilities.

Domain separation and Security Incident Response

Domain separation is supported in Security Incident Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

Domain separation in SIR overview

In the Security Incident Response application, domain separation enables service providers (SPs) to standardize SOC (Security Operations Center) and Security Incident Response (SIR) procedures across the customer base they serve with lowered operational costs and a higher quality of service. Separate customer workspaces for workflows, dashboards, reports, and so forth, ensures that customer data is separated and never exposed to other clients.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Domain separation support in Security Incident Response by version releases

Release	Support level	Notes
Geneva, Helsinki	No support	Initiation of data-level domain separation
Istanbul	Data only	
Jakarta	Level 2 (Data, Requestor, Fulfiller)	**New features**: 3rd-party Integrations support with Level 2 domain separation under a single instance of integration, including Threat Intelligence integrations
Kingston	Level 2 (Data, Requestor, Fulfiller)	**New features**: Sighting Search integration for SIR is enabled with multiple instances, but all instances still live under a single domain. Example: If there are two instances of a Splunk integration configured (SplunkCLOUD and SplunkCORP), both are still leveraged for incident response activities in a single domain, where the implementation was originally configured.
London	Level 2 (Data, Requestor, Fulfiller)	**New features**: All integrations reside across multiple domains
Madrid	Level 2 (Data, Requestor, Fulfiller)	All integrations can now reside across multiple domains. In the above example, SplunkCloud can be domain1 and SplunkCORP domain2.
New York	Level 2 (Data, Requestor, Fulfiller)	All integrations reside across multiple domains.
Orlando	Standard	All integrations reside across multiple domains.
Paris	Standard	All integrations reside across multiple domains.

Domain separation for the Security Incident Response application covers the following product functionality:

- Security alerts are directed to the appropriate domain of the user whose ID/ credential/ scope generates the incident and is registered as a Security Incident.
- Alerts generate “observables,”which represent stateful properties or measurable events: Security workflows in the domain of the security incident are used to orchestrate the response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Integrations are configured in the domain of the security incident for response automation.
- Capabilities are configured in the domain of the security incident for response automation. These capabilities (as of the Kingston release) include:
  - Threat Lookup
  - Enrich Observable
  - Enrich Configuration item
  - Get Running Process
  - Get Network Statistics
  - Block Request
  - Isolate Host
  - Sighting Search
  - Email Search and Delete
  - Publish to Watchlist
- Results from Response Automation (such as Threat Lookup or Sighting Search) are stored in the domain of the security incident.
- Other security incidents are cross-referenced in the same domain of the security incident based on a shared set of observables.
- Other users are cross-referenced in the domain of the security incident.
- Configuration Items are cross-referenced in the same domain as the security incident.
- Manual response tasks are added to the domain of the security incident.
- Knowledge base articles and run books are referenced in the domain of the security incident.
- Security Incident Response metrics pertinent to incidents in the domain are displayed on dashboards as well as in reporting.

Note: In the preceding cases, the overarching principles of visibility in separated domains in the NOW Platform apply. As always, an incident in the parent domain can reference artifacts in the child domain, but not the other way around.

How domain separation works in Security Incident Response

The Security Incident Response application manages the life cycle of a security incident end to end. The following use cases are domain-separation aware:

- **Ingestion of events and alerts** to create security incidents for the analyst in the customer SOC or the MSP to respond:
  - Email parsers (platform based, user-reported phishing, custom)
  - De-duplication events/alerts prior to incident creation
  - Auto extraction of observables
  - Applications in third-party SIEM store
- **Enrichment** of artifacts involved in the incidents (IP, URLs, domains, file hashes):
  - Asset enrichment (CMDB)
  - Users (Platform)
  - Automation: Observable enrichment (Ex: Whols)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Investigate** the incidents with the help of the artifacts and their reputation or association with known threats
  - Orchestrate: Playbooks and knowledge base articles
  - Automation: Threat Lookup (Ex: VirusTotal), Sighting Search (Ex: Splunk), Get Running Processes (Ex: Carbon Black)
- **Eradicate** the threat-related artifacts involved in the incident based on the investigation performed
  - Orchestrate: Playbooks and knowledge base articles
  - Automation: Email search and delete (Ex: Microsoft Exchange), Block IP (Ex: Palo Alto Firewall)
- **Measure** the efficiency or Incident response operations
  - Performance Analytics Dashboards: Productivity and incident trends
  - Reconstruction of incident investigation steps from work notes
  - Post-incident review

Domain separation setup

Setting up domain separation for Security Incident Response doesn't require any additional steps. All Security Incident Response tables acquire the Domain column after the instance is domain separated.

Domain-separated data

Data can be domain-separated, which means:

- Security incidents in one domain can't be viewed from other domains.
- Observables extracted from the security incident are placed in the same domain and can't be viewed from other domains.
- Up to the Kingston release, configured third-party integrations exist in the global domain and are accessible to all other domains in the instance.
- In the Madrid release, third-party integrations can be configured and activated on a per-domain basis. This means that the integration activated and configured in one domain cannot be leveraged in another domain.
- Automations that run on the observables using third-party integrations (for Threat Investigation, Containment, or Eradication), place their results in the domain of the security incident and the results can't be viewed from another domain.
- Orchestration workflows created in one domain aren't visible in another domain.
- Capabilities (as delineated in the preceding capabilities function list) that are invoked stay generic across domains with domain-specific implementation of the capability being called. For example, a Sighting Search on an IP can invoke a Splunk implementation in one domain and a QRadar implementation in another.

Configuration

All aspects of product configuration are self-contained in a domain-separated environment. Setup can be tailored for individual domains.

Note: Business logic and the processes in #2-5 below can be administered within the tenant domain.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following tasks must be configured:

1. System Administration
   - Assign roles to users and groups of users: User roles installed with Security Incident Response
   - Install one or more third-party integration plugins to work with Security Incident Response: Security Incident Response integrations
2. Security Incident Response Administration
   - Add or review roles: Components installed with Security Incident Response
   - Configure groups and users: Create a security incident group
   - Set up incident escalations: Escalate a security incident
   - Set up security incident risk score calculators: Understanding security incident calculators
   - Set up service level agreements: Create a Security Incident Response SLA
   - Set up security incident process definitions: Understanding Security Incident Response process definition
   - Set up post-incident review processes: Manage post incident activities
3. Security incident email settings
   - Set the email parsing inbox: Security Operations email parsing
   - Set up email parsers for alert ingestion: Create email parsers in Security Operations
   - Set up email matching rules for user-reported phishing: Create rules to validate user-reported phishing attacks
   - Set up email inbound actions: Inbound email actions
4. Security incident playbook settings
   - Review and set up runbook documents: Create a Security Incident Response runbook
   - Set up security incident workflows: Security Operations common functionality
5. Capability configurations
   - Block request: Security Operations Integration- Block Request capability
   - Email search and delete: Security Operations Integration- Email Search and Delete capability
   - Enrich configuration item: Security Operations Integration- Enrich CI capability
   - Enrich observable: Security Operations Integration- Enrich Observable capability
   - Get network statistics: Security Operations Integration- Get Network Statistics capability
   - Get running processes: Security Operations Integration- Get Running Processes capability
   - Isolate host: Security Operations Integration- Isolate Host capability
   - Publish to Watchlist: Security Operations Integration- Publish to Watchlist capability
   - Sighting search: Security Operations Integration- Sightings Search capability
   - Threat lookup: Security Operations Integration - Threat Lookup capability

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

How tenant domains manage their own application data

- Tenant domain owners create their own email parsing rules for ingesting security incidents.
- Tenant domain owners can configure specific integrations exclusively for use within the domain.
- Tenant domain owners can create their own incident response workflows.
- Tenant domain owners can create their own incident categories, incident response knowledge base articles, and runbooks to be associated with incident response workflows.
- Tenant domain users create and close their own security incidents.

Business logic and processes that can be domain separated by instance owner

- Security Incident Response users and groups
- Security Incident Response integrations (starting with the Madrid release)
- Email parsing rules for incident creation
- Business rules to consolidate multiple events or alerts into a security incident
- Workflows for incident response orchestration
- Security incident risk score calculators
- Security incident escalation path
- Security incident SLAs
- Security incident process definitions
- Security incident post-incident review processes

Related topics

Domain separation for service providers

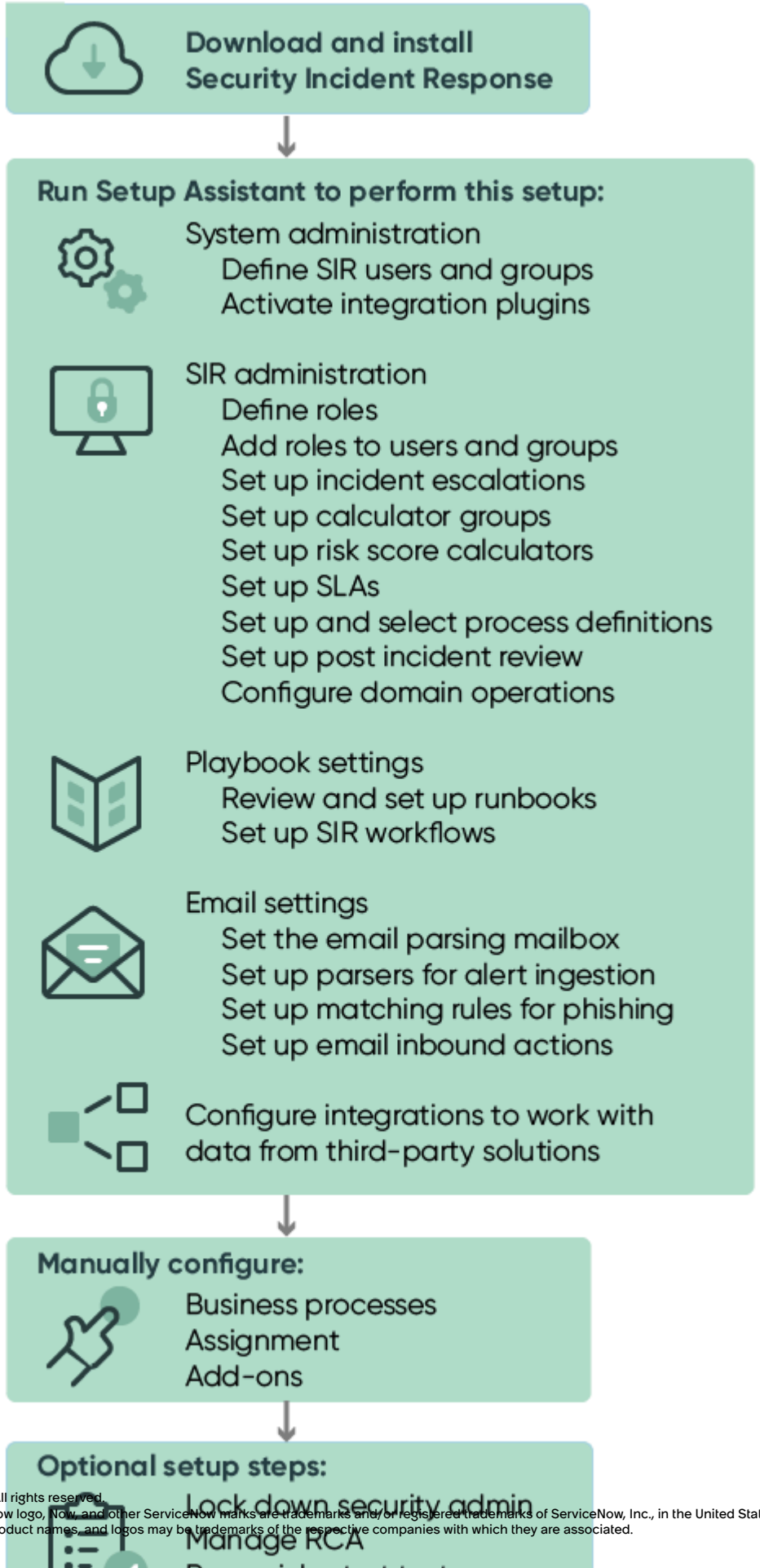
Security Incident Response setup

Setup for Security Incident Response involves some mandatory steps and several optional steps, depending on your specific requirements. After you have downloaded Security Incident Response from the ServiceNow Store and installed it, you are ready to run the Setup Assistant to perform basic configuration for Security Incident Response and third-party integrations.

The Security Incident Response setup process

The following diagram illustrates the setup process. It is separated into two sub-processes, downloading and configuring the Security Incident Response application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The first setup step is to download the Security Incident Response application from the ServiceNow Store. When the download is complete, several dependent applications, including the Setup Assistant, are loaded and ready for use to configure Security Incident Response.

Setup Assistant

The Security Incident Response Setup Assistant is a wizard-like application that guides you, step-by-step, through the setup of your base Security Incident Response instance.



The setup steps are fairly self-explanatory; however, if you require additional explanation, you can find additional assistance in the Setup Assistant reference. After you have completed the setup using the Setup Assistant, you can perform other optional setup procedures, as needed. These procedures include options for:

- Setting up the request life cycle
- Creating catalogs and requests
- Configuring notifications
- Setting up manual and auto-assignment
- Enabling the knowledge base, managed documents, and task activities

A new and improved Security Incident Response Workspace is available. For more information, see Security Incident Response Workspace.

Install and configure Security Incident Response

Before you run Security Incident Response in your instance, you must download it from the ServiceNow Store and complete configuration steps.

Before you begin

Role required: admin

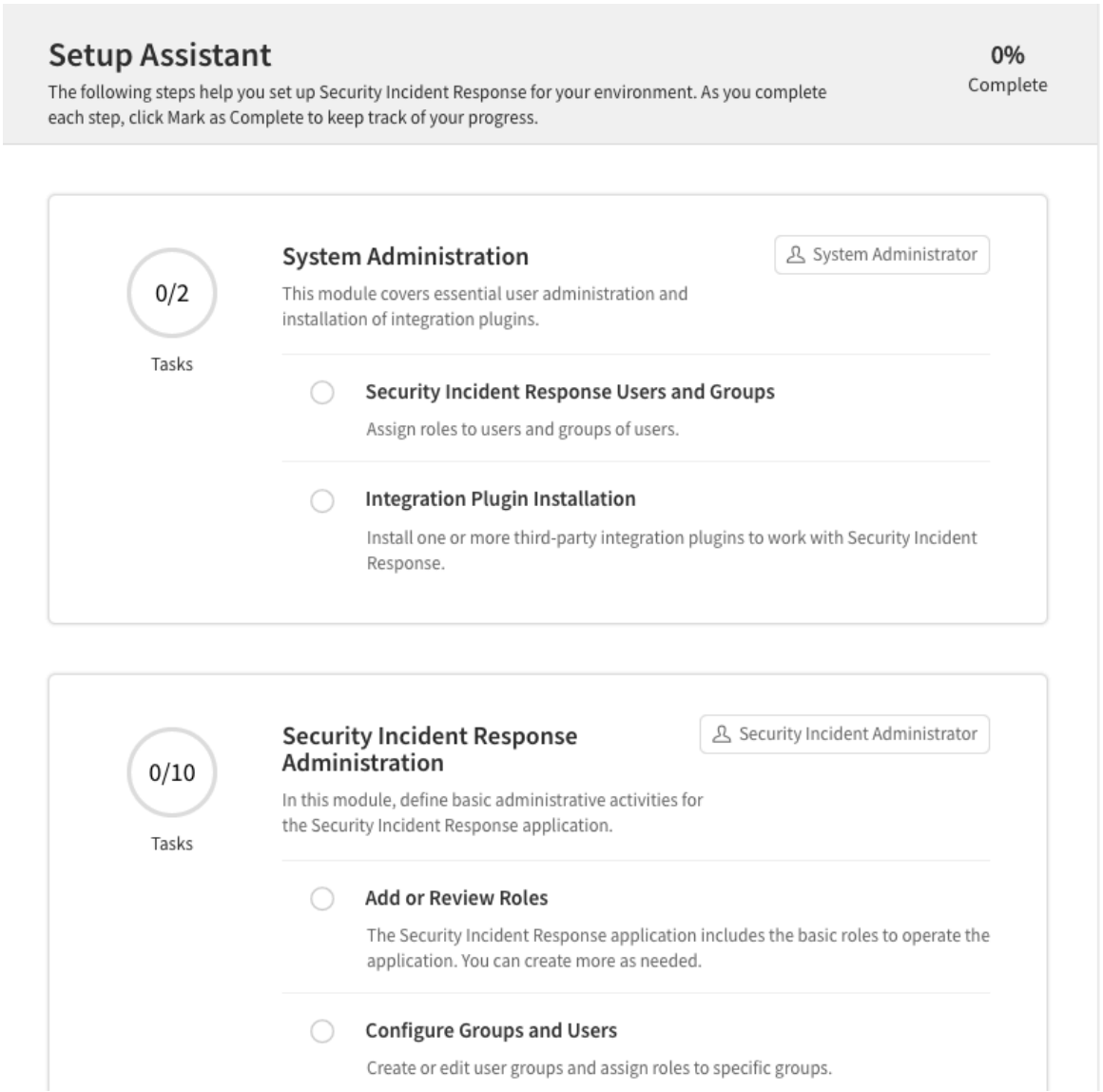
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important:

- Installing the Security Incident Response 13.4.5 version or later from the ServiceNow Store will automatically install the Security Incident Response Workspace (sn_si_aw) 1.5.1 version or later by default. For more information on the dependent applications, refer to the SIR Workspace plugins section.
- Please note that the Security Incident Response Workspace versions 1.5.1 and above can only be installed/upgraded through an installation/upgradation of Security Incident Response and cannot be installed independently.
- The latest features in Security Incident Response are exclusively available in the Security Incident Response Workspace. Please install or upgrade to the latest Security Incident Response or Security Incident Response Workspace version to access and leverage features such as Shift-Handover, Risk Score Calculator, etc.

Procedure

1. Follow the instructions for downloading an application from the ServiceNow Store.
2. After you have downloaded the Security Incident Response application and all of its dependency applications, navigate to **Security Incident** > **Analyst Workspace Setup** > **Setup Assistant**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Follow the instructions on the forms to configure the Security Incident Response base system. For additional information on some of the more complicated setup tasks, see Setup Assistant reference, as needed.

Download and install the Security Analyst Workspace

Before you run the Security Incident Response new UI in your instance, you must download it from the ServiceNow® Store and install it.

Before you begin

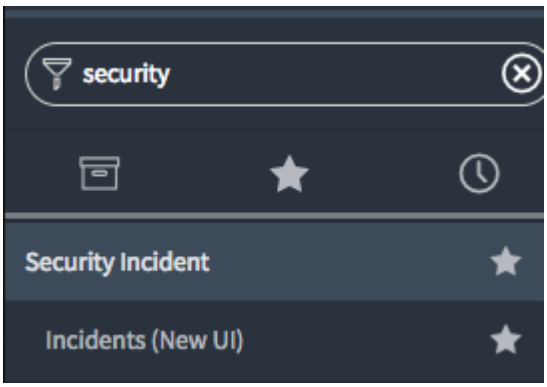
To ensure a smooth installation, verify that you have the required ServiceNow roles for your instance. The following roles are required for installation, configuration, and verification of expected results:

- If not already assigned, the System Administrator [admin] installs the application and assigns the Security Incident Response Admin [sn_si.admin] role.
- The Security Incident Response Admin [sn_si.admin] oversees configuration and verifies expected results.

Role required: admin

Procedure

1. Follow the instructions for downloading an application from the ServiceNow Store and install the **Security Incident Response UI** application.
2. After installation is complete, you can open the Security Analyst Workspace by navigating to **Security Incident** > **Incidents (New UI)**



Components installed with Security Incident Response

Several types of components are installed when you download and activate the Security Incident Response application, including user roles, tables, properties, and scheduled jobs.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Properties installed

Users with the System Administrator [admin] role can view the properties. Users with the Security Administrator [sn_si.admin] role can modify them.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
The default category nodes that are displayed in the Relationship Graph tab within the Workspace. The default values represent the table names corresponding to the related records. sn_si_aw.defaultCategories	• **Type**: string • **Default value**: sn_ti_m2m_task_observables,sn_si_m2m_task_affected_user,sn_
Default start time for all agents when no schedule is set, formatted as 08:00 sn_si.default.start.time	• **Type**: string • **Default value**: 08:00 • **Location**: **Security Incident** > **Administration** > **Properties**
Default end time for all agents when no schedule is set, formatted as 17:00 sn_si.default.end.time	• **Type**: string • **Default value**: 17:00 • **Location**: **Security Incident** > **Administration** > **Properties**
Include Destination type observables along with other context type observables in the security incident user and CI relationships sn_si.link_dest_ip	Determines whether a security incident observable with a context ty Destination is displayed under the **Configuration Items** or **Affected** tabs. By default, observables with a Destination context type are exc include the observables, choose Yes.
Allow customization when creating a Problem or Change Request from a Security Incident sn_si.popup	When a problem or change is created, this property opens a pop-up modify the request. If this properties are set to **false**, the problem or change request has priority, short description, and description as the security incident w option to add or edit those fields. • **Type**: true | false • **Default value**: true • **Location**: **Security Incident** > **Administration** > **Properties**
Associate Sightings Search results with CIs in the CMDB. sn_si.associate_ci_with_sighting_search	When set to true, sightings search results include associated config items that are in your CMDB. • **Type**: true | false • **Default value**: true • **Location**: **Security Incident** > **Administration** > **Properties**
Risk score in the range is highlighted green, formatted as 0-49 sn_si.risk.score.green	In the Security Incidents list, security incidents with a risk score betw 49 are marked with a green dot.
Risk score in the range is highlighted orange, formatted as 50-79	In the Security Incidents list, security incidents with a risk score betw and 79 are marked with an orange dot.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
sn_si.risk.score.orange	
Risk score in the range is highlighted red, formatted as 80-100 sn_si.risk.score.red	In the Security Incidents list, security incidents with a risk score betw and 100 are marked with a red dot.
This parameter enables or disables Sightings Search Configurations that have implemented this feature. sn_si.enable_sighting_search	When set to true, sightings searches can be performed on activated integrations. • **Type**: true | false • **Default value**: true • **Location**: **Security Incident** > **Administration** > **Properties**
The number of rows of raw data that are saved when a Sighting Search is performed. Range 0-100 sn_si.sighting_search_raw_data_rows	This property defaults to 50 rows of raw data. Half of the result rows reported from the beginning of the search time frame and half from t the search time frame. So, if you select 50 rows, 25 come from the st search time frame and 25 from the end of the search time frame.
Automatically advance the Incident State to Contain when a Response Task advances to Work In Progress sn_si.rollup_task_state	While using flows or workflows, consider setting this property to **fals** enables you to control the Incident State from within flows or workflo helps avoid any potential conflicts while transitioning from one incid another. • **Type**: true | false • **Default value**: true • **Location**: **Security Incident** > **Administration** > **Properties**
Assignment properties for Security Incident Response	
Location Weight sn_si.location.weight	A rating used when calculating the criteria to use for auto-assigning analyst. If, for example, location is considered for a task, the location value is added to the security analyst rating. • **Type**: integer • **Default value**: 10 • **Location**: **Security Incident** > **Administration** > **Properties**
Skills Weight sn_si.skills.weight	A rating used when calculating the criteria to use for auto-assigning analyst. If, for example, skills are considered for a task, the skills weig added to the security analyst rating. • **Type**: integer • **Default value**: 10 • **Location**: **Security Incident** > **Administration** > **Properties**
Set the maximum number of security analysts to be processed by auto-assignment at a time	The system has an absolute limit of 300 security analysts. If you spe than 300, it sets the value to that level. The system cannot auto-disp task for a dispatch group that contains more security analysts than t configured.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
sn_si.max.agents.processed	• **Type**: integer • **Default value**: 100 • **Location**: **Security Incident** > **Administration** > **Properties**
Time Zone Weight sn_si.timezone.weight	A rating used when calculating the criteria to use for auto-assigning analyst. If, for example, the security analyst time zone is considered the time zone weight value is added to the security analyst rating. • **Type**: integer • **Default value**: 10 • **Location**: **Security Incident** > **Administration** > **Properties**
Amount of time (in minutes) to add between the end of a task and the travel start of the next. sn_si.work.spacing	An example of a valid time value is 10. • **Type**: integer • **Default value**: 0 • **Location**: **Security Incident** > **Administration** > **Properties**
Specified journal fields containing `code` tags that render content as HTML. sn_si.journal_field.html_enabled	• **Type**: string • **Default value**: work_notes, comments • **Location**: **Security Incident** > **Administration** > **Properties**
Calculate the Impacted services in background. sn_si.refresh_impacted.event	Affected Services/Impacted CIs related list is generated through eve enabled the refresh gets executed in the background and security ta added to the incident. Set the value to **true** to perform the operation in background. • **Type**: true | false • **Default value**: false • **Location**: **Security Incident** > **Administration** > **Properties**
Retrieve the critical service from a pre-calculated data. sn_si.critical_service.calculator.use_cache	Enables the critical service calculator to use a pre-calculated data of configuration items. Set the value to **true** to lookup from a pre calculated data • **Type**: true | false • **Default value**: false • **Location**: **Security Incident** > **Administration** > **Properties**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roles installed

Role title [name]	Description	Contains roles
Security Incident Administrator [sn_si.admin]	Full control over all Security Incident Response data. Also administers territories and skills, as needed. **Note:** In the base system, the administrator also has access to sn_si.admin. Security Incident Response can be restricted from the administrator as long as at least one other user is assigned the security administrator role.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.ingestion_profile_admin • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manage • sn_si.special_access_read_mana • sn_si.special_access_write_mana • sn_ti.malicious_attachment_acce • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Profile Admin [sn_si.ingestion_profile_admin]	Configure the plugins, create, edit, delete, and manage profiles for Splunk, Splunk ES, and Azure Sentinel Integration for Security Operations application.	N/A

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	Note: Users with the sn_si.admin role can perform all operations available to a Profile Admin, as the sn_si.admin role inherits the required permissions by default. The sn_si.ingestion_profile_admin role is assignable to users by the sn_si.admin.	
Security Incident Analyst [sn_si.analyst]	Manage security incidents. Underlying role for basic Security access. Users with this role can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_acce
Security Incident Basic [sn_si.basic]	Underlying role for basic Security access. Users with this role can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user
Chief Information Security Officer (CISO) [sn_si.ciso]	View and manipulate the CISO dashboard. Also, if the Vulnerability Response plugin is activated, users with this role can add vulnerability significance definition treemaps to the	• pa_viewer • sn_si.basic • sn_si.read

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	dashboard. You can also do the same with Security Incident Response plugin.	
Security Incident External [sn_si.external]	View any security incidents that belong to their particular group. **Note:** The following two rules are applicable throughout ServiceNow irrespective of scoped admin or scope app. • When you add any user to a group, you are also assigning roles to that group. Similarly, when you remove a user from a group, the inherited roles will also get removed. • Every role is assignable by some higher precedence role.	service_fulfiller
Security Incident Integration User [sn_si.integration_user]	External tools can provide new security incident records and update security incident records.	import_transformer
Security Incident Knowledge Administrator [sn_si.knowledge_admin]	Manage, update, and delete the information in the Security Incident knowledge base.	• knowledge_admin • sn_si.read
Security Incident Manager [sn_si.manager]	Same access as security analysts.	• pd_author • pd_operator • sn_si.basic
Security Incident Read [sn_si.read]	Read security incidents.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snip • sn_ti.observable.read • workspace_user
Security Restriction Access Manager [sn_si.restriction_access_manager]	Allows users or groups to 'enforce restriction' on security incidents. This is applicable only for field change.	N/A
Security Incident Special Access sn_si.special_access	Provides access to specific security incidents to users	N/A

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role title [name]	Description	Contains roles
	outside of the Security Operations organization.	
Security Special Access Enabler [sn_si.special_access_enabler]	Provides special access role to a user outside of the Security Operations organization to specific security incidents.	N/A
Security Incident Special Access Read Manager [sn_si.special_access_read_manager]	Manage the Security Incident Special Access [sn_si.special_access] role. Use this role to modify the **Read access** field in the security incident form. This role is assignable by sn_si.admin.	sn_si.special_access_enabler
Security Incident Special Access Writer Manager [sn_si.special_access_write_manager]	Manage the Security Incident Special Access [sn_si.special_access] role. Use this role to modify the **Privileged access** field in the security incident form. This role is assignable by sn_si.admin.	sn_si.special_access_enabler

Scheduled jobs installed

Scheduled job	Description
Lookup Security Incident Observables	Performs a lookup for observables on a user-defined schedule.

Tables installed

Table	Description
News Feed Configuration [sn_si_feed_configuration]	Configuration records used to define the content displayed in the security incident news feed.
Post Incident Review Assignment Rule [sn_si_pir_condition]	Automates selection of participants of a post incident review survey when a security incident is closed.
Security Incident [sn_si_incident]	Stores a security incident, the responses to the incident, all linked tasks, changes, problems, and incidents related to this security incident.
Security Incident Attack Vectors [sn_si_attack_vector]	Attack vector options.
Security Incident Audit Log [sn_si_audit_log]	Stores security incident enrichment audit logs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Security Incident Calculator [sn_si_calculator]	A calculator to set certain security incident fields when certain conditions are met.
Security Incident Calculator Group [sn_si_calculator_group]	A grouping of security incident calculators. The order of the calculator group determines which group is evaluated first, and in each group, one calculator at most is used.
Security Incident Enrichment Firewall [sn_si_enrichment_firewall]	Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to Palo Alto Networks Firewall.
Security Incident Enrichment Malware Results [sn_si_enrichment_malware]	Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to malware.
Security Incident Enrichment Network Statistics [sn_si_enrichment_network_statistics]	Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to network statistics.
Security Incident Enrichment Running Processes [sn_si_enrichment_running _processes]	Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to running processes.
Security Incident Enrichment Running Services [sn_si_enrichment_running_service]	Extends from the base table (sn_sec_cmn_enrichment_data_base) and includes all enrichment records specific to running services.
Security Incident Email Search [sn_si_m2m_incident_email_search]	Maps email search records to security incidents.
Security Incident Import [sn_si_incident_import]	Import table for security incidents. Used to create security incidents from external systems.
Security Incident Process Definition [sn_si_process_definition]	Stores configuration for Security Incident process flows.
Security Incident Process Definition Selector [sn_si_process_definition_selector]	Stores the Security Incident Process Definition to use for security incidents.
Security Incident Related Customer Service Case [sn_si_m2m_incident_customerservice_case]	Maps customer service cases and security incidents
Security Incident Related Enrichment Data [sn_si_m2m_incident_enrichment]	Maps security incidents and related enrichment data records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Security Incident Response Task [sn_si_task]	Manages subtasks related to handling a security incident. These tasks can be assigned to security personnel, or to people in other departments, to manage interdepartmental communication and task tracking.
Security Incident Response Task Template [sn_si_task_template]	Used to create a Security Incident Response task. These templates are often used in catalog entries, to automatically create a set of appropriate subtasks for a particular type of security incident.
Security Incident Runbook Document [sn_si_runbook_document]	Associates security incident conditions or filters with a knowledge article. Used to specify runbook procedures for security incident remediation.
Security Incident Template [sn_si_incident_template]	Used to create a security incident. These templates are often used in catalog entries to create a prebuilt security incident.
Security Request [sn_si_request]	A security-related request to the security team.
Security Scan Request [sn_si_scan_request]	A request for a threat lookup.
Severity Calculator sn_si_severity_calculator	Defines the severity, impact, risk, and criticality values for a security incident.
Task Affected User [sn_si_m2m_task_affected_user]	A many-to-many table associating security incidents with affected users.
Template Workflow Activity Outcome Evaluator [sn_si_wf_activity_outcome_evaluator]	Maps a capability with an evaluation script. A new subflow can be added to a template workflow to set a response task outcome rather than having an analyst manually set it.

Other additional Security Incident Response setup tasks

If you are an administrator in the global domain, you configure how Security Incident Response handles day-to-day operations.

Before you begin
Role required: sn_si.admin

Note:

These options are standard to many service management applications, and as such, they use service management terminology. For example, Request is used for the main task (that is, the security incident) and Task is used for subtasks or Response Tasks.

If you are an administrator in a domain lower than the global domain, you can view the Configurations screen, but cannot modify the settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Administration** > **Configuration**.
   The options for configuring the applications are organized under these tabs:
   - The **Business Process** tab contains options for setting up the request life cycle, creating catalogs and requests, and configuring notifications.
   - The **Assignment** tab contains options for setting up manual and auto-assignment.
   - The **Add-ons** tab contains options for enabling the knowledge base, managed documents, and task activities.
2. Fill in the fields on the **Business process** tab.

Configuration screen — Business Process tab

Field	Description
Lifecycle	
Work notes are required to close or cancel a request or task	Enable this option to require the user to enter work notes before a security incident or response task can be closed or canceled.
Copy task work notes to request	Enable this option to synchronize response task work notes with the work notes on the security incident. So when work notes in the task are added, the same work notes appear in the parent security incident.
Catalog and Request Creation	
Create or update requests by inbound email	Enable this option to create or update security incidents from inbound emails.
Requests are created using	Select **catalog or regular form** to activate the catalog and enable automatic publishing of security incident templates to the catalog. Select **regular form only** to deactivate the catalog and disable automatic publishing of security incident templates to the catalog.
Templates create a dedicated catalog item	Enable this option to activate automatic publishing of catalog items for the application.
Notifications	
For a request or task, when the selected field changes, send notification to recipients	You can configure notifications to be sent to specific recipients when selected fields in security incidents and response tasks change. **a.** From **Table**, select **Request (security incident** or **Task (response task)**. **b.** From **Field**, select the field to use for generating notifications. When a change is made to the selected field, a notification is sent to the identified recipients. **c.** From **Recipients**, select one or more recipients. **d.** If you select **a specific user** or **a specific group**, you are prompted to select a user or group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	e. To define more notifications using other fields or recipients, repeat the preceding steps for the next set of notification settings. **f.** To remove a notification, click the ⊖ icon to the right of the notification.

3. Click the **Assignment** tab and fill in the fields.

Configuration screen — Assignment tab

Field	Description
Assignment method for requests	Select the method for assigning security incidents: ○ **using auto-assignment**: Security incidents are automatically assigned. ○ **using a workflow**: Security incidents are assigned by the selected workflow. ○ **manually**: Security incidents are manually assigned.
Use this workflow to assign requests	Select the workflow for dispatching security incidents. This field appears when **using a workflow** is selected from the **Assignment method for requests** list.
Assignment method for tasks	Select the method for assigning response tasks: ○ **using auto-assignment**: Response tasks are automatically assigned. ○ **using a workflow**: Response tasks are assigned by the selected workflow. ○ **manually**: Response tasks are manually assigned.
Use this workflow to assign tasks	Select the workflow for assigning response tasks. This field appears when **using a workflow** is selected from the **Assignment method for tasks** list.
Assign requests or tasks based on assignment group coverage areas	Enable this option to limit the assignment of security incidents and response tasks to groups that cover the location of the task.
Scheduling	
Auto-selection of agents consider time zone for tasks	Enable this option to consider the time zone of the agent when assigning a task. This field appears when auto-assignment is selected for security incidents or response tasks.
Additional Factors	
Auto-selection of agents consider location of agents	Enable this option to give preference to agents who are closer to the task location, when assigning any tasks. This field appears when auto-assignment is selected for security incidents or response tasks.
Auto-selection of agents for tasks	Select the degree to which agent skills must be matched to a task when determining auto-assignment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
requires them to have skills	○ Select **all** to require that an assigned agent must have all the skills to perform the task. An agent who lacks even one skill is eliminated. ○ Select **some** if you want agents who have most of the skills required to perform the task. ○ Select **none** if you want to auto-assign agents without taking skills into account. This field appears when auto-assignment is selected for security incidents or response tasks.
Auto-selection attempt to assign the same agent to all tasks in a request	Enable this option to auto-assign all response tasks for a security incident to the same agent.

4. Click the **Add-ons** tab and fill in the fields.

Configuration screen — Add-ons tab

Field	Description
Documentation	
Enable a dedicated knowledge base	Enable this option to activate the knowledge base for Security Incident Response.
Enable managed documents	Enable this option to add a related list to managed documents.
Enable task activities	Enable this option to log task interactions and communications, such as phone calls and email messages.

5. Click **Save**.

Lock down security administration

To protect investigations and keep security incidents private, you can restrict Security Incident Response access to security-specific roles and ACLs. Non-security administrators can be restricted from access, unless you expressly allow them entry.

Before you begin

When the Security Incident Response application is activated, the System Administrator user is granted the sn_si.admin role by default. The System Administrator is the only administrator who can set up security groups and users.

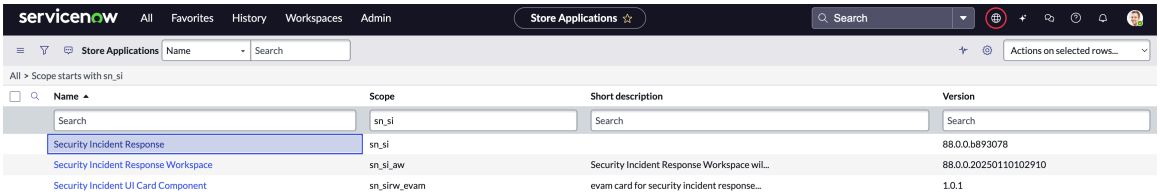
A security role is required to have access to Security Incident Response features and records.

Role required: sn_si.admin

Procedure

1. After the Security Incident Response plugin has been activated, a user with the admin role assigns the Scoped Admin (sn_si.admin) role to at least one user.
2. The user with the admin role changes to the Security Incident scope.
3. Navigate to **All** > **sys_store_app.list**.
4. Type **sn_si** in the **Scope** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Security Incident Response**.
6. Scroll down to the **Related Links** and click **Remove from the role contained by admin**.
7. Log out and log back in.
   The admin user cannot access the Security Incident Response application.

Related topics

Application administration

Manage Restricted Caller Access

The Restricted Caller Access (RCA) feature enables an administrator to define cross-scope access to an application or application resource and allow or deny access requests. This feature is enabled in Security Incident Response by default so security analysts can protect sensitive security-related information.

A field called **Caller access** has been added to all tables and script includes in Security Incident Response, and the field defaults to **Caller Tracking**. This setting means that application scopes are allowed access to Security Incident Response tables and script includes. However, a tracking record is created for each record and stored in the Restricted Caller Access Privilege [sys_restricted_caller_access] table.

Note: Take care when changing records from **Caller Tracking** to **Caller Restricted**. Records with this status cannot be accessed until an administrator manually allows access to it. The administrator must navigate to **System Applications** > **Application Restricted Caller Access**, locate the table or script include for which access has been requested, and change the **Status** field from **Requested** to **Allowed**.

Related topics

Restricted caller access privilege settings

Set the application scope, application resource, and event access

Run quick start tests for Security Incident Response

Validate that Security Incident Response still works after you make any configuration changes, such as applying an upgrade or developing an application. Copy and customize these quick start tests to pass when using your instance-specific data.

Security Incident Response quick start tests require activating Security Incident Response plugin (com.snc.security_incident) and loading the demo data.

Security Incident Response tests

Test	Description	Release version
SIR: Create Security Incident	Determine whether a user can successfully create a security incident from the security incident form.	Xanadu

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response tests (continued)

Test	Description	Release version
SIR: Create Security Incident via Security Incident Catalog	Determine whether a user can successfully create a security incident from the catalog.	Xanadu
SIR: Security Incident life cycle	Validate the response tasks of the Policy Violation workflow.	Xanadu
SIR: Threat Lookup	Validates the Threat Lookup capability.	Xanadu
SIR: PIR Assessments OOTB configuration	Use this test to validate PIR assessments and base system configurations.	Xanadu
SIR: PIR Assessments conditional configuration	Verify that security incidents matching the mandatory conditional rule are not closed without completing the post incident assessment. Verify that the security incidents matching the optional conditional rule can be closed without completing the post incident assessment. Verify that assessments are not generated for the security incidents that do not match any rule.	Xanadu
SIR: PIR run time verification	Verify that PIR reports are configured and attached to the security incidents as per the new design.	Xanadu
SIR: PIR design time setup verification	Verify that the security incident is mapped with the report template based on the administrator configuration.	Xanadu
SIR: Link Security Incident to a existing Major Security Incident	Link a Security Incident to an existing Major Security Incident and validate data from Security Incident rolled up to Major Security Incident.	Xanadu
SIR: Promote Security Incident as Major Security Incident	Promote a Security Incident as Major Security Incident and validate data from Security Incident rolled up to Major Security Incident.	Xanadu
SIR: Propose Security Incident as Major Security Incident	Propose a Security Incident as Major Security Incident and validate data from Security	Xanadu

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response tests (continued)

Test	Description	Release version
	Incident rolled up to Major Security Incident.	
Verify that only Allowed Members can access the security incident once Enforce Restriction is ON	Verify that only the allowed members can access the security incident once the Enforce Restriction is enabled.	Xanadu
Verify that only Allowed Groups can access the security incident once Enforce Restriction is ON	Verify that only the allowed groups can access the security incident once the Enforce Restriction is enabled.	Xanadu
Validate Read Access	Validate the view access.	Xanadu
Validate Write Access	Validate the edit access.	Xanadu

Related topics

Quick start tests

Setup Assistant reference

The Setup Assistant walks you through the steps you need to perform to set up the Security Incident Response base system. This section provides additional information on the complicated steps for which you may require more explanation.

Create a Security Incident Response process definition

You can create a process definition to define the way security incidents transition from one state to the next. Process definitions give service desks and end users help tracking the problem throughout its life cycle.

Before you begin

Role required: sn.si_admin

Procedure

1. Navigate to **All** > **Security Incident** > **Administration** > **Process Definition**.
2. Click **New**.
3. Fill in the fields, as appropriate.

Creating process definitions

Field	Description
Name	Name of the record which describes the process encoded in the script include file. The name is displayed as a choice in the **Process Definition Selector** list.
Script include	The name (including the `sn_si.` prefix) of the script include containing the definition of the process. The script must be in the Security Incident (`sn_si`) application scope. See Create a custom Security Incident Response process definition script include

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	for more information. If this field does not contain a valid script include name, the default ProcessDefinition_NIST_Stateful definition is used.
Description	Helpful information about the script include.
Order	Determines the position in the process definition list.
Active	When checked, it makes this process definition selectable from the **Process Definition Selector** page.

4. Click **Submit.**

Related topics

Security Incident Response Process Selection

Understanding Security Incident Response process definition

Understanding Security Incident Response process definition

Security Incident Response Process Definition replaces state flows and provides end users and service desks with the status of a problem. A process definition helps track the problem through its life cycle. Security Incident Response is a Service Management (SM) application, which has its own set of states. Invalid states are reported as part of Process Selection.

Security Incident Response Process Definition

The default process definition (NIST Stateful) defines the following incident states:

Note: Available states vary based on the current state of the incident.

Security Incident process definition states

State	Description
Draft	The request initiator adds information about the security incident, but it isn't yet ready to be worked on.
Analysis	The incident has been assigned and the issue is being analyzed.
Contain	The issue has been identified and the security staff is working to contain it and perform damage control. These actions can include taking servers offline, disconnecting equipment from the internet, and verifying that backups exist.
Eradicate	The issue has been contained and the security staff is taking steps to fix the issue.
Recover	The issue is resolved and the operational readiness of the affected systems is being verified.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident process definition states (continued)

State	Description
Review	The security incident is complete and all systems are back to normal function, however, a post incident review is still needed.
Closed	The incident is complete but before a security incident can be closed, you must fill out the information on the **Closure Information** tab.

Security Incident task process definitions

The following process definitions are used for security incident tasks.

Task process definition states

State	Description
Ready	The task is ready to be worked on after it's assigned to an agent.
Assigned	The task is assigned to an agent.
Work In Progress	The assigned agent is working on the task.
Complete	The task is complete.
Canceled	The task was canceled.

NIST supports the following two models:

- **NIST Stateful**

  This process definition enables analysts to move from one state to another in a sequential order without skipping any step. For example, if the Analyst starts with the **Draft** state, then the sequential order of this process definition is **Draft**>**Analysis**>**Contain**>**Eradicate**>**Recover**. So, the NIST Stateful process definition is unidirectional and enables analysts only to progress only to the forward states.

  Here's another example, if the Analyst starts with the Analysis state, then the sequential order of this process definition is **Analysis**>**Contain**>**Eradicate**>**Recover**.

- **NIST Open**

  This process definition enables analysts to move from one state to another, either forward or backward. For example, if the Analyst starts with the **Analysis** state, then the order of the process definition can either be **Analysis**>**Contain**>**Eradicate**>**Recover** or **Analysis**>**Draft**. So, the NIST Open process definition is bidirectional and enables analysts to move to the forward or backward states depending on their requirements.

Security Incident Response Process Selection

Security Incident Response Process Selection lists processes with invalid states for security incidents and response tasks.

An administrator can correct the incident or task to valid states either manually or by using a script. An empty related list (no incidents; no tasks) indicates that every active task is in a valid

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

state. Available states vary based on the current state of the incident. For more information, see Correct an invalid security incident or task state with process definition.

Select a Security Incident Response process definition

You can select the process definition to use for the appropriate states for your company security incidents and response tasks.

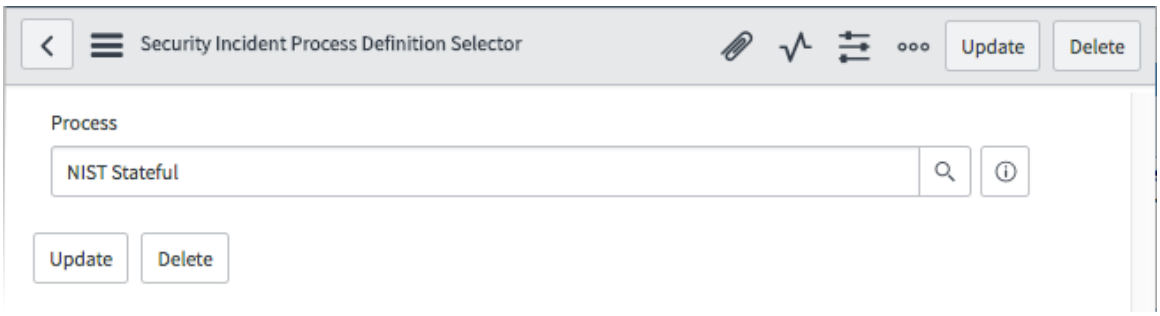
Before you begin

Role required: admin and sn_si.admin

About this task

Procedure

1. Navigate to **All** > **Security Incident Response** > **Administration** > **Process Selection**.
2. Click the search icon to list the available process definitions.



3. Select a process definition.
4. Click **Update**.

Create a custom Security Incident Response process definition script include

Create a custom Process Definition script for the appropriate states for your company security incidents and response tasks.

Before you begin

Role required: sn_si.admin

About this task

The sn_si.ProcessDefinition main script include controls process definitions. **Process Definition** determines which definition is in use (using **Process Selection**). It calls the appropriate script include file to determine the initial states and transitions for both security incidents and response tasks.

Procedure

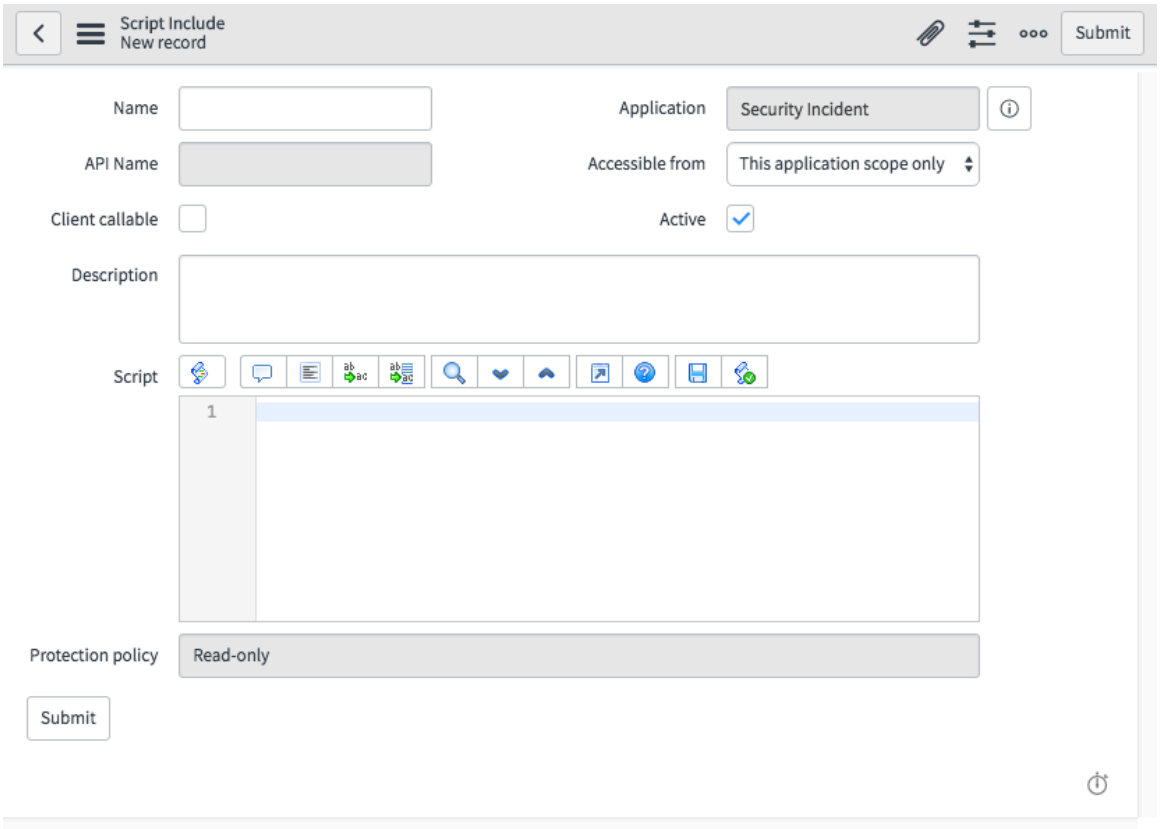
1. Navigate to **All** > **System Definition** > **Script Includes**.
2. Click **New.**
3. Fill in the fields, as appropriate.

Creating process definitions

Field	Description
Name	Name of this script include.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
API Name	Created based on the name of the script include.
Client callable	Makes the script include available to client scripts, list and report filters, reference qualifiers, or, if specified, as part of the URL.
Application	Security Incident
Accessible from	Choose **This application scope only** .
Active	When checked, it makes this script include selectable from the **Process Definition** page.
Description	Helpful information about the script include.
Script	Defines the server-side script to run when called from other scripts. The script must define a single JavaScript class or a global function. The class or function name must match the Name field. For information on script contents, see Process Definition script include.



4. Click **Submit.**

Related topics

Process Definition script include

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Process Definition script include

The Process Definition script include provides methods for defining a process definition.

Implement the constants, attributes, arrays, and method calls described here to customize a process definition script include.

Where to use

Use this script include to create a process definition.

Script include body

The script include body is composed of three sections:

- Constants: Initial state definitions
- Security Incident and Response Task: Process definition arrays
- Method calls: Retrieving information

Constants

Constants are used to define the initial states of security incidents and response tasks.

The use of constants is optional but encouraged for readability. For example:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Which are later used by the following methods:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

The next set of constants defines the states for both security incidents and response tasks.

Each array also contains the definition of which states are available when the incident or task is in a specific state.

For example:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

The example is an array of objects. Each object defines a state and possible transition states.

The order of the state's object determines the desired order for the flow.

When the task is in the 'Draft' state (value 1), possible states are: 1 (Draft, which is no change) and 10 (Ready, the next step in the process).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

There is no limit on the number of transitions out of a state. The 'Close Complete' and 'Canceled' state are final states and therefore have no possible state transitions.

The order of the attributes in the object is not important. If it makes the definition clearer, put the label first.

Attributes

Required attributes in a state definition object are:

- state: numerical value of the state
- label: human readable text associated with the state
- choice: an array of state values the state can transition to (determines the content of the state dropdown)

Optional attributes are:

- mandatory: list of field IDs that become mandatory in this state
- readonly: list of field IDs that become read-only in this state
- visible: list of field IDs that become visible in this state
- notmandatory: list of field IDs that become non-mandatory in this state
- notvisible: list of field IDs that would no longer be visible in this state

Note:

If optional attributes are used, it is the author's responsibility to ensure that fields are made visible/invisible, mandatory/non-mandatory, visible/hidden, or readonly appropriately between states.

For example, hiding a field in one state does not make it visible in another state later unless the 'visible' attribute is used.

Process flow definition arrays

To define the information displayed in the process flow formatter (the bar at the top of the Security Incident and Response task forms), the system requires information on what to display for each state.

For example:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ",
 description:"<p>Security Incident Response Task is in
 draft</p>"},
 {label:"Ready", condition:"state=10^EQ",
 description:"<p>Security Incident Response Task is ready to be
 assigned</p>"},
 {label:"Assigned", condition:"state=16^EQ",
 description:"<p>Security Incident Response Task is
 assigned</p>"},
 {label:"Work in Progress", condition:"state=18^EQ",
 description:"<p>Work has started on this Security Incident
 Response Task</p>"},
 {label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ",
 description:"<p>Security Incident Response Task is
 complete</p>"},
],
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The TASK_PF array is a collection of labels, conditions, and descriptions used to determine the text displayed in the process formatter bar (including order and activity).

In the example, the text 'Ready' is the second item displayed. It is highlighted when the task satisfied the condition 'state=10^EQ'.

When the pointer hovers over the text, the description 'Security Incident Response Task is ready to be assigned' is displayed.

Note:

States can be combined to a single formatter state.

In the example, both the 'Close Complete' and the 'Canceled' states show up as 'Closed' in the top bar.

Method calls

The following methods must be present in the script include as they are used by sn_si.ProcessDefinition:

Return type	Method summary	Description
String	getInitialIncidentState: function()	return the initial incident state numerical value
String	getInitialTaskState: function():	return the initial task state numerical value
Array of string	getIncidentStates: function():	return the incident state's array
Array of string	getTaskStates: function():	return the task state's array
Array of objects	getIncidentProcessFlows: function():	return the incident process flow definition array
Array of objects	getTaskProcessFlows: function():	return the task process flow definition array

The next set of methods are called whenever an incident or a task is updated and allows actions to be taken on specific change transitions.

Return type	Method summary	Description
void	performIncidentStateChange: function(current, previous)	In the examples, this method is used to set SM-related values and ensure that an incident advances out of 'Draft' once someone is assigned to it.
void	performTaskStateChange: function(current, previous)	In the example, this method is used to update timestamps (on assignment and closing) and advance the task from 'Ready' to 'Assigned' once the assigned_to field is filled.

The same actions performed by these two methods can be accomplished using a business rule. By defining them in the script include, switching process definitions is made easier.

Correct an invalid security incident or task state with process definition

An administrator can correct the security incident or task to valid states, either manually or using a script. Available states vary based on the current state of the incident.

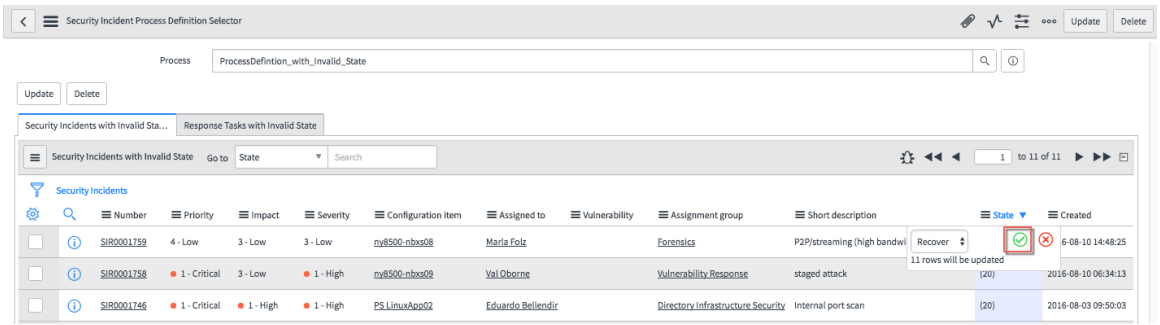
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
After you have switched process definitions, the new definition may not support some of the old states. To correct the orphan incident or task states, you can change your process definition, edit your script include, or manually open each incident or task to update the state. Generally, updating the state (which can be done in bulk) is the easiest solution.

To change states in bulk, do the following:

Procedure
1. Navigate to **All** > **Process Selection**.
2. Highlight the **State** field for the incidents or tasks you want to change.
3. Double-click the **State** field in the first record, select the new **State,** and click the green check mark ( ) to complete the change.



4. Click **Update**.

Create a security incident group

Set up a security incident group and assign the appropriate roles and users to the group.

Before you begin
Roles required:

- If you have the user_admin role, you can create security incident assignment groups.
- If you have the sn_si.admin role, you can create and edit security incident assignment groups.

About this task
Users in a group inherit the roles of the group, so you do not have to assign roles to each user separately.
It is a good practice to create as many groups as needed in your organization. It is also a good practice to create one group for administrators and assign the admin role to this group only.

Procedure
1. Navigate to **All** > **User Administration** > **Groups** or **Security Incident** > **Setup** > **Groups**.
2. Click **New**.
3. On the form, fill in the fields.

Note:

For more information, see Create a user group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Make sure that you select the **security incident** type for this group.
   a. If the **Type** field is not visible, configure the form to add it.
   b. Click the lock icon beside the **Type** field.
   c. Click the reference lookup icon ()
   d. Search for and select the **security incident** type.
5. Right-click the form header and select **Save**.
6. In the **Roles** related list, add the roles that each member of this group receives.
   For example, if you are making a group for Security Incident Response team members, add sn_si.analyst. If you are making a group for Security Incident Response administrators, add sn_si.admin.
7. In the **Group Members** related list, add users to this group.
8. Click **Update**.

Create a security incident calculator group

Security incident calculator groups are used to group calculators.

Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to **All** > **Security Incident** > **Setup** > **Security Incident Calculator Groups**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the security incident calculator.
Application	The application that contains this record.
Order	The order in which the security incident calculator is run. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Description	A description of this calculator group.
Created by	Enter the name of the user who created

4. Click **Submit**.

Create a security incident calculator

Security incident calculators allow you to calculate the severity of a security incident based on pre-defined formulas. You can define your own security incident calculators, as needed.

Before you begin
Role required: sn_si.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Setup** > **Security Incident Calculator Groups**.
2. Click the name of the group for which you want to create a calculator, or you can create a calculator group.
3. Click **New**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the security incident calculator.
Calculator Group	Name of the group to which this calculator belongs. **Note:** Creating or changing the calculator group becomes available after you have entered a **Name** and **Table**.
Table	Select the table to be used for this calculator. When you add calculators to tables other than Vulnerability [sn_vul_vulnerability] and Vulnerable Item [sn_vul_vulnerable_item], you must add business rules and UI Actions to those tables. To see examples: ○ Navigate to **System Definition** > **Business Rules**, and locate the **Calculate Severity** business rule on the Vulnerable Item [sn_vul_vulnerable_item] table. ○ Navigate to **System UI** > **UI Actions**, and locate the **Calculate Severity** UI action on the Vulnerable Item [sn_vul_vulnerable_item] table. Also, the vulnerability admin role must be granted full read, write (or save_as_template) capabilities on any table used by a calculator to properly see the values to apply to the template.
Application	The scoped application to which the calculator belongs.
Order	The order in which the security incident calculator runs. A calculator with an order entry of 100 runs before a calculator with an order entry of 200.
Active	Turn the calculator on or off.
Description	A description of this calculator.

5. Right-click the form header and select **Save**.
   The **Conditions** and **Values to Apply** tabs appear.
6. Fill in the fields in the **Conditions** tab, as appropriate.

Field	Description
Use filter group	Select this check box to use a predefined filter group or create a new filter group to define the calculator criteria.
Filter group	Select the filter group to use for defining a calculator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	This field appears only if you selected the **Use filter groups** check box.
Use advanced condition	Select this check box to indicate that a script condition is used to determine when this calculator is applied. When you select the check box, an **Advanced condition** scripting field appears. If you selected the **Use filter group** check box, this field is hidden. **Note:** Before you define advanced conditions and write scripts for determining when the security incident calculators are applied, return to the Security Incident Calculators list. Explore the calculator records shipped with the base system.
Condition	Defines basic filter conditions for determining whether the calculator is used. If you selected either of the **Use filter group** or **Use advanced conditions** check boxes, this field is hidden.

7. Click the **Values to Apply** tab and fill in the fields on the form, as appropriate.
You have the choice of creating a script for defining the values to apply to the calculation or defining a template based on fields in the selected table.

Field	Description
Use script values	Select this check box to define field values with a script.
Script values	Defines what values to apply the calculations to. This field appears only if you selected the **Use script values** check box.
Template	Right-click the form header and select **Save**. Select the fields and values you want to use for the calculator.

8. When you have completed all entries, click **Submit**.

Understanding security incident calculators

Security incident calculators are used to update record values when pre-defined conditions are met. The calculators are grouped based on the criteria used to determine how the records are updated.

The Security Incident Response base system includes the following security incident calculator groups and calculators. Within each group, the first calculator that matches the conditions is run.

Security incident calculators in the base system

Security Incident Calculator Group Name	Calculators included in group	Description
Business Impact	Aggregate from Severity Calculators	This calculator delegates to the Security Criticality Calculator that

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident calculators in the base system (continued)

Security Incident Calculator Group Name	Calculators included in group	Description
		determines criticality by weighing the values of other fields.
Severity	Business Impacted	This severity calculator defines its selection criteria using a simple condition builder.
	Critical service affected	This severity calculator defines its selection criteria using an advanced condition. If the configuration item in the security incident is associated with a highly critical business service, the **Risk score**, **Business Impact**, and **Priority** fields are elevated as defined by the calculator.
	Critical service changes	This severity calculator defines its selection criteria using an advanced condition. If the security incident meets the conditions, a script runs to define what levels the fields are elevated to. If the configuration item in the security incident is associated with a most critical or somewhat critical business service, the **Risk score**, **Business Impact**, and **Priority** fields are elevated as defined by the calculator.
	Multi-Attack Vectors	This severity calculator defines its selection criteria using a simple condition builder. If the configuration item in the security incident is associated with web, email, and impersonation attack vectors, the **Risk score**, **Business Impact**, and **Priority** fields are elevated as defined by the calculator.
	Set priority with category and services	This severity calculator defines its selection criteria using an advanced condition builder. The security incident priority is set to **1 - Critical** when the following conditions are met:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident calculators in the base system (continued)

Security Incident Calculator Group Name	Calculators included in group	Description

		• The security incident has associated affected services and one of them is critical.
		• The security incident category is one of the following:
		  ○ Denial of Service
		  ○ Spear Phishing
		  ○ Malicious code activity
		Note: This calculator is available in the base system when you have the Starter Security Operation pricing tier.

	Set priority with observables	This severity calculator defines its selection criteria using an advanced condition builder.
		The security incident priority is set to**1 - Critical** when the following conditions are met:
		• The security incident has associated affected services and one of them is critical.
		• The security incident category is one of the following:
		  ○ Denial of Service
		  ○ Spear Phishing
		  ○ Malicious code activity
		• One of the associated observables or indicators has a sighting count that exceeds two sightings with active indicators (that is, the observables or indicators are confirmed as being bad from multiple sources).
		Note: This calculator is available in the base system when you have the Advanced Security Operation pricing tier and you activate the Threat Feeds plugin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident calculators in the base system (continued)

Security Incident Calculator Group Name	Calculators included in group	Description
User criticality	Get user criticality	This severity calculator defines its selection criteria using a simple condition builder. This severity calculator causes user business criticality to change to **1 - Critical** when the **Department** field is changed to **Finance**.
	Get user group criticality	This severity calculator defines its selection criteria using an advanced condition builder. This severity calculator provides example of a calculator that runs on data in a related list.

Severity calculators

When you create a security incident, the **Risk score**, **Business Impact**, and **Priority** fields contain default values. When you save the incident, a business rule automatically validates the information in the security incident against conditions defined in each of your active severity calculators. They are validated one security calculator at a time, in the order defined by the **Order** field in each calculator. If information in the security incident matches the conditions defined in one of the calculators, the severity field values are updated accordingly to the rules set up in the calculator.

For example, assume that you create a security incident for an affected CI, and the CI is highly critical. When the security incident is saved, the CI information is compared to the conditions defined in the severity calculators. When the security incident is validated against the **Critical service affected** severity calculator, the severity fields are automatically updated, and a message similar to the following appears at the top of the security incident.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

You can use these severity calculators as is or you can edit them to more closely meet the needs of your business. For example, if you want to identify web and email threats that are specific to the Finance business unit, you can change the conditions of the **Multi Attack Vectors** calculator:

- [Attack Vector] [contains] [Web]
- [Attack Vector] [contains] [Email]
- [Business Unit] [contains] [Finance]

You can also update the severity values in an existing security incident at any time by opening the record and clicking the **Calculate Severity** related link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident risk score calculators

The **Set priority with category and services** and **Set priority with observables** calculators are used to calculate a risk score for a security incident.

User criticality calculators

The two calculators in the **User criticality** group (**Get user criticality** and **Get user group criticality**) provide examples of how you can drive criticality based on criteria defined in a user record or based on the group to which a user belongs.

They can be edited as needed, or new user criticality calculators can be created.

The **Get user criticality** calculator causes user business criticality to change to **1 - Critical** when the **Department** field is changed to **Finance**.

The **Get user group criticality** calculator causes user business criticality to change to **1 - Critical** when the user is added to the **Database** group.

Note: **Get user group criticality** is an example of a calculator that runs on data in a related list. If you want to add more groups to initiate a criticality change, add a comma-separated list of group sys_ids in the first line of the script. Example: `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id]`.

Security incident risk score calculations

The risk score is calculated as an arithmetic mean that represents the risk based on the priority of a security incident, the type of security incident (Denial of Service, Spear Phishing, or Malicious code activity), and the number of sources that triggered a failed reputation score on an indicator.

The risk score aids in prioritizing security incident work for the analysts.

Important: If you want to use the new Risk Score Calculator, refer to Define the new Risk Score Calculator Rules.

The **Set priority with category and services** and **Set priority with observables** security incident calculators are used to calculate a risk score for a security incident. Additionally, the following business rules trigger automatic calculation of risk scores:

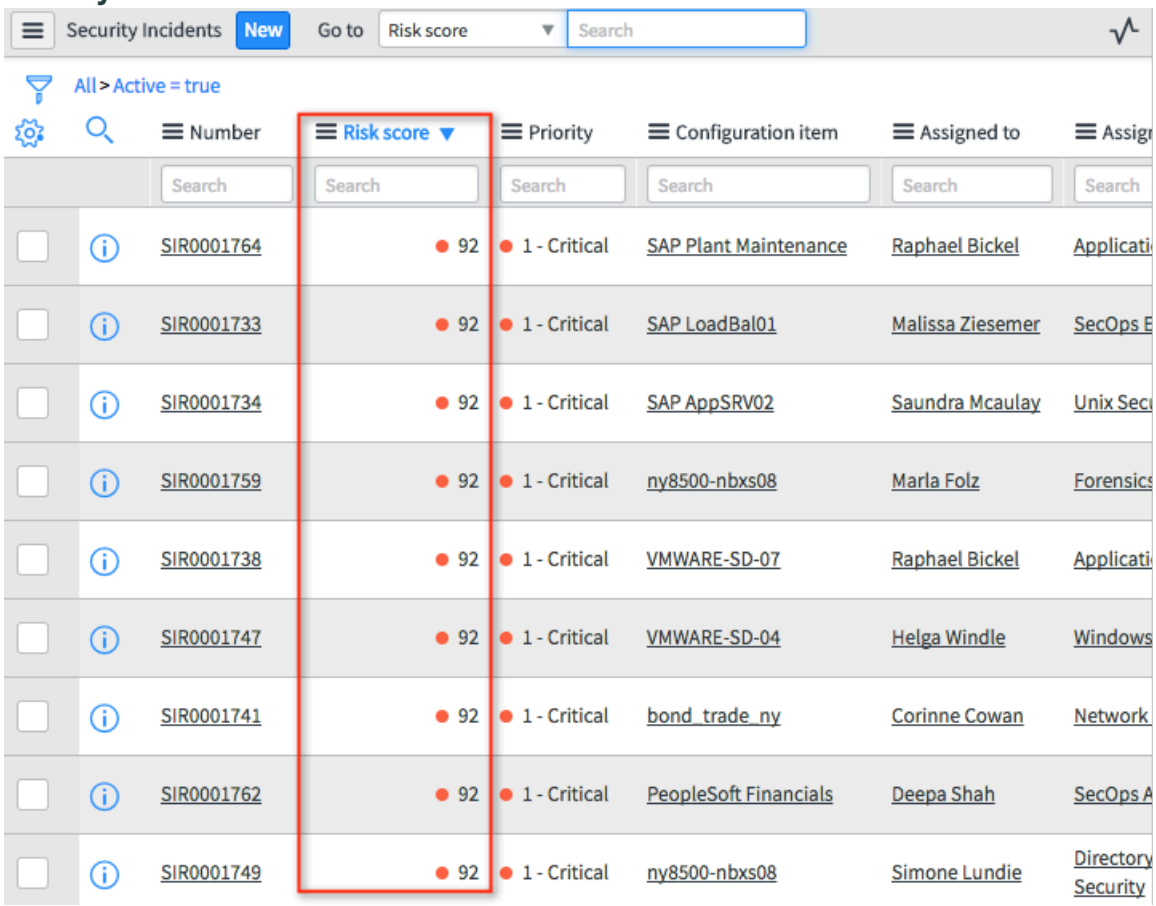
- Calculate Severity
- Update risk score
- Update SI risk score

Note: The risk calculator available in the base system depends on your Security Operations pricing tier.

When you look at a list of security incidents in the base system, notice the **Risk score** column.

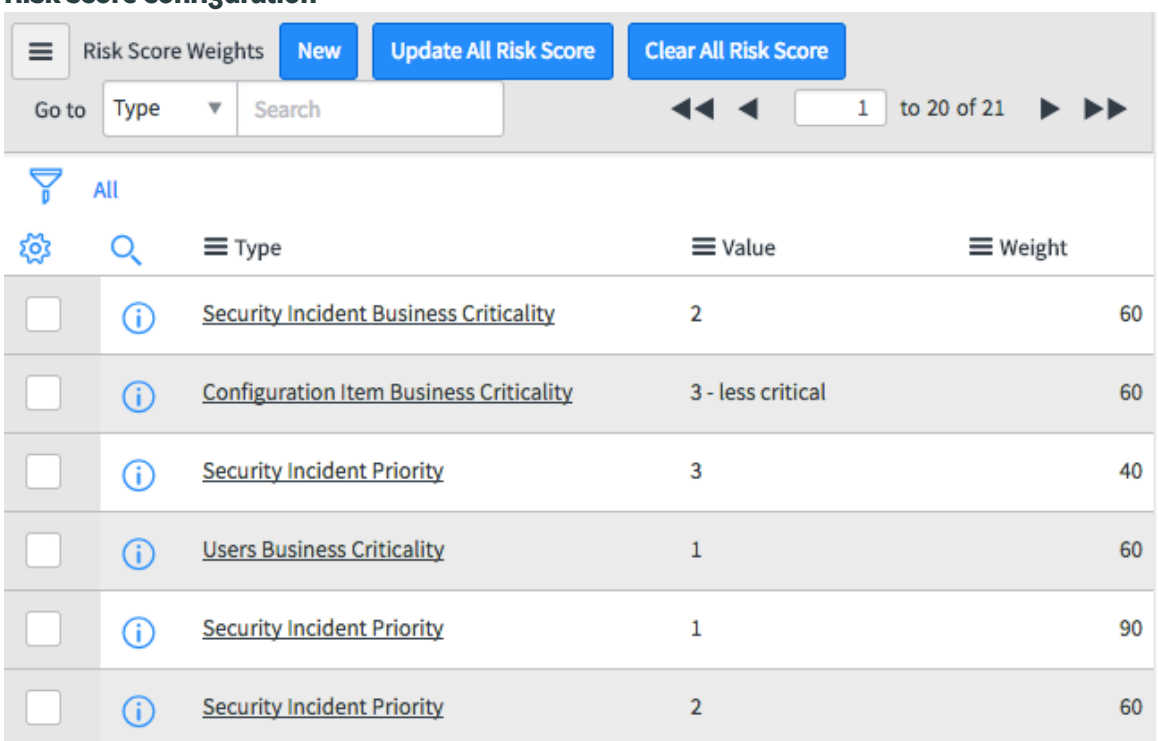
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incidents



The risk score is calculated using weights defined in **Risk score configuration**.

Risk score configuration



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, if a security incident has a **Business impact** set to **2-High** and a **Priority** set to **3-Moderate**, the respective weights in the Risk Score Weights table are looked up and calculated thus:

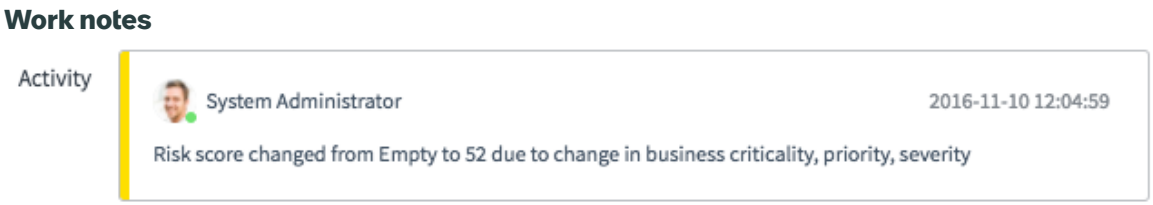
Security Incident Business Impact with a value of 2 = a weight of 60.

Security Incident Priority with a value of 3 = a weight of 40.

(60 + 40)/2 = a risk score of 50.

The position of the security incident in the security incident list is then re-ordered based on its updated risk score.

If, in the example above, the **Business impact** or **Priority** of the security incident are changed, the risk score is recalculated, and the changes are reflected in the work notes.



The work notes are updated when the following fields are changed (causing the risk score to be updated):

- **Business impact** on the Security Incident form
- **Priority** on the Security Incident form
- **Severity** on the Security Incident form (hidden by default)
- **Business impact** on the **Affected Users** related list
- **Business impact** on the **Affected Services** related list
- **Business impact** on vulnerabilities on the **Vulnerable items** related list

Additionally, the work notes are updated in the following situations:

- When an association between affected users and a security incident is created or modified
- When an association between affected services and a security incident is created or modified
- When an association between vulnerable items and a security incident is created or modified

Work notes are also updated whenever **Update All Risk Scores** and **Clear All Risk Scores** on the Risk Score Weights form are clicked.

Maintain risk score weights

The risk score weights used to calculate risk scores in security incidents can be removed or updated on an individual basis. They can also be removed or updated for all security incidents. The ability to remove them from security incidents is useful when changing weight values.

Before you begin

Role required: sn_sec_cmn.admin

Note: Users with the sn_si.read role can view the risk score configuration in Security Incident Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Setup** > **Risk Score configuration**.

   Note: Users with the sn_si.read role can view the risk score configuration by navigating to **Security Incident** > **Alerts & Events** > **Risk Score Configuration**.

2. To add a new risk score weight, click **New** and enter information in the fields.

Field	Description
Type	Select the type of risk score you are defining.
Value	Specify the value associated with the selected type. If multiple values are available for the type, you may want to define multiple risk score weight records. Example: Security Incident Priority with a value of 1, Security Incident Priority with a value of 2, and so forth.
Weight	The weight associated with the selected type/value pair. Valid entries are between 0 through 100, with 0 being the lowest weight and 100 the highest.

3. Click **Submit**.
4. Perform any of these steps, as needed.
   - To clear a risk score weight record, open it from the list and click **Delete**.
   - To clear all risk score weight records, click **Clear All Risk Scores**.
   - To update all risk score weight records, click **Update All Risk Scores**.

Create a Security Incident Response SLA

You can define a Service Level Agreement (SLA) for Security Incident Response.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Security Incident** > **Setup** > **SLAs**.
2. Click **New**.
   For field descriptions and detailed instructions, see Create an SLA definition.

Repair security incident SLAs

You can repair SLA records to ensure that SLA timing and duration information is accurate.

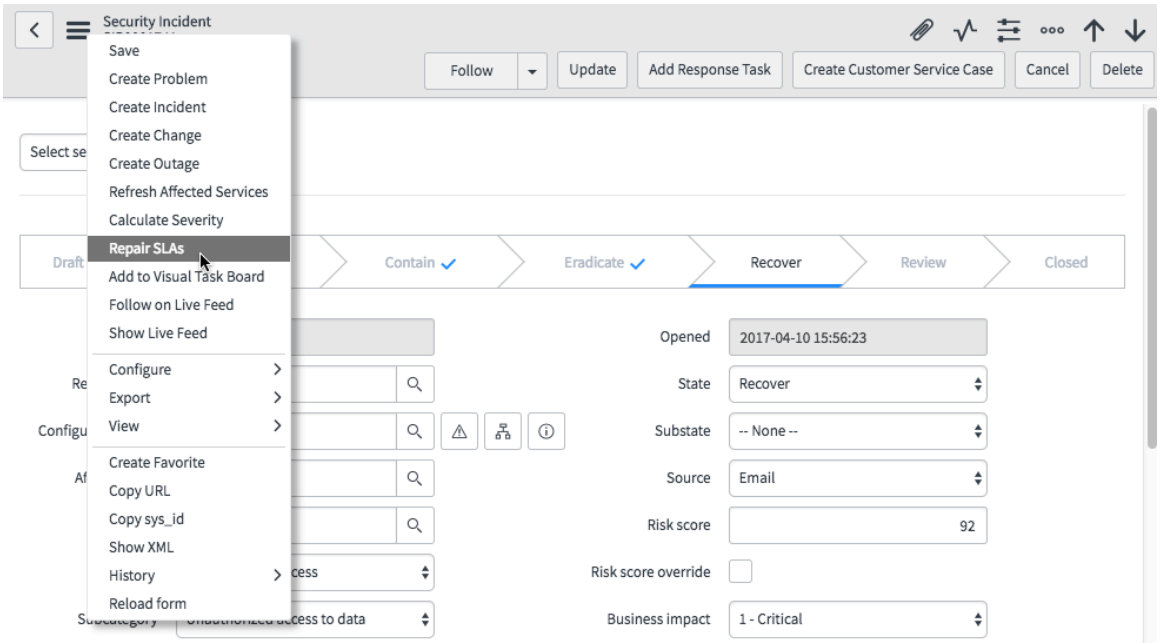
Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident you want to repair SLAs for.
2. Click the form header context menu and select **Repair SLAs**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click **OK** in the Warning confirmation box.
   For more information, see Repair SLAs.

Create a Security Incident Response runbook

A runbook is an association between a published knowledge article and a specific task. While you are performing the task, a knowledge article in the runbook automatically opens, providing information pertinent to the task.

Before you begin

There must be existing knowledge articles in the Security Incident Response Runbook knowledge base. When you create a security incident knowledge article, be sure to select **Security Incident Response Runbook** in the **Knowledge base** field. After you publish the article, you can click the **Create Runbook** button.

Role required: sn.si.knowledge_admin

About this task

You can use runbooks during the security incident or response task creation processes, or you can associate the knowledge base articles in a runbook with tasks in the playbook.

Procedure

1. Navigate to **All** > **Security Incident** > **Manual Runbook** > **Create New Runbook**.
2. Fill in the fields, as appropriate.

Field	Description
Knowledge article	Select a knowledge article to include in the runbook.
Active	Check the box to make the runbook available from the **Filter Navigator**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Use filter group	Select this check box to use a predefined filter group or create a new filter group to define the runbook criteria.
Filter group	Select the filter group to use for defining a runbook. This field appears only if the **Use filter groups** check box is selected.
Table	Select either Security Incident [sn_si_incident] or Security Incident Response Task [sn_si_task]. If you selected the **Use filter group** check box and selected a filter group, this field defaults to the table associated with the selected filter group.
Condition	Set the conditions that connect this runbook to the incident or task. If you selected the **Use filter group** check box and selected a filter group, the **Condition** fields are not displayed.

3. Right-click the form header and select **Save**.
   The Knowledge Article Details tab and a series of buttons appear.
4. To view the details of the runbook, click the **Knowledge Base Details** tab.
5. To see the knowledge article as it would appear to the user, click **View Article**.
6. To edit the details of the knowledge article, click **Edit Article** .

Create rules to validate user-reported phishing attacks

When your employees receive emails that appear to be phishing attacks, they can report them to you using a phishing email address. The suspicious email is validated using rules defined by your organization.

Before you begin

Before email matching rules can be used to identify potential phishing attacks, define an email address to which emails forwarded from your employees would be sent for processing. You have the following options for defining this email address (assuming your company email domain is acme.com):

- Define an email address such as **acme+phishing@service-now.com**. The **+phishing** tag is supported by SMTP to enable filtering and your instance can receive emails sent to it.
- Define an email address, such as **phishing@acme.com** (your Exchange mailbox), which in turn forwards it to **acme+phishing@service-now.com** (your instance mailbox defined through a mail forwarding rule).

Role required: sn_sec_cmn.write

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task
When an employee encounters a suspicious email, they should forward it as an attachment to your phishing email address. If the attached email matches a rule defining a threat, a security incident is created.

Procedure
1. Navigate to **All** > **Security Operations** > **Email Processing** > **User Reported Phishing**.
2. Click **New**.
3. Fill in the fields, as needed.

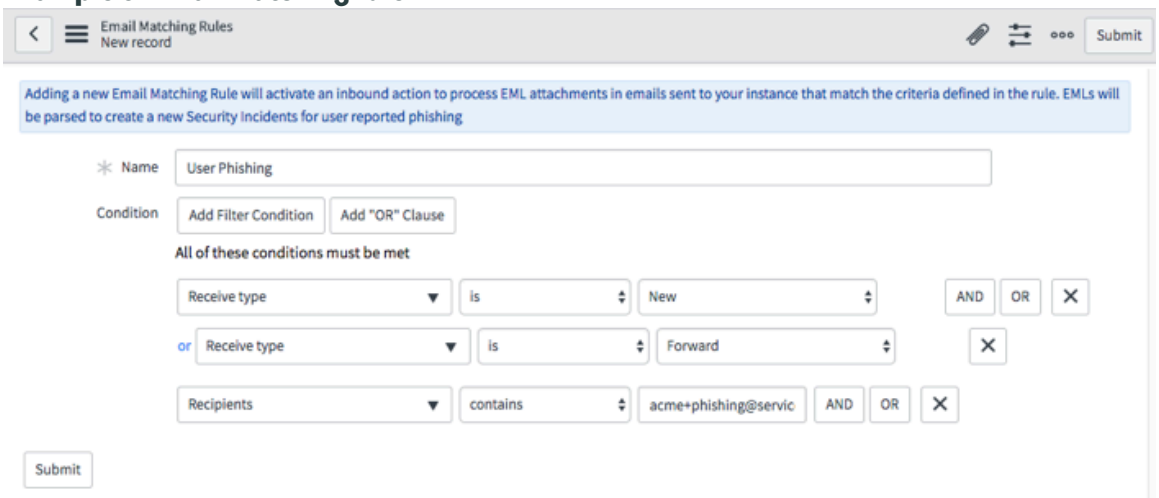
Email Matching Rules form

Field	Description
Name	Name for this email matching rule. For example, User Reported Phishing.
Conditions	Use the condition builder to validate whether an email sent to your company phishing email address is a phishing attack. See the following example.

4. Click **Submit**.

Example:
This example shows a matching rule for handling user-reported phishing.

Example of Email matching rule



Configure the Security Analyst Workspace

Configure the user interface of the Incident record in the Security Analyst Workspace to specify the fields you want to display.

Before you begin
Role required: sn_si.analyst

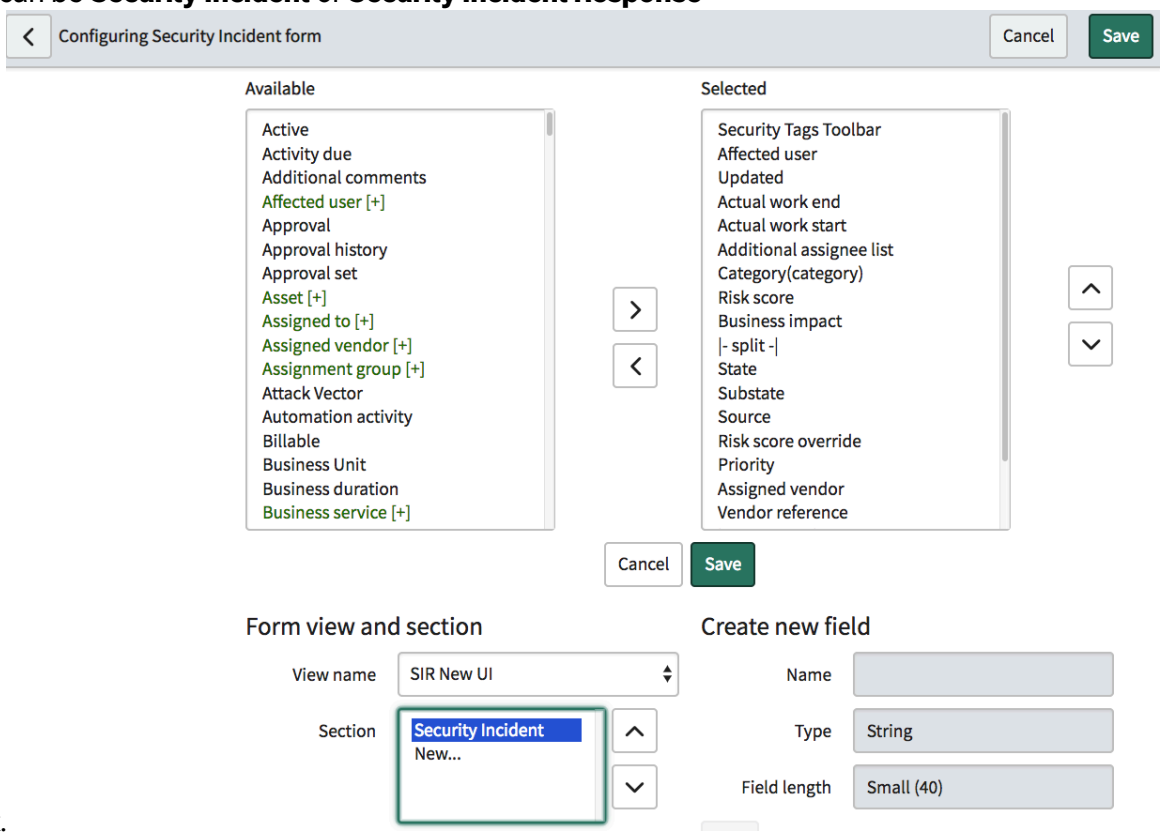
About this task
Specify the fields to be displayed in your Incident record and the order in which the fields must appear on the Security Incident form and the Response Task form. You can also set a limit on the number of fields that you want to display.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can create rules to determine which view should be used for a specific form. Several views are included with the base system, including the Default and SIR New UI views. Several view rules are also shipped with the base system, including the All Others Response Task rule. This rule enforces the Default view on the Response Task form when the condition specified in the view rule is met. The Security Analyst Workspace uses the SIR New UI view. If the form fields displayed in the Security Analyst Workspace do not match the form fields in the classic environment, a view rule is most likely enforced. To use the **SIR New UI** view for the form, you must disable the view rule. See Control when the system displays a view for details.

Procedure

1. Navigate to any security incident list (for example, **All** > **Security Incident** > **Incidents** > **Show All Incidents**).
2. To open the security incident record, click a security incident link.
3. To navigate to the Configuring Security Incident form page, click the menu icon and select **Configure** > **Form Layout**.
4. From the **View name** list, select **SIR New UI**.
5. In the **Section** field, select the appropriate section.
   This can be **Security Incident** or **Security Incident Response Task**.



6. Select the fields and the order in which you want them to appear in the Incident banner in the new UI.
7. Click **Save**.

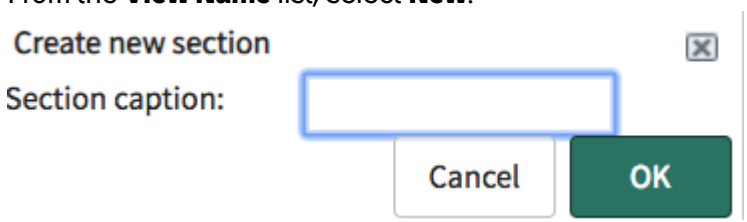
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- Certain fields are hidden by default in the Incident and Response Task banners. Change the fields that are hidden or displayed by modifying the `sn_app_secops_ui.form.excluded_fields.incident` and `sn_app_secops_ui.form.excluded_fields.response_task` properties as described in Security Analyst Workspace properties.
- Specify the number of fields that can be displayed in the Incident and Response Task banners and on the first line of the Incident banner by setting these properties:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

8. To configure the styles of the dotted circles that appear next to a field value in the Incident record, for example, navigate to **System UI** > **Field Styles** and modify or create a new style record for the specific table and field name.
   The property background-color in the Style field of the style record determines the color of the dotted circle.
9. To view the updated incident banner, click **Security Incidents** > **Incidents (New UI)** to navigate to the Incident record in the Security Analyst Workspace and refresh the page to view the updated Incident banner.
10. To configure the Response Task banner in the Incident record, navigate to **Security Incidents** > **Response Tasks** > **Show All Tasks** and repeat the steps.
11. If you are creating a new task table extending from the base Security Incident Response Task table, you must also add the SIR New UI view to the table.

    a. From the **View Name** list, select **New**.



    b. Enter **SIR New UI** (case sensitive) in the Create New View window and click **OK**.

Result

The security incident and response task banners are updated in the Security Analyst Workspace (Manage security threats using the Security Analyst Workspace).

Set up primary and secondary filters for Security Analyst Workspace

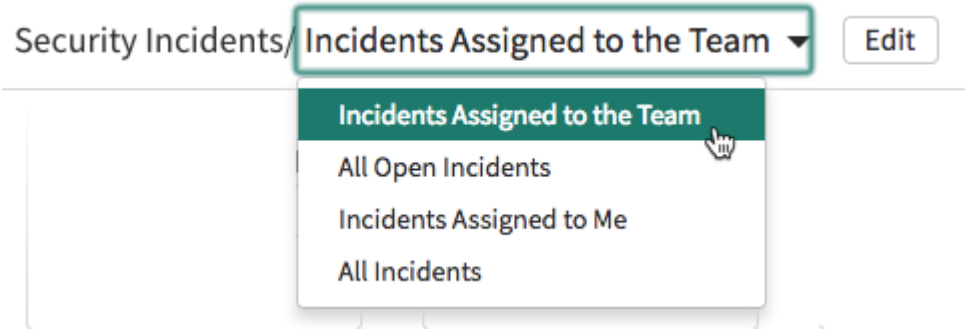
The Security Analyst Workspace base system includes a set of primary filters for narrowing down the list of security incidents for analysis (for security incidents assigned to you, all open incidents, and so forth) and a set of quick (or secondary) filters for narrowing down the list even further (by new incidents, open incidents, only critical incidents, and so forth).

Before you begin

You can use the Classic environment to define additional primary and secondary filters.

As you define filters to be used in the Security Analyst Workspace, you can assign tags to indicate whether they can be used as primary or secondary filters. Primary filters are shown at the top of the security incident list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Click **Edit** next to the Quick Filters option to select secondary (or quick) filters.



Role required: admin or sn_sec_cmn.write

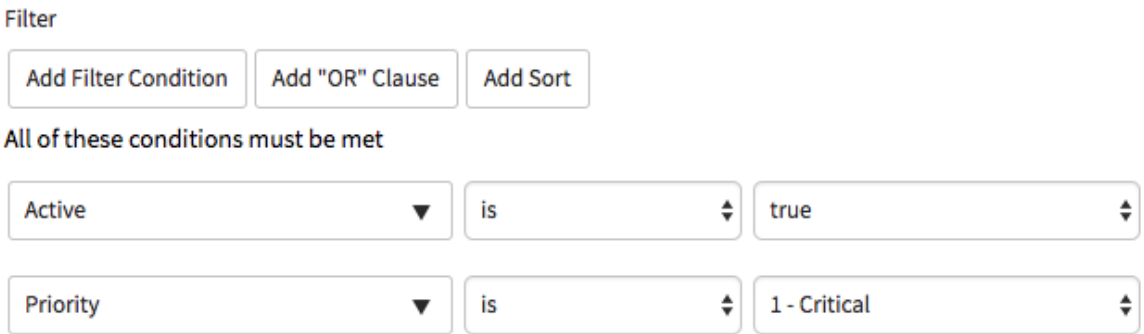
Procedure

1. Navigate to **All** > **System Definition** > **Filters**.
2. Click **New** and complete the following steps.

   a. Enter a **Title**.

   b. Select **Security Incident [sn_si_incident]** from the **Table** choice list.

   c. Add your filter conditions.
   For example, the **Open Incidents with Priority = Critical** filter, uses these conditions.



   d. Click **Submit**.

3. If the **Tags** column is not visible on the filter list, click the gear icon and personalize the view to add it.
4. Locate the filter you created and add one of the following tags to indicate how the filter should appear in the Security Analyst Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **SN_SI_Primary**: If this tag is selected, the filter can be selected from the primary filter slushbucket in the Security Analyst Workspace.
- **SN_SI_Primary_OOB**: If this tag is selected, the filter appears in the **Selected** side of the primary filter slushbucket by default.
- **SN_SI_Secondary**: If this tag is selected, the filter can be selected from the secondary (quick) filter slushbucket.
- **SN_SI_Secondary_OOB**: If this tag is selected, the filter appears in the **Selected** side of the primary filter slushbucket by default.

Related topics

Create and edit filters

Security Analyst Workspace properties

These system properties are used to configure the Security Analyst Workspace.

There are two types of properties:

- Properties that are typically not modified like sys_ids and product keys.
- Properties that are modified as required like long poll intervals and user interface configurations.

Note: The Security Analyst Workspace properties are located at this location: **Security Incident** > **Analyst Workspace Setup** > **Analyst Workspace Properties**.

Security Analyst Workspace properties

Property Name	Description
Fields that are hidden by default in the response task banner. sn_app_secops_ui.form.excluded_fields.response_task	• **Type**: string • **Default value**: ○ number ○ short description ○ comments ○ work_notes ○ comments_and_work_notes ○ work_notes_list ○ automation_activity
Fields that are hidden by default in the incident banner. sn_app_secops_ui.form.excluded_fields.incident	• **Type**: string • **Default value**: ○ number ○ short description ○ comments ○ work_notes ○ comments_and_work_notes ○ work_notes_list

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Analyst Workspace properties (continued)

Property Name	Description
	○ automation_activity ○ security_tags
Background color style is applied to the fields listed here. sn_app_secops_ui.form.color_coded_fields	• **Type**: string • **Default value**: ○ business criticality ○ impact ○ priority ○ risk_score ○ severity
If true, tables extended from the sn_si_task base response task table, will also have access to email templates created for the base response task table. sn_app_secops_ui.extend.base.response_task.email_templates	• **Type**: true | false • **Default value**: true
Sets the width of each summary field in each response task banner. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Type**: integer • **Default value**: 10
Sets the width of each summary field in each incident banner. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Type**: integer • **Default value**: 15
Sets a limit on the number of summary fields allowed in the incident banner. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Type**: integer • **Default value**: 12
Sets a limit on the number of summary fields allowed in the response task banner. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Type**: integer • **Default value**: 12
Sets a limit on the number of summary fields allowed in the first line of the incident banner. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Type**: integer • **Default value**: 3

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Analyst Workspace properties (continued)

Property Name	Description

Comma separated list of fields that may have user photos.
 	
sn_app_secops_ui.form.user_fields
	• **Type**: string
	• **Default value**:
	  ○ affected_user
	  ○ caller
	  ○ sys_updated_by
	  ○ sys_created_by
	  ○ opened_by
	  ○ closed_by
	  ○ submitted_by

Sets the width of each summary field in each incident peek view. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Type**: integer • **Default value**: 13.5

Comma separated list of fields that display time.
 	
sn_app_secops_ui.form.time_fields
	• **Type**: string
	• **Default value**:
	  ○ opened_at
	  ○ sys_created_on
	  ○ sys_updated_on

Controls the frequency (in milliseconds) at which the sighting search results are refreshed. sn_app_secops_ui.poller_interval.search_action	• **Type**: integer • **Default value**: 30000 **Minimum**: 15000
Controls the frequency (in milliseconds) at which the count or query data is refreshed. sn_app_secops_ui.poller_interval.related_list	• **Type**: integer • **Default value**: 30000 **Minimum**: 15000
Controls the frequency (in milliseconds) at which the result data is refreshed (for the playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Type**: integer • **Default value**: 30000 **Minimum**: 15000

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Analyst Workspace properties (continued)

Property Name	Description
ID for the Security Operations Integration - Isolate Host workflow. sn_app_secops_ui.workflow.id.isolate_host	• **Type**: string • **Default value**: d72041f1ff203200c68c84648e94fa5e
ID for the Security Operations Integration - Watchlist workflow. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Type**: string • **Default value**: 35800c0eff343200c68c84648e94fa85
ID for the Security Operations Integration - Block Request workflow. sn_app_secops_ui.workflow.id.block_request	• **Type**: string • **Default value**: 11a6a5270b9032008f9108e3c5673a24
ID for the sn_si_analyst user role. sn_app_secops_ui.roles.id.sn_si.write	• **Type**: string • **Default value**: 66878663ff123100158bffffffff8d
ID for the sn_si_read user role. sn_app_secops_ui.roles.id.sn_si.read	• **Type**: string • **Default value**: ae878663ff123100158bffffffff8e
ID for the sn_si_admin user role. sn_app_secops_ui.roles.id.sn_si.admin	• **Type**: string • **Default value**: 22878663ff123100158bffffffff8d
ID for the Microsoft Exchange - Perform Email Search and Delete workflow. sn_app_secops_ui.email.phishing.manual.workflow	• **Type**: string • **Default value**: ed9f289cc310220031fbdccdf3d3aeb4
ID for the Add to Deny list custom action under the Explore tab in the Security Analyst Workspace. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Type**: string • **Default value**: DENY_e9bd0ac50b632200263a089b37673a0b
ID for the Add to Allow list custom action under the Explore tab in the Security Analyst Workspace sn_app_secops_ui.explore.action.direct.id.allow_list	• **Type**: string • **Default value**: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Analyst Workspace properties (continued)

Property Name	Description
ID for the Run Threat Lookup UI Action. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Type**: string • **Default value**: da5ff4420b540300263a089b37673ae7
ID for the Threat Lookup integration capability. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Type**: string • **Default value**: 39344d4f0b273200263a089b37673ab1
ID for the Observable Enrichment custom action under the Explore tab in the Security Analyst Workspace. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Type**: string • **Default value**: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e
ID for the Enrich Observable integration capability. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Type**: string • **Default value**: 9ad183640b1003009f66e94685673af4
ID for the Publish to Watchlist UI Action. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Type**: string • **Default value**: 8ee94002ff743200c68c84648e94faf9
ID for the Block Request UI Action. sn_app_secops_ui.explore.action.id.block_request	• **Type**: string • **Default value**: 7158f6e40b2032008f9108e3c5673adf
ID for the Run Sightings Search UI Action. sn_app_secops_ui.explore.action.id.sightings_search	• **Type**: string • **Default value**: 43f91a6f0b032200b97c67d985673a2c
ID for the Create Child Security Incident UI Action. sn_app_secops_ui.explore.action.id.create_child_incident	• **Type**: string • **Default value**: 5a6882645363530099d5ddeeff7b1272
ID for the Add Security Annotation UI Action. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Type**: string • **Default value**: 1e3a3e723b5332005a9149a4d2efc4eb

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Analyst Workspace properties (continued)

Property Name	Description
ID for the CI Enrichment Custom Action under the Explore tab in the Security Analyst Workspace. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Type**: string • **Default value**: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e
ID for the Isolate Host UI Action. sn_app_secops_ui.explore.action.id.isolate_host	• **Type**: string • **Default value**: d6244e0aff203200c68c84648e94fad3
ID for the Add Multiple Observables UI Action. sn_app_secops_ui.explore.action.id.multiple_observable	• **Type**: string • **Default value**:138de478d78322007a6de294de6103aa
Product key for ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Type**: string • **Default value**:ServiceNow_ServiceNow_5Devs2_August_2018__MTU

Additional Security Analyst Workspace configuration

Configure the Security Analyst Workspace and define filters, UI actions, and related lists.

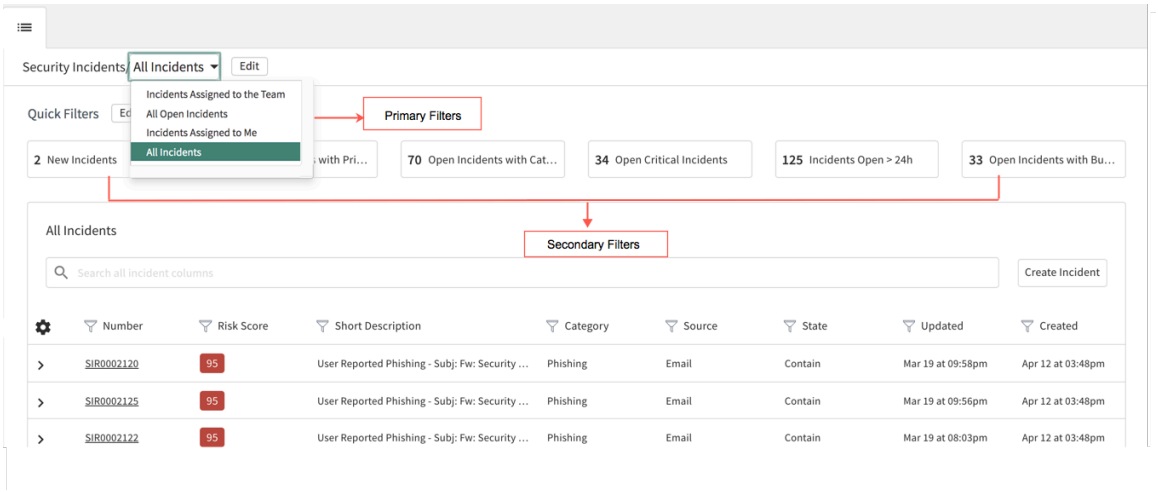
- Landing page filter configuration
- Enable UI Actions
- Form UI actions
- Related List configuration
- Related List UI Actions
- Form configuration system properties
- Enable playbooks for analyst selection

Landing page filter configuration

You can add new filters or modify existing filters that appear in the Security Analyst Workspace.

The Security Analyst Workspace has primary and secondary filters that allow you to filter the list of security incidents so you can quickly find the security incidents you want to analyze. Fore more information, see Manage security threats using the Security Analyst Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Create a new filter

1. Navigate to **Security Incidents** > **Analyst Workspace Setup (New UI)** > **Landing Page Filter Configuration**.
2. Click **New**.
3. Enter a title for the filter, specify the filter condition and click **Submit** to return to the previous page.

   You will see the newly added filter listed on the page.
4. Add a tag for this filter to indicate whether this is a primary or secondary filter. The following tags are available:
   - SN_SI_Primary
   - SN_SI_Secondary

Edit existing filters

You can also do the following:

- Modify existing filters: Click the Title of an existing filter. Modify the title and the filter condition and click **Update**.
- Modify tags: Select a filter and click the Tag column in the Landing Page Filter Configuration. You can delete the existing tag or add a new tag for the filter.

Enable UI Actions

Before you configure any UI Actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace.

Note: To modify the UI actions, log in as a user with the following roles:

- ui_action_admin
- ui_page_admin
- web_service_admin

There are two types of UI actions that can be configured for the Security Analyst Workspace:

- Dialog Based UI Action
- Server-side UI Action

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Dialog Based UI Action

To enable dialog-based UI actions in the Security Analyst Workspace, make the following changes to the UI pages associated with the respective standard UI Actions.

1. **HTML section**: Modify the HTML section to include the *react* input tag. The *react* input tag value is used in the client script section to identify if the UI Page has been launched from the Security Analyst Workspace. An example is shown below:

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Client script**: Additional logic needs to be written in the client script when the *react* flag is true. This is needed to handle the **Submit** and **Cancel** button events shown as part of the dialog window.
   a. onCancel () event handler needs to dispatch the 'SIR_WORKBENCH_POPUP_CANCEL' event from the Security Analyst Workspace
   b. onSubmit () event handler needs to dispatch the 'SIR_WORKBENCH_POPUP_SUBMIT' event from the Security Analyst Workspace
3. The execution of the processing script is skipped from the Security Analyst Workspace context as the 'onSubmit' action has been modified to return false when the *react* input tag value is true. The logic of the processing script needs to be handled either via a client callable script (invoked via GlideAjax API) or REST resource endpoint.

Refer the following sample UI pages for more details:

- Related List UI action example: Publish to watchlist (UI page name: publish_to_watchlist)
- Form UI action example: Create Problem (UI page name: create_prb_change_inc)

Server side UI Action

To enable server side UI actions, you must do the following:

The logic of the standard UI action script must be handled as part of a scripted REST resource.

Refer to the following sample Form UI actions for more details:

- Create Outage
- Cancel

Form UI actions

You can configure the UI actions that are displayed in the Security Analyst Workspace.

Prerequisites:

Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

To configure a Form UI action for the Security Analyst Workspace, follow these steps:

1. Navigate to **Security Incidents** > **Analyst Workspace Setup (New UI)** > **Form UI Actions**.
2. Enter the following details:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
Action	Select an UI action from the choice list.
Type	Select the type of action. This can be: ○ Dialog based action: This type of action is used when user interaction or inputs are required to execute specific business logic. ○ Server side action: This action executes the required business logic without any additional user input. **Note:** Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.
Application	The name of the application scope (Security Incident Response UI) in which the UI action is being added is displayed here.
Dialog Based Action If you select Dialog based action in the Type field, enter the following details:	
UI Page	Select the UI page associated with the action.
Dialog Title	Enter a title for the dialog action.
Dialog Width and Height	Enter the height and width of the dialog in pixels.
Script	For the selected UI Page, you can specify additional query parameters here. The template provided with the base system constructs and returns `sysparm_sys_id` parameter only. You can override this by specifying different parameters here.
Server-side Action If you select Server side action in the Type field, enter the following details:	
Scripted Rest Resource	Select the Scripted Rest Resource that defines the action. **Note:** The **SIR UI ANALYST** ACL must be added to the Rest resource.

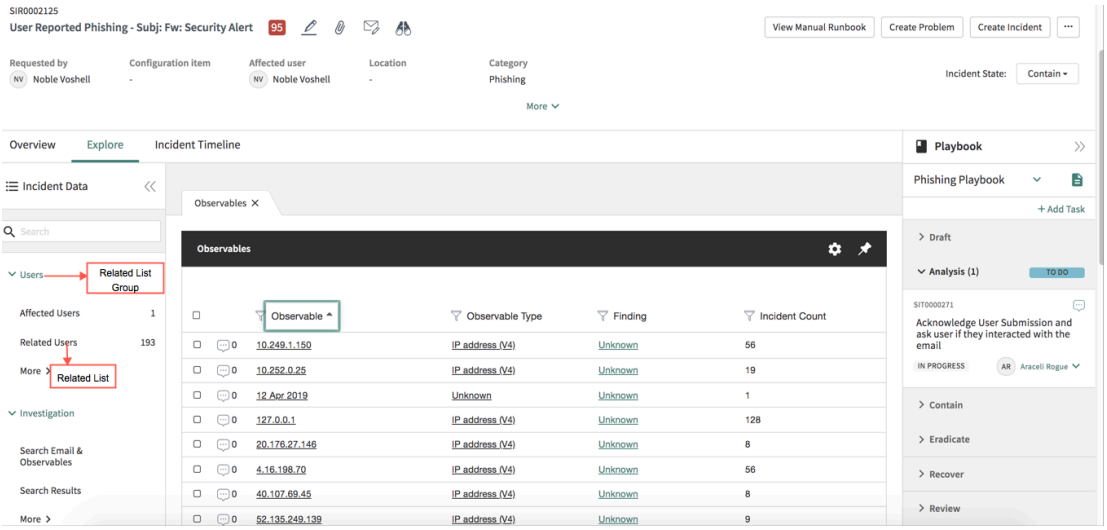
3. Click **Submit**.
4. Navigate to **Security Incidents** > **Incidents (New UI)** page.
5. Click on a security incident number to view the security incident record. You can see the new UI action at the top of the page.

To modify an existing Form UI action, click the Action Name to navigate to the Form UI Actions page. You can modify the Action Name, Type, and the rest of the fields based on the selected type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related List configuration

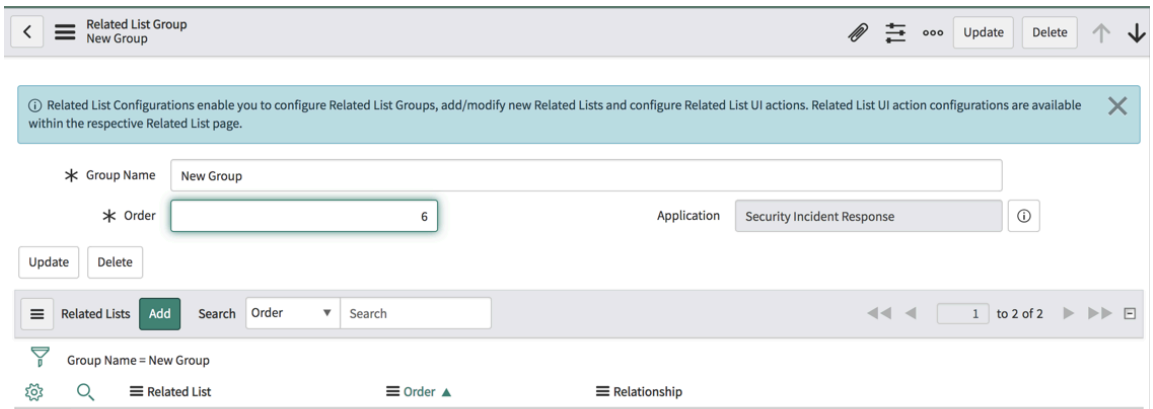
You can add new related lists or new related list groups, and modify existing groups or related lists that appear in the Security Analyst Workspace.



Add a Related List Group

To add a Related List Group, follow these steps:

1. Navigate to **Security Incidents** > **Analyst Workspace Setup (New UI)** > **Related List Configurations**.
2. Click **New** to add a new Related List Group. Enter the Group Name and the Order in which it should be appear on the Incidents (New UI) page.
3. Click **Submit**. The newly added group appears in the Related List Groups page.



Add a Related List

To add a new Related List, follow these steps:

1. Click on a Related List Group link.
2. In the Related Lists section, click **Add** to add a new related list.

   If you don't see the **Add** button, check if you are in same application scope as the Related List Group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the Related List to be included in the group.

   Note: If you do not see a specific related list, do the following:

   a. Navigate to **System UI** > **Related Lists** and search for Related Lists present in the *sn_si_incident* table.

   b. Click on the *sn_si_incident* table associated with the **SIR New UI**view.

   c. In the Related List Entries section, click **New** to add the Related List to the **SIR New UI** view.

4. Specify the order in which it should appear and click **Submit**.

   The Related List that you have added will appear in the Security Analyst Workspace.

To modify an existing Related List Group, click the Group Name to navigate to the Related List Group page. You can modify the Group Name, Order, and add or delete Related Lists from the group.

Related List UI Actions

You can add new UI actions to the related lists that appear in the Security Analyst Workspace.

Prerequisites:

Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

To add a new Related List UI action, follow these steps:

1. Navigate to **Security Incidents** > **Analyst Workspace Setup (New UI)** > **Related List Configurations**.
2. Click on the Group Name. The Related List Group configuration page is displayed.
3. Click on the Related List for which you want to add a UI action.
4. Click **Add** in the Related List UI Actions section.
5. Enter the following details:

Field Name	Description
Action	Select a UI action from the choice list.
Type	Select the type of action. This can be: ○ Dialog based action: This type of action is used when user interaction or inputs are required to execute specific business logic. ○ Server side action: This action executes the required business logic without any additional user input. **Note:** Before you configure any UI actions, you must perform certain steps to enable them so that they are available for configuration in the Security Analyst Workspace. See Enable UI Actions for details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
Application	The name of the application scope (Security Incident Response UI) in which the UI action is being added is displayed here.
Dialog Based Action If you select Dialog based action in the Type field, enter the following details:	
UI Page	Select the UI page associated with the action.
Dialog Title	Enter a title for the dialog action.
Dialog Width and Height	Enter the height and width of the dialog in pixels.
Script	For the selected UI Page, you can specify additional query parameters here. The template provided with the base system constructs and returns `sysparm_incident_id`, `sysparm_record_table`, and `sysparm_related_sys_ids` parameters only. You can override them by specifying different parameters here.
Server side Action If you select Server side action in the Type field, specify the following:	
Scripted Rest Resource	Select the Scripted Rest Resource that defines the action. **Note:** The **SIR UI ANALYST** ACL must be added to the Rest resource.

6. Click **Submit**.
7. Navigate to **Security Incidents** > **Incidents (New UI)** page.
8. Click on a security incident number to view the security incident record. Launch the respective Related List to view the new UI action.

Form configuration system properties

These system properties define the form refresh intervals for the playbook tasks.

To configure these properties, navigate to **Analyst Workspace Setup (New UI)** > **Analyst Workspace Properties**.

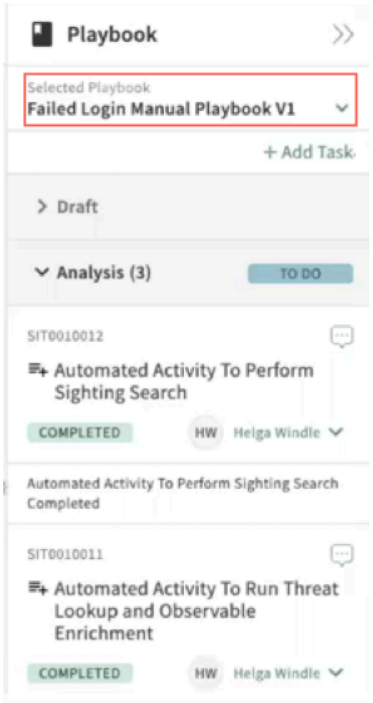
Property	Default value	Description
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	The interval time used by the playbook component to refresh its response tasks for every configured interval time.
sn_app_secops_ui.poller_interval_times.playbook_tasks	9 times	The number times playbook component polls for response tasks.
sn_app_secops_ui.poller_interval.related_list	30000 ms	This interval time is used by the Explore component to refresh its Related List counts for every configured interval time.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enable playbooks for analyst selection

Add new playbooks to the playbook selection list.

You can select an appropriate playbook to investigate security incidents in the Security Analyst Workspace (Manage security threats using the Security Analyst Workspace). The playbook selection option supports only the playbooks which are designed using Flow Designer.



After you have created a playbook using Flow Designer, follow these steps to include it in the Selected Playbook choice list:

1. Navigate to *sys_hub_flow* table.
2. Search for the new playbook you have created using Flow Designer.
3. Add the **sir_playbook** tag to the playbooks that you want to include in the Selected Playbook choice list.

> **Note:** If you have old playbooks that have not been migrated from workflows to Flow Designer, they will not appear in the list. But, if a playbook created using workflows is assigned to a security incident either by a trigger condition or by manual selection (using **Run Orchestration** option in the classic environment), this playbook is launched when you open the security incident in the Security Analyst Workspace.

Troubleshooting Security Incident Response

This section covers important troubleshooting tips and frequently asked questions related to Security Incident Response.

Access Control Rules issues

Access Control Rules allow access to the specified resource if all the following three conditions are met:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The user has one of the roles specified in the **Role** list, or the list is empty.
- Conditions in the **Condition** field evaluate to true, or conditions are empty.
- The script in the **Script** field (advanced) evaluates to true, or sets the variable **answer** to true, or is empty.

For more information on Access Control Rules, see Exploring Access Control Lists

Important: If the **Admin overrides** option is unchecked for a security incident table, and if the Admin is able to access the security incident table, see KB1444673

Security Incident Response Platform Analytics Solutions

Platform Analytics Solutions contain preconfigured dashboards. The dashboards present important metrics for analyzing your Security Incident Response process, such as new security incidents or the average age of open security incidents.

Platform Analytics data visualizations use Performance Analytics indicator data to show you data over time, helping you analyze your business processes and identify areas of improvement. With Platform Analytics Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

Important: Set up and test Platform Analytics Solutions on a non-production instance before enabling them in production.

The Security Incident Response Performance Analytics Solution is available from the ServiceNow Store. For information about downloading and installing this application, see Security Operations and the ServiceNow Store.

Note: To evaluate the functionality, you can activate Performance Analytics solutions and in-form analytics on instances that have not licensed Performance Analytics. However, you have the following limitations:

- You cannot create new indicators.
- You cannot collect data older than 180 days.

For full functionality, license Performance Analytics. For more information, see Activate your Performance Analytics subscription.

Important: By default, the data collection limit for the *(com.snc.pa.dc.max_records)* property in Performance Analytics is set as 5,000 records. But you can increase this limit per your requirements, such as 50,000 records. However, increasing this limit may impact performance during data collection or when performing operations on the Snapshot table. To learn more about the Performance Analytics properties, see Performance Analytics properties.

Related topics

Platform Analytics Solutions

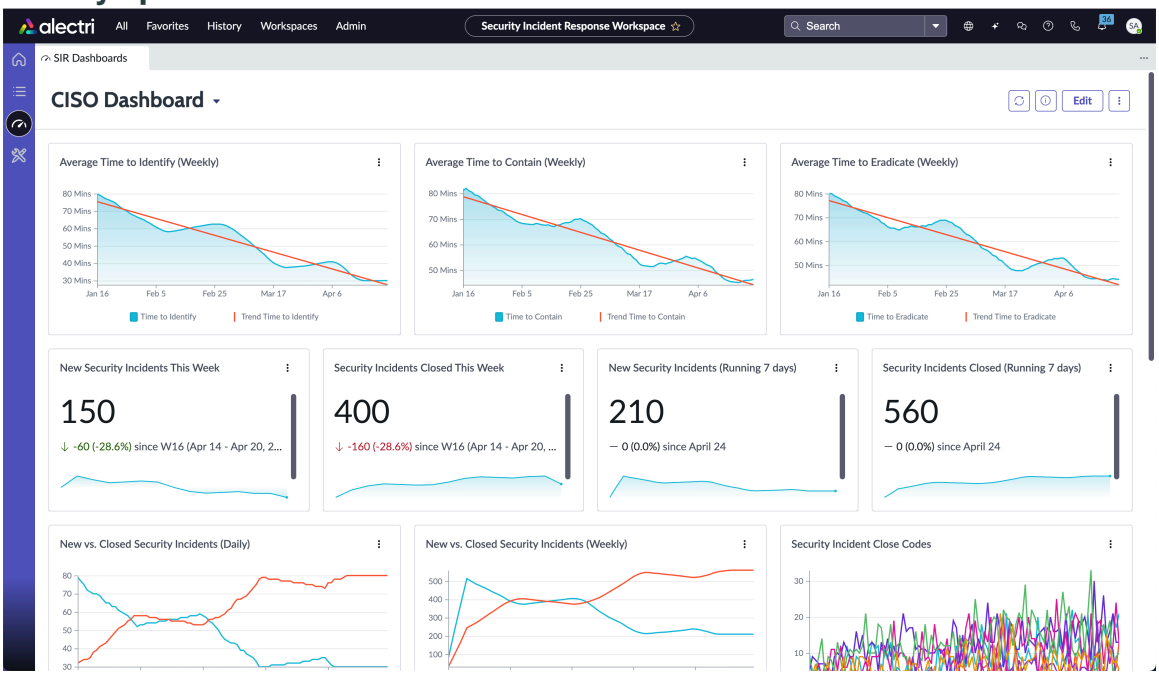
Activate your Performance Analytics subscription

CISO dashboard

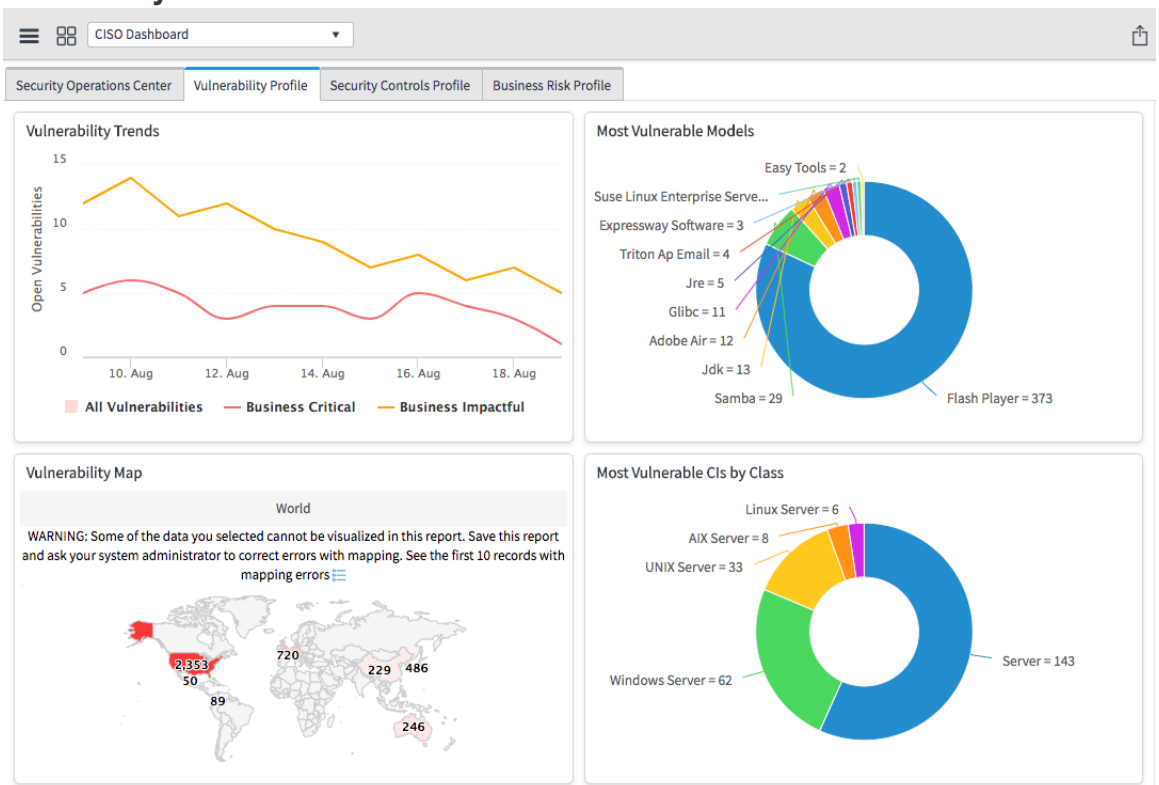
This dashboard reveals the overall security posture of your organization, including security vulnerability and incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations Center tab

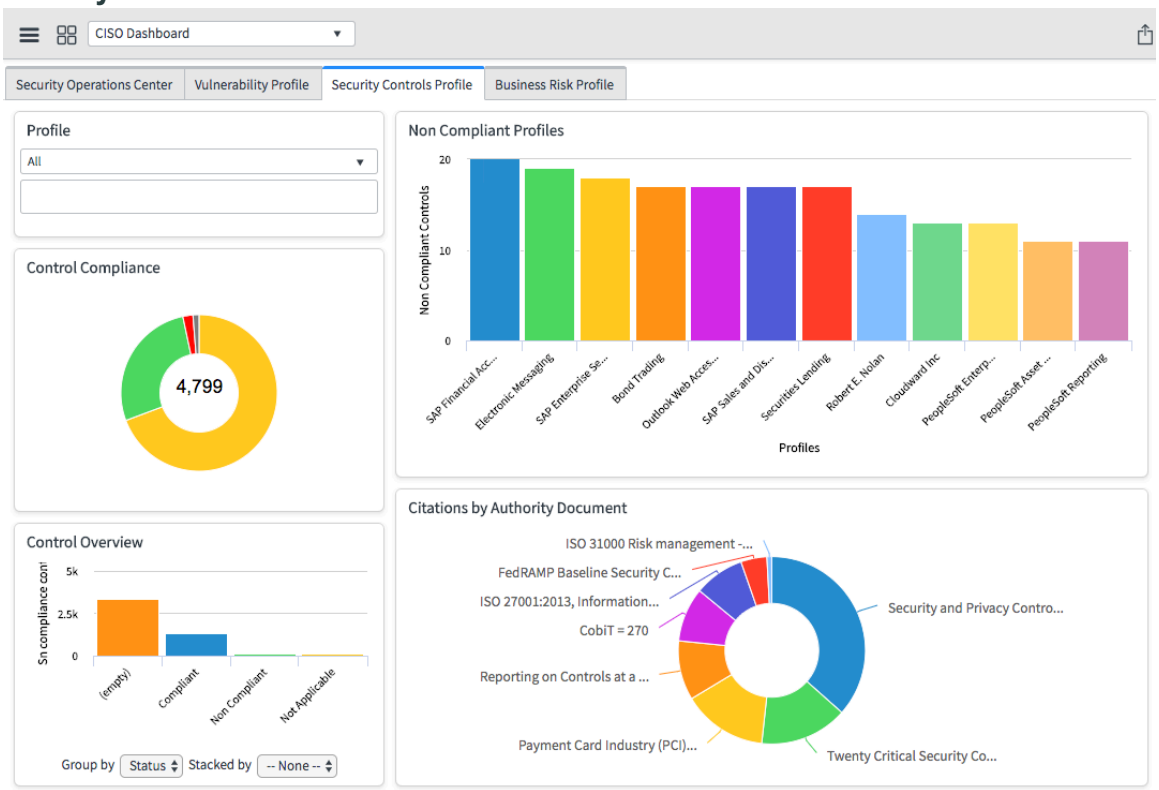


Vulnerability Profile tab

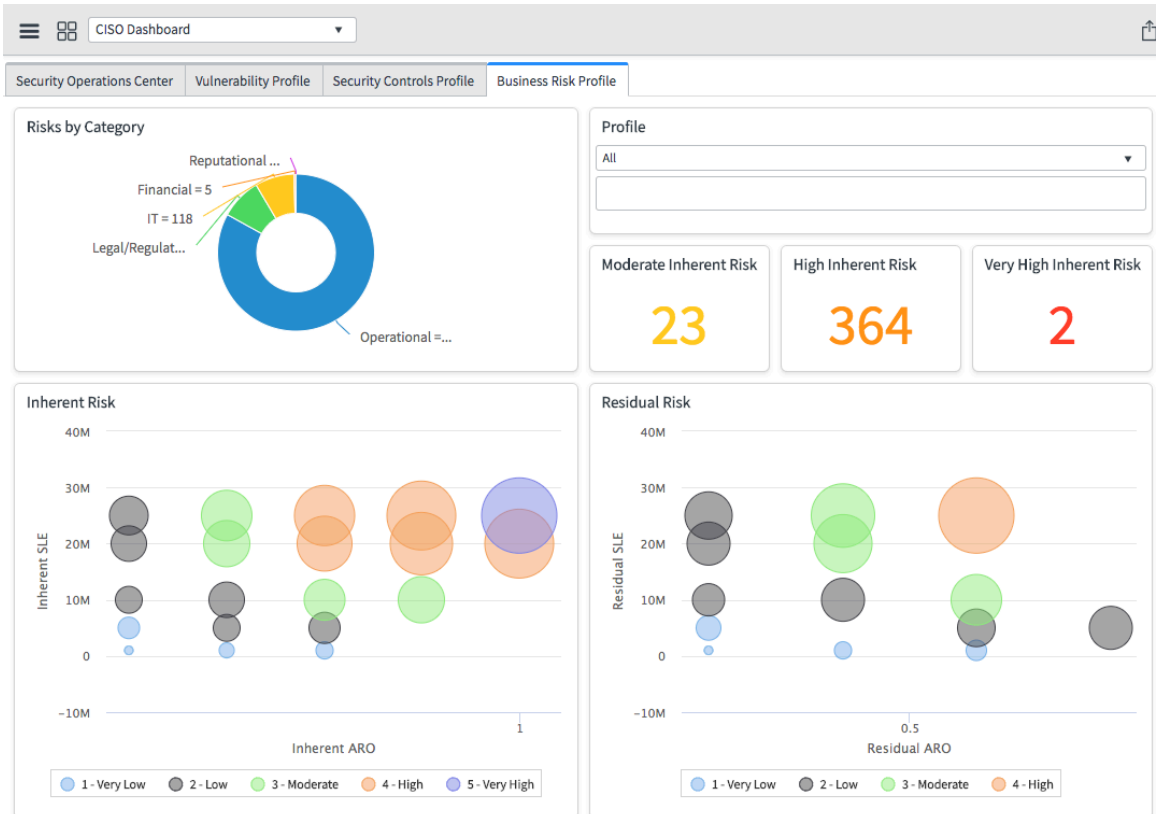


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Controls Profile tab



Business Risk Profile tab



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

End users and roles

End user and goal	Required role
CISO: Needs clear visibility regarding the current security posture of the overall organization	sn_si.ciso

CISO dashboard indicators

The CISO dashboard presents the following key performance indicators:

SI - Average Time to Identify

A 7-day average of the time in minutes it takes to identify a security incident, calculated daily.

Average Time to Contain

A 7-day average of the time in minutes it takes to contain a security incident, calculated daily.

Average Time to Eradicate

A 7-day average of the time in minutes it takes to eradicate a security incident, calculated daily. Both Average Time to Contain and Average Time to Eradicate are based on the indicator SI - Average Duration Time broken down by Security Incident State.

New Security Incidents This Week

The weekly sum of the score of the daily Number of new security incidents indicator.

Security Incidents Closed (weekly)

The 7-day running sum of the daily Number of closed security incidents indicator.

New Security Incidents by Priority

Daily breakdown of the Number of new security incidents indicator by Priority.

New vs Closed Security Incidents (weekly) volume

The 7-day running sum time series of the Number of new incidents indicator charted against the 7-day running sum time series of the Number of closed incidents indicator.

Security Incident Heatmap

A global map showing the number of open security incidents in each country.

Security Incident Treemap

An interactive treemap where you can select to see:

- Security incidents per business service, broken down by business criticality
- Security incidents broken down by category or subcategory of incident
- Security incidents per assignment group or per assignee
- 'Victim stats' of security incident per affected resource or affected user

Breakdowns

The following breakdowns apply to the indicators on the dashboard:

- Business criticality
- Security Group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Incident Age
- Security Incident Category
- Security Incident Close Code
- Security Incident Priority
- Security Incident State
- SI - Business Service
- Vulnerability

Data visualizations

The dashboard includes the following visualizations:

Title	Type	Description
Security Incidents Open for More Than 30 Days by Assignment Group and State	Heatmap	Displays models with the most vulnerable items.
Risks by Category	Donut	Lists the age of reopened vulnerable items.
Citations by Authority Document	Donut	Number of active vulnerabilities
Security Incidents With Assignee That is not Active	Heatmap	Displays the number of open vulnerable items associated with vulnerabilities, (Common Vulnerability Enumeration (CVE) records), from most to least.
Security Incidents Not Updated for More Than 30 Days by Assignment Group and State	Heatmap	Displays publishers with the most vulnerable items.
Vulnerability Map	Map	A world map showing vulnerabilities by location
Most Vulnerable Models	Donut	The applications that contain the most vulnerabilities
Most Vulnerable CIs by Class	Donut	CIs by server type
Services with Critically Significant Vulnerabilities	List	
Non-compliant profiles	Bar	Non-compliant controls by profile
Control Overview	Bar	Number of compliant and non-compliant controls
Policy Exceptions	List	Policy exceptions with priority, owner, and short description
Risks by Category	Donut	The number of risks in each category of risk

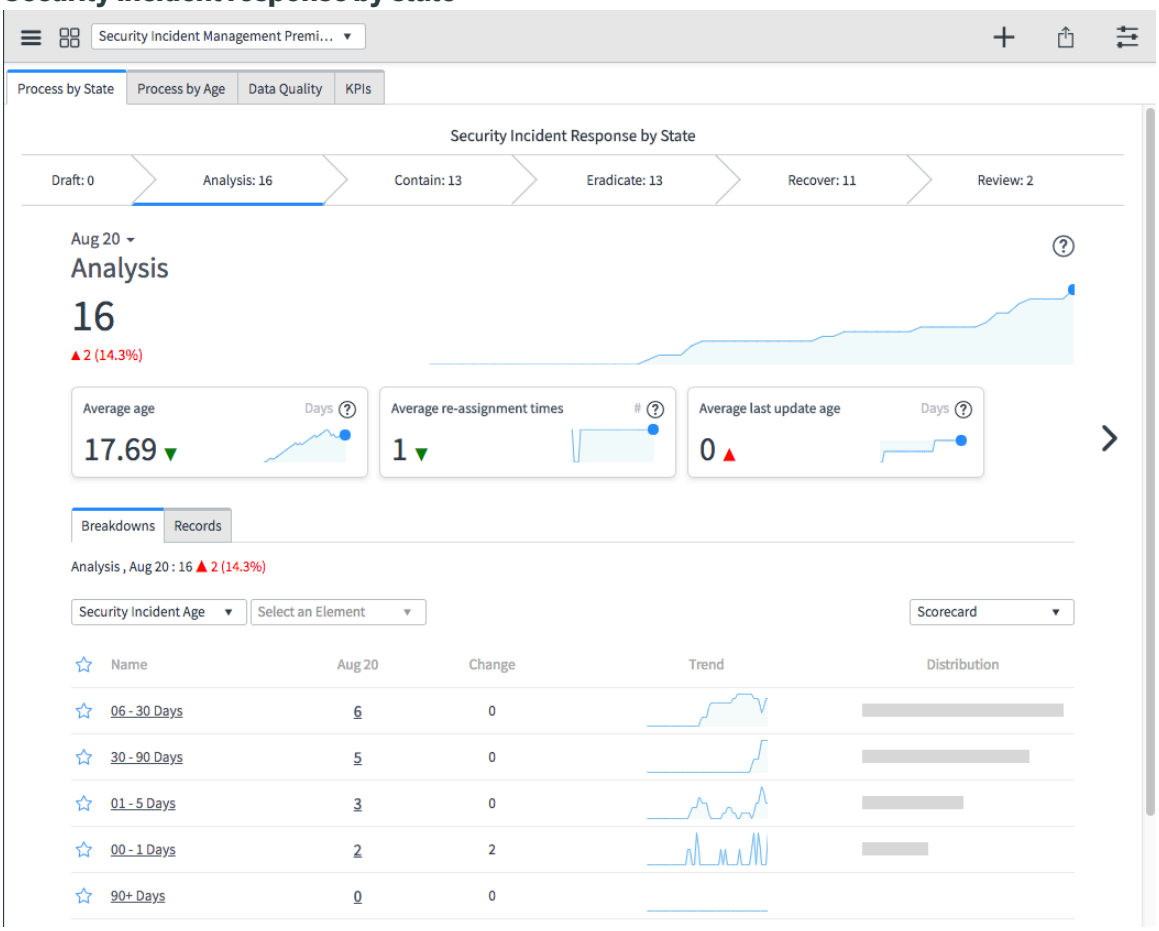
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Title	Type	Description
Inherent Risk	Bubble	Inherent SLE vs Inherent ARO
Residual Risk	Bubble	Residual SLE vs Residual ARO
Moderate, High, and Very High Risks	Scores	The numbers of moderate, high, and very high risks, respectively
Risk by Profile	Stacked Bar	Risk count where you can select what to group by and what to stack by

Security Incident Management Premium dashboard

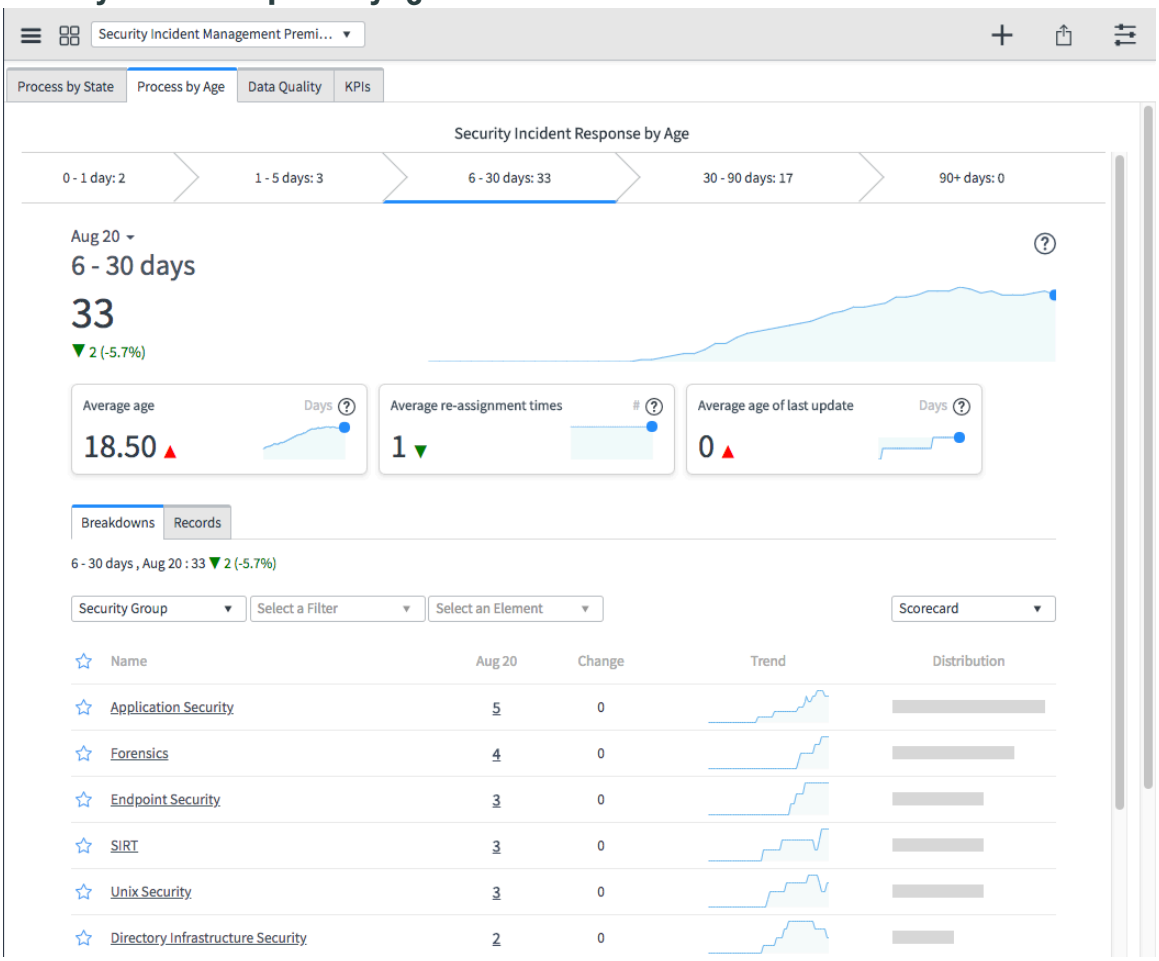
This dashboard uses advanced Platform Analytics visualizations to aid security managers to track the volume, performance and progress of security incidents from initial analysis/detection to containment, eradication, and recovery. The licensed version of Performance Analytics is therefore required.

Security incident response by state



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident response by age



End users and roles

End user and goal	Required role	Benefits
Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.	sn_si.manager	Can review the overall security posture with the ability to adjust the members of assignment groups.
Security Response Administrator: Needs to pinpoint areas of concern quickly and have full control over all Security Incident Response data while administering territories and skills, as needed.	sn_si.admin	Can adjust risk calculation parameters to ensure vulnerable items that are most pertinent to the organization are being addressed first.
Security Response Analysts: Need to quickly prioritize which vulnerabilities to focus on based upon criticality to the organization.	sn_si.analyst	Tier 1 and 2 security analysts work on security incidents. They can create and update security incidents, requests, and tasks, as well as problems, changes, and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

End user and goal	Required role	Benefits
		outages related to their incidents.

Security Incident Management Premium indicators

The Process by State and Process by Age tabs contain workbench widgets with the following indicators:

Average age

The Average age of open security incidents indicator uses the formula `[[Summed age of open security incidents]] / [[Number of open security incidents]] / 24` to give a result in days.

Average reassignment times

The Average re-assignment of open security incidents indicator uses the formula `Summed re-assignment of open security incidents / Number of open security incidents`.

Average age of last update

The Average age of last update of open security incidents indicator uses the formula `Summed age of last update of open security incidents / Number of open security incidents / 24` to give a result in days.

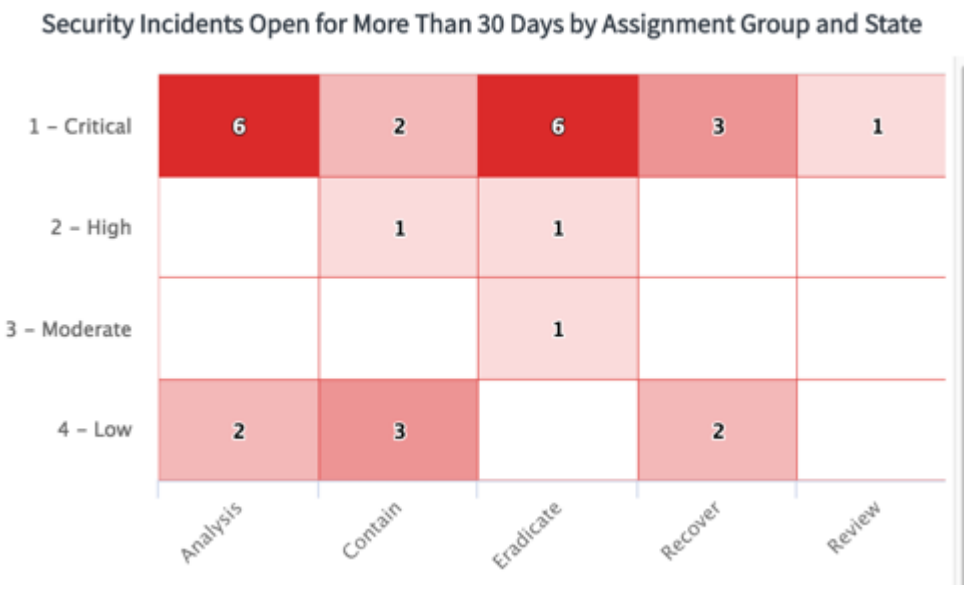
% not updated in 5 days

The % of open security incidents not updated in last 5 days indicator uses the formula `( [[Number of open security incidents not updated in the last 5 days]] / [[Number of open security incidents]] ) * 100`.

The Data Quality tab has interactive filters for the Category of the security incident and the levels of Risk, Priority, and Severity. These filters are applied simultaneously to the following indicators:

Security Incidents Open for More Than 30 Days by Assignment Group and State

The Number of open security incidents filtered for an age of 30 days and broken down by Assignment group and State.



Security Incidents With Assignee That is not Active

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Number of open security incidents with no assignee or an assignee who is not active.

Security Incidents Open for More Than 30 Days by Assignment Group and State

The Number of open security incidents not updated in the last 30 days indicator broken down by Assignment group and State.

The KPI tab has the following additional indicators:

- % of new critical security incidents
- Average Age of Open Security Incidents
- Average Close Time of Security Incidents
- % Of Security Incidents that have been reassigned
- % of Security Incidents closed on first assignment
- % of security incidents closed by self-service
- % of security incidents not solved
- Average Close time of security incident tasks

Breakdowns

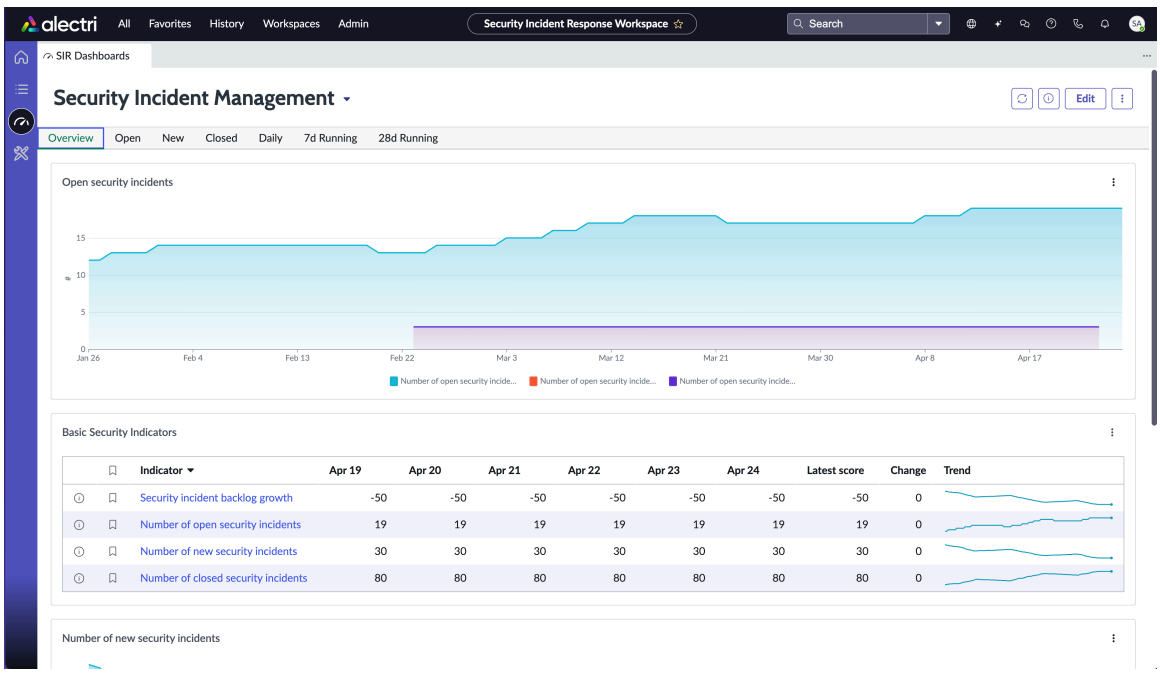
The following breakdowns apply to the indicators on the dashboard:

- Security Group
- Security Incident Age
- Security Incident Category
- Security Incident Priority
- Security Incident State

Security Incident Management dashboard

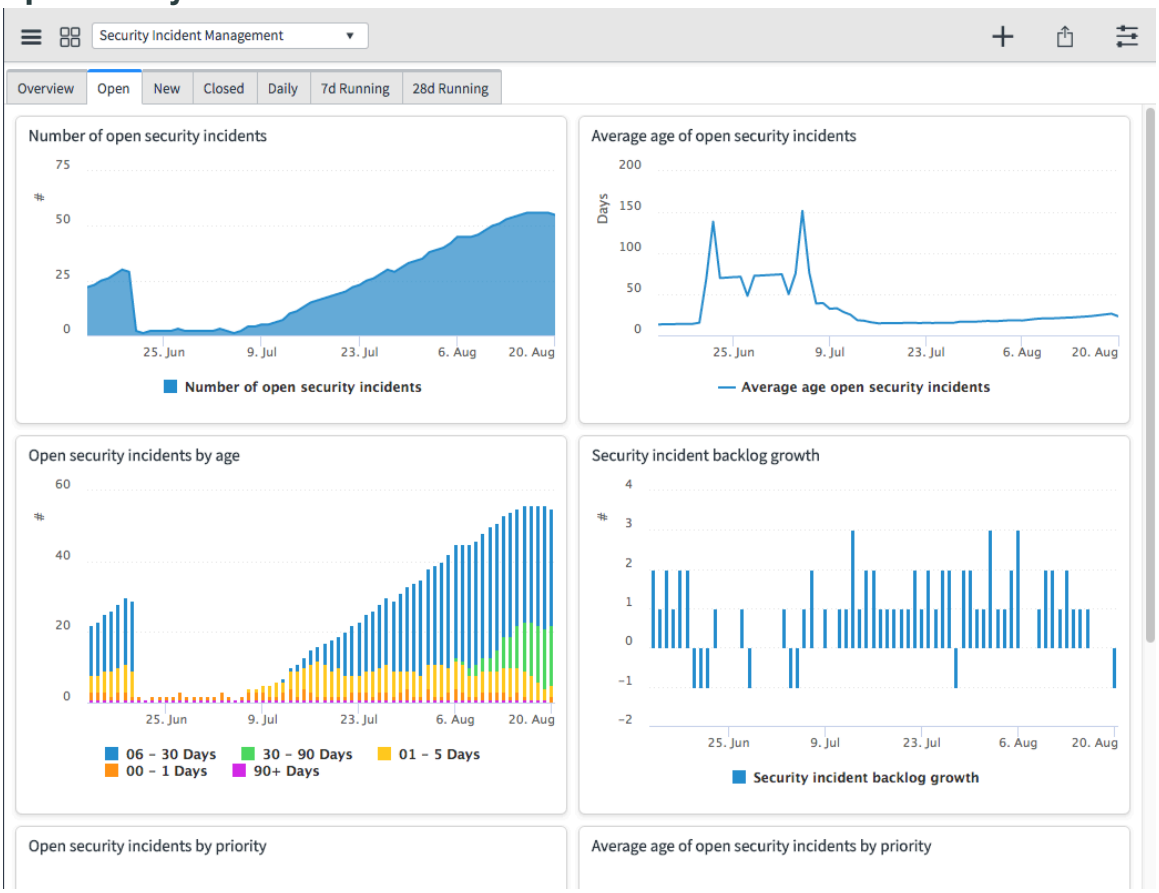
With this dashboard, security managers can easily track the volume, performance and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.

Overview tab

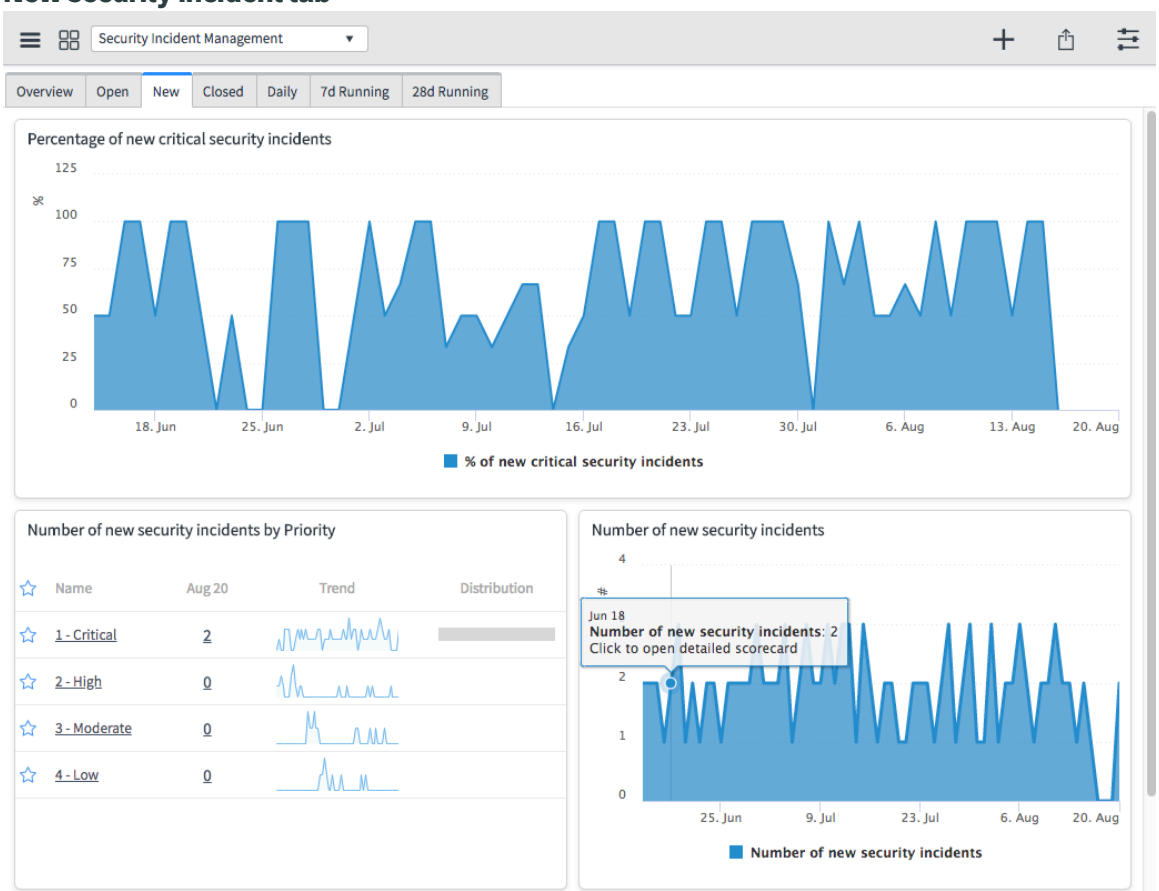


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Open security incidents tab

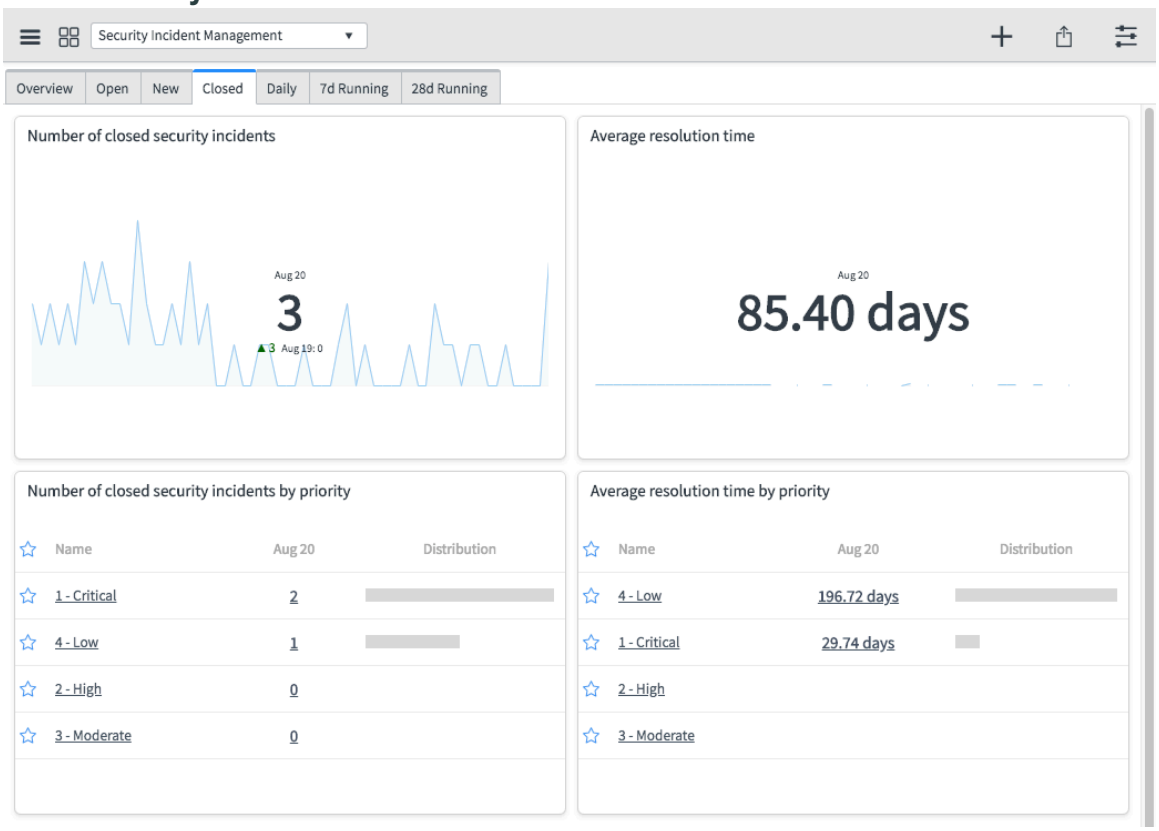


New security incident tab

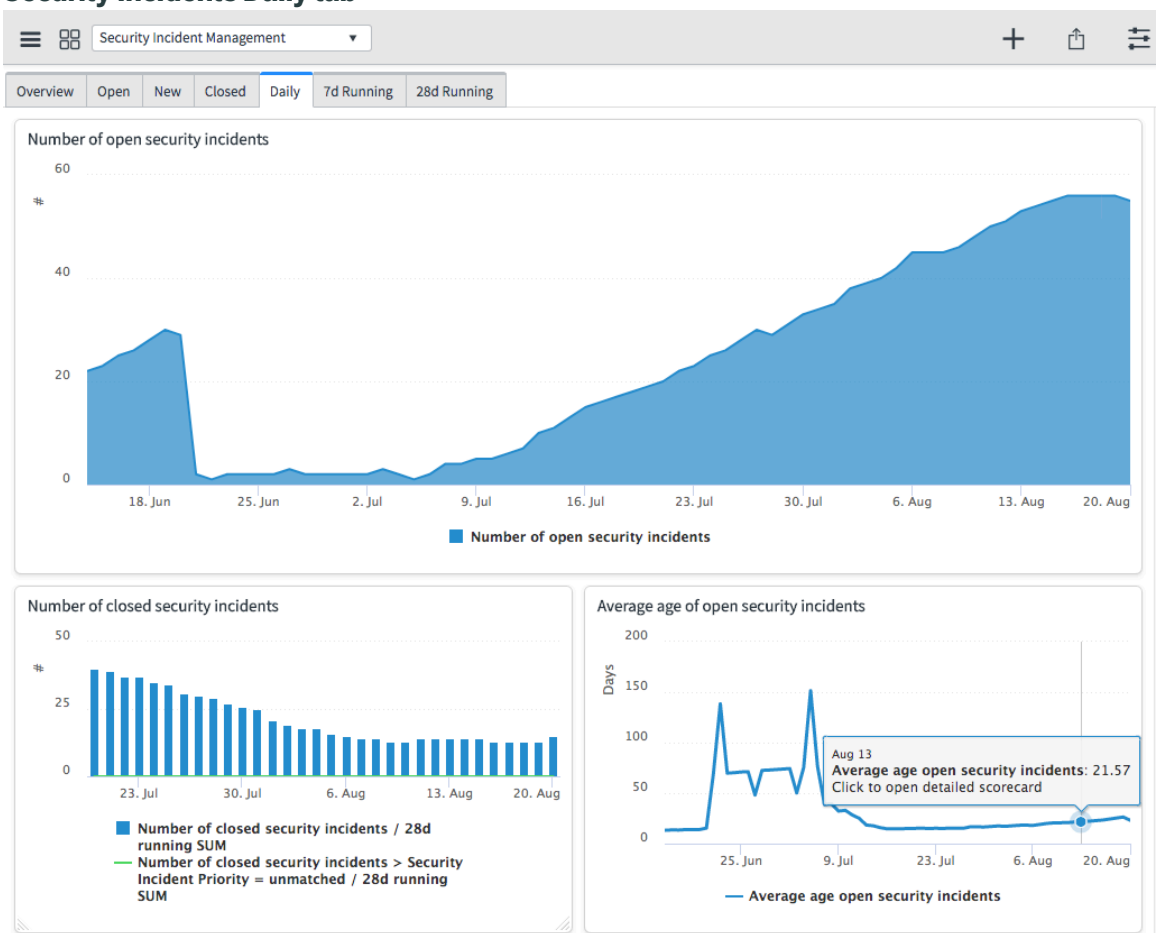


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Closed security incidents tab



Security Incidents Daily tab



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **7d Running** and **28d Running** tabs follow the format of the **Daily** tab.

End users and roles

End user and goal	Required role	Benefits
Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.	sn_si.manager	Can review the overall security posture with the ability to adjust the members of assignment groups.
Security Response Administrator: Needs to pinpoint areas of concern quickly and have full control over all Security Incident Response data while administering territories and skills, as needed.	sn_si.admin	Can adjust risk calculation parameters to ensure vulnerable items that are most pertinent to the organization are being addressed first.
Security Response Analysts: Need to quickly prioritize which vulnerabilities to focus on based upon criticality to the organization.	sn_si.analyst	Tier 1 and 2 security analysts work on security incidents. They can create and update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.

Security Incident Management indicators

The Security Incident Management dashboard presents the following key performance indicators:

New Security Incidents

A chart of the number of new security incidents.

Open Security Incidents

A chart where you can compare the number of open security incidents, the number of open security incidents not updated in the last 30 days, and the number of open security incidents not updated in the last 5 days.

Basic Security Indicators

The last 6 days of scores of the number of new security incidents, the number of closed security incidents, the security incident backlog growth, and Number of open security incidents indicators.

New Security Incidents by Priority

The number of new security incidents broken down by priority.

Breakdowns

The following breakdowns apply to the indicators on the dashboard:

- Security Group
- Security Incident Age

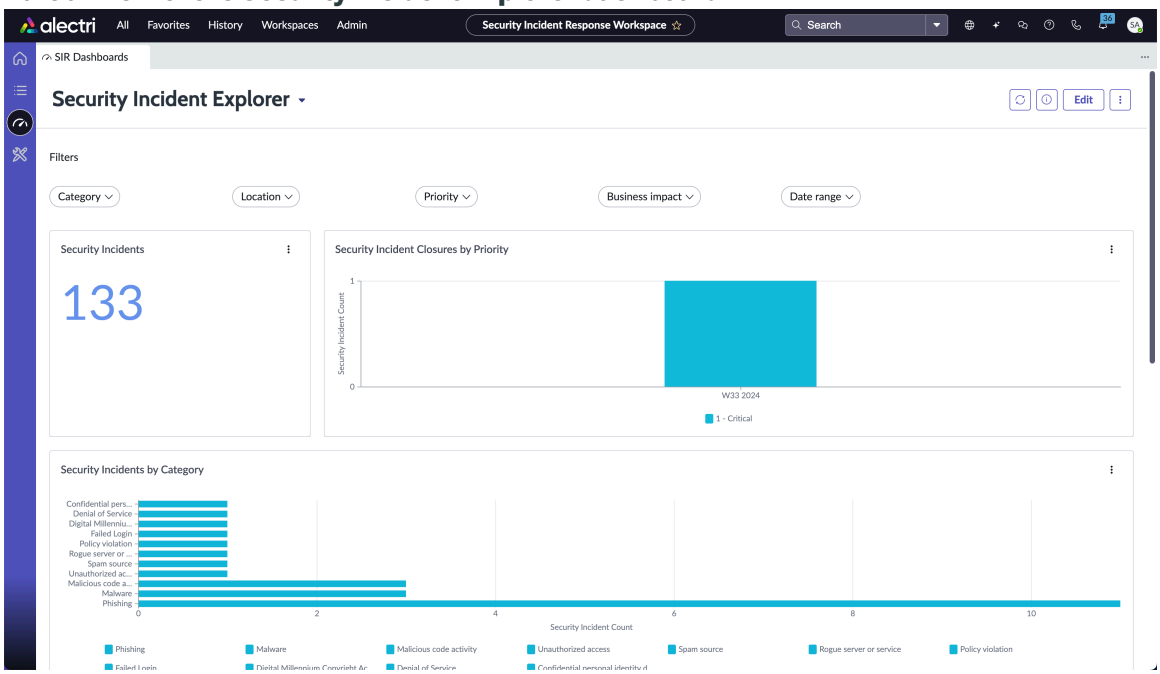
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Incident Category
- Security Incident Priority
- Security Incident State

Security Incident Explorer dashboard

With this dashboard, security managers are able to view security incidents summarized and grouped by category, subcategory, location, priority and business impact. These views let managers quickly gain insight into the frequency in which attacks are occurring and which business services are affected.

Partial view of the Security Incident Explorer dashboard



End users and roles

End user and goal	Required role	Benefits
Security Response Manager: Needs clear visibility into the overall state and volume of security incidents associated with applications and services.	sn_si.manager	Can review the overall security posture with the ability to adjust the members of assignment groups.
Security Response Administrator: Needs to pinpoint areas of concern quickly and have full control over all Security Incident Response data while administering territories and skills, as needed.	sn_si.admin	Can adjust risk calculation parameters to ensure vulnerable items that are most pertinent to the organization are being addressed first.
Security Response Analyst:s Need to quickly prioritize which vulnerabilities to focus	sn_si.analyst	Tier 1 and 2 security analysts work on security incidents. They can create and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

End user and goal	Required role	Benefits
on based upon criticality to the organization.		update security incidents, requests, and tasks, as well as problems, changes, and outages related to their incidents.

Security Incident Explorer indicators

The Security Incident Explorer dashboard presents the following key performance indicators:

Security Incidents

The total volume of open and pending security incidents.

Security Incident Closures by Priority

The number of closed security incidents broken down by Priority.

Security Incidents by Attack Category

The number of open security incidents broken down by Category.

Security Incident Assignment Heatmap

A two-level breakdown of the number of open security incidents by assignment group and priority.

Security Incident Heatmap

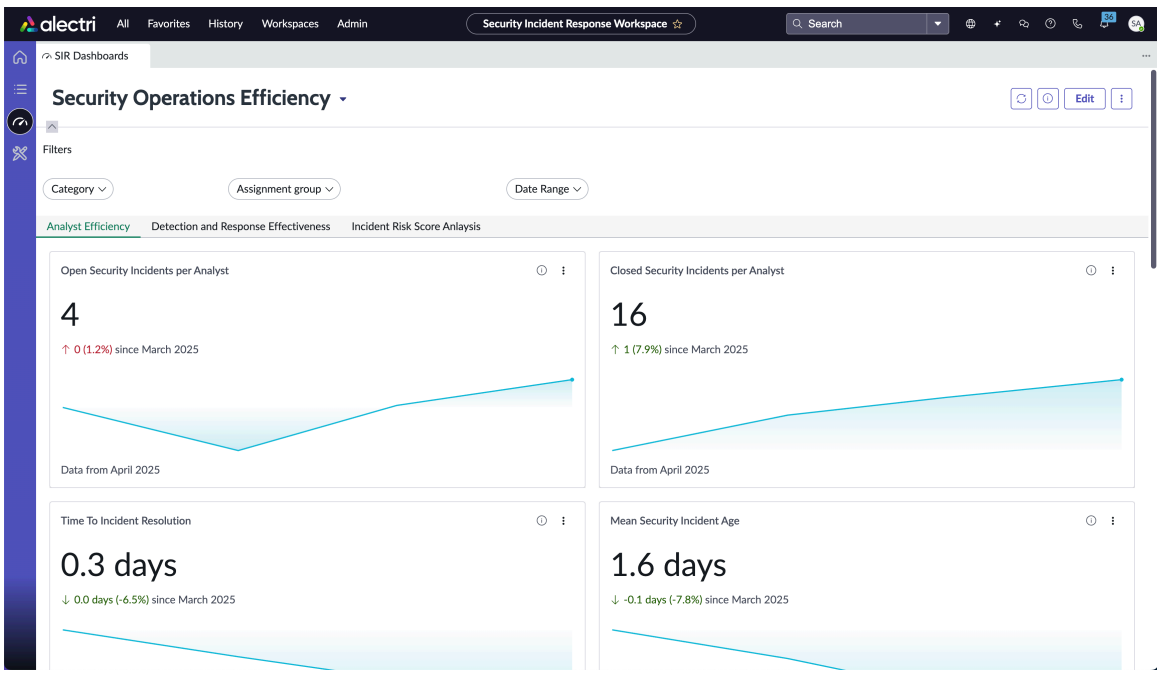
A global map showing the number of open security incidents in each country.

Security Operations Efficiency dashboard

Security operations center (SOC) managers can view overall efficiency metrics and measure the individual performance of the SOC team members in the organization.

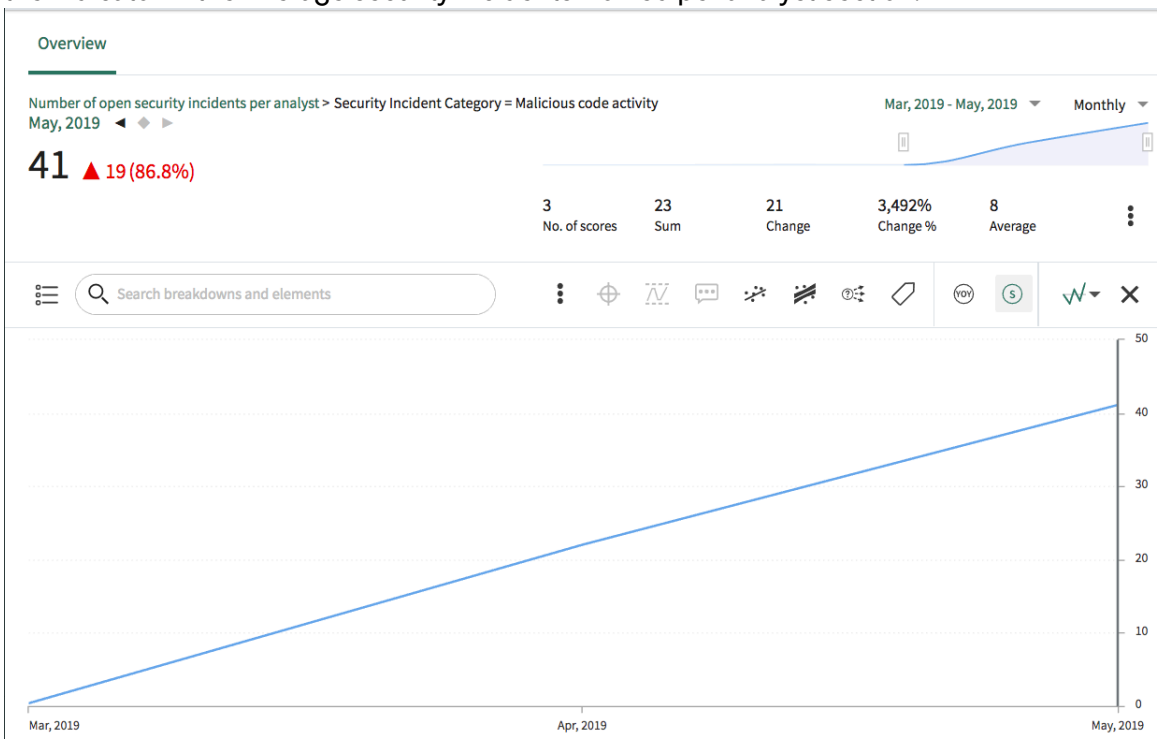
The SOC manager can use the Performance Analytics dashboard to improve efficiency and develop a picture of how SOC is performing in both general and specific areas over time.

Analyst Efficiency tab



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Click any of the indicators to drill down for further details. For example, click the indicator in the Average security incidents worked per analyst section.



The graph shows that the number of open security incidents have increased from 0 in March to over 40 in May. Notice the data displayed in the header:

- Trend indicator: Shows the change in number of open incidents in the latest time period for which the data has been collected. This chart shows data for the period March 2019 to May 2019 and the number of open incidents has increased by 19 in the month of May. Analyst efficiency is better if the number of open incidents has decreased over a period of time.
- No. of scores: The period for which the data has been collected (March to May 2019).
- Sum: The number of new open incidents for the period between March and May.
- Change: The number of new open incidents between March and April.
- Average: The average number of open incidents per analyst for the selected period.

Analyst Efficiency tab

Indicator	Description
Average security incidents worked per analyst	Average number of open security incidents per analyst for the specified period. The formula used is `[[Number of open security incidents / By month AVG +]]/[[Number of Security Agents]]`
Closed security incidents per analyst	The total number of incidents closed by each analyst in the selected category in the specified period. The formula used is `[Number of closed security incidents > Security Incident Category = <category_name> / By month SUM +]]/[[Number of Security Agents / By month AVG +]]`
Average security incident resolution	The average time taken by each analyst to close security incidents in the specified period. The formula used to show the result in days is `([[Summed duration of closed security incidents > Security Incident Category = <category_name> /`

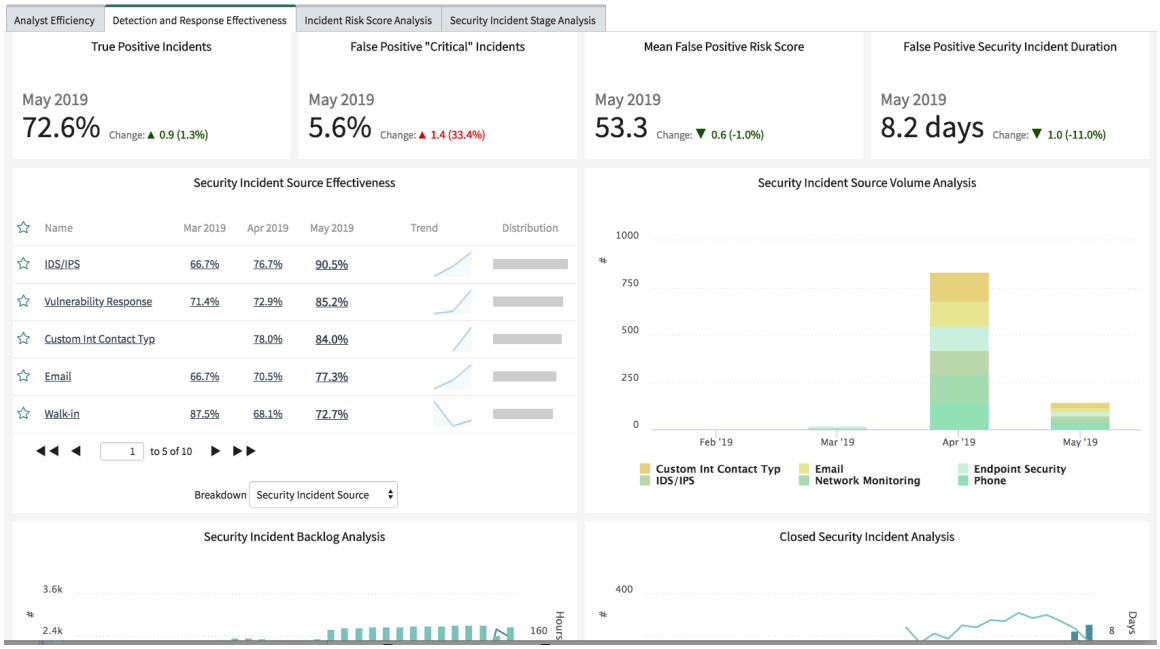
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Analyst Efficiency tab (continued)

Indicator	Description
	`By month AVG +]] / [[Number of closed security incidents > Security Incident Category = <category_name> / By month AVG +]]) / 24`
Average security incident age	The average number of days for which security incidents remain open for each analyst. The formula used to show the result in days is `([[Summed age of open security incidents > Security Incident Category = <category_name> / By month AVG +]]/ [[Number of open security incidents > Security Incident Category = <category_name> / By month AVG +]]) / 24`
Security incident backlog analysis	The total number of open security incidents in the specified period. Select an option from the Breakdown list to view the backlog for each analyst, security group, priority, and so on. You can also compare the number of open security incidents between two selected months.
Closed security incident analysis	The total number of security incidents that are closed in the specified period. Select an option from the Breakdown list to view the count for each analyst, security group, priority, and so on. You can also compare the number of security incidents that were closed between two selected months.
Security incident age	The average number of days for security incidents remain open in the specified period. Select an option from the Breakdown list to view the security incident age for each analyst, security group, priority, and so on. The formula used to show the result in days is `([[Summed age of open security incidents > Security Incident Category = <category_name> > Security Assignment Group = <group_name> / By month AVG +]]/ [[Number of open security incidents > Security Incident Category = <category_name> > Security Assignment Group = <group_name> / By month AVG +]]) / 24`
Security incident resolution time	The average number of days taken to resolve security incidents during the specified period. Select an option from the Breakdown list to view the security incident resolution time for each analyst, security group, priority, and so on. The formula used to show the result in days is `([[Summed duration of closed security incidents > Security Incident Category = Malicious code activity > Security Assigned To = John Ashby / By month AVG +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity > Security Assigned To = John Ashby / By month AVG +]]) / 24`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Detection and Response Effectiveness tab



Detection and Response Effectiveness tab

Indicator	Description
True positive incidents	Percentage of true positive security incidents in the selected category for the specified period. The formula used is `(1 - ([[Number of false positive security incidents > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]])) * 100`
False positive critical incidents	Percentage of false positive critical security incidents in the selected category for the specified period. The formula used is `([[Number of false positive security incidents > Security Incident Risk Score = Critical Risk > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]]) * 100`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Detection and Response Effectiveness tab (continued)

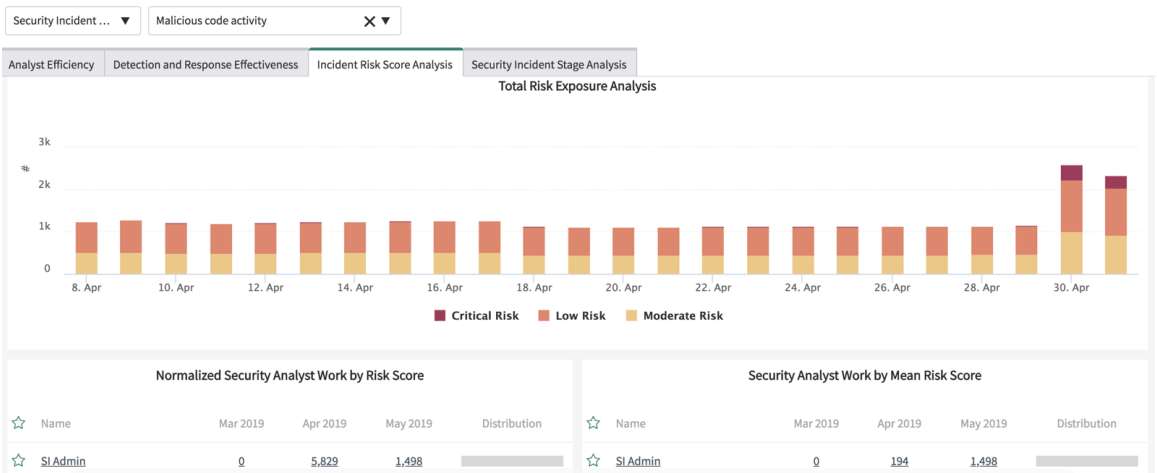
Indicator	Description
	Note: Any security incident where the `Closed code = Invalid vulnerability or False positive` is treated as a false positive incident
Mean false positive risk score	Average monthly risk score of closed security incidents that were identified as false positive incidents. A lower risk score indicates that the security analysts spent lesser time analyzing false positive incidents. The formula used is `([[Number of false positive security incidents > Security Incident Risk Score = Critical Risk > Security Incident Category = Malicious code activity / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity / By month SUM +]]) * 100`
False positive security incident duration	Average number of days that the security analysts spent in investigating false positive incidents. The formula used is `([[Summed duration of false positive security incidents]] / [[Number of false positive security incidents]]) / 24`
Security incident source effectiveness	Percentage of true positive security incidents identified by a specific source for the specified period. The source can be email, network activity,customer support, and so on. This data helps measure the effectiveness of the security incident source. The formula used is `(1-([[Number of false positive security incidents > Security Incident Category = Malicious code activity > Security Incident Source = IDS/IPS / By month SUM +]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity > Security Incident Source = IDS/IPS / By month SUM +]])) * 100`
Security incident source volume analysis	Number of closed security incidents for current month for each Security incident source. You can also compare the number

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Detection and Response Effectiveness tab (continued)

Indicator	Description
	of security incidents for each source type between two selected months.
Security incident backlog analysis	The total number of open security incidents in the specified period and the average number of days for which the incidents remain open. You can also compare the number of open security incidents between two selected months. The formula used to calculate the average backlog period is `([[Summed age of open security incidents > Security Incident Category = Malicious code activity]]/ [[Number of open security incidents > Security Incident Category = Malicious code activity]]) / 24`
Closed security incident analysis	The total number of closed security incidents in the specified period and the average resolution time for these incidents. The formula used to calculate the average resolution time is `([[Summed duration of closed security incidents > Security Incident Category = Malicious code activity]] / [[Number of closed security incidents > Security Incident Category = Malicious code activity]]) / 24`

Incident Risk Score Analysis tab

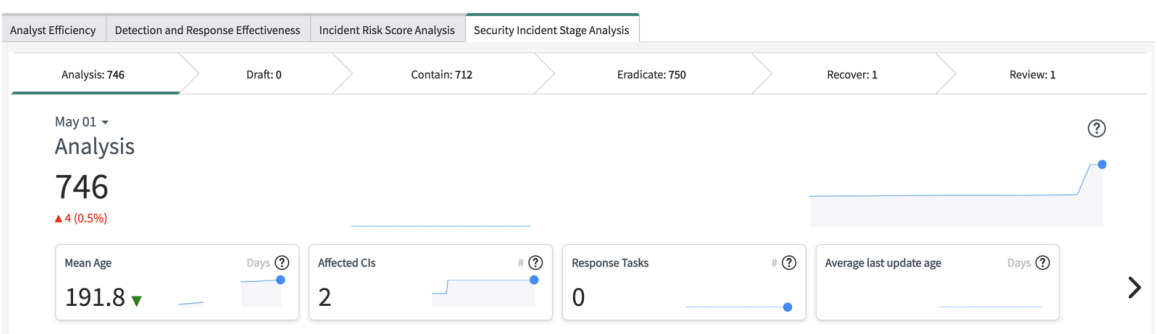


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident Risk Score Analysis tab

Indicator	Description
Total risk exposure analysis	Total number of open incidents in each risk category (low, moderate, and critical) in the specified period. You can also compare the number of incidents in the different risk categories between two months.
Normalized security analyst work by risk score	The total risk score for each security analyst for the specified period. This is calculated based on the number of true positive security incidents that the security analyst closed. The formula used is `[[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]] - [[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month SUM +]]`
Security analyst work by mean risk score	The average risk score for each security analyst for the specified period. The formula used is `[[Summed Risk Score of Closed Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]] - [[Summed Risk Score of False Positive Security Incidents > Security Incident Category = Malicious code activity > Security Assigned To = SI Admin / By month AVG +]]`

Security Incident Stage Analysis tab



You can see the number of open incidents on a specific day and the status (analysis, draft, contain, eradicate, recover, or review) of these incidents. On each stage, you can view average

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

age, affected CIs, response tasks, and so on. Click on a link to view additional details or the breakdown of these incidents.

Security Incident Response Workspace

The ServiceNow® Security Incident Response Workspace is a reimagined interface that provides a next-gen user experience for the security analysts and SOC managers. The security analysts can use this to manage the life cycle of security incidents from an initial analysis to containment, eradication, and recovery.

Get started with SIR Workspace

Select a tile to get started.

Explore Workspace  Learn about SIR Workspace concepts and features	**Admins using Workspace**  Configure SIR Workspace and features
Analysts using Workspace  Learn how Analysts use SIR Workspace	**View SIR Dashboards**  View SIR Workspace dashboards

Request apps on Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Important:

- Installing the Security Incident Response 13.4.5 version or later from the ServiceNow Store will automatically install the Security Incident Response Workspace (sn_si_aw) 1.5.1 version or later by default. For more information on the dependent applications, refer to the SIR Workspace plugins section.
- Please note that the Security Incident Response Workspace versions 1.5.1 and above can only be installed/upgraded through an installation/upgradation of Security Incident Response and can't be installed independently.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

More resources

Visit the Security Incident Response forum on the ServiceNow Community.

Exploring SIR Workspace

Explore Security Incident Response Workspace to understand how the security analysts and managers perform their day-to-day operations with an improved user experience, do a complete incident investigation, and get an overview of the security incidents, response tasks and SLAs assigned to the security analyst and team.

This section describes the following:

- SIR Workspace plugins and required roles.
- Key SIR Workspace features.

SIR Workspace plugins

The following are the required applications to work with Security Incident Response Workspace (sn_si_aw) plugin.

Applications

Installing the Security Incident Response application version 13.4.5 or later automatically installs the Security Incident Response Workspace and the following apps.

- Enterprise Security Case Management PAD Commons [sn_escm_pad_cmn]
- Security Operations Common Workspace [sn_escm_ws_cmn]
- Security Incident UI Card Component [sn_sirw_evam]
- Security Operations spoke [sn_sec_spoke]

Important:

- Installing the Security Incident Response 13.4.5 version or later from the ServiceNow Store automatically installs the Security Incident Response Workspace (sn_si_aw) 1.5.1 version or later by default.
- The Security Incident Response Workspace versions 1.5.1 and above can only be installed/upgraded through an installation/upgradation of Security Incident Response and can't be installed independently.

Enterprise Security Case Management PAD Commons requires the Playbook Experience [playbook_experience] plugin.

For information on the Security Incident Response roles, tables, properties, and scheduled jobs, see Components installed with Security Incident Response.

SIR Workspace features

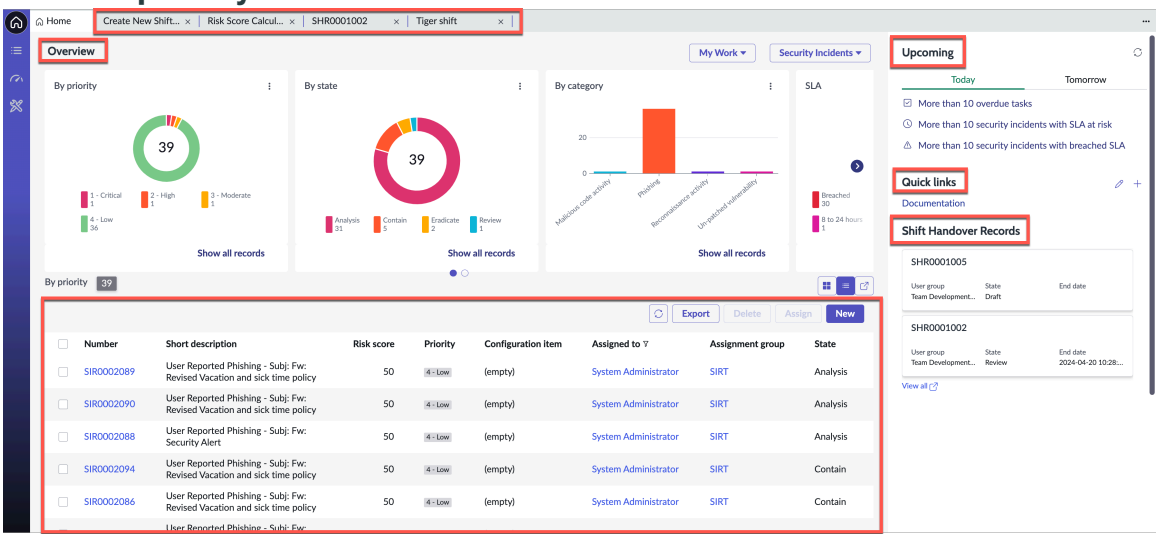
The Security Incident Response Workspace consists of the following key features.

- Overview section
- Upcoming section
- Quick Links section
- Shift Handover Records section

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- List view
- Multi-tab interface that supports opening multiple security incidents

SIR Workspace key features



SIR Workspace interface overview

The SIR Workspace Overview page consists of the Security Incidents and Response Tasks details that are under security analysts and their team.

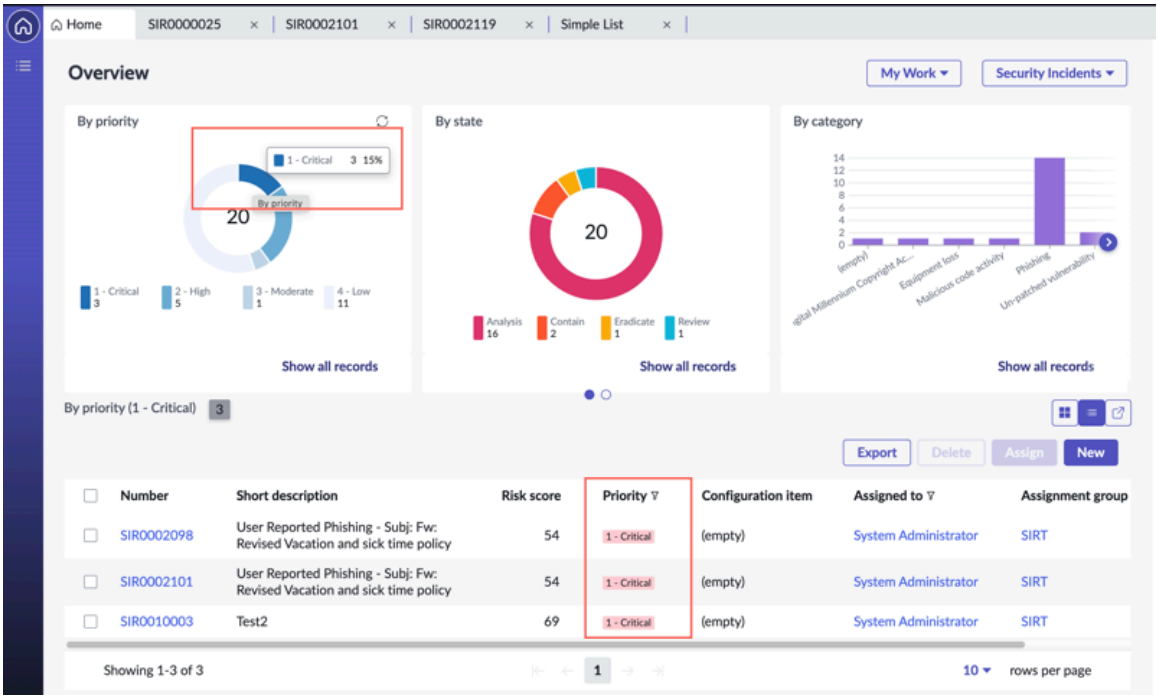
There are various widgets present under each filter grouped by priority, category, state, and SLA, which are in the security analysts' queues and security analysts team's queue.

When filters are applied on the widgets, the bottom half of the overview page is populated with the corresponding security incidents or response tasks presented as cards or list items. The analyst can toggle between the card view or the list view as desired.

For example, on the **Priority** widget if you want to select all the critical incidents or response tasks then click on the **Critical** segment (example screen shot below) of the widget and those incidents or response task which are critical gets displayed in the list or card view.

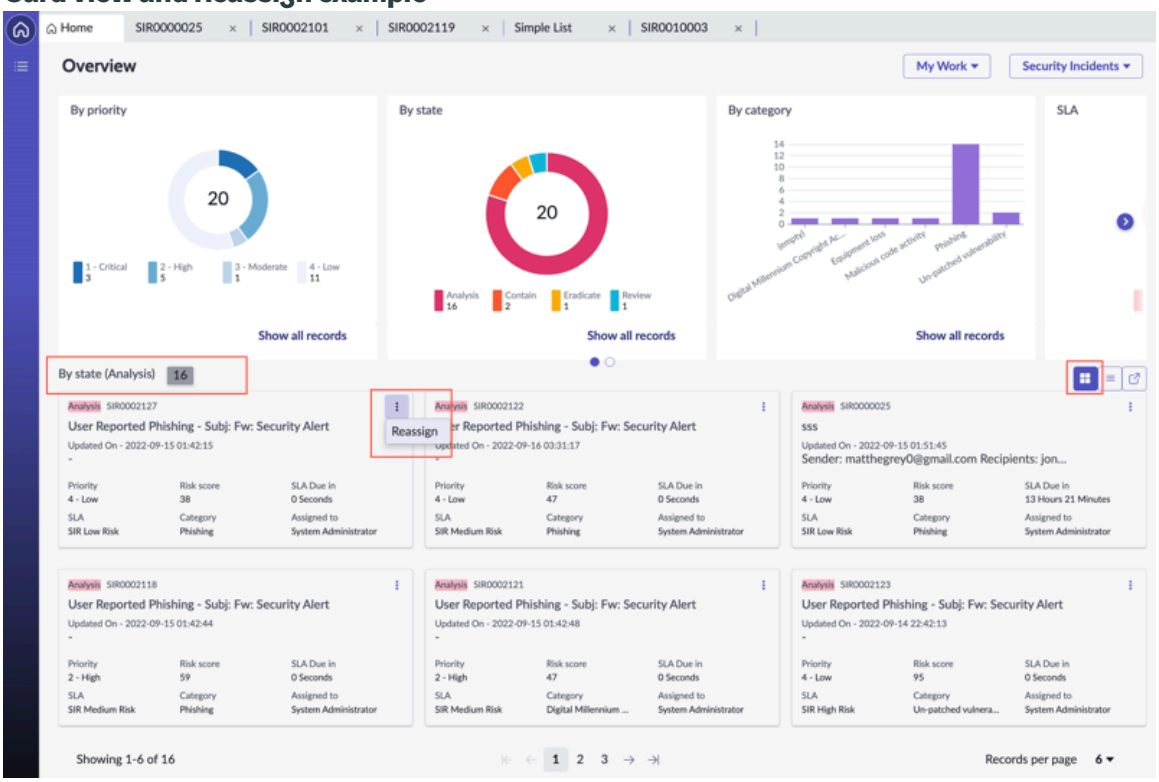
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview section



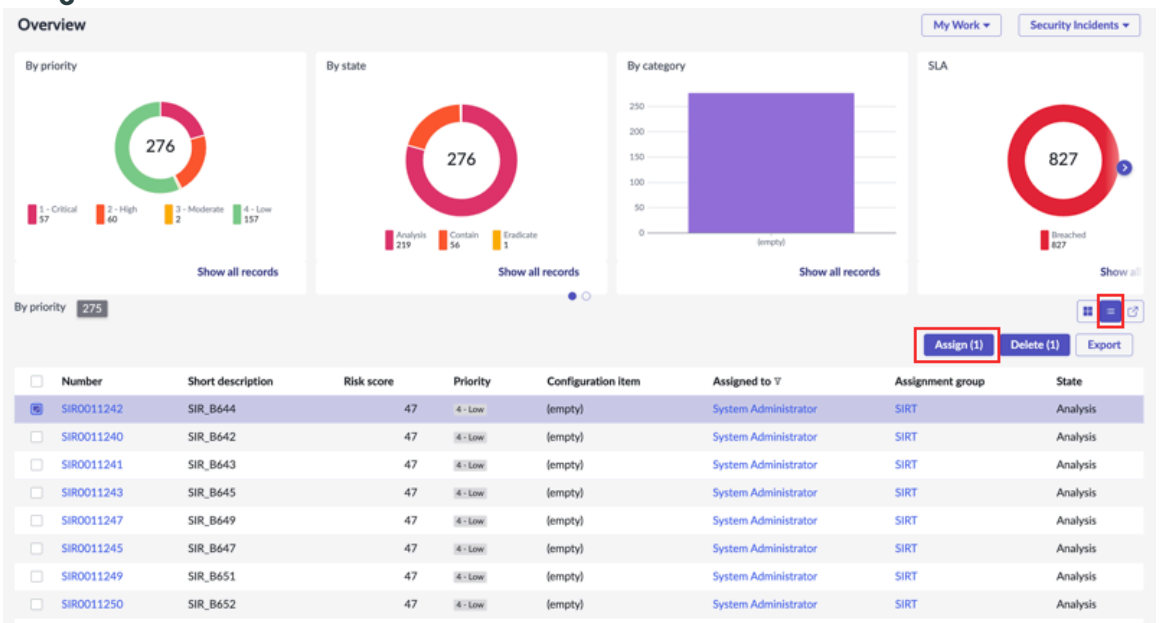
You can assign or reassign the security incidents or response tasks directly from this view by clicking on the ellipse icon and select the **Assign** (option in card view) or directly the **Assign** button (option in list view) accordingly to assign an incident.

Card view and Reassign example



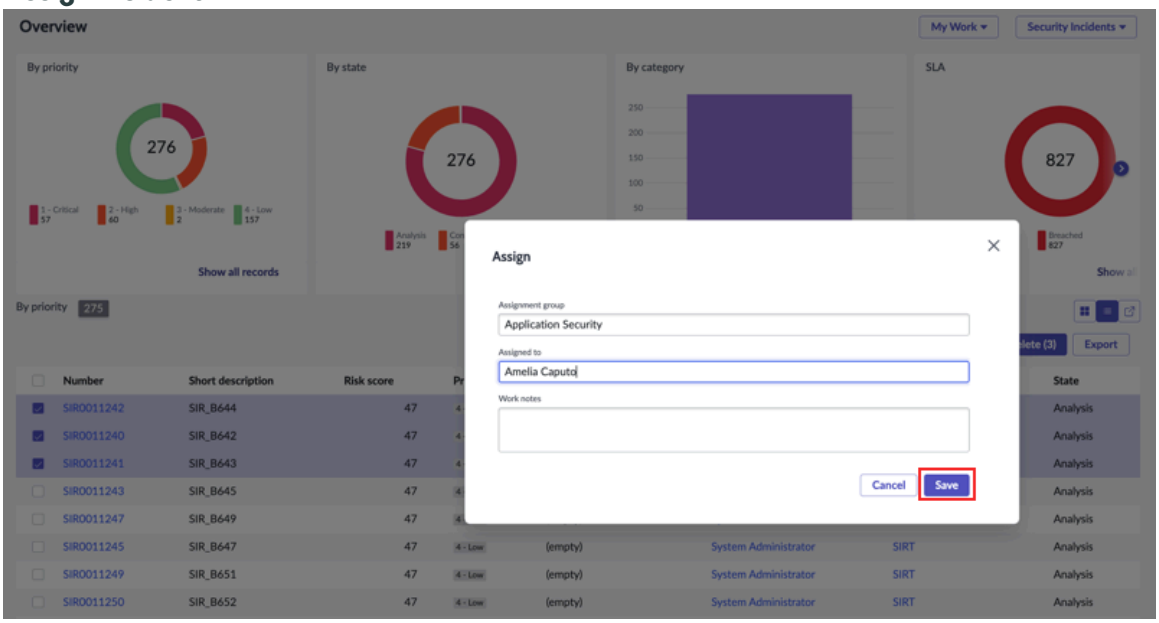
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign incident



Here is an example of the list view. The user can assign incidents from the list view as well.

Assign incident



Add or modify the assignee details such as Assignment group and Assigned to, add worknotes, if required.

Note: You can assign one or more security incidents or response tasks to the assignment groups. The selected number is displayed on the **Assign** button.

The user can delete security incidents from this view. Click the **Delete** button to delete the security incident, the record will be deleted from the list view.

The user can export the list content as well. Click the **Export** button to export the list in the desired format.

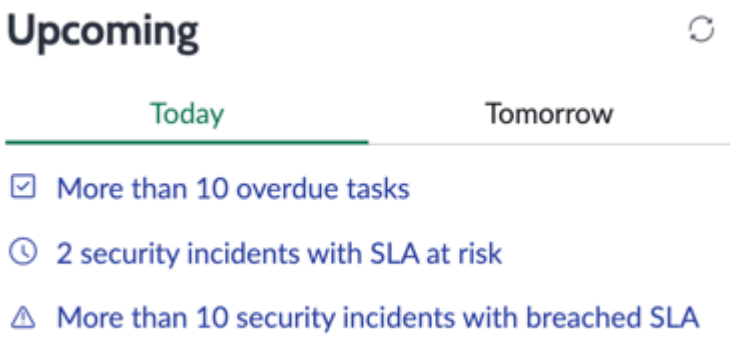
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Upcoming section

This section displays the upcoming tasks such as the security incidents and response tasks that are due as on the same day and next day.

The security incidents and response tasks list that is displayed is based on the due date field and SLA definition defined for those records.

If this section contains more than one security incident or response task then the incident or records opens all those records in a new tab.



View upcoming tasks

The Security Analyst can view the upcoming tasks related to the Security Incidents and Response Tasks that are due, overdue or breached the defined SLA.

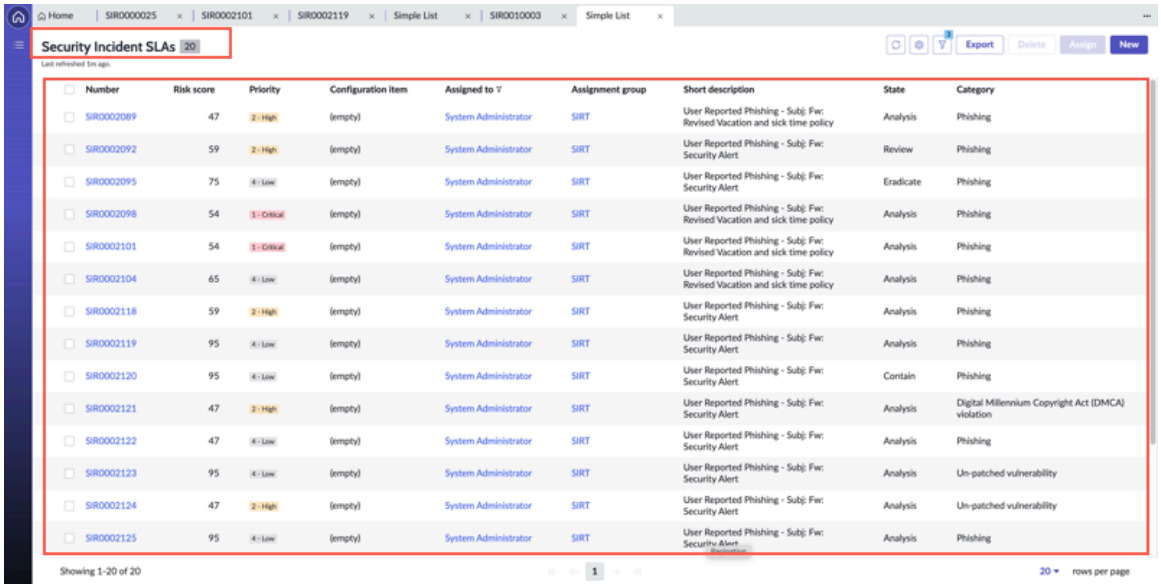
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Upcoming**.
2. Click **Today** tab to view the tasks that are due on the same day.
3. Select **Tomorrow** tab to view the tasks that are overdue to the next day.
   The upcoming section lists the security incidents or response tasks that are overdue based on the due date and that breached the SLA definition.
4. Click **Refresh** icon to refresh the upcoming section list.
   For example, if you click on the link, **More than 10 security incidents with breached SLA** then the list of breached SLA incidents are displayed in a new tab within the workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: You can perform New, Assign, Export, and Delete operations from any list view.

Quick links section

Quick links work like bookmark links. You can add external URLs and quickly access them from within the workspace.

Working with quick links

Add quick links for easy reference.

Before you begin

Role required: sn_si.analyst

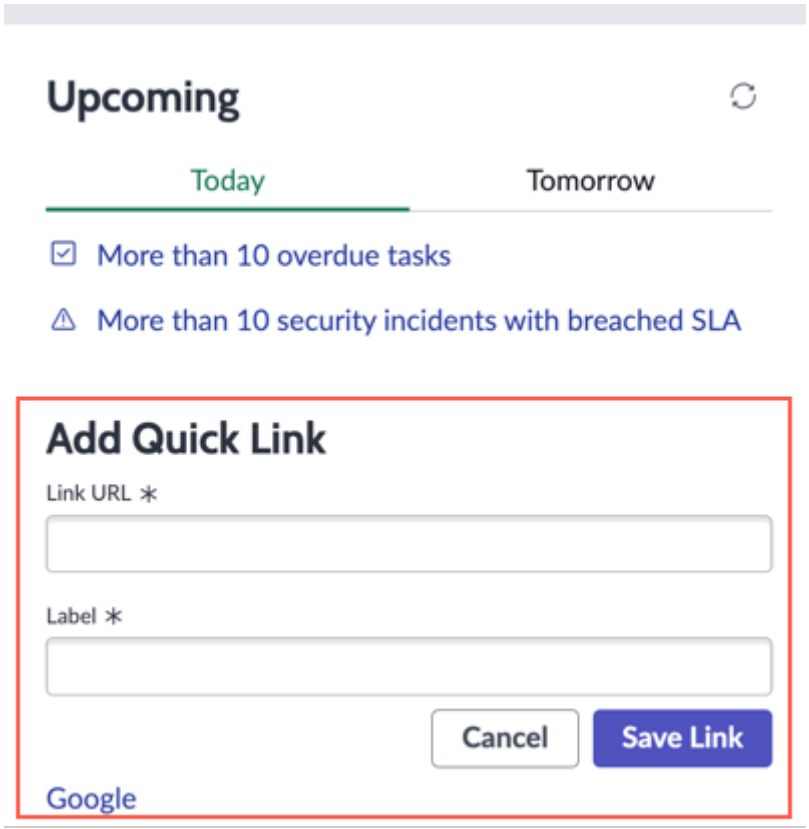
About this task

You can add and modify any useful quick links and bookmark those links that helps in the incident resolution.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Quick links**.
2. Click **Add Quick Link** icon to add the links.
3. Enter the link to the URL and Label.
4. Click **Save Link**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The new link gets added below the quick links section.

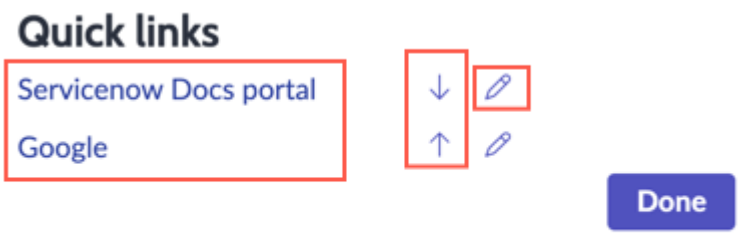
5. **To modify or delete the links:**

   a. Click **Edit Link** icon.

   b. Modify the desired link or display text which is the label of the URL.

   c. Click **Save**.

   d. Click **Done**.



   e. Use the upward and downward arrows to move the position of the links.

   f. Click **Delete** to delete the links while editing that were bookmarked.

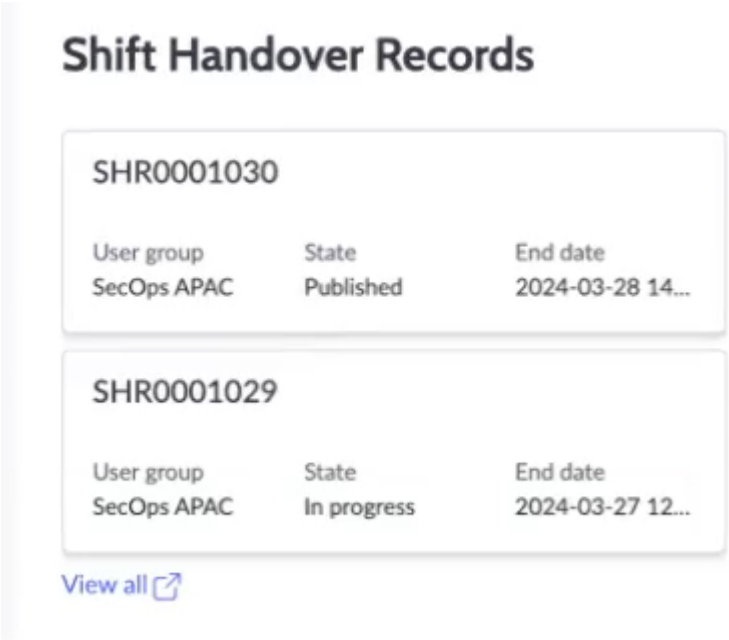
Shift Handover Records section

The section displays the list of Shift Handover records in the Security Incident Response Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Shift Handover records section on the Security Incident Response Workspace displays the last two Shift Handover records based on the End date, State, and User group fields defined for those records. To view all the Shift Handover Records, select **View all**.

Shift Handover Records section



List view in SIR Workspace

The list view consists of the security incidents, response tasks, phishing emails, and assessments.

The list view has pre applied filters such as Assigned to Me, Assigned to Team, Unassigned, All Open, All, and so on.

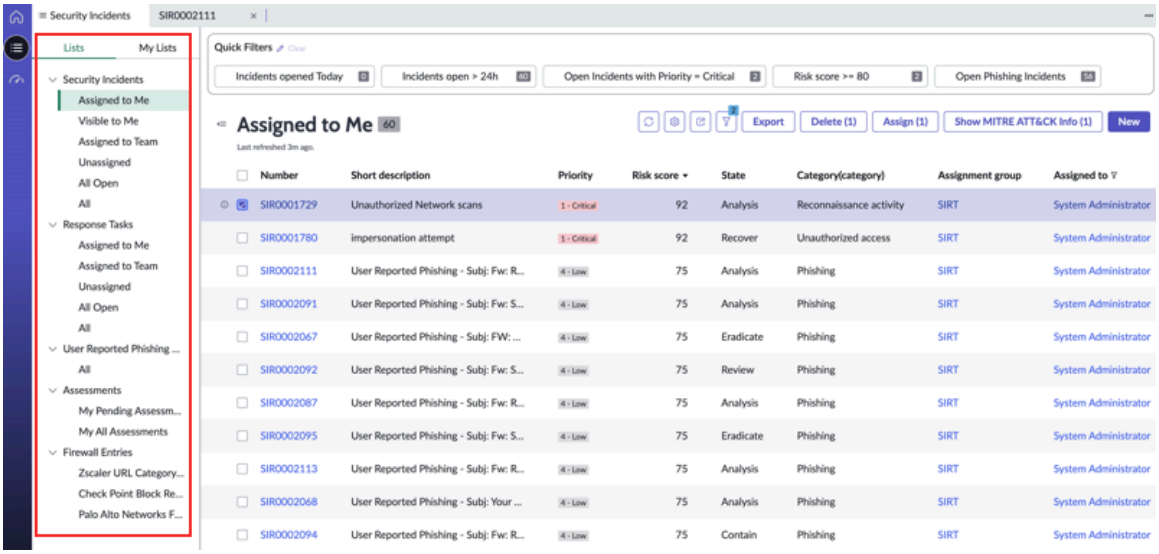
Using these list categories and filtered lists, analysts can quickly find the required Security Incidents and Response Tasks records that they need to work on.

To get to the list view, you need to click the list icon ( ). When you click a record in a list view, the record opens in a new tab.

List types

The following gives you an example view of the lists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The list pane contains the following sections:

Lists

List item	Description	Capability
Security Incidents	View the list of security incidents and navigate to the desired incident to start working on them. The following lists are available: • **Visible to Me**: Security incidents that are visible to the logged in user. • **Assigned to Me**: Security incidents that are assigned to the analyst. • **Assigned to the Team**: Security incidents that are assigned to all the teams that the analysts belongs to. • **Unassigned**: List of unassigned security incidents. • **All Open**: List of all open security incidents. • **All**: List of all security incidents.	• On the List view, the Analyst can configure the list of columns by clicking on the gear icon which is available above the incident columns. • The analyst can select one or more security incident(s) and assign those incidents to the other users. • The analyst can delete the security incidents. • The analyst can create a new security incident. • The analyst can apply the quick filters. Apply the filters by clicking on the **Quick Filters** option instead of using the advance **Filter** option. Using the quick filters, you can quickly filter the list of security incidents that needs immediate attention. For more information, see Working with quick filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Capability
		• The analysts can refresh the list of incidents. • The analyst can export the list view to Excel, CSV, JSON, and PDF formats.
Shift Handover Records	View the list of Shift Handover records. The following lists are available: • **Assigned to the Team**: Shift Handover records that are assigned to all the teams/user groups that the analysts belongs to. • **All**: List of all security incidents.	Shift Handover supports the following three roles: • Admin: Shift owner role • Security Analyst: Shift analyst role • Security Manager: Shift owner role, but doesn't have access to user group to which the Shift Handover record is assigned to. • The users with the Shift Owner/Analyst role who are part of the user group in the active shift can add or modify content in the shift handover records in the draft state. • The users who don't have the Shift owner/analyst role or are not part of the user group in the active shift can only view the content in the Shift Handover records.
Response Tasks	View the list of response tasks and navigate to the desired response task to start working on them. The list view contains: • **Assigned to Me**: Response tasks that are assigned to the analyst. • **Assigned to the Team**: Response tasks that are assigned to the teams to the analysts belongs to. • **Unassigned**: List of unassigned response tasks.	• On the List view, the Analyst can configure the list of columns by clicking on the gear icon which is available above the incident columns. • The analyst can select one or more response task(s) and assign those tasks to other users. • The analyst can create a new response task. • The analyst can apply the quick filters. Apply the filters by clicking on the **Quick Filters** option instead of

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Lists (continued)

List item	Description	Capability
	• **All Open**: List of all open response tasks. • **All**: List of all response tasks.	using the advance **Filter** option. Using the quick filters, you can quickly filter the list of response tasks that needs immediate attention. • The analysts can refresh the list of response tasks. • The analyst can export the list view to Excel, CSV, JSON, and PDF formats. For more information, see Export Security Incidents or Response Tasks.
Phishing Emails	View the list of all Phishing emails. The list view will be sorted based on the last update.	• Report Phishing Email. For more information, see Report Phish Email on how to report a phishing email. • Delete phishing emails. • Export the phishing emails list view to Excel, CSV, JSON, and PDF formats.
Assessments	View the list of assessments needed to perform post incident review. • **My pending Assessments**: List of pending assessments. • **My All Assessments**: List of all assessments.	Take assessments.

Personalize a list

Security analysts or managers can personalize the security incidents or response tasks or phishing emails custom list view based on their individual preferences.

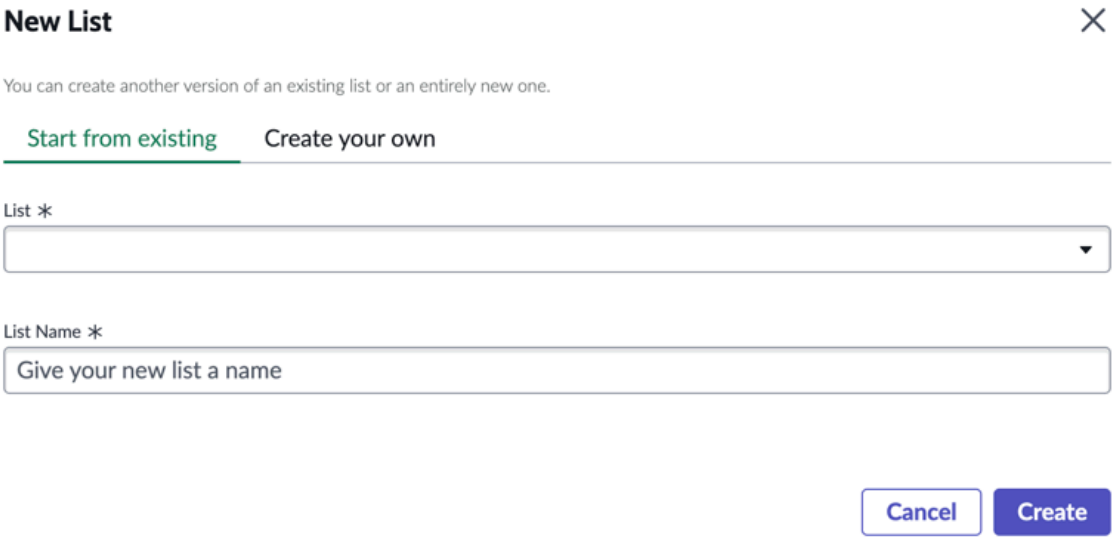
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click **List View**.
3. Click **My Lists**.
4. Click **Add new list**, available at the bottom of **My Lists** view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Security analysts can create either another version of an existing list or an entirely a new customized list.

5. **To create from an existing list view:**

   a. Click on **Start from existing** link.

   b. Select the **List** from the drop-down list.

   > **Note:** Whatever list you select from the drop-down list, the list name will be the copy of your main List. For example, if you select **Assigned to Me** within the security incidents section, then the List name will be **Assigned to Me Copy** of the security incidents section.

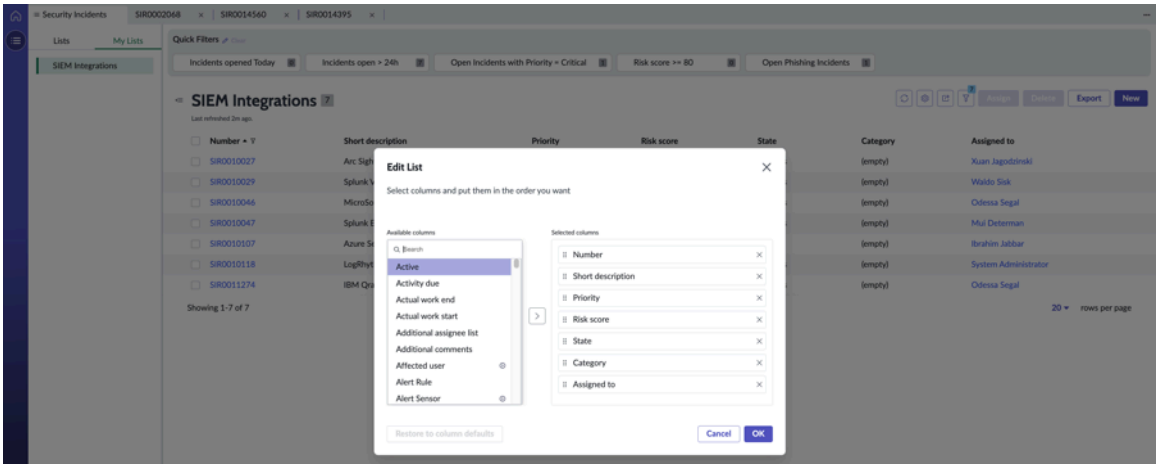
   c. Select the columns to be personalized and add filters.
   Build a filter by adding conditions that contain a field, operator, and value(s).

   d. Click **Create**.

   > **Note:** To customize your own list view, you can add custom columns, filters, set conditions, sort by the order as required.

   e. After a personalized list view is created, then click on the gear icon and customize the list columns by choosing **Edit columns** option to edit the columns and put them in order that you prefer.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can also:

- **Rename** the personalized list view.
- **Delete** the personalized list view.
- Save the personalized list view as desired using **Save as** option.
- **Reset width** of the list view.

Note: You can also directly perform these operations using the other List Actions buttons such as assigning, deleting, exporting the list view which are provided.

6. To create your own list:

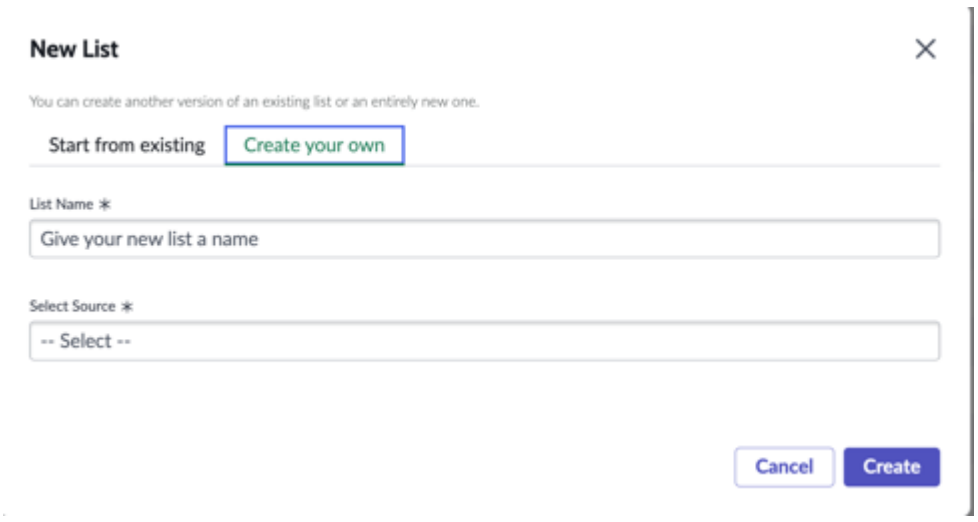
a. Click on **Create your own** link.

b. Provide a **List Name**.

c. Select the **Source** and **Columns**.

d. Add filters.
Build a filter by adding conditions and provide the order in which the list should be appeared.

e. Click **Create**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A new list gets created as defined and customized by you underneath the **My Lists** section.

Note: you can **Reorder** your personalized view by moving their positions.

Assign Security Incidents

Assign security incidents.

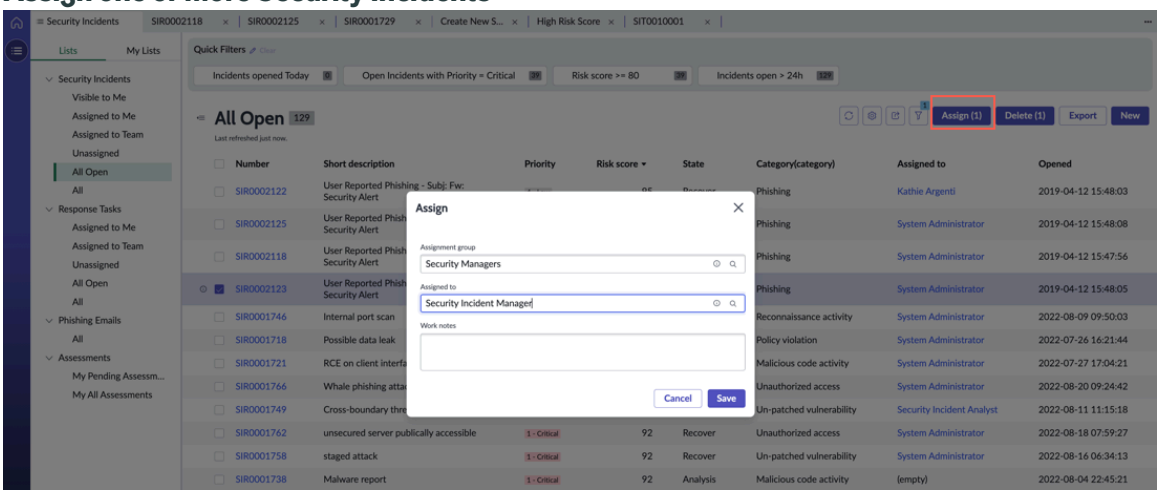
Before you begin

Role required: sn_si.basic

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the list ( ) icon.
3. Click **Lists**.
4. For example, go to **Security Incidents** > **All Open**.
5. Select one or more security incidents.
6. Click **Assign**.
7. Fill the details such as Assignment group, Assigned to, and add Work notes if required.
   The incident will then be assigned to the user.
8. Click **Save**.

Assign one or more Security Incidents



Close multiple security incidents

Close multiple security incidents at the same time to avoid having to close related incidents individually, such as incidents created with a common root cause or false positive incidents.

Before you begin

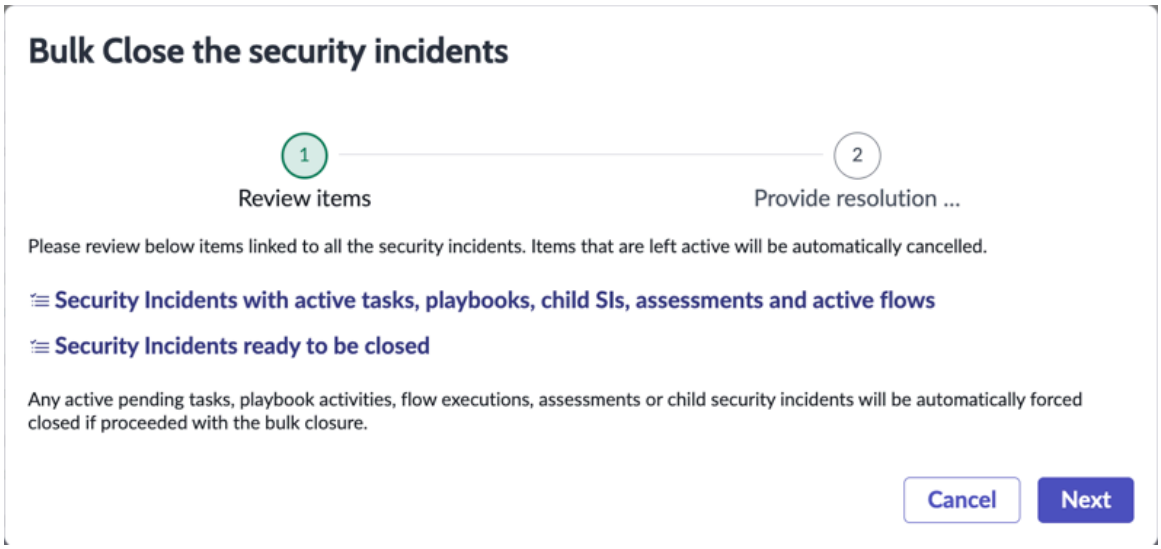
Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select the Security Incidents icon .
3. In the **Lists** tab, select **Security Incidents** > **All Open**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select one or more security incidents to close and select **Close**.
   The Bulk Close the security incidents window displays links to access lists of the security incidents selected to be closed.
   - If at least one selected security incident has pending activities such as active tasks, playbooks, child SIs, assessments, or active flows, the **Security incidents with active tasks, playbooks, child SIs, assessments and active flows** link is displayed.
   - If at least one security incident selected for closing has no pending closing activities, the **Security incidents ready to be closed** link is displayed.



   Any active pending active tasks, playbooks, child SIs, assessments, and active flows will automatically be closed when you proceed with the bulk closure.

5. **Optional:** If you're not sure whether active items for incidents should be closed, review the security incidents with active items.
   a. Select the **Security incidents with active tasks, playbooks, child SIs, assessments and active flows** link.
   b. Open the security incident you want to review.
   c. If any changes are necessary, make them and select **Save**.
   d. Close the incident tab.
   e. Select **Take me back**.
6. Select **next**.
7. In the **Close Code** field, select the applicable close code.
   The available close codes are:
   - Investigation completed
   - Threat mitigated
   - Patched vulnerability
   - Invalid vulnerability
   - Not resolved
   - False positive
8. In the **Close notes** field, enter any notes.
9. Select **Bulk Close**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

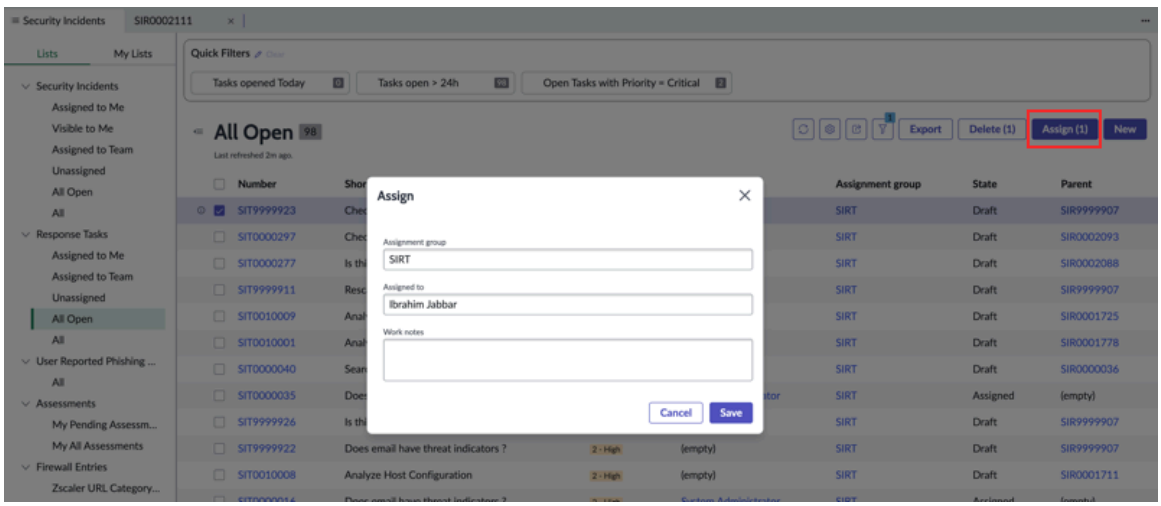
Result
The incident closing activity runs in the background.

Assign Response Tasks

Assign Response tasks for a security issue.

Before you begin
Role required: sn_si.basic

Procedure
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the list ( ) icon.
3. Click **Lists**.
   For example, go to **Response Tasks** > **All Open**.
4. Select one or more response task(s).
5. Click **Assign**.
6. Fill the details such as Assignment group, Assigned to, and add Work notes if required.
   The incident will then be assigned to the user.
7. Click **Save**.



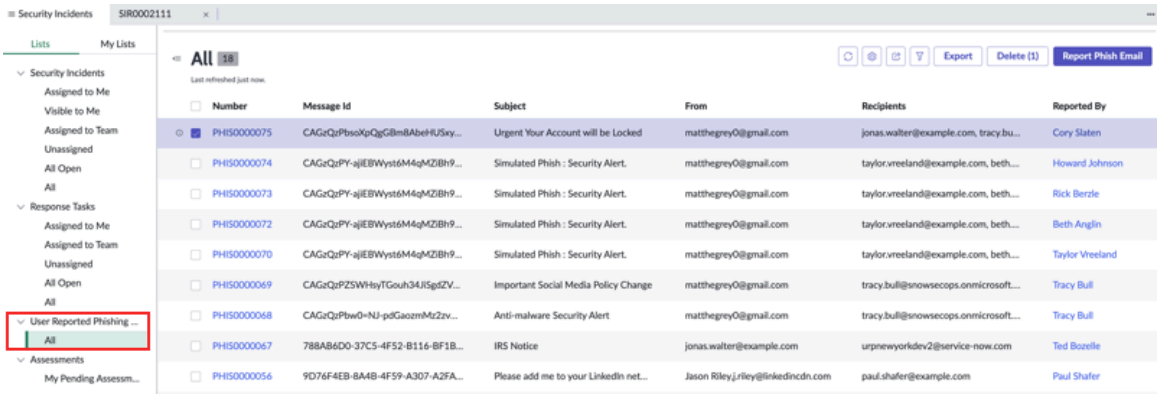
Report Phish Email

Report phishing emails from the lists view.

Before you begin
Role required: sn_si.analyst

Procedure
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the list ( ) icon.
3. Go to **User Reported Phishing Emails** > **All**.
   The user reported phishing emails list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click **Report Phish Email** button.
   Report a phishing email by uploading it.
5. Click **Add File** to add attachments.
6. Click **Upload**.

> **Note:** Report a Phish Email by uploading the attachments. You can upload only one phishing email at once and should be in .eml format.

7. Click **Submit**.
   The phishing email to log a security incident is created.

Working with quick filters

Quick filters are easily accessible filters that are available on, security incidents and response tasks lists.

Before you begin

Role required: sn_si.admin

The SIR Workspace provides quick filters feature that allows you to filter the list of security incidents or response tasks with ease.

You can use quick filters to configure new filters or modify existing filters that appear against these lists. The base system provides the following quick filters for each security incident:

- **Incidents Opened Today**
- **Incidents open > 24hrs**
- **Open incidents with Priority= Critical**
- **Risk >= 80**
- **Open Phishing Incidents**

The base system provides the following quick filters for each response task:

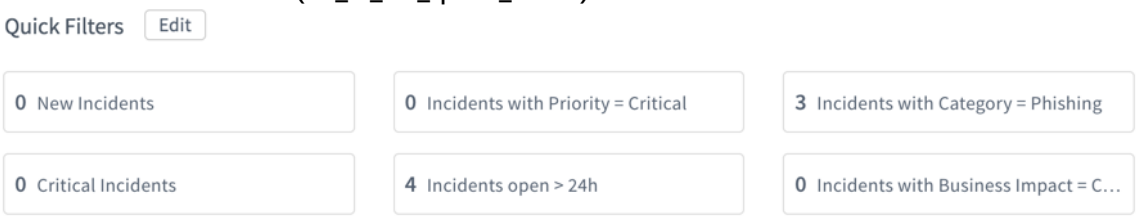
- **Tasks open > 24h**
- **Open Tasks with Priority = Critical**

> **Note:** An admin can configure the required list of quick filters according to the organization need.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **System Definition** > **Tables**.
2. Search for **Quick Filters** (sn_si_aw_quick_filters).

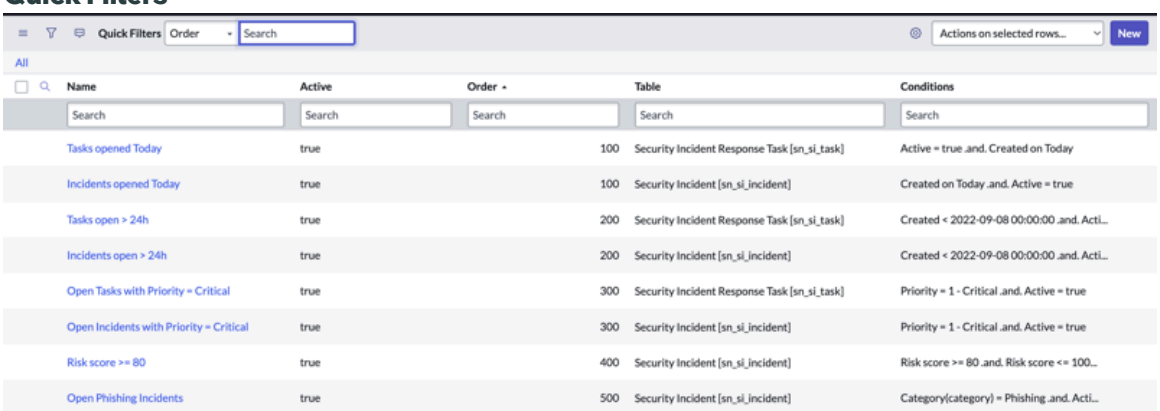


3. Go to **Related Links** > **Show List** section.
   The **Quick Filters** list page is displayed. OOTB, following is the list of quick filters shipped with the application.

Name	Table	Value
Tasks opened Today	Security Incident Task [sn_si_task]	True
Incidents opened Today	Security Incident [sn_si_incident]	True
Tasks open > 24h	Security Incident Response Task [sn_si_task]	True
Incidents open > 24h	Security Incident [sn_si_incident]	True
Open Tasks with Priority = Critical	Security Incident Response Task [sn_si_incident]	True
Open Incidents with Priority = Critical	Security Incident [sn_si_incident]	True
Risk score >= 80	Security Incident [sn_si_incident]	True
Open Phishing Incidents	Security Incident [sn_si_incident]	True

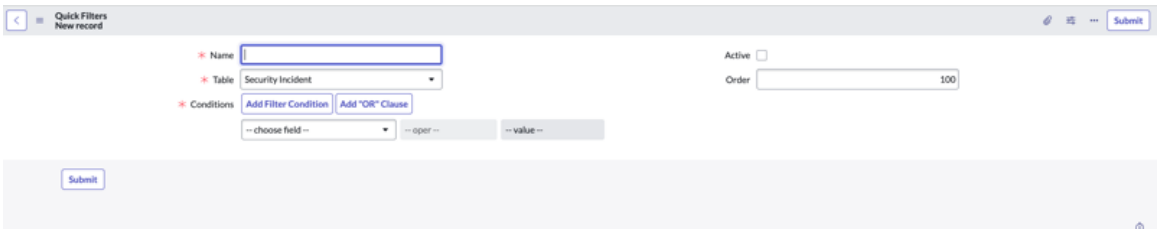
Note: The security admin can go ahead and configure these quick filters. As per the business need, admin can modify the existing value to false and create a new quick filter.

Quick Filters



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

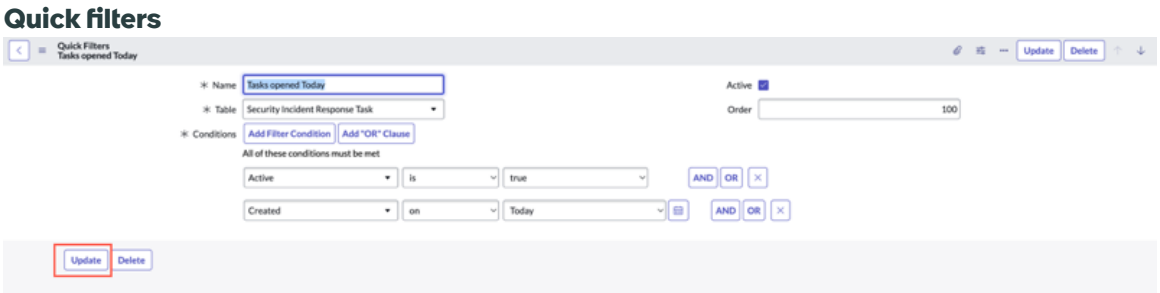
4. Click **New** to create a new filter.
5. Enter a name for the filter, select the Table, specify the filter condition.
6. Click **Submit** to return to the previous list page.
   You will see the newly added filter listed on the page.



Note:

- The quick filter will be applicable only if the **Active** check box is selected.
- Within the workspace, any logged in user can personalize the active quick filters which are available in the application. Users can hide or unhide the newly created quick filters. This feature is based on their user preference.
- If a user has modified the preferences for quick filters and a new quick filter is created after that, then if the quick filter is set to active, it will not apply to the user's preference. The user has to manually change the preferences in the personalized view.

7. Select any existing filter record to modify the existing quick filters.
8. Modify the name and filter condition.
9. Click **Update**.



Add or modify quick filters

Add or modify quick filters for security incidents or response tasks within the list view.

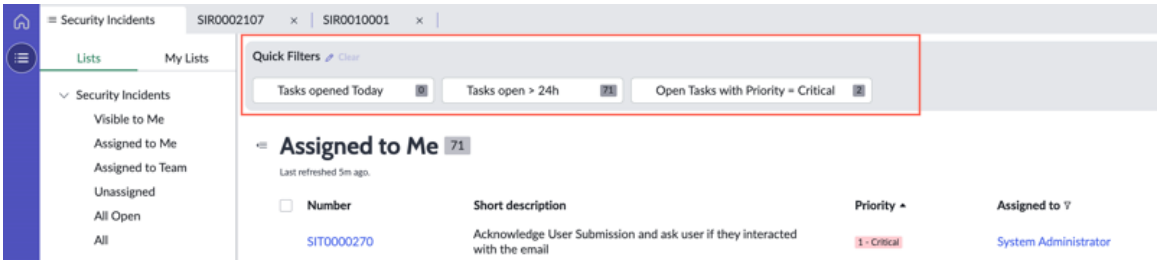
Before you begin

Role required: sn_si.basic

Procedure

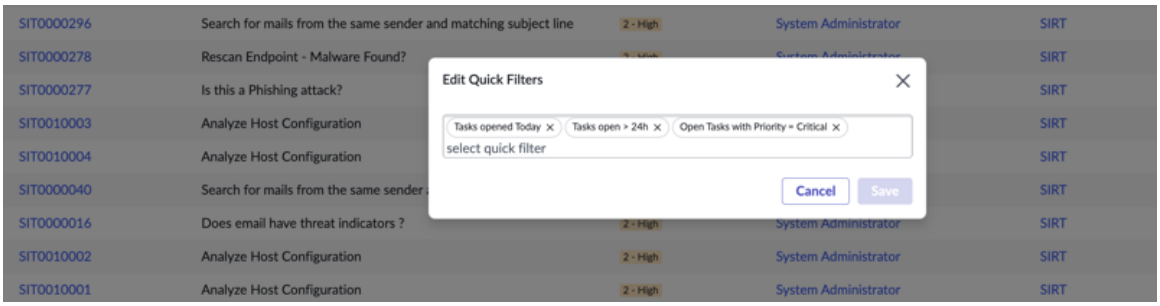
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the list ( ) icon.
3. For example, go to **Lists** > **Security Incidents** > **Quick Filters** section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click **Edit** icon to make the changes.

> **Note:** The change that you make will be persisted, and when the user returns back to this page the next time then the persisted preference is displayed.



5. Click **Save**.

Export Security Incidents or Response Tasks

Export the security incidents or response tasks from the list view.

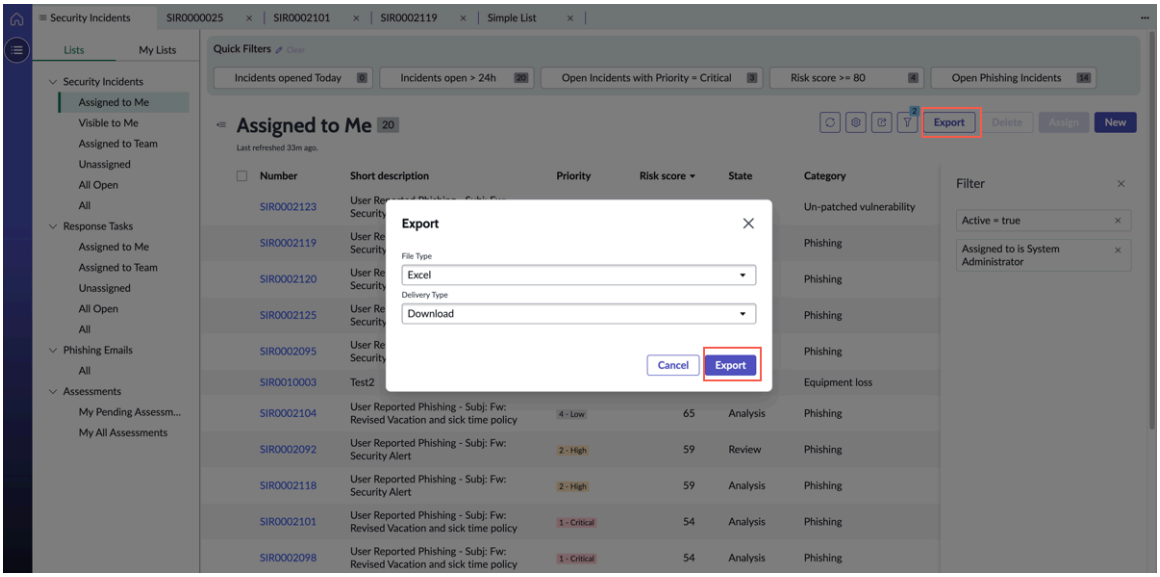
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the list icon.
3. Click **Lists**.
4. Go to **Security Incidents or Response Tasks** > **All Open**.
5. View the list and click **Export**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Select the **File Type** and **Delivery Type**.
   For example, **Excel** and either **Download** or **Email** the list.
7. Click **Export**.
   The file will be downloaded or emailed as per the option chosen.

Manage Shift Handover records

Use the Shift Handover records list view to create, edit, copy, or delete Shift Handover records. Each Shift Handover record is associated with a Shift Handover Report Template.

Before you begin

Role required:

- sn_escm_sh.shift_analyst: Minimum requirement to access the Shift Handover records.
- sn_escm_sh.shift_owner: Create, edit, and delete handover log records in the user groups the Shift Owner is part of. This role inherits the sn_escm_sh.shift_analyst role.
- sn_escm_sh.shift_analyst: View all the Shift Handover log records but can contribute only to In-progress Shift Handover records assigned to the Shift Analyst's group.
- sn_si.analyst - Inherits the sn_escm_sh.shift_analyst role.
- sn_si.admin - Inherits the sn_escm_sh.shift_admin role.
- sn_escm_sh.shift_admin - Inherits the sn_escm_sh.shift_owner role

Important: To learn how to configure the Shift Handover Template as an Admin, see Configure Shift Handover Templates.

About this task

The Shift Owner and the respective team or user group create the Shift Handover log records. The Shift Owner has to choose the Shift Handover template and user group that will work on the Shift Handover report. After the Shift Handover report is complete, it will be shared with the next active Shift Owner and team.

Shift Handover template key points:

- If some other analyst from the active shift team has already updated the report before you, and if changes are being processed, then you might see an error message that there are pending content updates. You must wait 30 seconds and then select **Change to "Review"**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

state again. You can see the consolidated report on the right-pane get updated with other analysts' updated content.

- If the Shift owner has modified the content in a section in the Review state, then the same content gets reflected for the Analyst when the record moves back to the In-progress state.
- The Shift owner must be mindful while editing the content in the Review state, and performing actions like merging two lines, merging two sections, removing a section, as this will affect the Shift Handover report of the other analysts.
- After publishing the Shift Handover report, the Shift owner can modify the content, but they can't change the record state.
- When someone is modifying the content and during that time, if the record state gets changed from In-progress to Review, then the unsaved content changes get discarded.
- Shift admin will have write access to all shift handover log records irrespective of user groups.

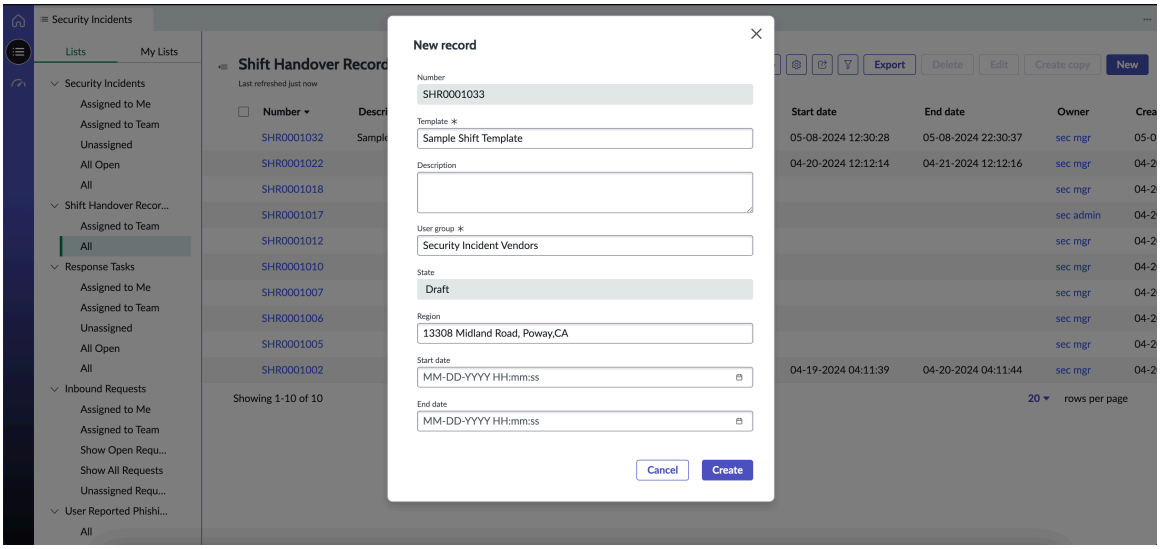
Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select the Security Incident List  icon.
3. On the **Lists** tab, select **Shift Handover Records**.
4. Select **All Records** to view the list of all the Shift Handover records.
5. Select **Assigned to Team** to view the list of Shift Handover records that are assigned to all the teams/user groups that the analysts belong to.
6. To create a new Shift Handover record, select **New**.
7. On the form, fill the fields.

Field	Description
Number	Unique number that is automatically generated for a Shift Handover record.
Template	Select the Shift Handover Template to use. For example, Sample Shift Template.
Description	Description for the Shift Handover record.
User group	Select the User Group/Team for the Shift Handover record to be assigned to. For example, Team Development Code Reviewers.
State	The current state of the Shift Handover record. By default, the initial state is Draft **Note:** The State can't be changed during the creation of a record. .
Region	Select the region for the Shift Handover record to be assigned to. For example, APAC.
Start date	Select the start date for the Shift Handover record.
End date	Select the end date for the Shift Handover record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

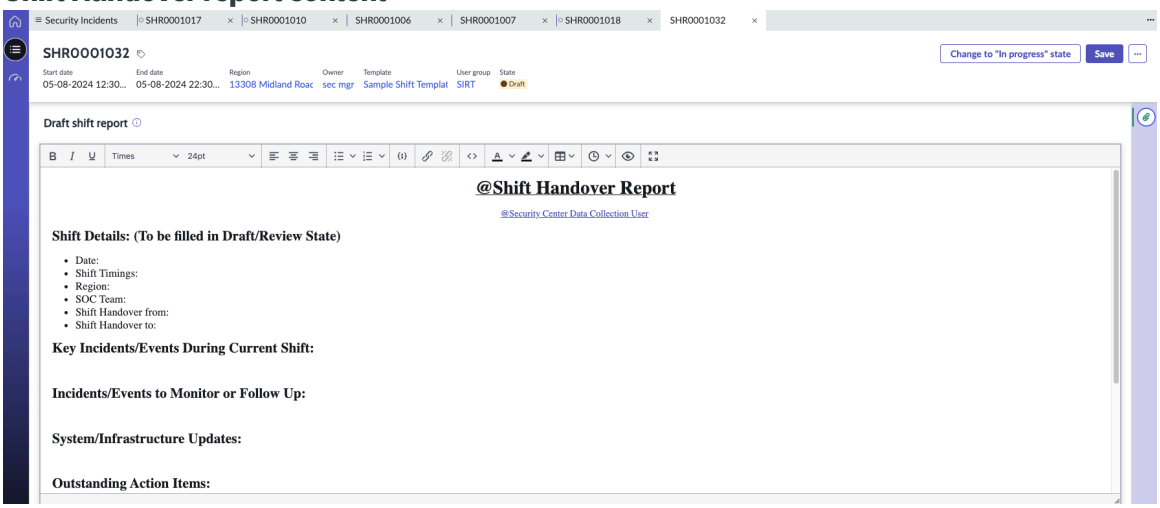
Create a Shift Handover record



8. Select **Create**.
   A new Shift Handover record is created based on the template that you selected and added to the list view.
9. Open the new Shift Handover record to update the status and details of the security incidents on the Shift Handover report.
   By default, the Shift Handover record is in the **Draft** state.

Note: Only the Shift Owner can modify the content.

Shift Handover report content



10. In the Draft shift report editor, use the Shift Handover report template sections to update the details of the security incidents and users.

    You can format your report with all the options in the editor, like fonts, colors, bullets, links, and attachments.

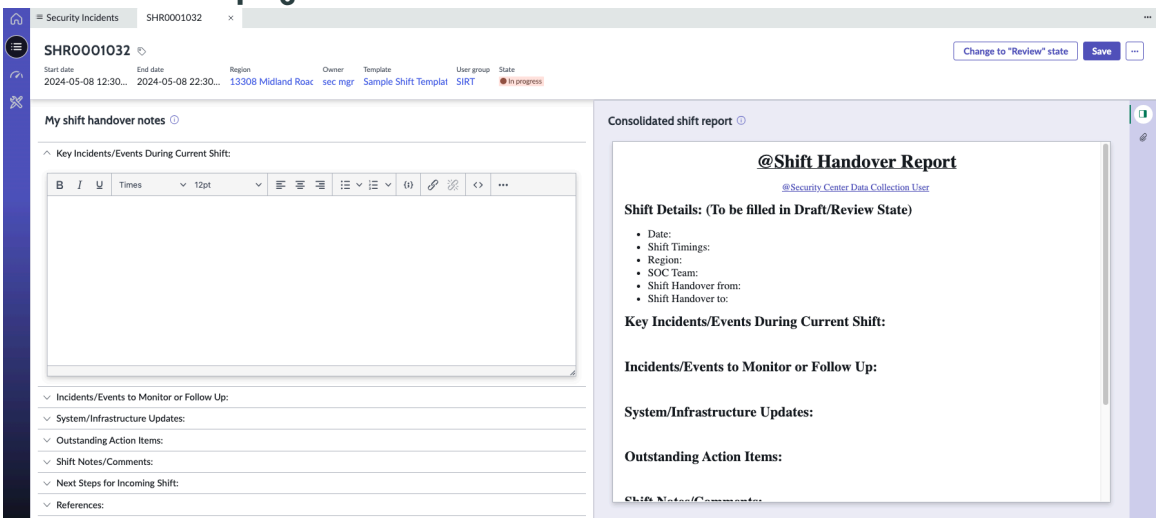
Note: The Shift Owner and Shift Analyst can both modify the content.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. After making the required changes to the Shift Handover report, select **Save**.

b. Select **Change to "In-progress" state** action to move the Shift Handover record to In-progress state.

Shift Handover in-progress

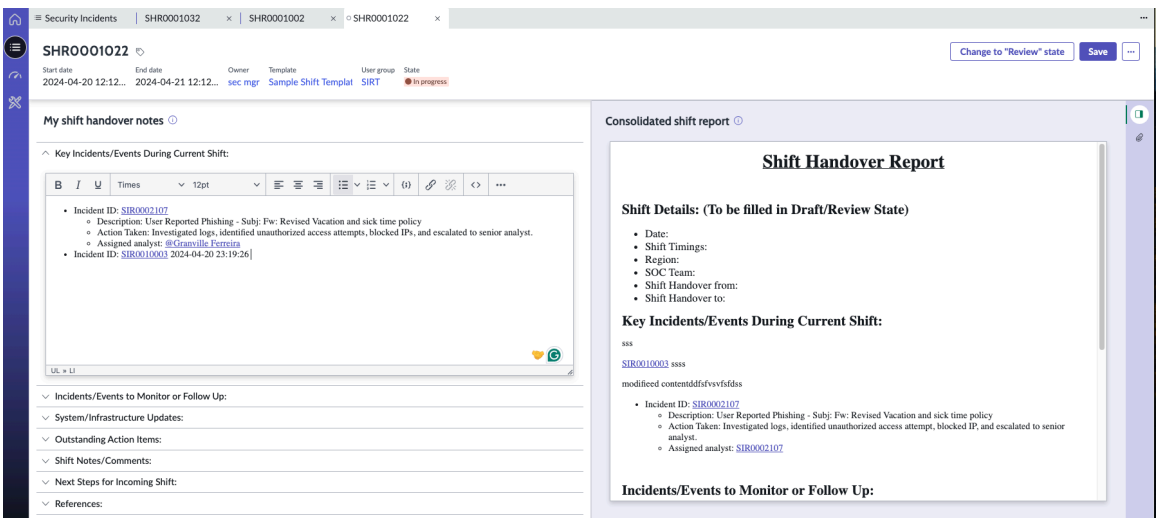


11. In the My shift handover notes editor, update the required details for all the sections like security incident and user details.

Note: The Shift Owner and Shift Analyst can both modify the content.

a. To mention a particular record in the editor, use **/** and choose **Select a record**, and then select a record from the list of tables that pops-up.
For example, if you select **Security Incidents** record, then a list of security incident appear. Select a security incident (**SIR0010025**) from the list and update the required Shift Handover details. You can also mention the fields associated with the security incident like short description, watch lust by using **/** after the security incident number.

Shift Handover Notes



b. To mention a particular user in the editor, use **/** and choose **Select a user**, and then select a user from the list that pops-up.

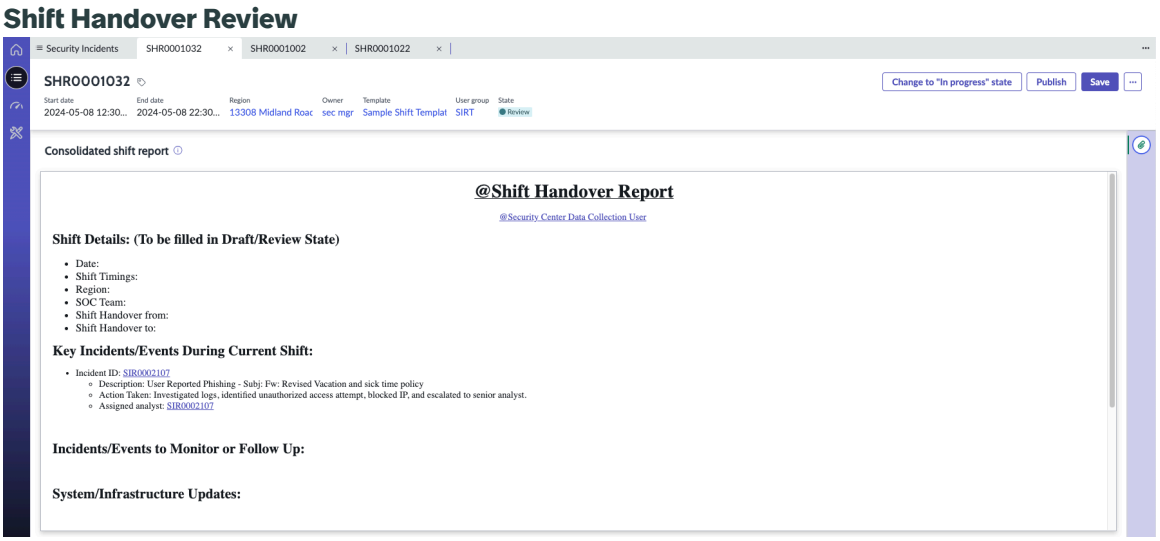
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. You can format your report with all the options in the editor, like fonts, colors, bullets, links, and attachments.

d. After making the required changes to the Shift Handover notes, select **Save**.

e. Select **Change to "Review" state** action to move the Shift Handover record to Review state.

Note: If some other analyst from the active shift team has already updated the report before you, and if changes are being processed, then you might see an error message. You must wait a few seconds and then select **Change to "Review" state** again.



12. In the Consolidated shift report, review the Shift Handover report and make the required changes.

Note: Only the Shift Owner can modify the content.

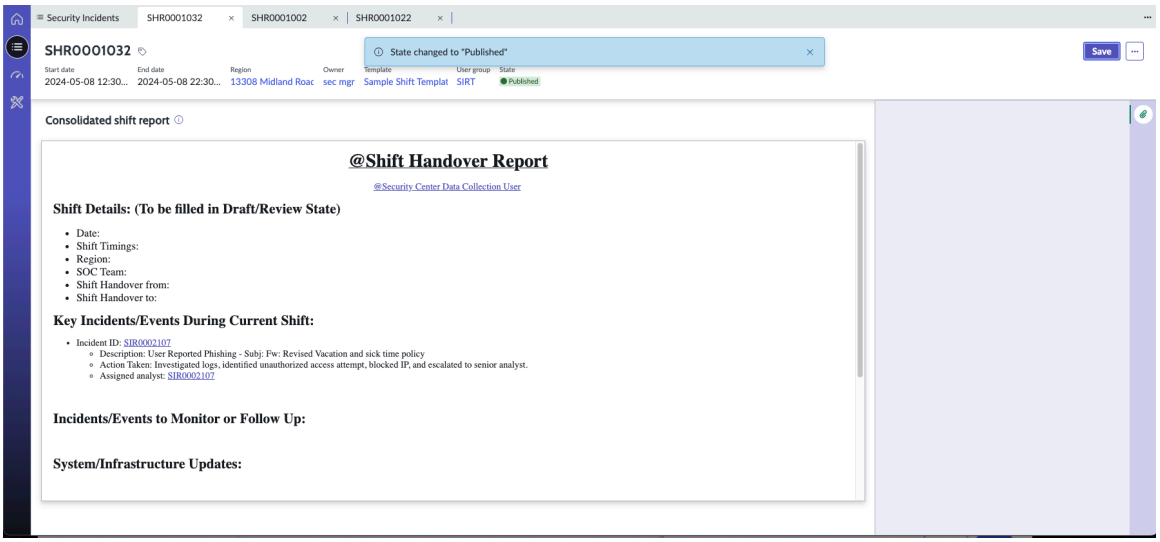
a. After making the required changes to the Shift Handover notes, select **Save**.

b. If the Shift Handover report requires more updates from the Analysts, you can select **Change to "In progress" state**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select **Publish** action to publish the Shift Handover report.

Shift Handover Publish



13. Select **Save** to save the Shift Handover report.
After you save, you can see a preview of the Shift Handover report with your latest updates on the Preview pane.

> **Note:** Though you can preview the updates you made on the Shift Handover report immediately, the other analysts might take a few seconds to see the changes.

14. As a Shift Owner, you can also perform the following actions on the Shift Handover list view.

a. To edit an existing Shift Handover record, select the record and select the **Edit** action.
You can modify only the Start time, End time, Description, and Region.

b. To create a copy of a Shift Handover record, select the record and select **Create copy** action.

c. To delete an existing Shift Handover record, select the record and select the **Delete** action.

Configuring SIR Workspace

This section describes the configurations needed to work with the Security Incident Response Workspace.

Set up view of SIR Records

This section describes how the related lists are grouped and presented on the SIR Related Records tab for easy navigation.

The workspace users can search the related list by name as well. For more information about configuring related lists, see SIR Workspace Related Records.

Configure SI design time investigation

Use this section to configure security incident design time investigation page to add multiple entry points and its associated records within the Security Incident Response Workspace.

Role required: sn_si.admin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following details the steps involved in configuring the investigation page on the Security Incident Response Workspace.

- Creating View for associated info tables
- Adding an entry point list
- Mapping View of the Associate Info to the entry point list
- Configure each associated list from the view to handle run time data rendering

Related topics

Explore Investigation Canvas

Creating View for associated info tables

The investigation screen leverages the related list views created on security incident to configure associated lists.

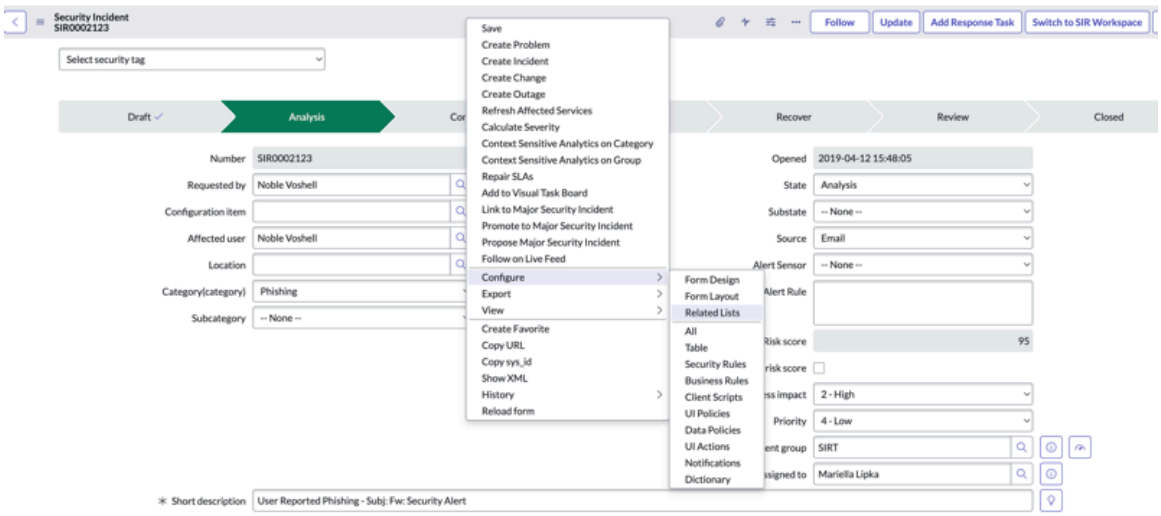
Before you begin

Role required: sn_si.admin

The following is a procedure to create a view and add related lists to it.

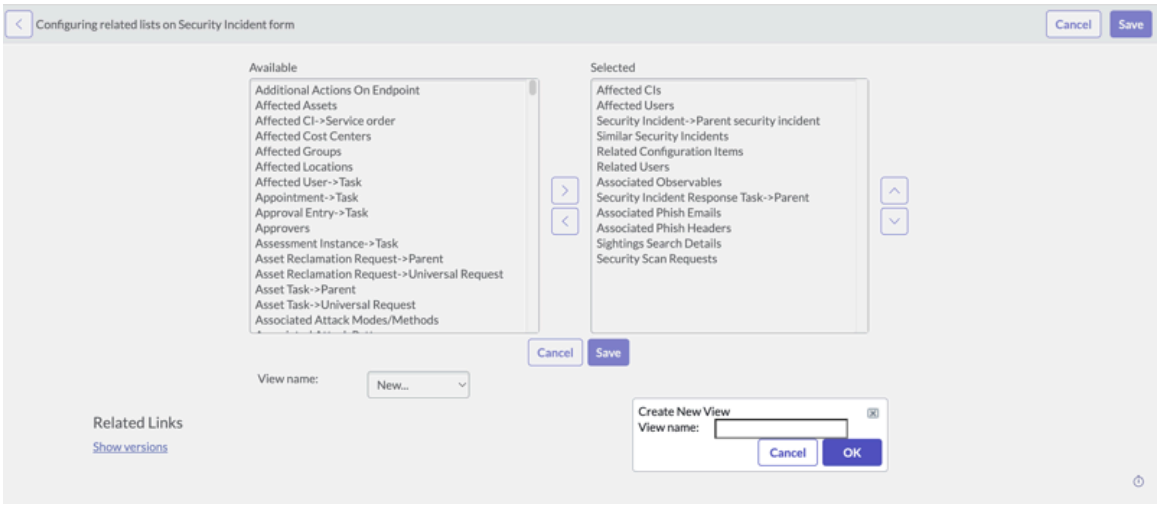
Procedure

1. Navigate to **Security incident** list.
2. Open any security incident in the Classic UI.
3. From the form context menu, navigate to **Configure** > **Related Lists**.
   The slush bucket window is displayed.



4. Go to **View name** drop-down list and click **New** to create a new view.
   You must add a name to the view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Add the desired related lists to the right bucket under the newly created view and save the view.
   This view will be used to render the associated info on the Investigation tab.

Adding an entry point list

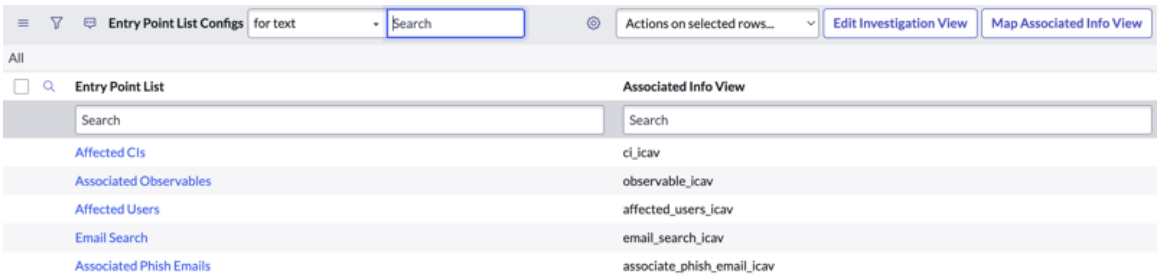
Configure the new entry point list to add it to the investigation page.

Before you begin

Role required: admin

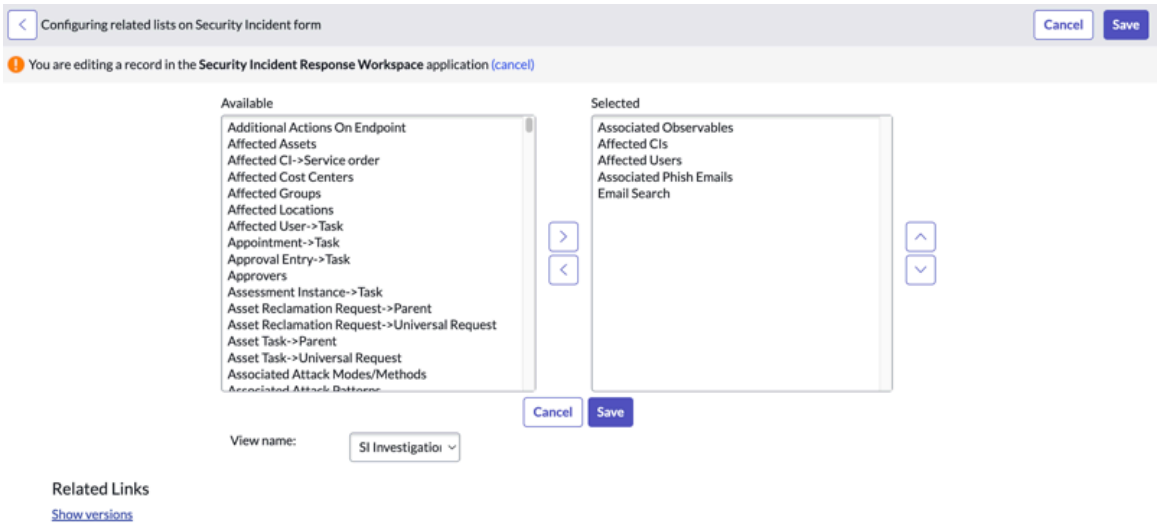
Procedure

1. Navigate to **sn_si_aw_entry_point_config.list**.
   The **Entry Point Lists Configs** page is displayed.



2. Click **Edit Investigation View** button to add an entry point list to the investigation screen.
   The **Configuring related lists on Security Incident form** is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Add or remove the entry point list from the slush bucket view.
4. Click **Save**.

> **Note:** The view corresponding to the Investigation screen holding the entry point lists is called **SI Investigation View** and this is by default selected when you navigate to **Edit Investigation View** page.
>
> The order in which the entry point lists is displayed on the investigation canvas is determined by the order in the slush bucket selected view.

Mapping View of the Associate Info to the entry point list

Map the associated info view to the newly added entry point list using the Map Associated Info View action.

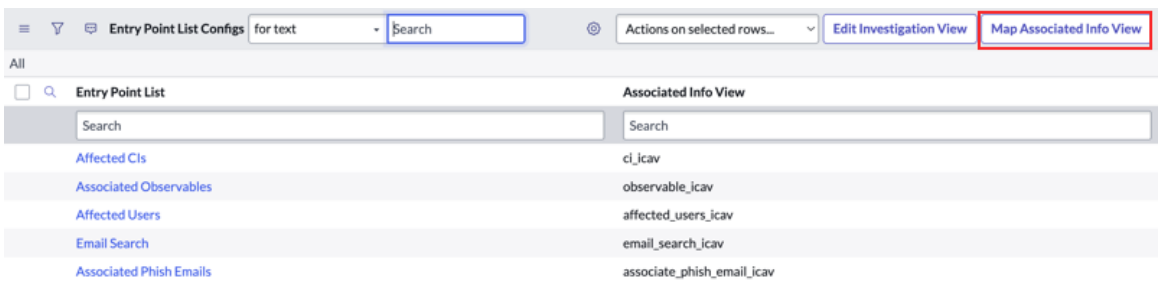
Before you begin

> **Note:** This step is required for the entry point list to be visible on the Investigation page. Even if you don't want any associated info lists to be shown under an entry point, you still need to create a dummy view and map it.

Role required: admin

Procedure

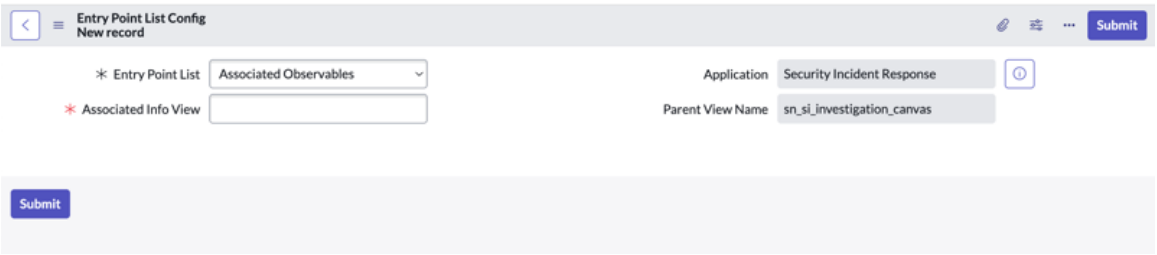
1. Click **Map Associated Info View** button on the **Entry Point Configs** page.



2. Select the newly added entry point list from the **Entry Point List** drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Enter the view name containing the associated info related lists in the **Associated Info View** field.
   For information on how to create a view for the associated info related lists, see Creating View for associated info tables.



4. **Save** the form.
5. Additionally, if required you can add or remove more associated lists using the **Edit Associated Info View**.
   You can also configure the entry point list layout using **Edit Entry Point List Layout** action. Add or remove columns from the slush bucket as desired, and save the form.

Configure each associated list from the view to handle run time data rendering

Configure each associated list from the view to handle run time data rendering.

Before you begin

Note: This step is mandatory for each associated list configured in the associated info view. Otherwise, the associated list will not be available on the investigation page.

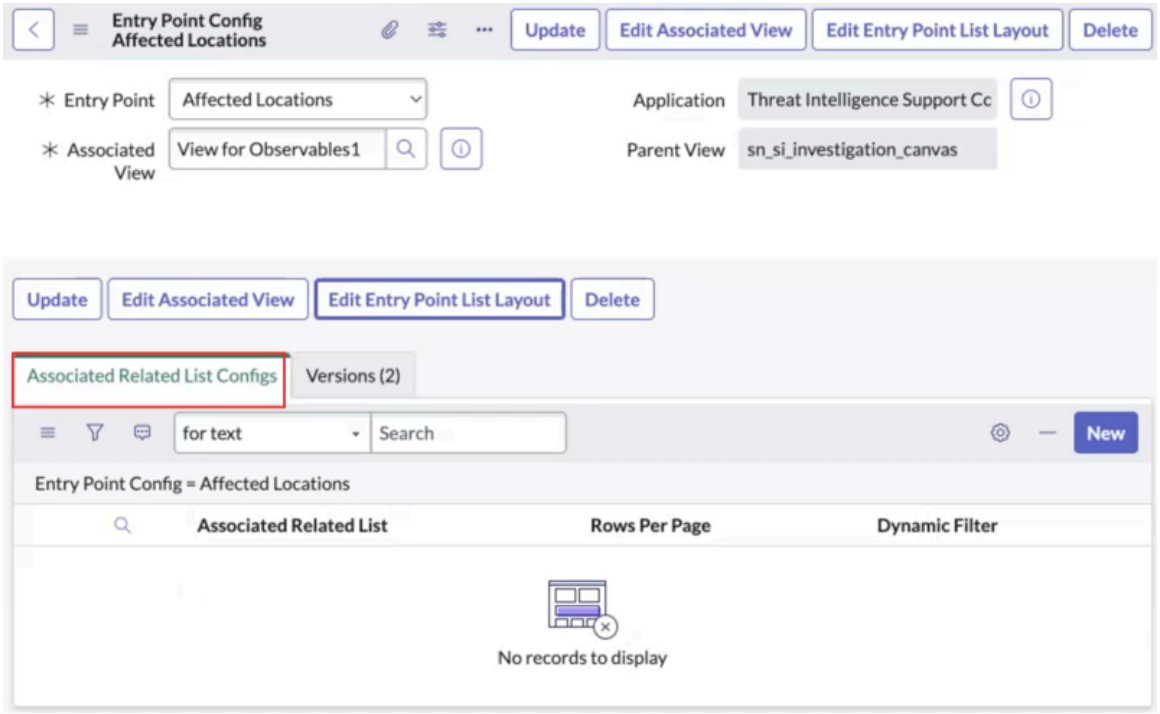
Each of the associated list added (while mapping an associated info view to an entry point list) Mapping View of the Associate Info to the entry point list (or from the view directly) need an additional configuration to filter the data with respect to the runtime record selection and filters selection.

Role required: admin

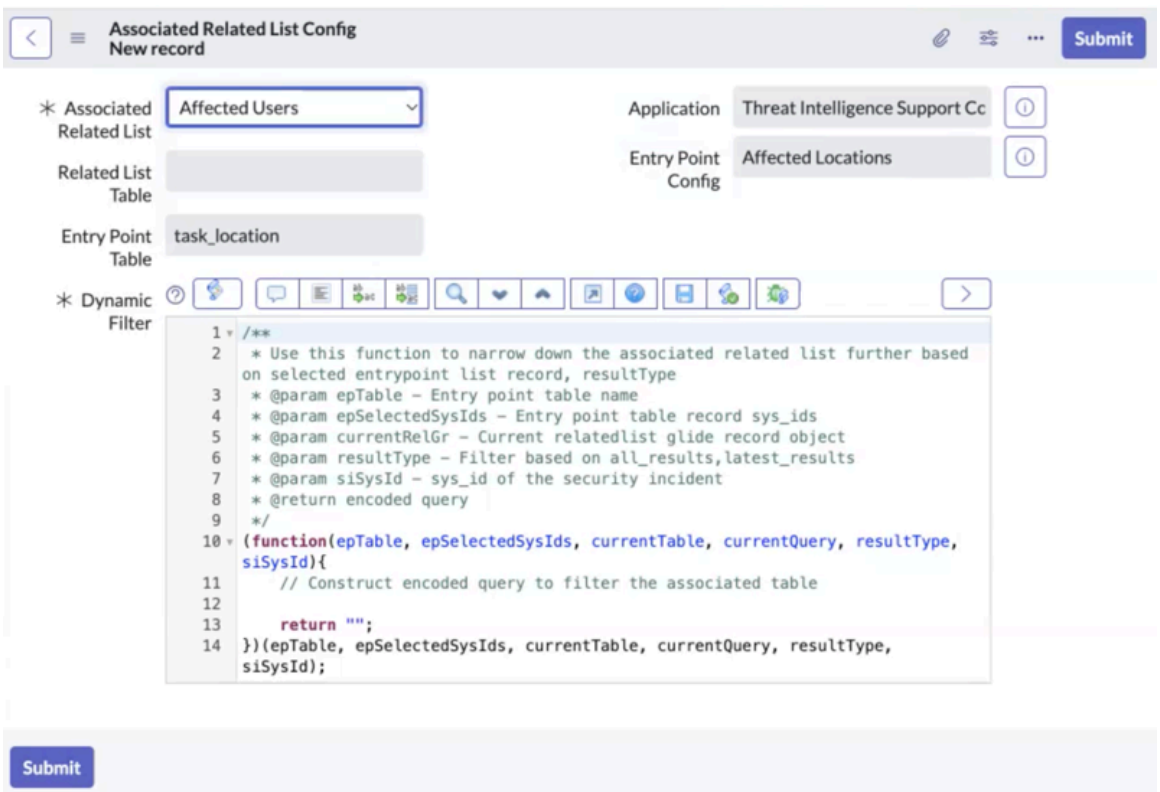
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Click **New** from the **Associated List Configs**.



2. Select **Associated List** field value.
3. Use the **Dynamic Filter** column to filter the associated list further based on the selected entry point list records and result type (latest results from each vendor implementation, all results). Refer to the existing examples that are shipped within the product.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Also, you can configure the associated list layout using **Edit Associated List Layout** action. In the slush bucket window, add or remove columns as required.

SIR Workspace Related Records

This section consists of the related lists items that are grouped into sections such as associated observables and configuration items.

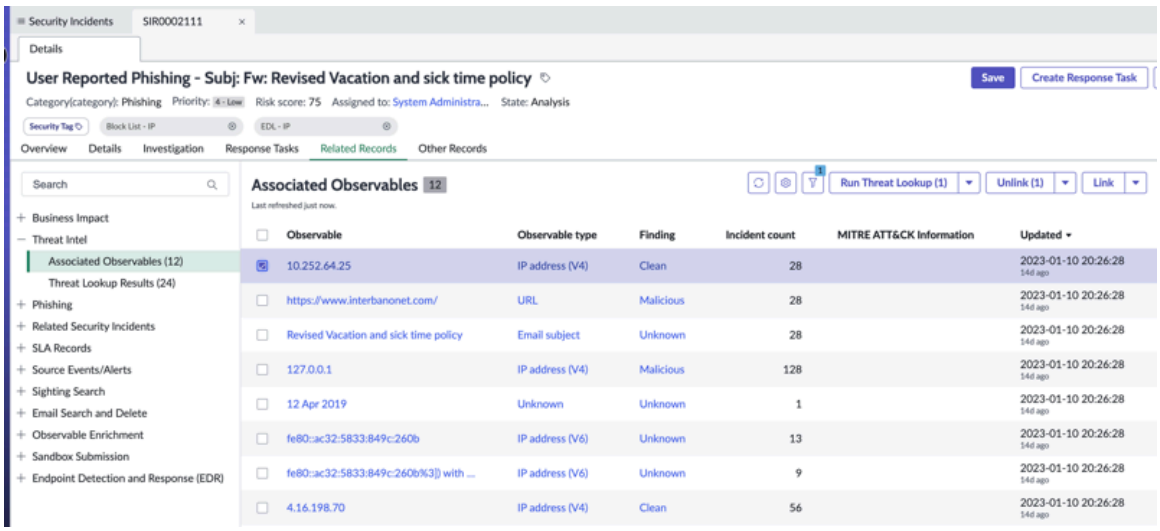
The following related lists groups that are available as a part of the base system. You can modify these groups or create groups within the application and their respective actions.

You can modify these groups or create new groups. For more information, see Configure Security Incident Related List on how to configure and group the related list for security incidents and response tasks. Each related list is fully functional within the SIR Workspace.

Related list	Grouped item
Business Impact	• Configuration Items • Affected Users • Related Configuration Items • Related Users • Affected Services
Threat Intel	• Associated Observables • Threat Lookup Results
Phishing	• Associated Phish Emails • Associated Phish Headers
Related Security Incidents	• Parent Security Incident • Child Security Incident • Similar Security Incident
SLA Records	Task SLAs
Source Events/Alerts	Source events or alerts are the SIEM integration enabled related list such as Source Email, LogRhythm Drill Down Logs, LogRhythm Events, Aggregated IBM QRadar Offense and so on. **Note:** This list is completely dependent on the integration that you have in your instance. To view the relevant SIEM integration related list, you must install the latest version.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related list	Grouped item
Sighting Search	• Sightings Search Results • Sightings Search Details • Sighting
Observable Enrichment	• Observable Enrichment Results • Associated MISP Events • MISP Enrichment Results
Endpoint Detection and Response (EDR)	• Host Details • Running Processes • Running Services • Logged On Users • Network Statistics • Get File • Isolate Host Entries • Additional Actions On Endpoint • Microsoft Defender for Endpoint-Related Machines Details



Note: In general, you'd be able to create new records, link, or unlink existing records or new records against the related list group as applicable.

Related topics

Configure Security Incident Related List

Configure Security Incident Related List

You can add new related lists or new related list groups, and modify existing groups or related lists that appear in the SIR Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

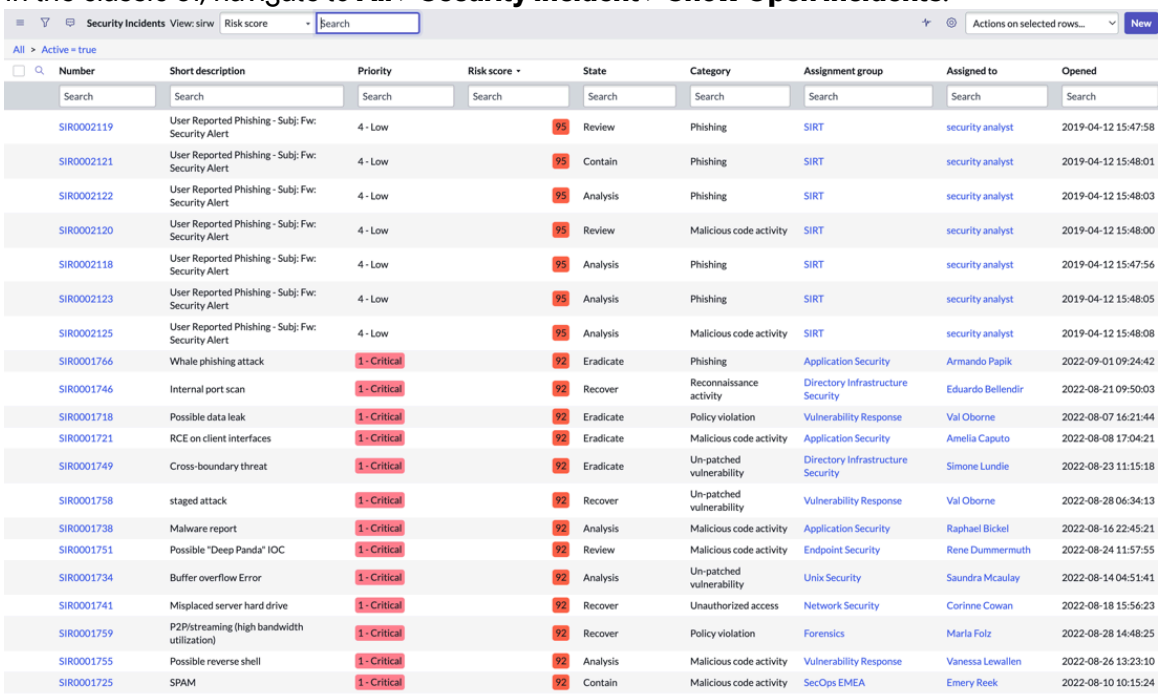
Before you begin

The security incident related list are grouped and displayed as group related list items on the **Related Records** tab on the workspace.

Role required: sn_si.admin

Procedure

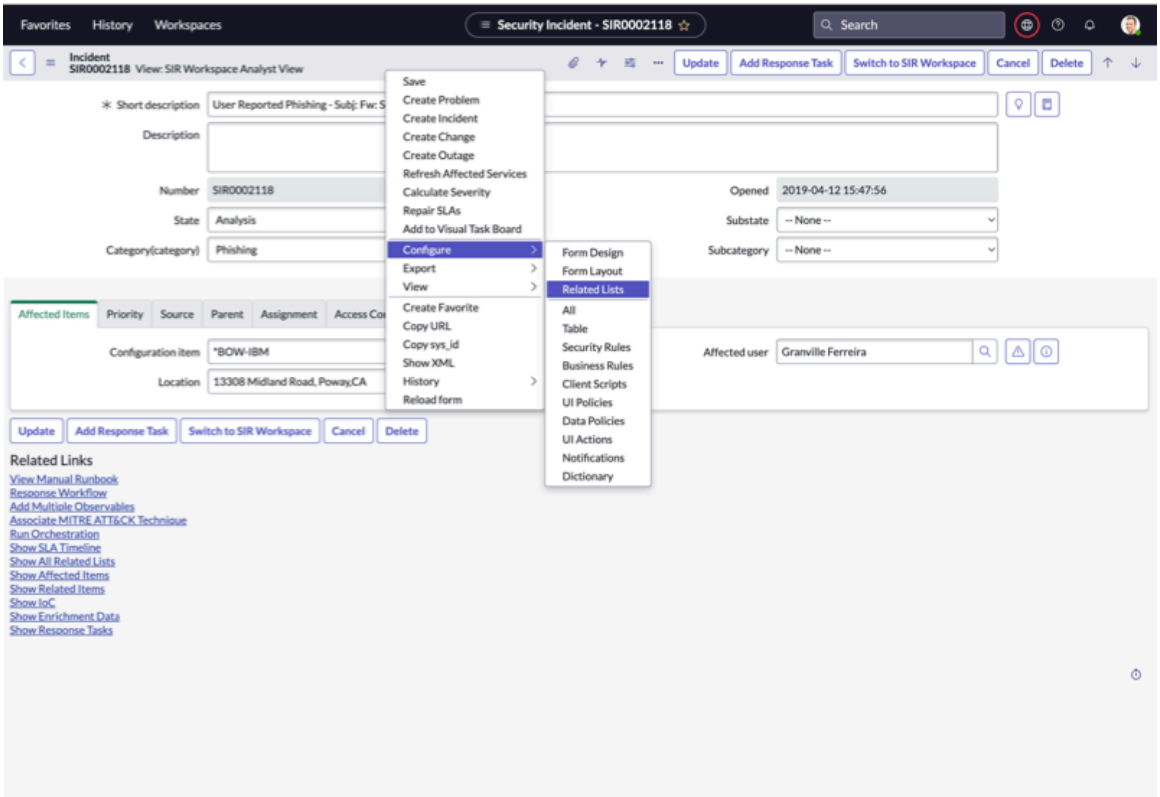
1. In the classic UI, navigate to **All** > **Security Incident** > **Show Open Incidents**.



Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

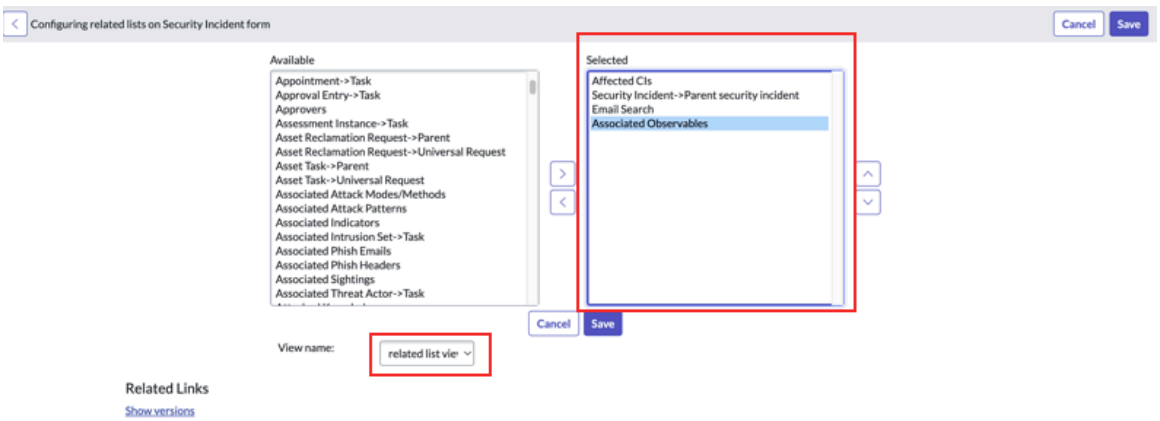
2. Select any incident record.
3. Right click on the incident context menu.
4. Go to **Configure** > **Related List**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Configuring related lists on Security Incident form** is displayed.

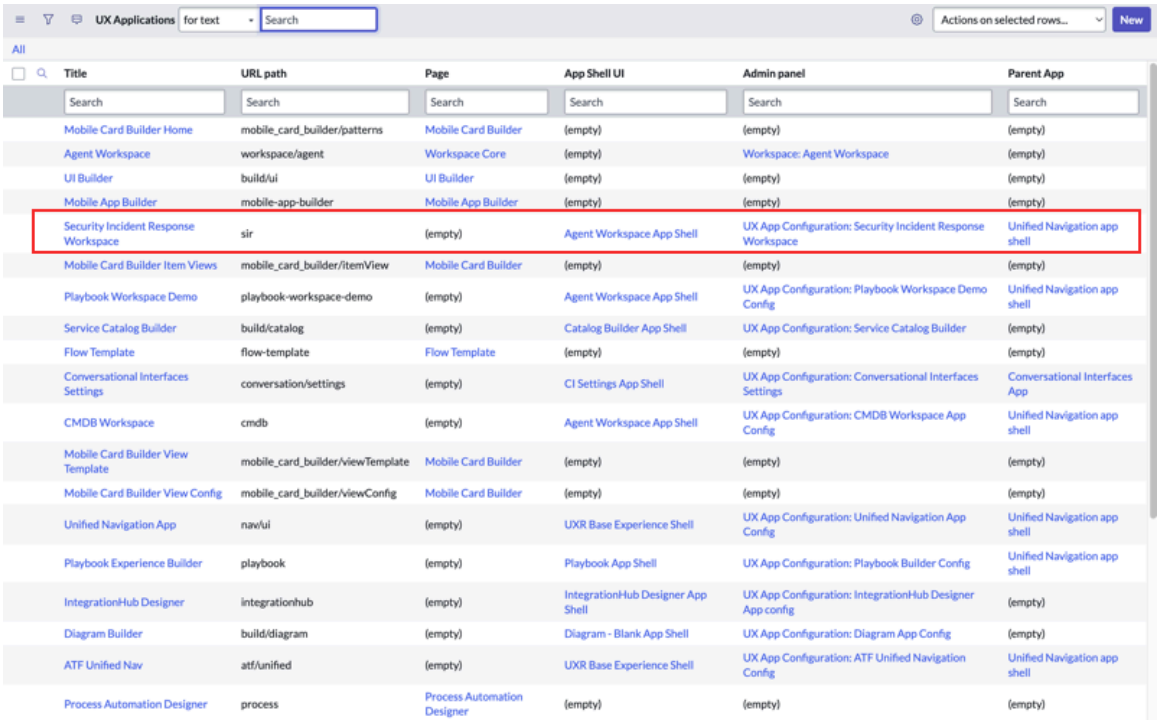
5. Go to **View name** and select **New**.
6. Enter a name for the view.
7. Select the newly created view.
   After you select the view, choose the required related list fields from the slush bucket.



Note: If you want to modify anything, select the view and remove or add the items.

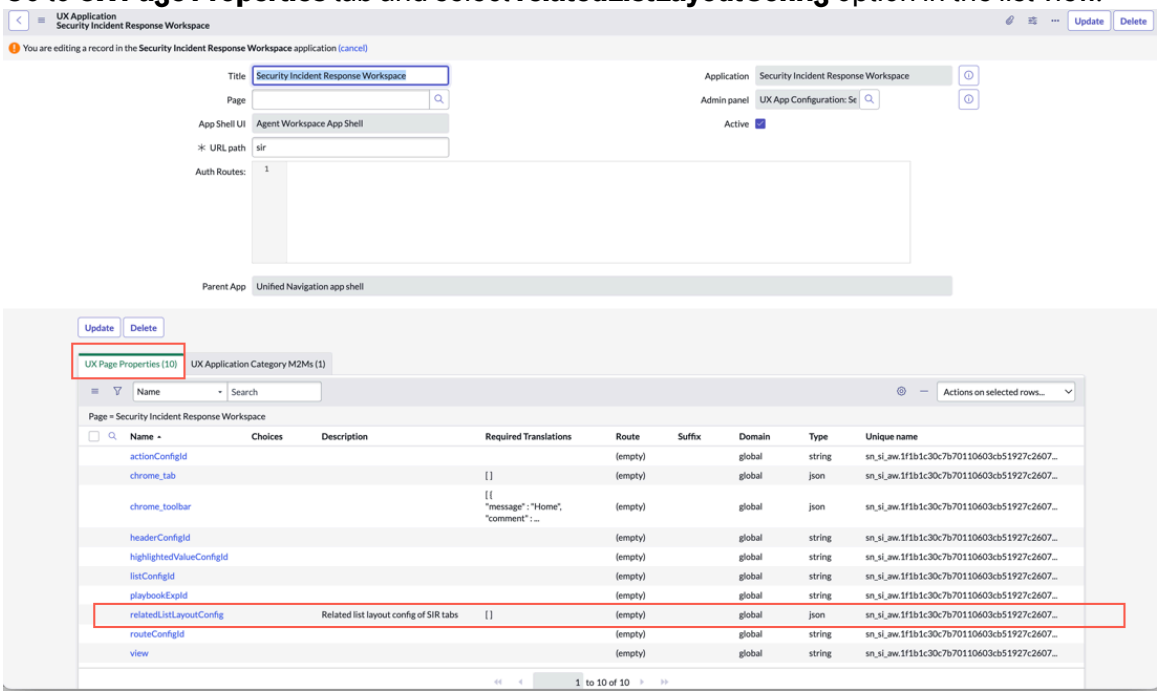
8. Click **Save**.
9. On the left navigation, navigate to **All** > **Now Experience Framework** > **Experiences**.
10. Select **Security Incident Response Workspace**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

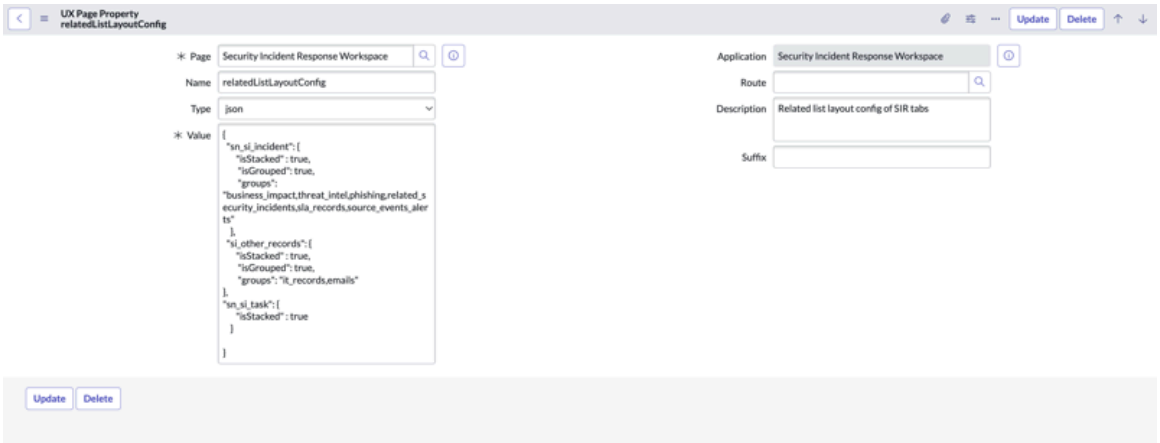


The **UX Application Security Incident Response Workspace** page is displayed.

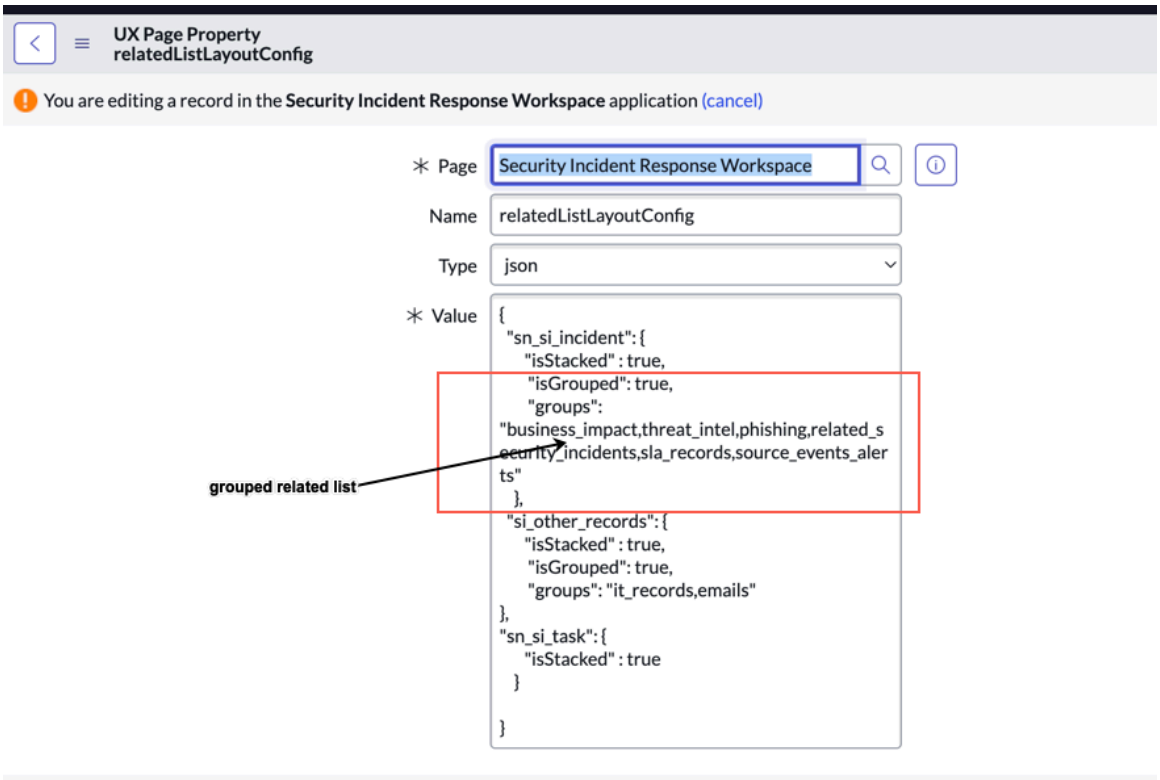
11. Go to **UX Page Properties** tab and select **relatedListLayoutConfig** option in the list view.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



12. Add the newly created view name separated by a comma to an already existing list of values in the **Value** text box under the **sn_si_incident.viewsUsedForGrouping** field.
For example, if you had created a new view name as, **Business Impact** then in the **Value** text box you must specify it as **business_impact** (which is separated by underscore within the view name and separated by a comma after an existing value) under the sn_si_incident:groups field.

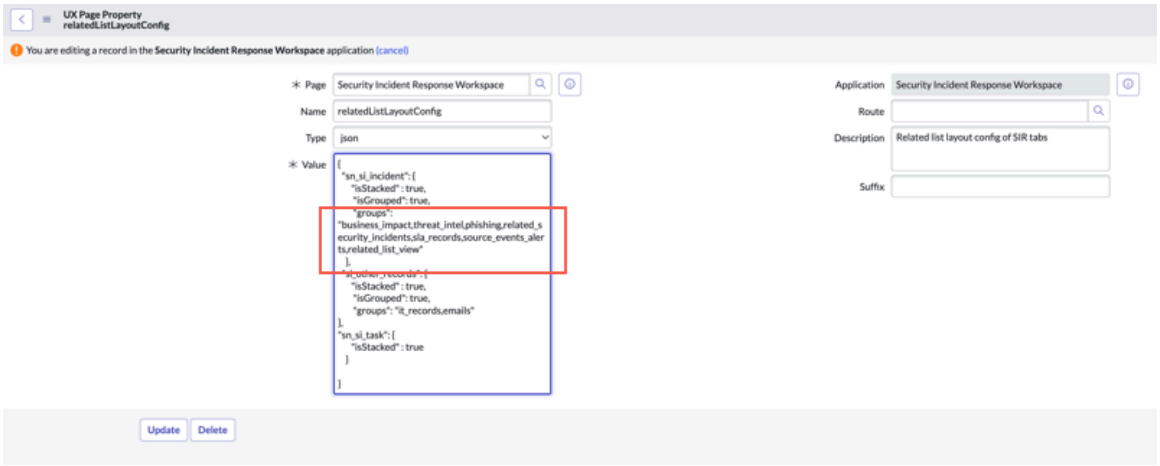


Note: If you add the new view name under **sn_si_incident.viewsUsedForGrouping** field then the entry will be created in the **Related Records** tab of the workspace.

If you update the view name entry in **si_other_records.viewsUsedForGrouping** then the related list group will get added in the **Other Records** tab of the workspace.

Below is an example view which shows the newly created views added.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: **requiredRolesForGrouping** contains comma separated sys_user_role record names. SIR Workspace user should have at least one of these roles, to use the grouped related lists. When a user does not have any of these roles then related lists view configured for the current user role using view rule configuration will be represented vertically without grouping. This property is ignored when **isGrouped** property is set to false. If this property is empty any user can access the grouped related lists.

13. Click **Save**.
14. Navigate to **Workspaces** > **Security Incident Response Workspace**.
15. Select any specific security incident.
16. Go to **Related Records** tab of the workspace.
    The grouped related lists are displayed.

Configure Response Task Related List

Use this section to configure response tasks new related lists that appears on the Security Incident Response application.

Before you begin

Role required: sn_si.admin

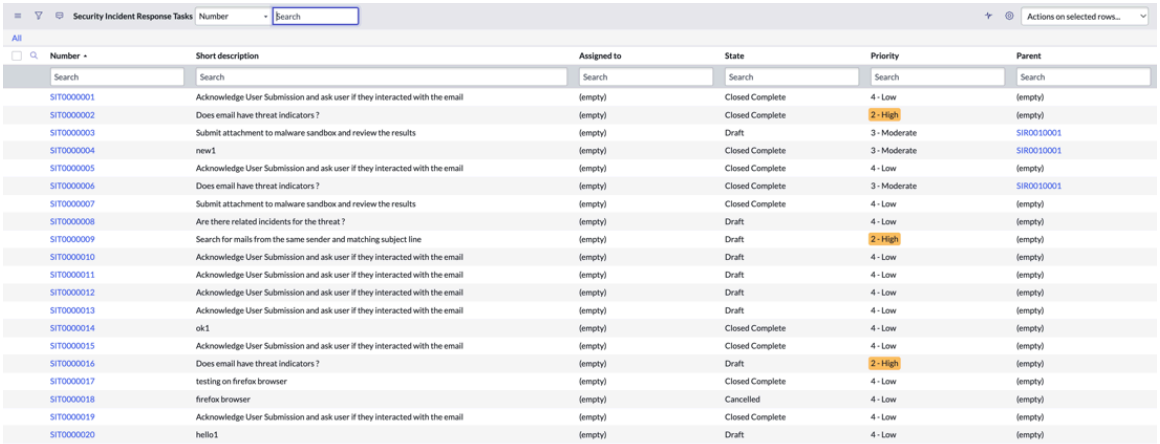
About this task

The response tasks related list is not grouped but displayed as individual related list items, as there are few default lists. View the response tasks related items from the **Response Tasks** tab of the security incident record of the workspace.

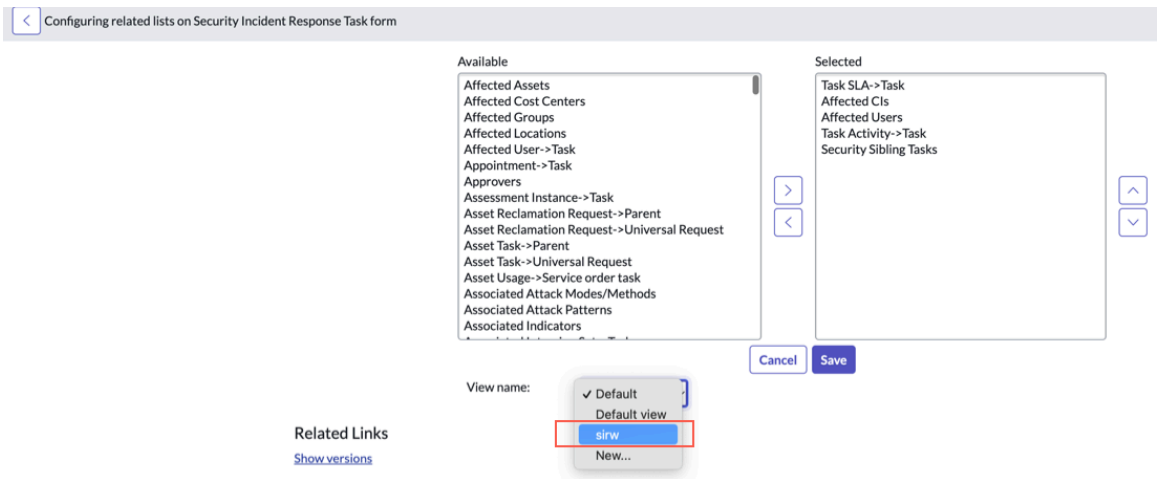
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Response Tasks** > **Show All Tasks**.

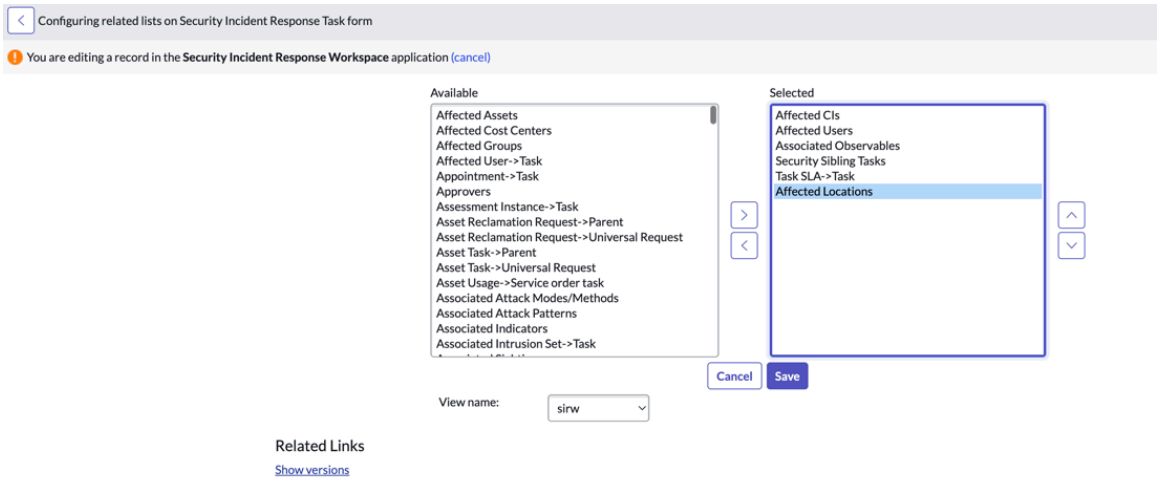


2. Select any response task record.
3. Right click on the Security Incident Response Task context menu.
4. Navigate to **Configure** > **Related List**.
   The **Configuring related lists on Security Response Task form** is displayed.
5. Go to **View name** and select **sirw** view.

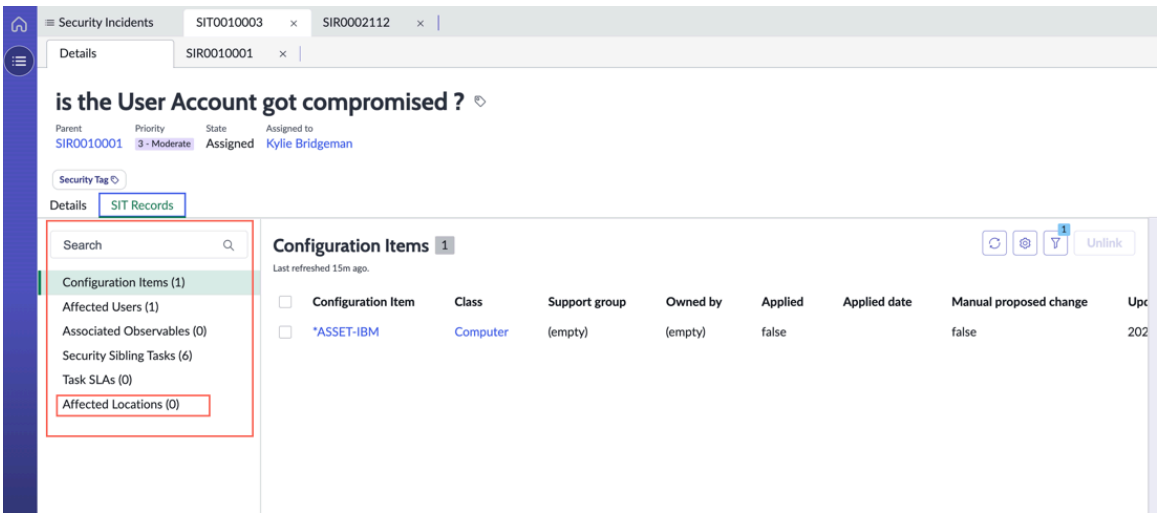


6. Select the desired related list fields from the slush bucket.
   For example, Affected Locations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Click **Save**.
8. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Response Tasks** > **SIT Records**.
   The configured related lists (For example, Affected locations as selected) is listed within the SIT records list.



Define the new Risk Score Calculator Rules

Use the new Risk Score Calculator to define and calculate the risk score of security incidents based on the user-defined criteria, which provide a transparent intelligence scoring of security incidents. The risk score is auto-calculated for the security incident records.

Before you begin

Role required: sn_si.admin.

Activate the new Risk Score Calculator by setting the `sn_si_aw.activate_new_risk_score_calculator` system property to true.

About this task

Define a risk score for the security incident records that are generated based on the user-defined parameters. The base system is provisioned with one risk scoring rule, which can be customized and enabled accordingly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- By default, the new Risk Score Calculator Rule is inactive, and you need to enable the rule to see the risk score of the security incidents.
- To calculate the risk score for additional related tables other than those available in the base system, refer to Risk Score Calculator for Additional Related Tables.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Administration**.
2. Navigate to **Rules Engine** > **Risk Score Calculator Rule**.
   The Risk Score Calculator Rule page is displayed.

   Note:

   - As a part of the base system, you're provided with one predefined risk scoring rule template to view, edit, or modify the risk score. However, you can't create or delete the predefined risk score rule template.
   - The changes you make will apply to any new security incidents or updates to the existing ones. To restate historical scores, use the **Recalculate Score** action.

3. Select the **Risk Score Calculator** rule.
4. On the form, fill the fields.

Field	Description
Name	Name of the risk score value. For example, Risk Score Calculator.
Overall weightage (Applicable to criteria builder)	Weightage of this field within the risk rule. This field isn't editable and displays the overall weightage calculated by the system based on the weight corresponding to enabled criteria. The overall weightage should always be 100%.
Description	Description of the risk score record. For example, calculates risk score based on weighted sum of predefined criteria scores.
Scoring Criteria	Indicates the scoring criteria for a security incident. You can define the Risk **Scoring Criteria** using the following options: - **Criteria Builder**: Use this option to add, edit, or remove, and enable and disable criteria that contribute to risk score calculation and verify that the total aggregated weightage is 100%. - **Use Script (Advanced)**: The scripting feature is an advanced feature to build a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	custom script that should return the risk score, which is an integer value ranging from 0 to 100.

5. To define the **Scoring Criteria** using the **Criteria Builder**, perform the following steps:

   Note: You can edit or modify the existing criteria or add a new criteria.

   a. To add a new criteria, select the **+New criteria** action.
   To ingest and map third-party risk scores, and factor them into security incident risk calculation or prioritization logic, use the **External risk score criteria** fields. To include NIST complaint incident prioritization, use the **Functional Impact**, **Information Impact**, **Recoverability** fields

   b. Select the **Table** for which you want to set the criteria.

   Note:

   - If the selected table is a security incident, the condition is applied to the security incident record for which the risk score is calculated. If the selected table isn't a security incident, the condition is applied only if the records are related to the security incident for which the risk score is calculated.
   - An additional Aggregate type is added to define the scores based on the number of relations associated with the security incidents.

   c. Select the **Type** criteria for the selected table.
   The Type value could either be **Field** or **Aggregate** based on the table you choose.

   d. Select the **Field** criteria for the selected table.
   If you selected the Type value as **Field**, then the Field criteria display the field values related to the table. If you selected the Type value as **Aggregate**, then the Field criteria display the aggregate values related to the table.

   Note: The Aggregate type supports only Count value.

   For example, if you select the Table criteria as **Security Incident**, then the Type criteria displays only **Field** option. The Field criteria display all the Field values related to the table, which could be Severity, Active, and so on Similarly, if you select the Table criteria as **Affected Users**, then the Type criteria displays both **Field** and **Aggregate** option. If you select the Type as Aggregate, the Field criteria display the aggregate values related to the table, which is **Count**.

   e. Enter the **Weightage** of the criteria between 0-100.
   The overall weightage of all the criteria should be 100%.

   f. Enter the name and a short description of the criteria.

   g. Select the **Enable scoring criteria** check box to enable the scoring criteria.

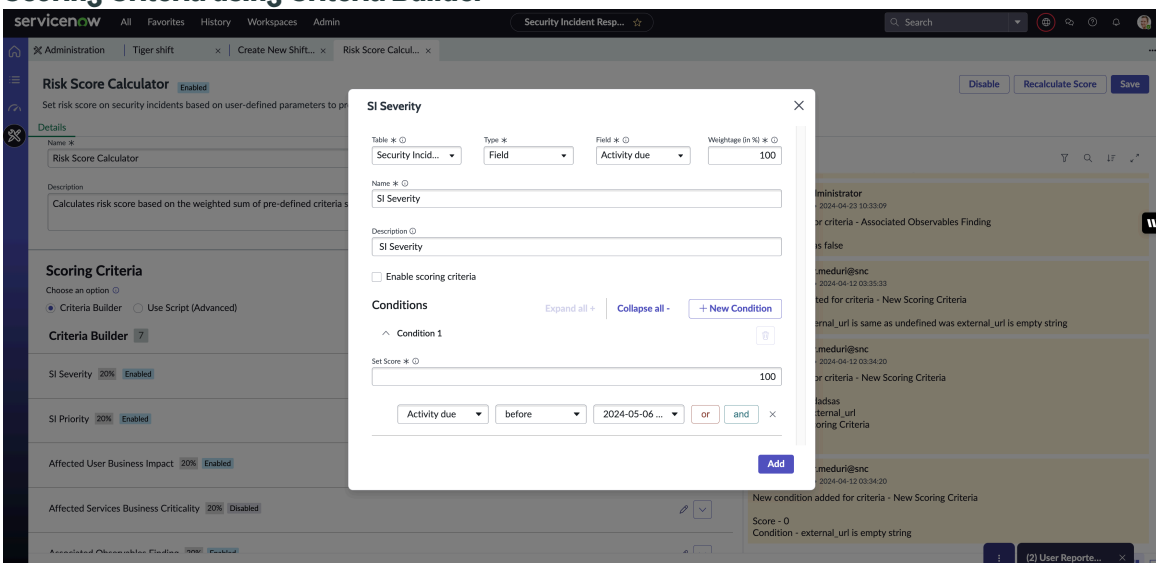
   h. Define the **Conditions** and set the score for the conditions.

   i. You can also add new conditions using the **New Condition** option, and delete existing conditions using the **Delete Criteria** icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

j. Select **Add** to add the configured criteria.

Scoring Criteria using Criteria Builder



6. Select the **Recalculate Score** option to recalculate the risk score.

For example, if there are changes to the risk score rule. In that case, you must reapply the scoring rule to the security incidents with the risk score already calculated in the past. Use the **Recalculate Score** action to trigger the recalculation job.

7. Select **Confirm**.

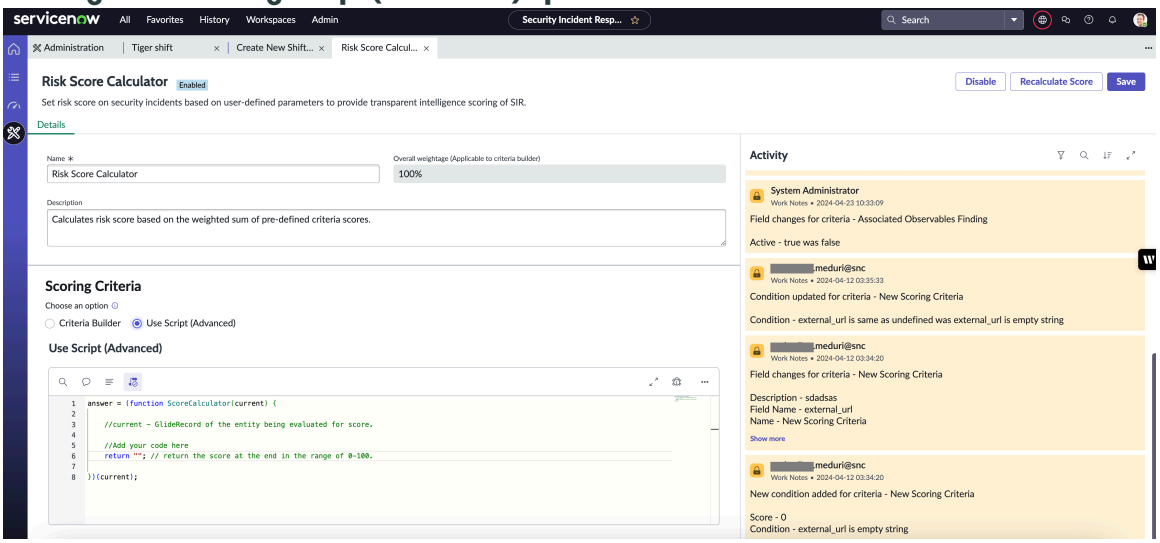
Note: Once your trigger this action, the process runs in the background and will take a few minutes to complete. You won't be able to make changes until it's finished.

8. To define the **Scoring Criteria** using **Use Script (Advanced)** option, perform the following steps:

a. Use this predefined script to build a custom script that should return the risk score, which is an integer value ranging from 0 to 100.
The advanced script field is auto-populated with a function, which takes the parameters **current** and this function should return the risk score, which is an integer value ranging from 0 to 100.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scoring Criteria using Script (Advanced) option



Here, the current parameter is the GlideRecord object of the entity (security incident) for which the risk score is being calculated. For the security incidents, it corresponds to the GlideRecord for the sn_si_incident table.

9. To disable the Risk Score Calculator, select **Disable**.
10. Select **Save**.

Risk Score Calculator for Additional Related Tables

The Risk Score Calculator is provisioned with one risk-scoring rule as part of the base system to calculate the risk score of security incidents based on user-defined criteria. However, you can customize and include additional related tables to calculate the risk score.

Before you begin

Role required: sn_si.admin.

Procedure

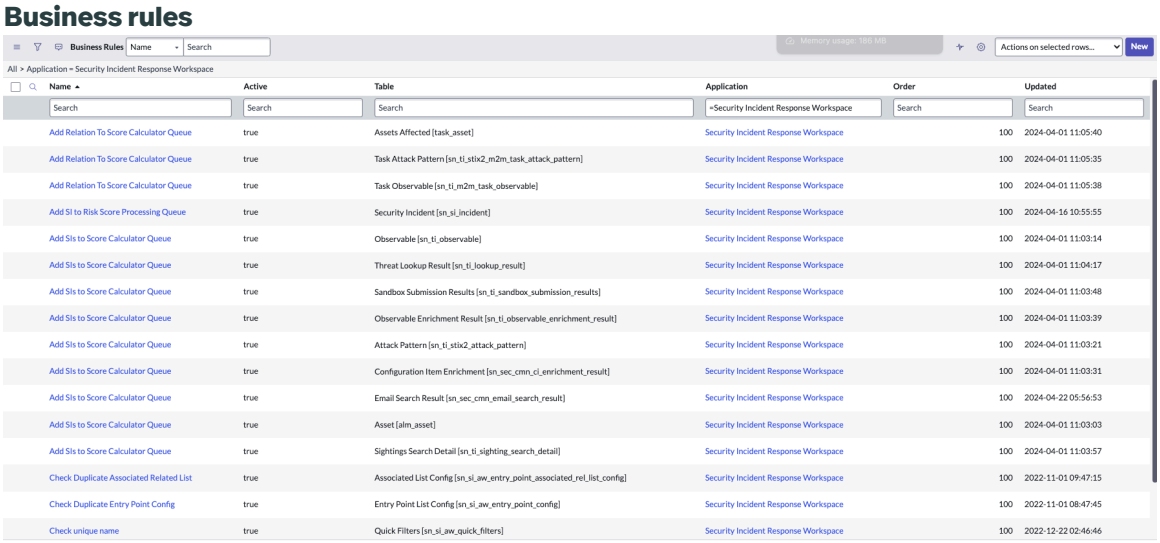
1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**.
2. Select any security incident record.
3. Select the **Additional actions** option next to the security incident number.
4. Go to **Configure** > **Related Lists**.
5. Go to the View name, and select **Risk Score Calculator**.
   After you select the view, choose the required related list that you want to add from the slush bucket. For example, Associated Sightings.
6. Select **Save**.
   You have successfully added the new related lists or tables for which you want to calculate the risk score.

> **Important:** To calculate the risk score for the security incidents that have new criteria with the newly created related lists, you have to define business rules on the base table of the related list.

7. Navigate to **All** > **System Definition** > **Business Rules**.
   You can use the following two business rules as reference to create your own business rules:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

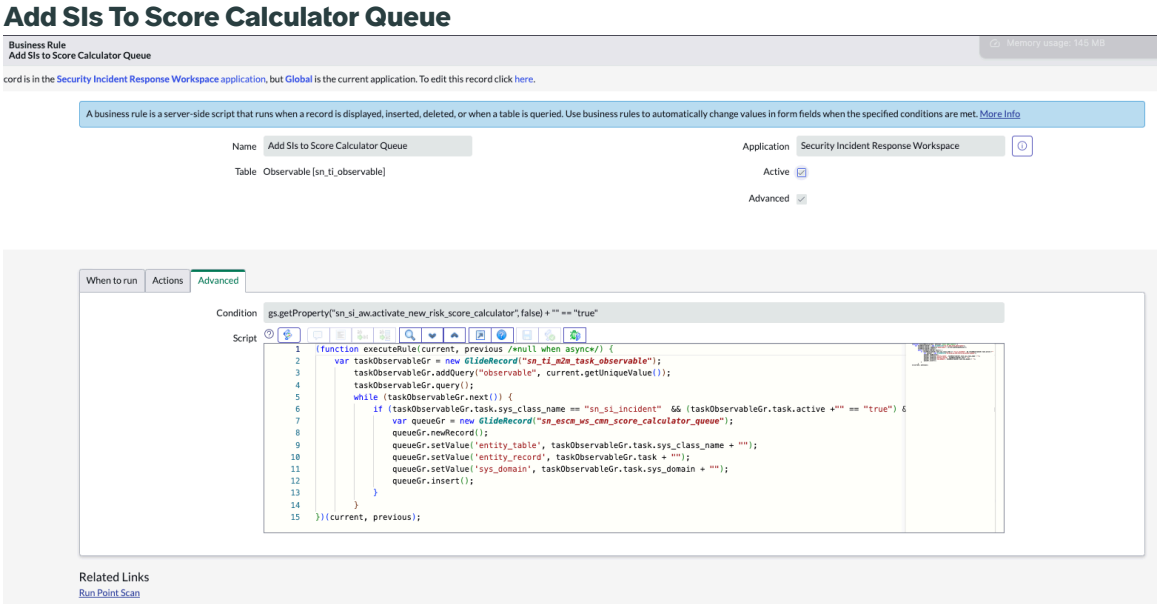
- Add Security Incidents (SIs) to Score Calculator Queue
- Add Relation to Score Calculator Queue (This is applicable for m2m tables)



8. For example, to get the associated observables criteria to work, we have defined two business rules.

   The first is the **Add SIs To Score Calculator Queue** business rule.

   For example, a new security incident is created and associated with an observable (`Observables [sn_ti_observable]`) table. After threat lookup, the observable is found to be malicious. You then need to add all the security incidents associated with this malicious observable to the Queue to recalculate the risk score of the security incidents.

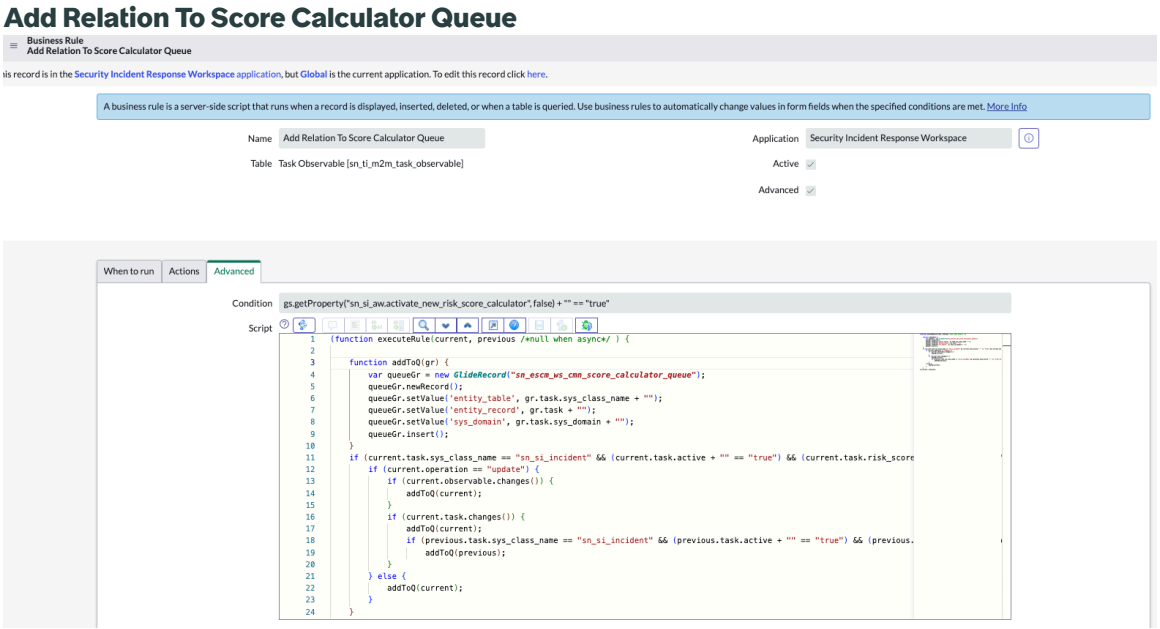


   The second is the **Add Relation To Score Calculator Queue** business rule.

   For example, a new security incident is created or deleted and associated with an observable (`Task Observables [sn_ti_m2m_task_observable]`) table. So, there's a change

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

in the association of the security incident. You then need to add that security incident to the Queue to recalculate the risk score of the security incident.



Configure Shift Handover

Configure Shift Handover settings to provide complete shift information to the next shift analysts.

Configure Shift Handover Templates

The Admin can define and configure different Shift Handover templates for the Shift Owner to create shift handover records and hand them over to the next shift team.

Before you begin

Role required:

- sn_escm_sh.shift_admin
- sn_si.admin inherits the sn_escm_sh.shift_admin role

About this task

To configure a Shift Handover template, the Admin either creates a new Shift Handover template or opens an existing template in the base system with the name **Sample Shift Template** and modifies the details and sections according to your requirements.

The Shift Owner can use the configured template to create Shift Handover log records, and then the Shift Handover report is shared with the next active Shift Owner and team.

Note: Only the active Shift Handover templates are visible for the Shift Owner to create handover log records.

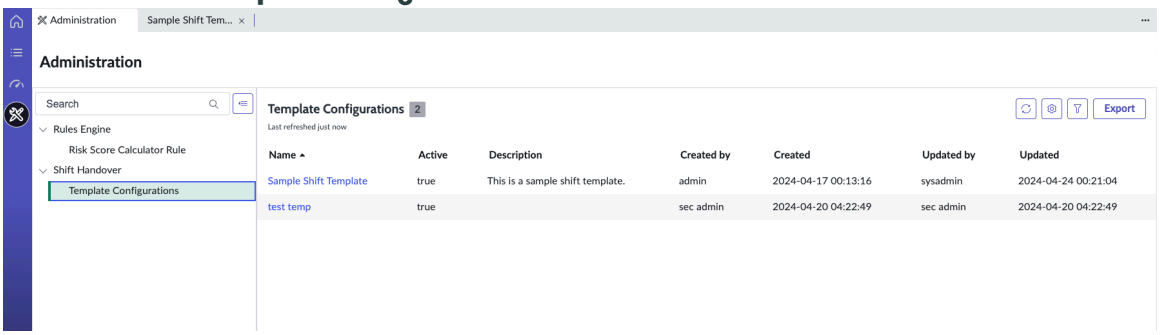
Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Administration**.
2. Navigate to **Shift Handover** > **Template Configurations**.
   The Template Configurations page is displayed.

Note: As a part of the base system, you're provided with one predefined Shift Handover template configuration to view, edit, or modify the shift handover template. However, you can't create or delete the predefined Shift Handover template configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Shift Handover Template Configurations



3. To create a new Shift Handover template, select **New**.
4. On the Details form, fill the fields.

Create a new Shift Handover template

Field	Description
Name	Name of the Shift Handover template. For example, SIR Template.
Application	Name of the application for which you're creating the Shift Handover template. For example, Security Incident Response Workspace.
Active	Option to indicate whether the Shift Handover template is active. Enable this option to activate the Shift Handover template.
Description	Description of the Shift Handover template.
Record mention configuration	Use this field to configure the Rich Text Editor's (RTE) record mention details. The input is an array of JSON objects with the following fields: ○ *`sourceTable`*: Name of the source table. ○ *`label`*: Name of the label to be displayed. ○ *`filterCondition`*: Encoded query for filtering ○ *`field`*s: Select the fields to query the pattern Sample configuration that you can copy and paste in the Record mention configuration field. `[ { "sourceTable": "incident", "label": "Incidents", "filterCondition": "active=true",`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

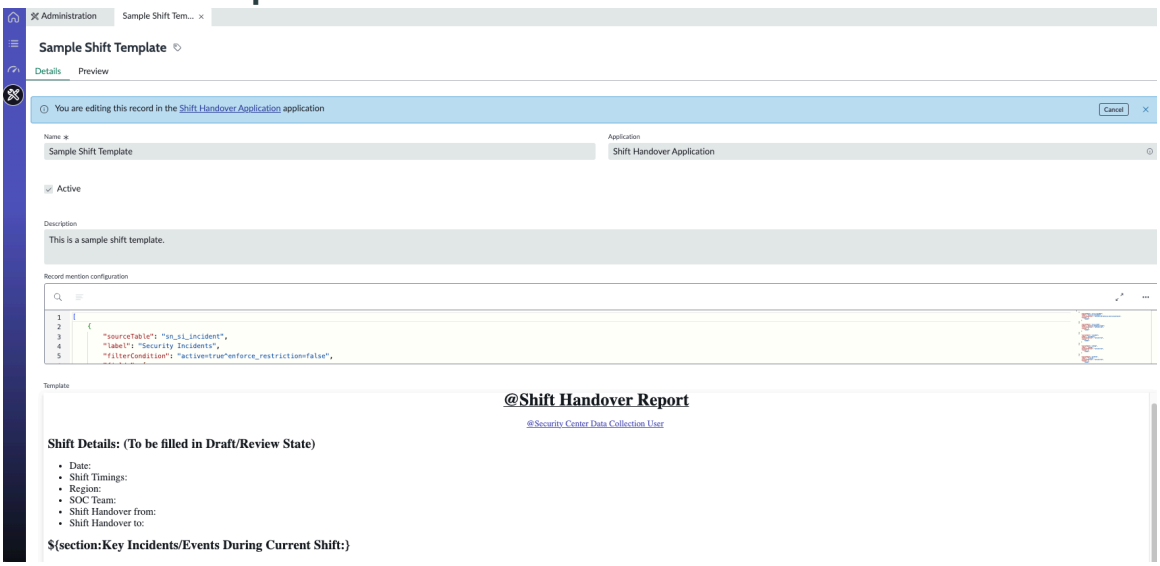
	<pre>"fields": [
	"number"
	]
	}
	]</pre>
	To copy the sample configuration, use the **Copy to clipboard** action in the Contextual Assistance pane. Then, you can make any additional modifications based on your requirements.

Template	Create a Shift Handover template using sections. Make sure that there is at least one section for the analysts to be able to contribute to the shift handover log records based on the template.
	
	The template can have static text, images, and so on, in the appropriate sections. You can copy and paste images directly in the Template field. You can create sections in the template using the following code:
	<pre>${section:Section Label}</pre>
	Example:
	<pre>${section:Key Incidents/Events During Current Shift}
	${section:Incidents/Events to Monitor or Follow Up}
	${section:System/Infrastructure Updates}
	${section:Next Steps for Incoming Shift}
	${section:References}</pre>
	Note: For more information, refer to the **Contextual Assistance** on the right-pane.

5. To use and modify an existing Shift Handover template, select **Sample Shift Template**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

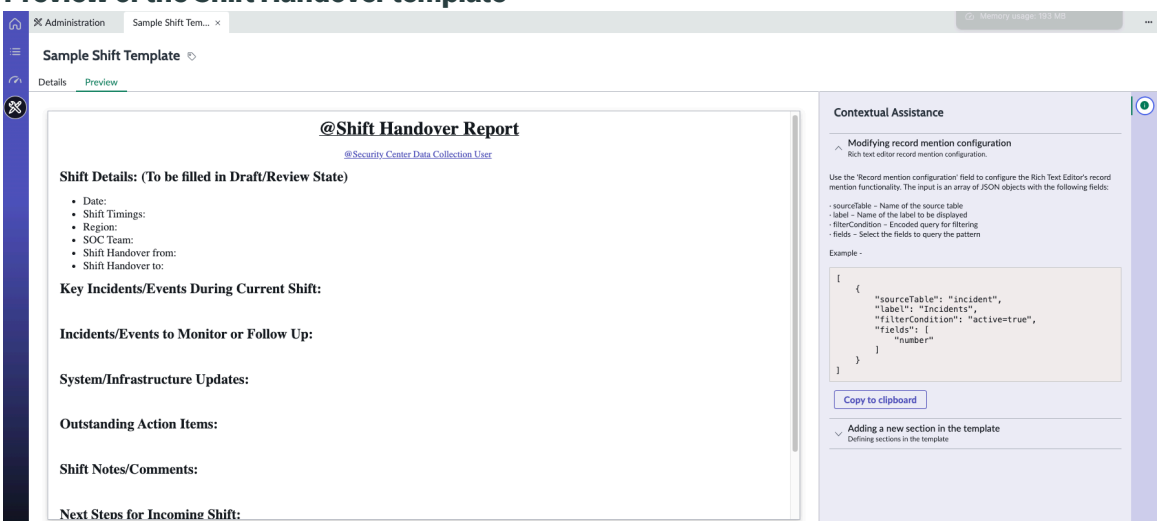
Shift Handover template



6. Update the Shift Handover template according to your requirements.
7. Select **Preview** to view the runtime preview of the Shift Handover template.

   The report generates a preview based on the Shift Handover template configuration.

Preview of the Shift Handover template



8. Select **Save** to save the Shift Handover template.

What to do next

To learn how to Manage Shift Handover records in the list view and perform actions like create, edit, copy, or delete Shift Handover records, see Manage Shift Handover records.

Create shifts through Security Incident Response Workspace

Create shifts through the Security Incident Response Workspace to use when configuring shift handover records.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_escm_sh.shift_admin
- sn_si.admin, which includes the sn_escm_sh.shift_admin role

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select **Administration**.
3. Select **Shift Handover** and then select **Shift Time Configurations**.
4. Select **New**.
5. In the **Shift** field, enter a name for the shift.
6. In the **Start Time** and **End Time** fields, provide the starting and ending times for the shift.

   Note: The time values are in your configured timezone.

7. Select **Save**.

Result

The new shift is added on the Shift Time Configurations page.

Security Incident Response conference call integration

The Security Incident Response Conference Call integration enables you to manage and initiate conference call and chat for analysts, managers and affected users.

With Security Incident Response conference call feature, you can collaborate with customers and peer agents to resolve security incidents over a call. You can also collaborate using a group chat.

You can initiate conference calls using third-party communication channels such as Microsoft Teams, Cisco Webex or Zoom meetings. To collaborate using chat, use the Sidebar chat of the SIR application.

Key features

The Security Incident Response call collaboration provides the following key features:

- SIR Managers/analysts can initiate a Microsoft Teams, Cisco Webex, or Zoom conference call directly from the security incident.
- SIR Managers/analysts can initiate a chat directly from the SIR application.
- Invite additional participants to the call or chat.
- View call recordings and chat details.
- Send invites to participants through emails and Microsoft Teams chat.

Manage Conference Call users and groups

The Admin can configure conference call settings to display a predefined list of users and groups to add to a call.

Before you begin

Role required: sn_si.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Conference Call**, and then **Call Configuration**.
3. From the Call Configurations page, select **Conference Call Config**.
   The configuration page displays to configure predefined list of users and groups.
4. On the Details form, fill the fields.

Field	Description
Name	Name of the conference call configuration.
Autofill Users	Option to auto-fill the configured users for a conference call. Selecting this option adds the configured users and groups to a conference call. **Note:** You can add or remove users/ groups when initiating a call as well.
Show Affected Users	Option to display the affected users for adding to a call.
Show Assignment Group Users	Option to display the assignment group users for adding to a call.
Default Groups	Option to add default groups for adding to a call.
Default Users	Option to add default users for adding to a call.

5. Select **Save** to save the conference call configuration.

Integrate SIR with third-party communication channels

The SIR Conference Call integration with third-party communication channels such as Microsoft Teams, Zoom, and Cisco Webex, enables you to manage and initiate a call directly from a security incident.

Key features

- Start and end conference calls directly from any security incident.
- Add or remove participants in a conference call.
- Track and report meeting details such as meeting duration and attendees for further analysis.

Prerequisites

Verify you've installed the following Integration Hub plugins on your ServiceNow instance.

- Notify plugin (com.snc.notify). For more information, see Configuring Notify
- Notify UI Components for Configurable Workspaces
- For integrating Microsoft Teams as a communication channel:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Microsoft Teams Communications spoke plugin (sn_msteams_com_spk).
  - Azure Active Directory User Mapping plugin (sn_now_azure).
- For integrating Zoom as a communication channel:
  - Zoom Spoke (sn_zoom_spoke)
  - Notify Zoom (sn_notify_zoom)
- For integrating Cisco Webex as a communication channel:
  - Notify Cisco Webex Connector (sn_notify_webex)
  - Cisco Webex Teams Spoke (sn_cisco_teams_spk)

For more information, see Request Integration Hub.

Configuration

Perform the following configuration for the communication channels you want use:

- To configure the Conference Call Cisco Webex integration using the Notify communication channel, see Configure Notify Cisco Webex Connector.
- To configure the Conference Call Zoom integration using the Notify communication channel, see Configure Notify Zoom connector in Notify.
- To configure the Conference Call Microsoft Teams integration using the pre-configured app, see Integrate Notify connector pre-published app with Microsoft Teams.
- To configure the Conference Call Microsoft Teams integration using the self-configured app, see Integrating Notify connector self-configured app with Microsoft Teams.

Configure report templates in Security Incident Response

You can create report templates that can be used to generate an incident summary or an executive summary for analysis and sharing.

Use Security Incident Response Report Templates feature to create report templates to generate reports that provide an analyst level or an executive level summary of an incident. You can format and configure the report on the basis of your requirements using various incident fields.

The following table explains the report templates that are provisioned within the base system.

Report templates in Security Incident Response

Name	Description
Analyst Status Reporting	Provides a complete information of an security incident for an analyst.
Executive Summary	Provides an overview of the status of an security incident for the management.

Note: By default, these reports are in the draft state and are in the read-only mode. You have to reuse these default templates to create and publish report templates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a Report Template in Security Incident Response

Create a new report template for analyst summary or an executive summary for an incident.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Reports**, and then **Report Templates**.
   The Report Templates page appears with all the templates available in the base system.
3. Select **New**.
   Displays the **Details** page of the template.
4. Enter the name and description of the template.
5. Select **Save**.
6. Select **Content** tab.
   Displays the content page of the template with a blank report.
7. Select **Expand** and insert the desired fields in the template body.
   - **Common SIR Fields**: The list of most used fields for an incident.
   - **All SIR Fields**: All the fields related to an incident. For example, when you are generating a incident report and want to add a field called Short description then you can select that field from the All SIR Fields. The Short description field is added as a variable in the report template. When you generate a report for the analyst, the short description if the incident is displayed in the report.
   - **Related Records**: The related records of a particular incident. For example, if you want to add any associated observables in the report, you can add it to your report template. These related records are displayed in the table format
   - **Scripts**: To add the date and time of the report, you can add the Current Date Time script to your report template. This will add the Report Created Date and Time in report.
   -
8. Select **Save Content** to save the contents of your report template.
9. Select **Preview** to preview your report format.

   After you add all the required fields to you report template, you need publish your report template.
10. Select **Publish** to publish the template.

    A confirmation message is displayed whether you want to publish the report template.
11. **Optional:** Select the **More actions** icon, and then select **Delete** to delete the report template.

System properties for reports

The system properties for Security Incident Response reports are explained below.

System properties for reports

Property	Description	Value
sn_si.sn_si_incident.load_all_records	Loads all the records for the lists in the report created	False

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System properties for reports (continued)

Property	Description	Value
	from a template. true - Load all records and false - loads specific number of records defined by sn_si.sn_si_incident.reporting_list_records_count property.	
sn_si.sn_si_incident.max_list_columns_allowed	Limits the number of columns which can be added when rendering lists in report pdfs. This will use the columns from the beginning from the view till the allowed limit.	5
sn_si.sn_si_incident.report_default_style_object	Use this property to control css of free form fields, left panel, report lists.	(JSON object)
sn_si.sn_si_incident.reporting_list_records_count	Loads specific number of records in the report editor.	200
sn_si_reporting_email_template_sys_id	Sys ID of the email client template for the SIR (sn_si_incident) table which will be used in shared report.	9ce97ae6434612104168 96ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	Field header	sn_si_incident_report_field_header,sn_si_incid
sn_si.sn_si_incident.defang_record_list_urls	Control whether the URLs from list are defanged or not.	False
sn_si.sn_si_incident.reporting_dot_walk_tables	List of tables available for dot-walking in reports.	(JSON object)

Duplicate a report template in Security Incident Response

Duplicate a report template to edit or reuse an existing template to create a new template.

Before you begin

Note: You have to create a copy of the Executive Summary and Analyst Status Reporting templates to reuse them.

To reuse the Executive Summary and Analyst Status Reporting, you have to create a copy of these and then

Role required: sn_si.admin

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Reports**, and then **Report Templates**.
   The Report Templates page appears with all the templates available in the base system.
3. Select the template.
4. Select **Duplicate**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The contents of the selected template are duplicated and copy of the selected template is available in the list of templates. The duplicate template is in the Draft state. You can customize the contents, and then rename the template as required.

What to do next
Edit a report template in Security Incident Response

Edit a report template in Security Incident Response

Edit a report template to reuse an existing template to create a new template.

Before you begin
Role required: admin

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Reports**, and then **Report Templates**.
   The Report Templates page appears with all the templates available in the base system.
3. Select the template.
   Displays the **Details** tab of the template in edit mode.
4. Update the name and description of the template.
5. Select **Save**.
6. Select **Content** tab.
   Displays the content page of the template with a blank report.
7. Select **Expand** and insert/remove the desired fields.
   - **Common SIR Fields**: The list of most used fields for an incident.
   - **All SIR Fields**: All the fields related to an incident. For example, when you are generating a incident report and want to add a field called Short description then you can select that field from the All SIR Fields. The Short description field is added as a variable in the report template. When you generate a report for the analyst, the short description if the incident is displayed in the report.
   - **Related Records**: The related records of a particular incident. For example, if you want to add any associated observables in the report, you can add it to your report template. These related records are displayed in the table format
   - **Scripts**: To add the date and time of the report, you can add the Current Date Time script to your report template. This will add the Report Created Date and Time in report.
8. Select **Save Content** to save the contents of your report template.
9. Select **Preview** to preview your report format.

   After you add all the required fields to you report template, you need publish your report template.

10. Select **Publish** to publish the template.

    A confirmation message is displayed whether you want to publish the report template.

On-Call scheduling in Security Incident Response

Use On-Call Scheduling in Security Incident Response to view and manage shifts for your analysts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With the On-Call Scheduling feature, you can view and manage shifts, approve or reject absence requests. You can also manage notification preferences, delivery channels, escalation trigger rules, and policies for your group.

Key features for sn_si.manager/rota_manager

- View the on-call schedule including any gaps and time-off requests for your group.
- Approve or reject time-off requests.
- Review and manage gaps and conflicts.
- Provide, replace, or delete coverage and delete time-off requests.
- Create a shift and add or delete members to the shift.
- View escalation, group, and performance reports.

Key features for sn_si.analyst/oc_read

- View your on-call schedules and see the other members of your shift.
- Submit a time-off request and refer another member of the group to cover your shift.
- Specify your availability and your preferred contact methods.
- View the members and escalation details for a shift.

Documentation for On-call Scheduling

For detailed information on configuring and using On Call Scheduling features, refer to the IT Service Management On-Call Scheduling documentation.

Category management in Security Incident Response

Configure security incident categories and subcategories for granular classification of incidents which helps in accurate routing of security incidents.

Create a category

Create an security incident category that you want to use to classify security incidents.

Before you begin
Role required: sn_si.admin

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Category Management**, and then **Category**.
3. Select **New**.
   The Details page appears. The Table, Element and Language fields are preconfigured for the current user.
4. In the **Sequence** field, enter the sequence number.
5. Select the **Inactive** check box to enable or disable the category.
6. In the **Label** field, enter a category name.
7. In the **Value** field, enter a category value.
8. **Optional:** Enter a value in **Dependent value**, if this category is dependent on any field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. **Optional:** In the **Hint** field, add a hint for this category.
10. Select **Save** to save the category.

Result
The new category is saved and appears on the Category page.

Create a subcategory

Create a subcategory for a category to further classification of a security incident.

Before you begin
Role required: sn_si.admin

Procedure
1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Category Management**, and then **Subcategory**.
3. Select **New**.
   The Details page appears. The Table, Element, and Language fields are preconfigured for the current user.
4. In the **Sequence** field, enter the sequence number.
5. Select the **Inactive** check box to enable or disable the subcategory.
6. In the **Label** field, enter a subcategory name.
7. In the **Value** field, enter a subcategory value.
8. In the **Dependent value** field, enter a category value to which this subcategory belongs.
9. **Optional:** In the **Hint** field, add a hint for this subcategory.
10. Select **Save** to save the subcategory.

Using SIR Workspace

Security Analysts and managers use SIR Workspace to perform day-to-day operations with an improved user experience, do complete incident investigation, and get an overview.

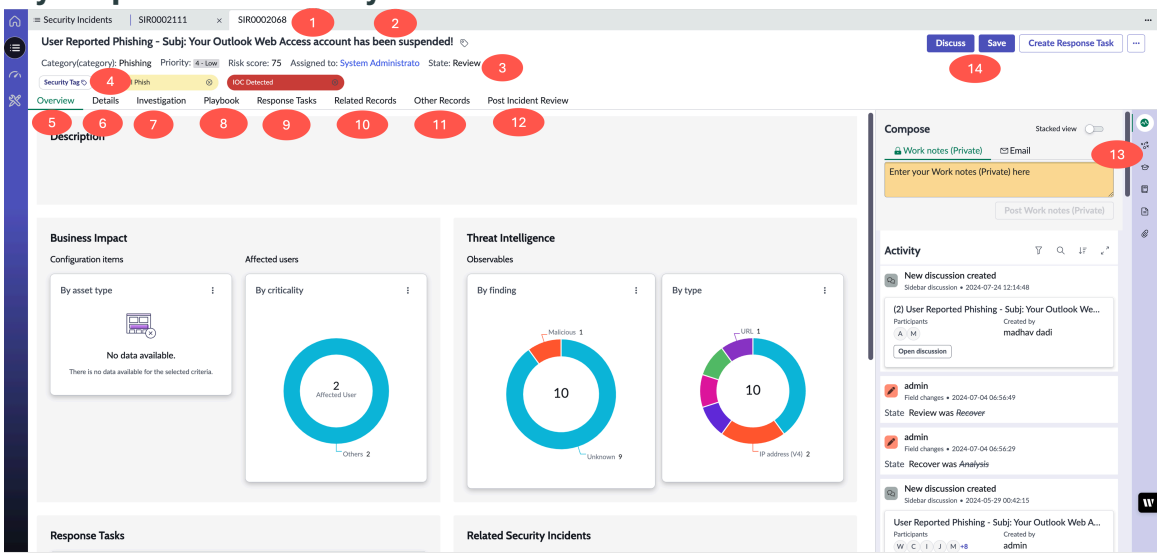
Working with Security Incident Records

The Security Incident Record consists of the following.

Key components available on a security incident record:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key components of a security incident



Number	Name	Description
1	Security incident number	The security incident number is available against the tab name.
2	Short description	Short description of the security incident which is displayed above the form banner.
3	Form banner	This is read-only section, which contains the key fields such as Category, Priority, Risk score, State, and the incident assignment details. **Note:** The regular platform tags can be applied here as well.
4	Security tags	Displays the security tags associated with a security incident.
5	Overview	Provides a snapshot overview of the security incident such as Description, Business Impact comprising of asset details by type, affected users by criticality, Threat intelligence items comprising of observables by finding and by type, Response Tasks, Related security incidents comprising of child security incidents and similar security incidents.
6	Details	The details tab displays the security incident form.
7	Investigation	The Investigation tab displays the incident investigation experience.
8	Playbook	Playbook is triggered through Process Automation Designer (PAD). If a process is created, and if the a trigger condition is set to trigger the playbook for a security incident. Then a playbook appears.
9	Response Tasks	The Response Tasks captures all the response tasks associated with a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Number	Name	Description
10	Related Records	The Related Records tab consists of all the related lists from the classic UI under this section. The related lists are grouped under various section such as business impact, threat intel, and so on for an easy navigation.
11	Other Records	Other records tab consists of IT records such as changes requests, incidents, and emails grouped and displayed in this section.
12	Post Incident Review tab	As the security incident progresses to the Review state, the Post Incident Review tab is displayed with the post incident assessments and reports within the tab.
13	Contextual menu	Provides easy access to the quick actions and is available across all the tabs for the analyst to access whenever required. The contextual menu provides easy navigation to the multiple resources such as: **1.** Activity Stream **2.** Playbook **3.** Analyst Assist **4.** Runbook **5.** Templates **6.** Attachments
14	Form UI actions	The various security incident form UI actions are displayed on the top right of the incident form. The available form UI actions are: • Discuss • Save • Create Response Task • Compose Email • Add Playbook • Open Associated Workflow(s) • Crete incident • Create Problem • Create Change Request • Create Outage • Calculate Severity • Link to Major Security Incident • Propose as Major Security Incident • Promote to Major Security Incident • Run Additional Action(s) on Endpoint

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Number	Name	Description
		• Associate MITRE ATT&CK Technique • Switch to Classic UI • Add to Security Case • Delete For more information, see Working with Form UI actions.

Security Incident Overview section

The Overview section on the workspace presents the key information associated with the security incident.

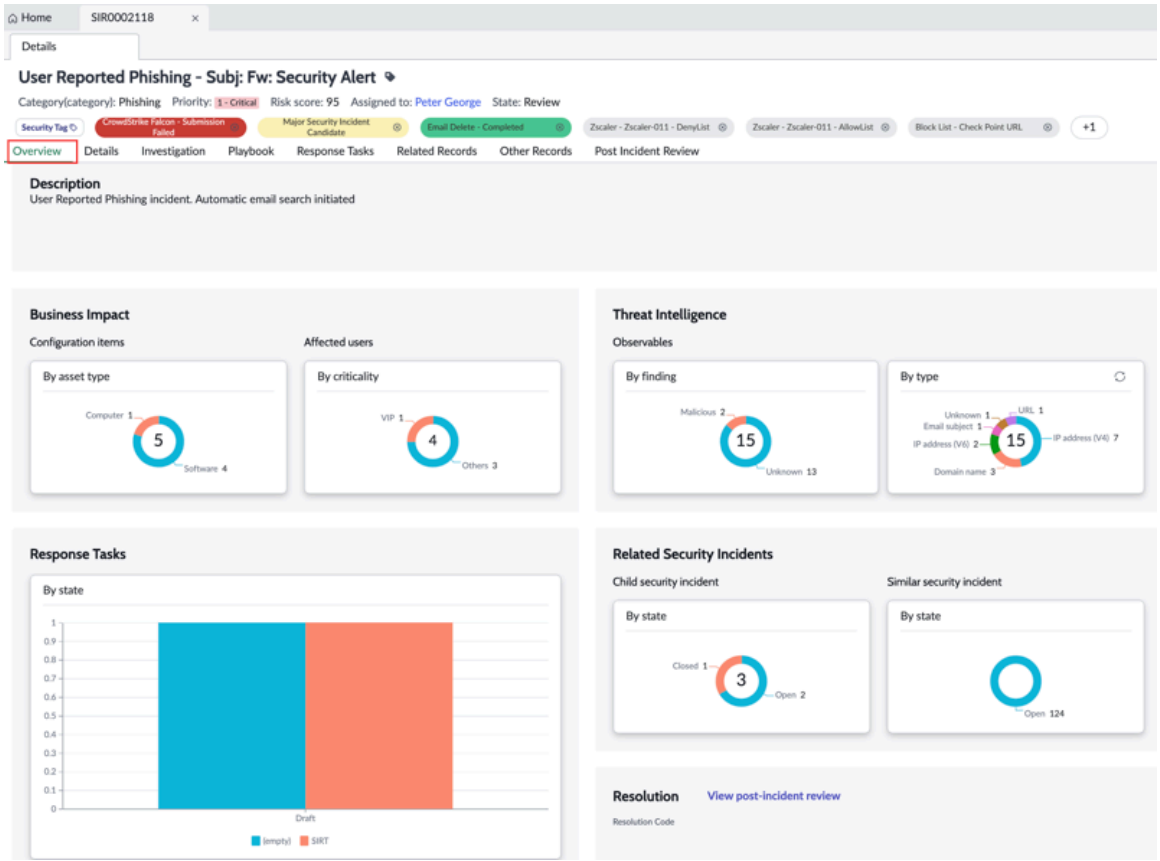
The donut charts are drill down enabled, when an analyst selects any of the chart items, then it navigates you to the respective record with a filtered list view of items within that corresponding tab. For example, if **Malicious Observables** is selected it takes you to the observables with a filtered list view of malicious observables on the **Related Records** tab.

The Overview section displays the following:

- Description of the security incident.
- Business impact details such as the configuration items by asset type and affected users by criticality - whether VIP users or other users.
- Threat intelligence items such as observables by finding whether the observables or malicious or unknown, and by type.
- Response Tasks by state and assignment group.
- Related security incidents comprising child security incidents by state - whether open or closed, and similar security incidents by state - whether open or closed.
- The Resolution section is displayed when an incident moves to the Review state, then the resolution section is displayed within the **Overview** section with an ability to view the post incident review.
- Resolution - view post incident review: Select the link to navigate to the **post incident review** page.
- After the incident is closed, the Resolution section displays the resolution code, resolution notes, and resolved by (user) along with the post incident review details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview section



Security Incident Details section

This section displays the security incident form fields that are rendered from the security incident classic UI.

The Classic UI has a view called **SIRW** View created. This view is mapped to the **Details** tab in the new workspace. Any customizations that are required need to be implemented in this view.

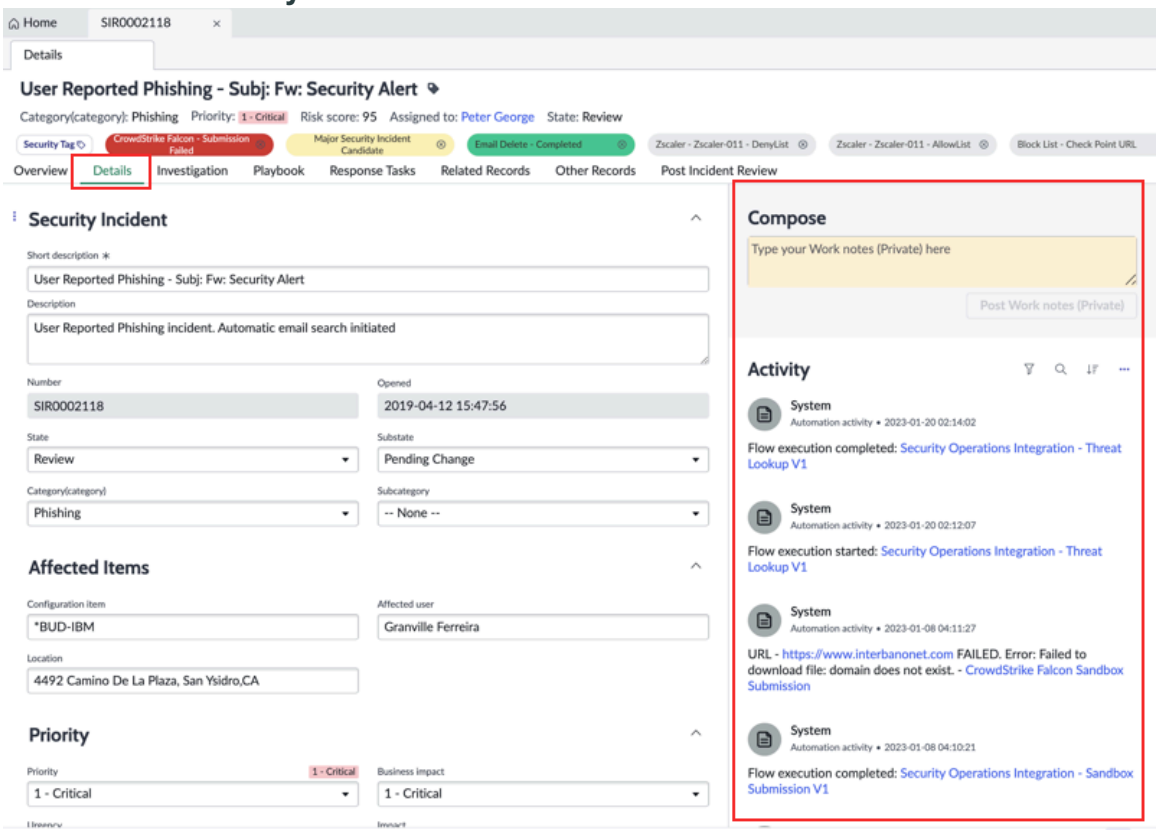
The form fields are grouped into the following sections and displayed on the Details tab form view, click on any of the section or jump to the respective section within the form:

- Security Incident
- Priority
- Source
- Parent
- Assignment
- Access Controls
- Affected Items
- Resolution

The **Details** tab contains the **Activity** stream section within the details form itself for a quick access to the security analysts to add any comments and post it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

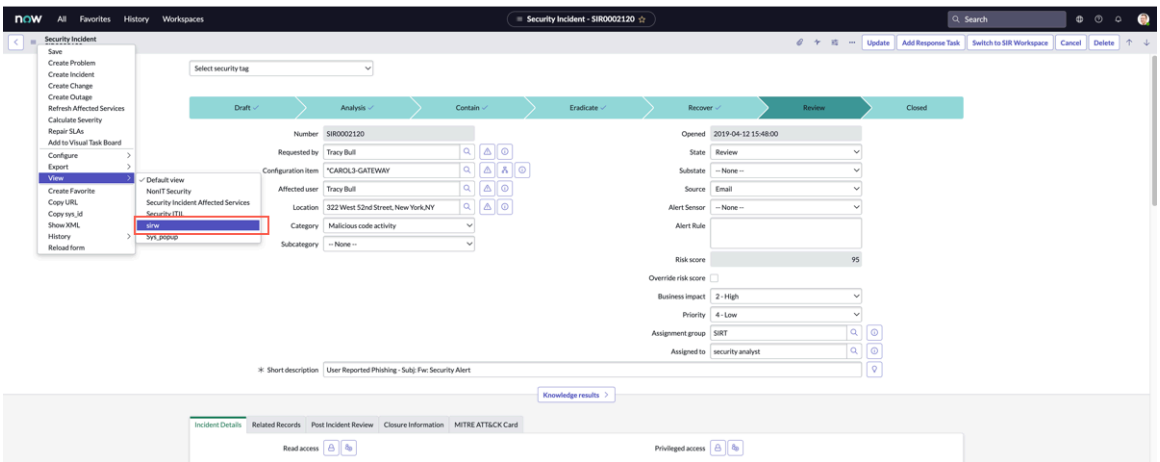
Details tab and Activity stream



View the SIR Analyst Workspace view:

1. Navigate to **All** > **Security Incident** > **Show Open incidents**.
2. Select any security incident record.
3. Click on the context menu and select **View** > **sirw**.

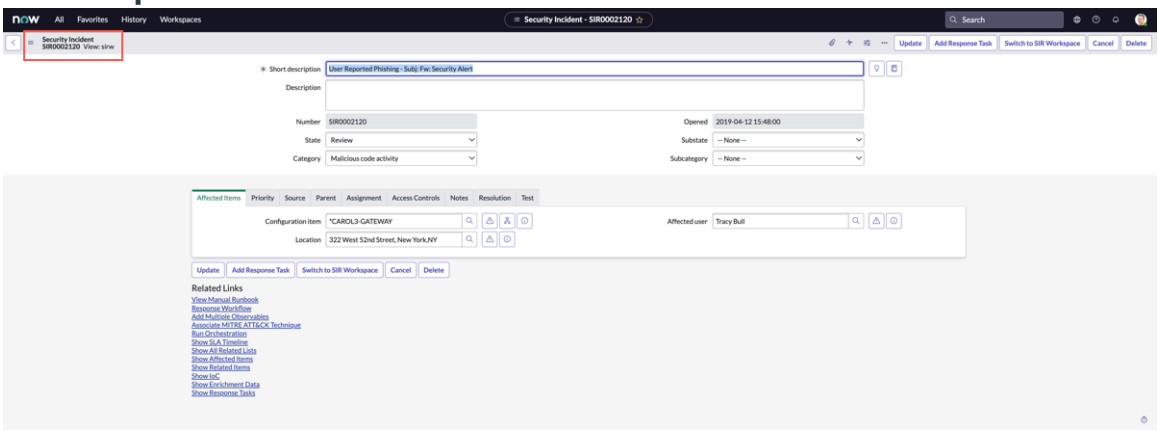
> **Note:** You can customize using **sirw** workspace view in the classic UI form.



4. The security incident workspace view is rendered as shown below.

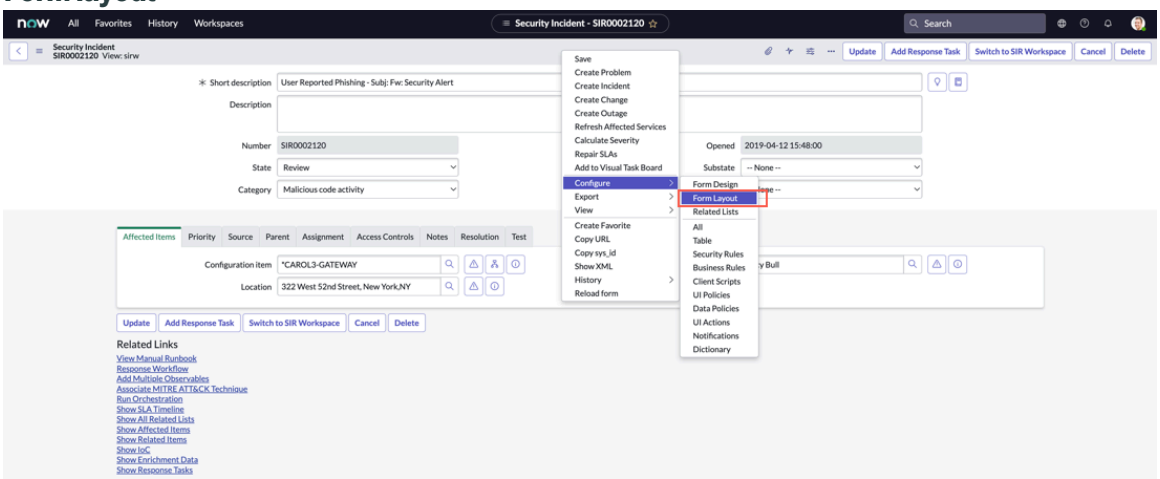
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SIR workspace view



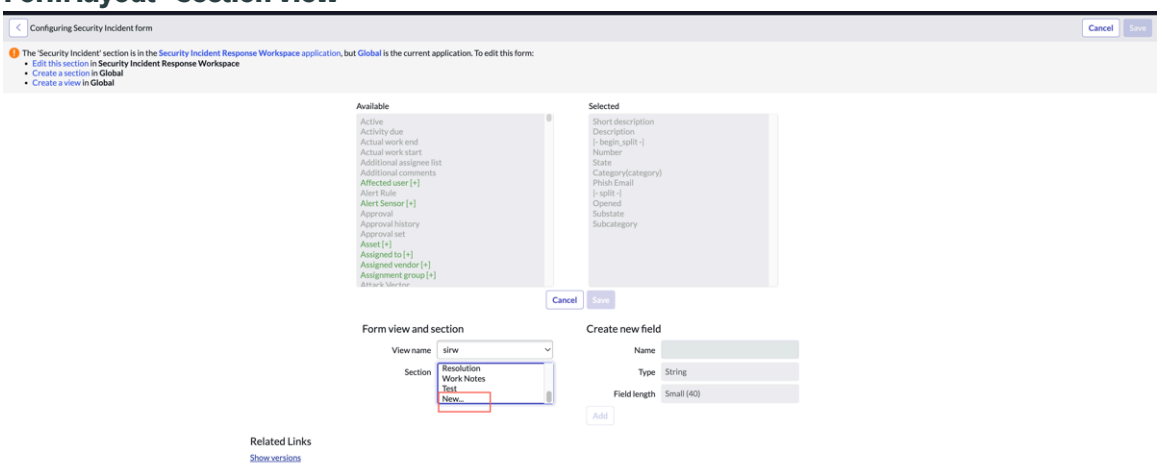
5. On the Security Incident record, right click and go to **Configure** > **Form Layout**.

Form layout



6. Drill down to the **Form view and section** and select **New** from **Section** to create a new section.

Form layout - section view

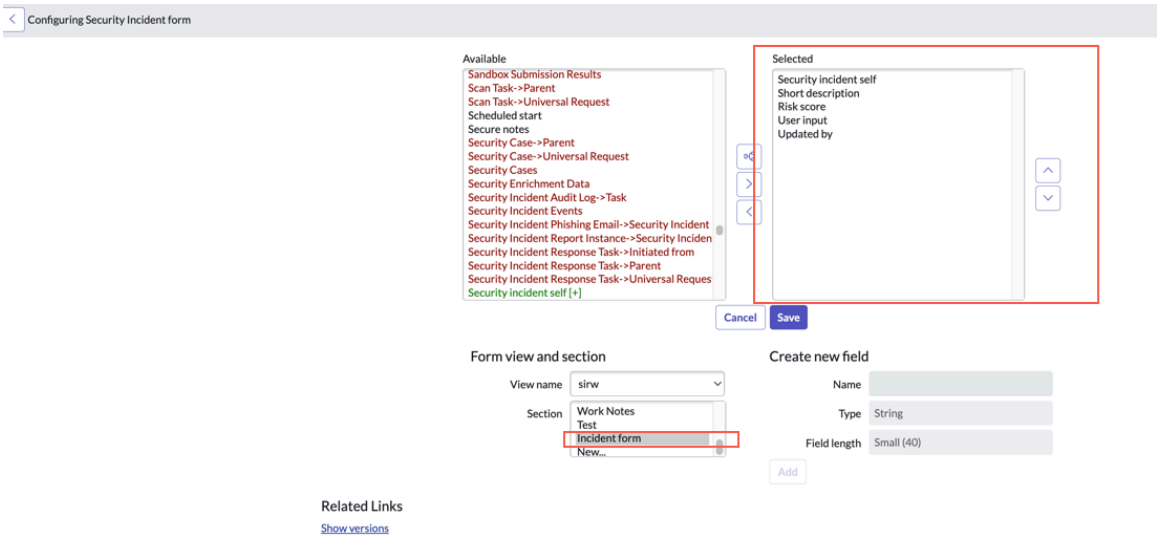


7. Provide the new section name and click **OK**.

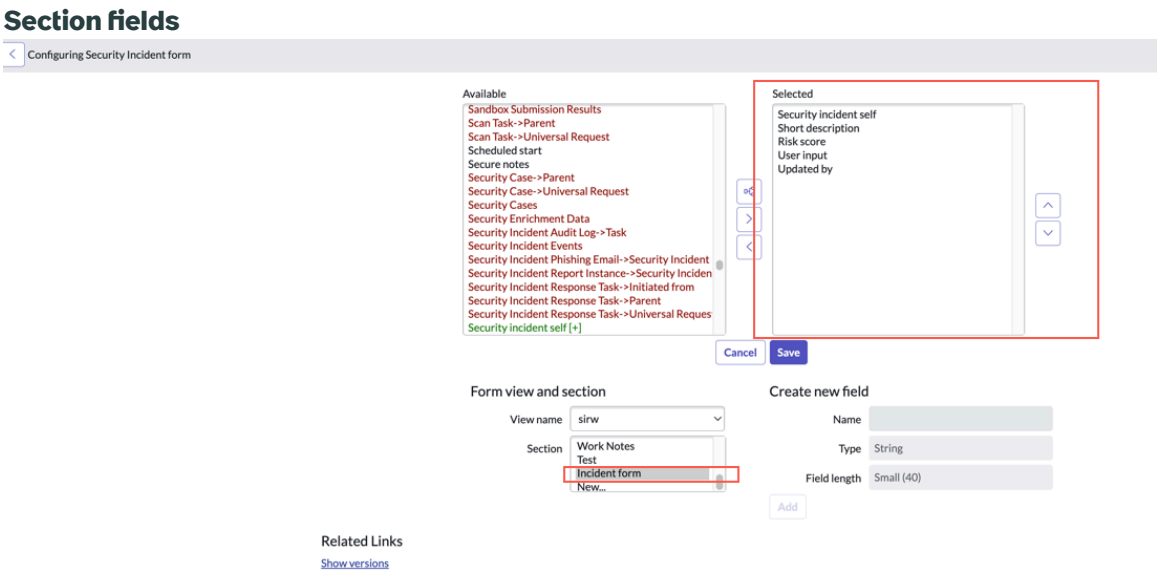
   For example, Incident form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. The new section is created and added to the **Section**.

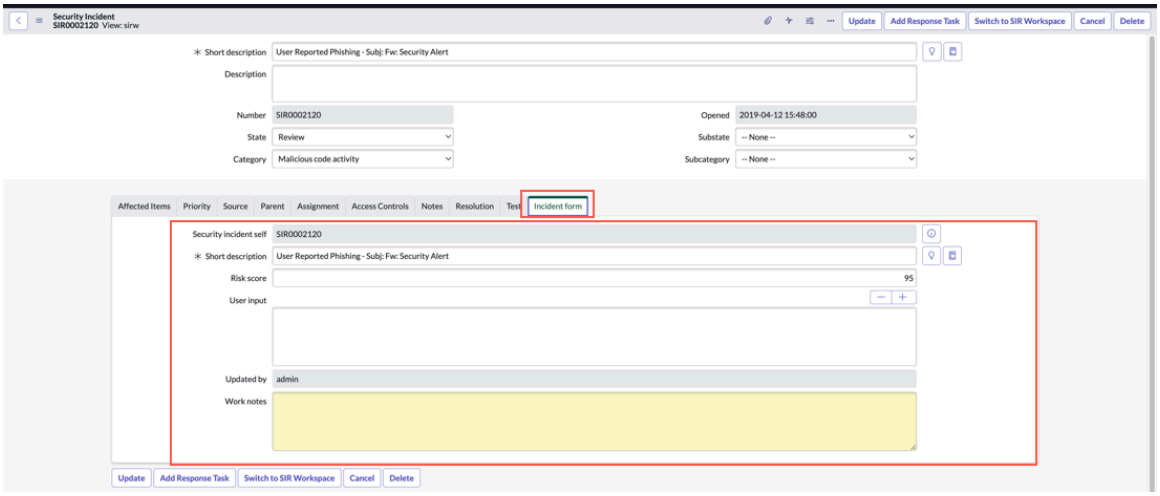


9. Select your new section and add the required section fields to the slush bucket and click **Save**.



10. The newly added section is displayed along with the existing section layout within the security incident form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



11. Now, click **Switch to SIR workspace** to jump to the security incident form and the customized section within the **Details** tab of the workspace.

Security incident Details tab

This section describes all the fields of the **Details** tab of a security incident.

Security incident Details form

Field	Description
Number	[Read only] The security incident number.
Requested by	The person requesting the work to be performed.
Configuration Item	The server, computer, router, or other configuration item affected by the security issue.
Affected user	The person affected by the security issue.
Location	The location of the requester or resource. If a **Configuration Item** isn't selected, this field is pre-filled with the location of the requester.
Category	The category that identifies the type of security issue. If a category is selected, a workflow for analyzing this issue is executed when the record is saved. For example, if you select **Denial of Service**, the Security Incident - Denial of Service - Template workflow is executed. For more information, see Understand Security Incident Response Orchestration workflows and workflow templates.
Subcategory	The subcategory that further defines the issue.
Opened	[Read only] Displays the date and time the incident was opened.
State	The current state of the security incident. Upon security incident creation, this field defaults to **Draft**.
Substate	Identifies whether the security incident includes a pending problem or change.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident Details form (continued)

Field	Description
Source	Identifies the source of the security incident, such as email, a phone call, or network monitoring.
Alert Sensor	Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee.
Alert Rule	The rule in the security product, which triggered the creation of this security incident.
Risk score	Displays the risk score calculated for this security incident. The value is based on the priority of the security incident, the type of security incident (Denial of Service, Spear Phishing, or Malicious code activity), and the number of sources that triggered a failed reputation score on an indicator. The risk score aids in prioritizing security incident work for analysts. Three security incident properties allow you to further designate a color-coded dot to appear next to the risk score in list view to make them more easily identifiable. If you change certain fields in the security incident, such as the **Business impact** or **Priority**, and save the record, the **Risk score** is automatically recalculated and displayed. The change is also reflected in the work notes and on the Risk Score Audits related list. **Note:** The risk score is also recalculated when affected users are associated with a security incident, affected services, or vulnerable items. You can also manually enter a new **Risk score**. This can be useful if you want to keep a particular security incident at the top of the list of security incidents you're analyzing. If you enter a new **Risk score**, the **Risk score override** check box is automatically selected. Regardless of the changes made in the security incident, a manually-entered risk score isn't automatically recalculated. **Note:** If you have upgraded your instance from a prior release, risk scores were calculated for all of your open security incidents. For more information, see Understanding security incident calculators.
Risk score override	Option to override the automatic update of the risk score. The override is reflected in the work notes.
External risk score	The calculated external risk score.
Business impact	Importance of this security incident to your business. The default value is Non-critical. If, after the security incident record has been saved, you change the value in the **Priority** and/or **Risk** fields, the **Business impact** is recalculated.
Functional Impact	The functional impact of this security incident. For example, service downtime, business disruption.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident Details form (continued)

Field	Description
	Following are the options: • Low • Medium • High **Note:** This field isn't available in the base system. To add this field, see Accessing Form Builder.
Recoverability	How easily and quickly you can restore the normal operations and recover from the impact of the security incident. Following are the options: • Regular • Supplemented • Extended • Not Recoverable **Note:** This field isn't available in the base system. To add this field, see Accessing Form Builder.
Information Impact	The data impact of the security incident. You can select all the applicable: • Privacy Breach • Proprietary Breach • Integrity Loss **Note:** This field is not available in the base system. To add this field, see Accessing Form Builder.
Priority	The order in which to address this security incident, based on the urgency. If this value is changed after the record is saved, it can affect the **Business impact** calculation.
Assignment group	The group to which this security incident is assigned.
Assigned to	The individual assigned to analyze this security incident. Assignments can be performed manually or automatically. For more information, see Assigning security analysts.
Short description	A brief description of the security incident.
Knowledge results	As you enter the short description, links to related articles from the knowledge base appear. Scanning the information could solve your issue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SIR Workspace Orchestration

Security Incident Response Workspace orchestration activities will help the security analysts to view the investigation canvas and perform various actions that are applicable.

SIR Workspace Investigation Canvas

Security Incident Response Workspace allows the Security Analysts to view the key information associated with the security incident during the incident remediation process. The key information also includes the related lists such as Observables, Threat Lookup Results, Sighting Search, Observable Enrichment, and so on.

In the classic UI, most of the orchestration actions associated with the out of the box integrations are available against the related lists. For example, Run Threat Lookup, Run Observable Enrichment, etc. are present against Associated Observables related list. Similarly Get Host Details, Get Network Statistics and so on, are available against Configuration Items related list.

When a Security Analyst performs these actions, results are populated in a different related list. For example, when a user performs Run Threat Lookup, the results are available in Threat Lookup Results table. Sometimes, results are available in multiple different tables. During this process, the Security Analysts has a disjointed and unorganized user experience in co-relating the information from multiple places.

In the re-imagined new SIR Workspace, the **Investigation** canvas (tab) provides all the necessary information grouped logically in one place for the Analyst to perform the investigation.

Explore Investigation Canvas

The primary objective of the investigation canvas is to present the necessary security incident data in one common place.

Within the SIR Workspace, the security incident investigation primarily revolves around a few key entry points.

The following are a few key entry points that are provisioned for the security analysts within the base system:

- Associated Observables
- Configuration Items
- Affected Users
- Associated Phish Emails
- Email Search

You can also configure the above entry points by adding or modifying or removing the entry points as applicable. For more information, see Configure SI design time investigation.

On the **Investigation** tab, the entry point table acts as the parent table. All the tables that hold the results of an orchestration action performed on the parent table are presented as children table within the entry point.

For example, for **Associated Observables** entry point, **Associate Observables** table is the parent table, and other tables such as Threat Lookup Results, Sandbox submission results, and so on are the children table.

The Security Analyst can perform all the orchestration actions on the Associated Observables table, and will be able to view all the associated information within the same page, without the need to navigate across multiple places.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

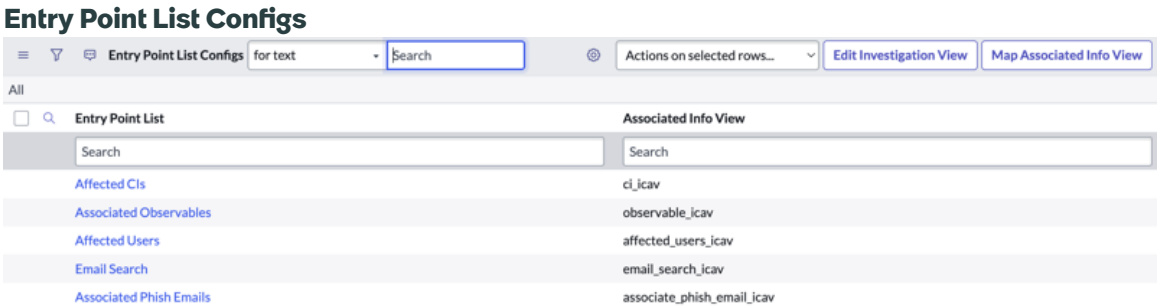
Note: When a user clicks on the interactable charts on the **Overview** page such as malicious observables, the user will be navigated to the filtered view of malicious observables within the investigation canvas. Alternatively, the user can directly begin the investigation by navigating to the investigation canvas which will have all the data.

The list of children table under an entry point is also configurable. For more information, see Configure SI design time investigation.

The following is a detailed example of an entry point (Associated Observable) that are configured and provisioned within the base system:

1. Select the **Associated Observables** entry point from the drop down list.

   Here the parent table is also **Associated Observable**.



2. Select one or more observables from the parent table.
3. Run the desired capability.

   For example, select **Run Threat Lookup** to fetch the threat lookup results for a selected observable.

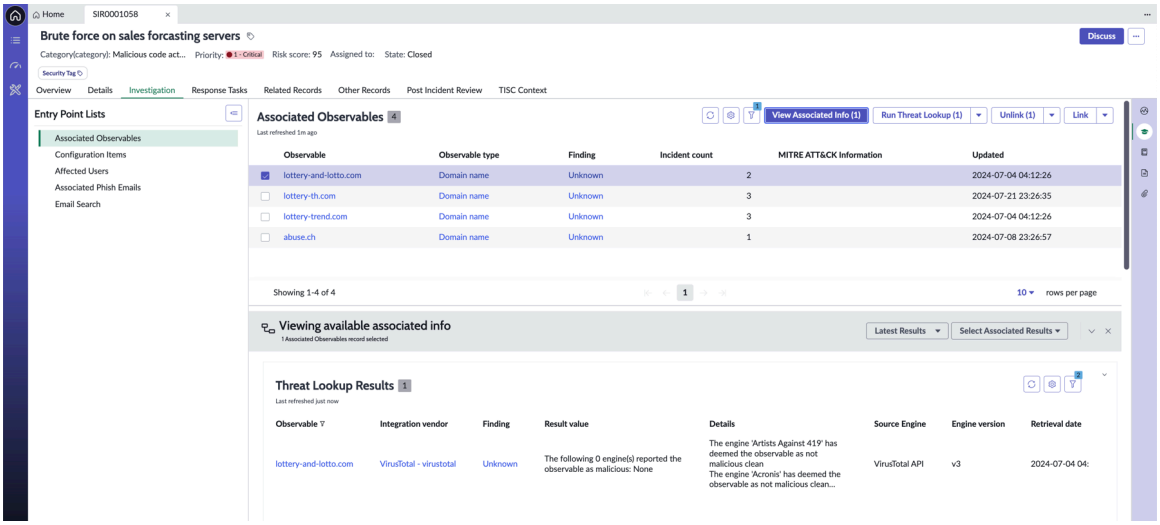
   Note: When a corresponding observable action is executed, the process is run in the backend and the results are displayed below the Observables list.

4. Click **View Associated Info** to view the observables results. The results are displayed on the same page.

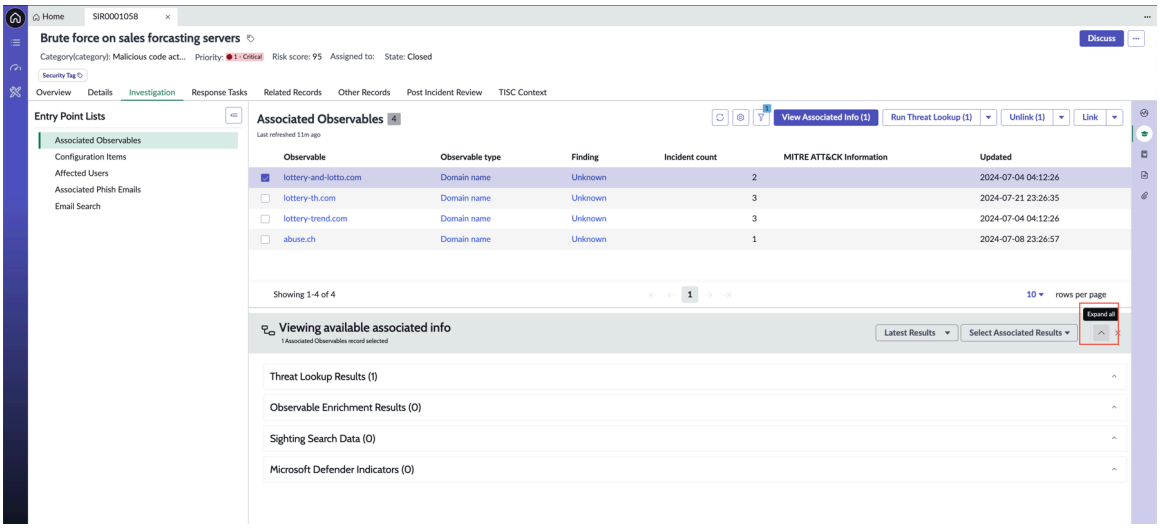
   Note: You can view the results using filters by results, select either **All results** or **Latest Results**, whichever is the desired view. By default, the latest results are displayed. If there are multiple implementations (of integrations), then latest results per implementation will be shown.

   In addition, you can filter the results **by associated related lists** which are the children table results. By default, all the configured children table related lists are displayed. For more information, see Configure SI design time investigation. However, you can choose to select only those children tables that are required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



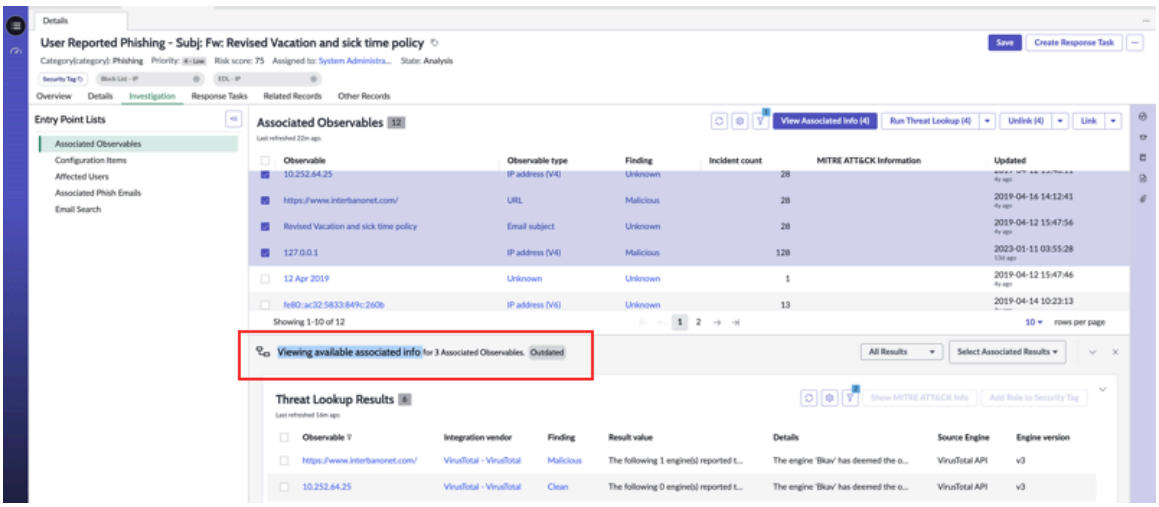
5. By clicking **View Associated Info** you can view all the associated children table data in one place, however you can close the related lists view by selecting **Close View** button. Once you close the view, you can only see the observables parent table as earlier.
6. Click **Expand all** upward direction icon within the **Viewing available associated info** results table to expand all the related lists children table data.



7. Click **Collapse all** downward direction icon to collapse all the related lists children table data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The banner on top of the associated info section that contains all the children table data shows how many observable related information is being presented to the user. For example, initially if you select two observables and click **View Associated Info**, the banner shows, **Viewing available associated info for 2 Associated Observables.**. If you select for example, another observable, the banner says that the information is outdated (screenshot below). You will have to click **View Associated Info** again to get the latest data.



In addition to the above comprehensive view of the Observables associated information, if you would want to view more information about a record on the parent table then click the observable and the parent table record form opens in a different tab with a more detailed view of the selected record. All the associated children table data of that particular selected record is also presented under the **Associated info** section.

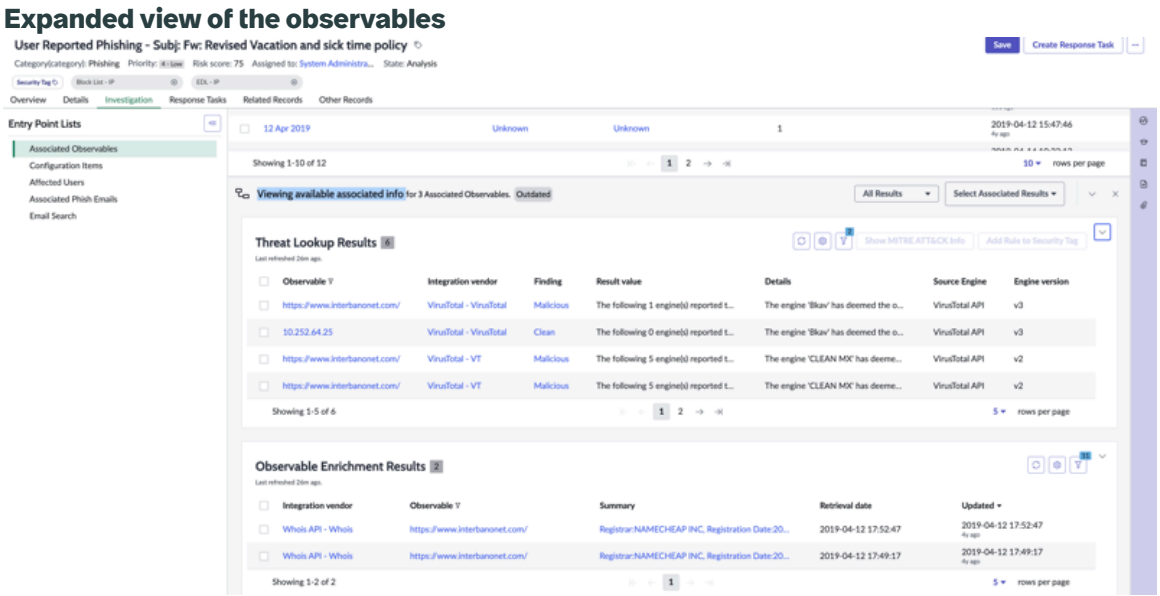
However, the associated info section displays only the latest results of the children table, as seen in the investigation canvas, in the read-only mode. No actions are possible in this view. The form page of the children table can be opened in a new tab that will render the fully functional page with any actions, if any.

You can switch between the different tables using the drop-down list. You can also expand or collapse each form under the associated info section.

Within the **Observable** form page (parent table record form page) you can perform certain actions as available. Whenever you perform an action, you can click refresh on the associated info banner to refresh the data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Click **Expand all** to expand all the related lists children table. By default, all the children are expanded.



Related topics

Configure SI design time investigation

Unified experience framework for integrations powered by Capability Framework

In the classic UI, the experience is disjointed when performing orchestration activities such as running threat look, performing sighting search, and so on. Each capability has its own experience while executing it. In the new workspace, there is unified experience across all capabilities.

The unified experience is applicable only for those integrations and orchestration activities that fall within the capability framework. There can be actions specific to integration, for example, Create Indicators in Microsoft Defender. These actions will have its own experience as required by the use-case.

The new framework consists of modal screens with three steps as explained below.

1. **Implementations**: The first step involves selecting one or more implementations that are present against the selected capability.

   For example, when the Analyst clicks **Run Threat Look Up**, the Analyst will be able to select one or more implementations that are present for **Run Threat Look Up capability**.

   Each implementation will have the details of the Integration Source. Refer to the table below. Additional information is also presented against each implementation.

   Additional Information can include for example information on any filters, types of observables supported, etc. The Additional Information can be configured as desired. For more information, to UX framework technical configuration procedure.

Unified Implementation Framework Modal

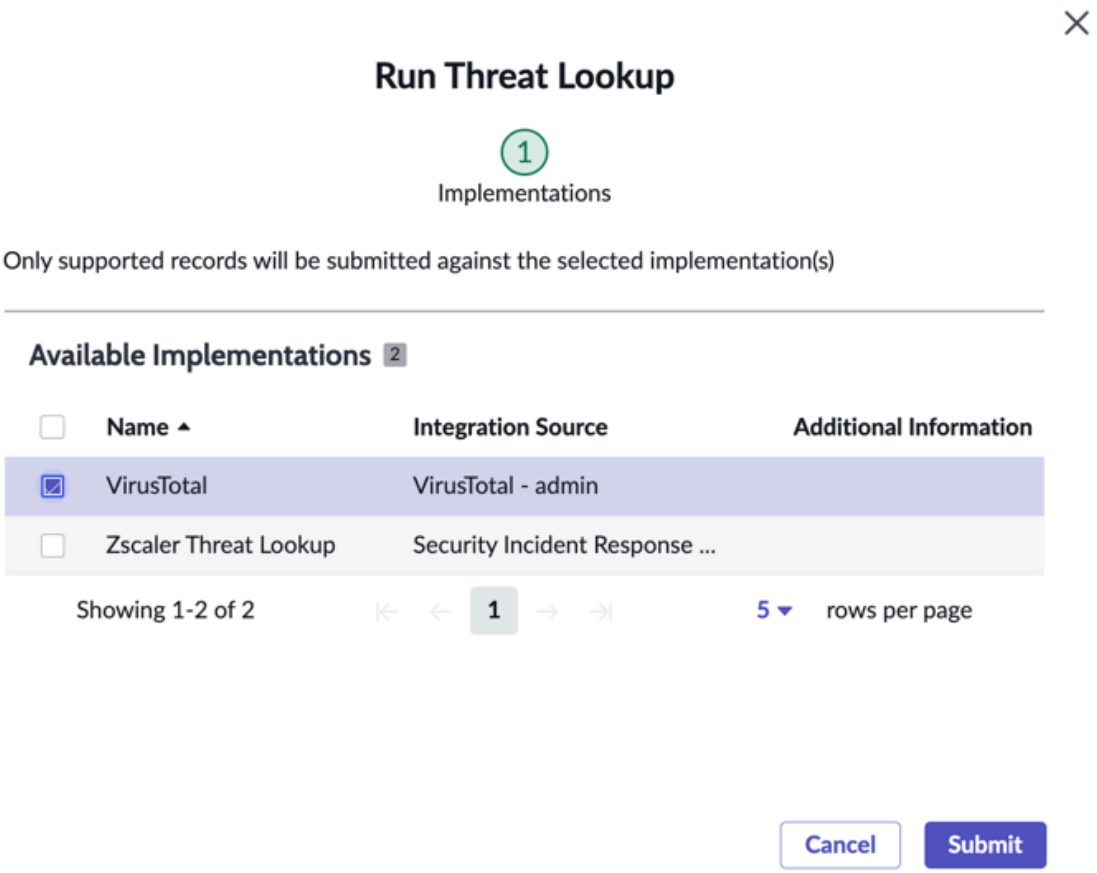
Implementation	Description
Name	Name of the implementation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Implementation	Description
Integration Source	The source of the implementation such as the configuration that is being used.
Additional Information	This column captures the static information which adds more context to the security analyst against the selected implementation(s) to proceed with an action. For example, supportability or filtered information. Also, if an implementation supports only a certain type of observables such as Domain or URL, then you can add that additional information here in this column to provide the context to the user. **Note:** The UI framework would basically allow the selection of any type of implementation and any type of observables. During the submission, the existing base system integrations that are shipped will take care of the filtering in the backend and submit only the supported type of observables. The rest of the records that don't match the supportability will be ignored. Hence, a UI information message is displayed while you select the capability: **Only supported records will be submitted against the selected implementation(s).**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

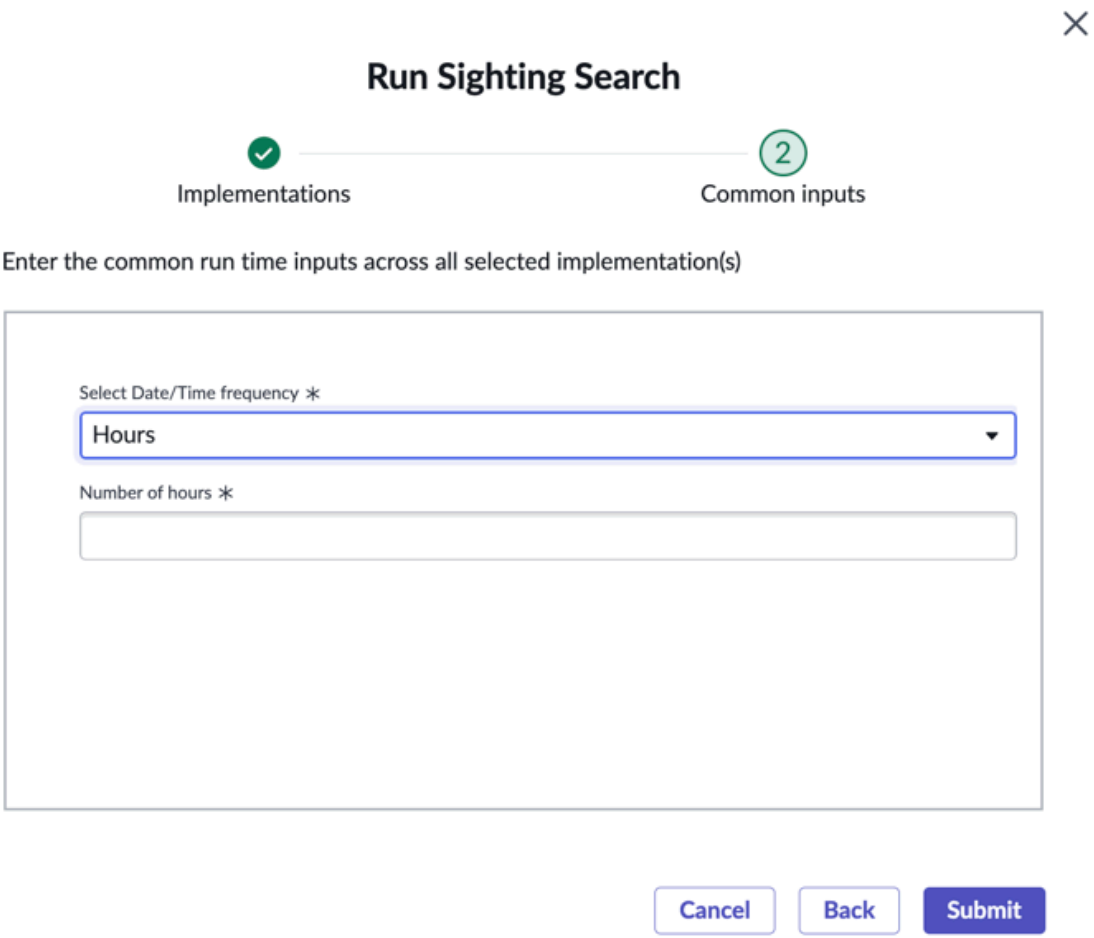
Screen 1: Implementation(s)



2. **Common inputs**: Add common inputs for the selected implementations or for all the selected applicable implementations. This is the screen 2 of your implementation. For example, as of now only **Sightings Search** has the common inputs screen. This implementation is a combination of screen 1 (Implementations) and screen 2 (common inputs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Screen 1 + Screen 2

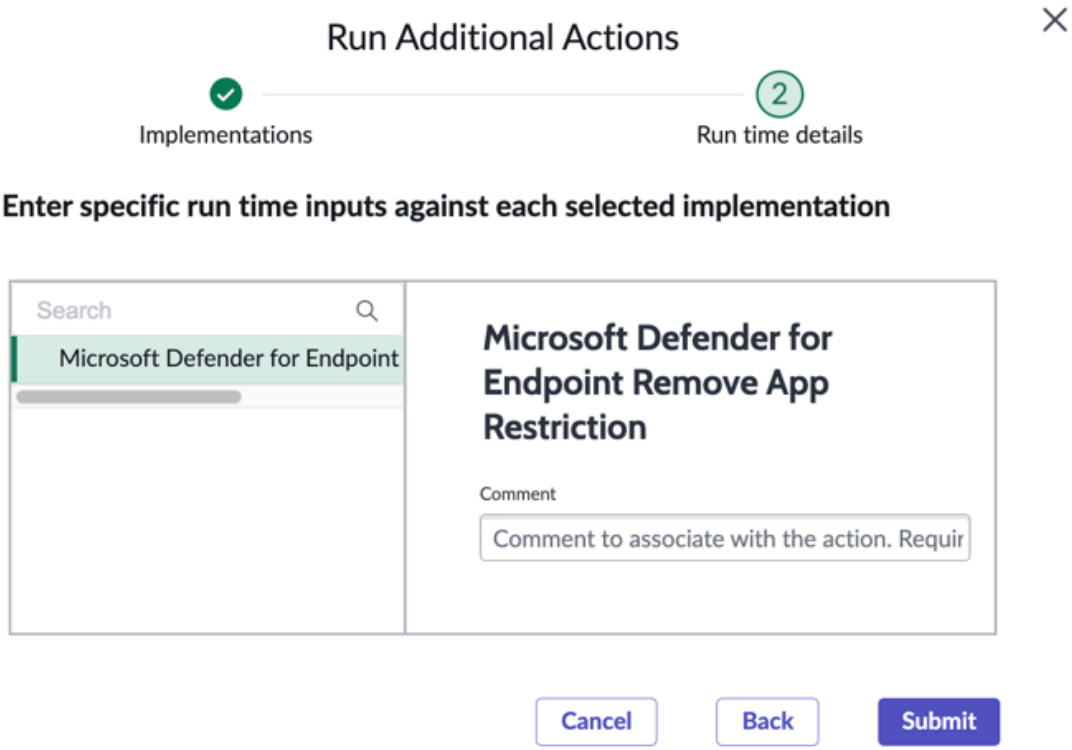


3. **Run time details**: Add specific run time inputs for the selected implementations which are different from each other implementation. This is the screen 3 of your implementation. This

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

implementation is a combination of screen 1 (Implementations) and screen 3 (specific run time inputs).

Specific inputs



Note: Not all three steps are always required. Depending on the capability and the type of inputs required, the runtime details step and common inputs step will be visible.

Unified experience capabilities and modal screens

The following table below describes the capabilities and applicable screens.

Capability	UX Frameworks Screens Applicable	Integrations Supported
Run Threat Look Up	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for Run Threat Look Up. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	• Virus Total • Hybrid Analysis • Security Incident Response Integration with Zscaler • Phistank • Metadefender • Threatcrowd • Have I Been Pawned? • Crowd Strike Falcon Intelligence

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Capability	UX Frameworks Screens Applicable	Integrations Supported
Run Observable Enrichment	Only Screen 1 – Select Implementations is applicable There are no common inputs or implementation specific inputs applicable for Run Observable Enrichment. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	• MISP • Microsoft Defender Endpoint • Shodan • RiskIQ • WHOIS • Reverse WHOIS
Run Sighting Search/Run Web Sighting Search/Run Email Sighting Search	Screen 1 – **Select Implementations** and Screen 2 – **Common Inputs** are applicable. Sighting search takes date and time frequency as common inputs across multiple implementations of Splunk and other integrations. This screen will be presented to the Security Analyst to capture date and time frequencies. For integrations that don't require these inputs, for example FireEye HX, they will be ignored. After selecting one or more implementations and providing common inputs, the Security Analyst will be able to submit the action.	• Splunk-incident Enrichment • Carbon Black • Elastic search • FireEye HX • McaFee ESM • MSFT Defender for endpoint • Splunk Sighting • Qradar sighting search • MISP
Submit to Sandbox	Screen 1 – Select Implementations and Screen 3 – Implementation specific inputs are applicable. Submit to Sandbox takes different inputs for different implementations. There are no common inputs for this capability currently.	• CrowdStrike Falcon X Sandbox Integration • Security Incident Response Integration with Zscaler

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Capability	UX Frameworks Screens Applicable	Integrations Supported
	For example, when the Analyst selects Crowdstrike Falcon X Quick Scan, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux, and Zscaler, the inputs vary. Crowdstrike Falcon X Quick scan and Zscaler don't need further run time inputs. Crowdstrike Falcon X Windows 64 takes optional run time inputs that differs from Crowdstrike Falcon X Linux. So, these can be provided in screen 3 specifically against individual selected implementations as applicable.	
Publish to Watchlist	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for **Publish to Watchlist**. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	Crowdstrike Falcon Host
Allow/Block Request	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for **Allow/ Block Request**. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	• Palo Alto Network NGFW • Check Point NGFW • Security Incident Response Integration with Zscaler

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Capability	UX Frameworks Screens Applicable	Integrations Supported
Get Host Details	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for Get Host Details. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	• FireEye HX • Microsoft Defender for Endpoint
Get File	Screen 1 – Select Implementations and Screen 2 – Common Inputs are applicable. Get File takes file name, path as common inputs. After selecting one or more implementations and providing common inputs, the Security Analyst will be able to submit the action.	FireEye HX
Get Network Statistics	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for Get Network Statistics. So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	• FireEye HX • NetStat
Get Running Processes	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for Get Running Processes.	• FireEye HX • Carbon Black • System Command

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Capability	UX Frameworks Screens Applicable	Integrations Supported
	So, only screen 1 is presented to the Security Analyst to select one or more implementations. After selecting the implementations, the Security Analyst will be able to submit the action.	
Get Running Services	Only Screen 1 – Select Implementations is applicable. There are no common inputs or implementation specific inputs applicable for Get Running Services. So, only screen 1 is presented to the Analyst to select one or more implementations. After selecting the implementations, the Analyst will be able to submit the action.	FireEye HX
Isolate Host / Un-Isolate Host	Screen 1 – Select Implementations and Screen 3 – Implementation specific inputs are applicable. Isolate Host/Un-isolate Host takes different inputs for different implementations. There are no common inputs for this capability currently. For example, when the Analyst selects FireEye HX and Microsoft Defender for Endpoint, the inputs vary. FireEye HX doesn't need run time inputs. On the other hand Microsoft Defender takes inputs such as Isolation Type and Comments. So, these can be provided in screen 3 specifically against individual selected implementations as applicable.	• FireEye HX • Microsoft Defender Endpoint • Carbon Black

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Capability	UX Frameworks Screens Applicable	Integrations Supported
Run Additional Actions	Screen 1 – Select Implementations and Screen 3 – Implementation specific inputs are applicable. Run Additional Actions Host takes different inputs for different implementations. There are no common inputs for this capability currently. For example, when the Analyst selects FireEye HX Standard Investigative Details Script, FireEye HX Triage Acquisition and Crowdstrike Falcon Insight reg unload, the inputs vary. FireEye HX Standard Investigative Details Script and FireEye HX Triage Acquisition take Comments as the input that could be different for both. Crowdstrike Falcon Insight reg unload takes Subkey as the input. So, these can be provided in screen 3 specifically against individual selected implementations as applicable. **Note:** Currently supports only single selection of implementation. In future releases multi selection of implementation will be supported.	• FireEye HX • Microsoft Defender for Endpoint • Crowdstrike Falcon Insight

Unified Experience example

This example demonstrates the unified experience framework capabilities.

Example 1: Select implementations: Threat Lookup

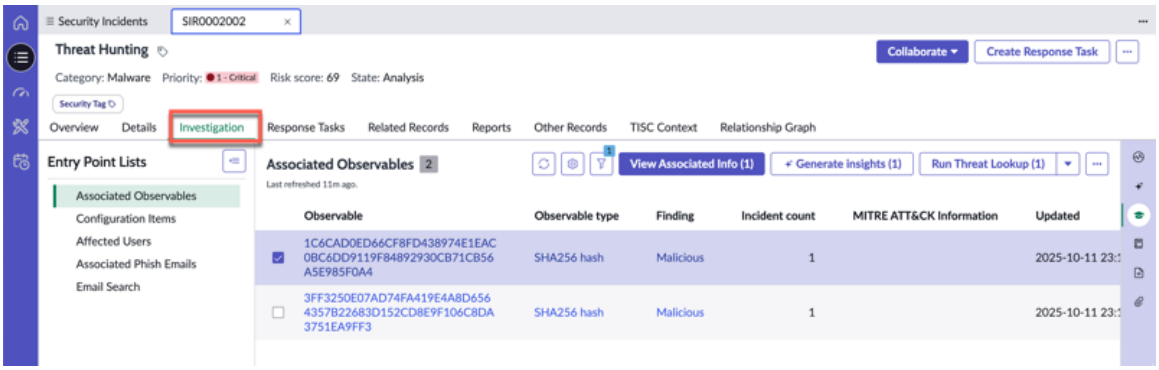
The example below demonstrates the implementation(s).

Example 1: Only Screen 1: Threat Look Up

You can perform **Run Threat Lookup** related integration capabilities action using the **Investigation** tab from the SIR Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. On the **Investigation** tab, navigate to the **Entry Points Lists** section displayed on the left side of the page.
2. Select any entry point and run the integration capability action.



Note: You can also navigate to the **Related Records** tab on the workspace to perform the integrations capabilities action.

Threat Look Up is one of the example which is described in detail on how to perform the integrations.

Select implementations

Select one or more implementations as applicable.

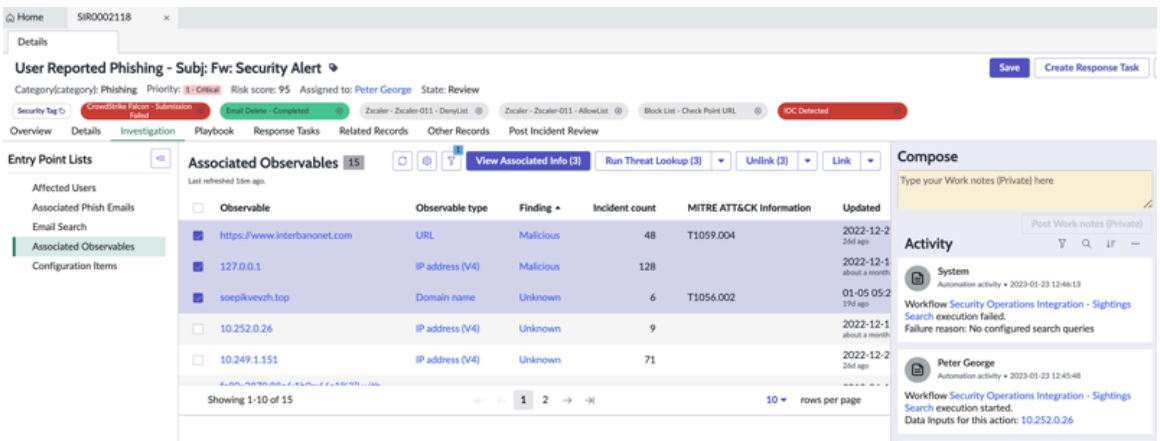
Before you begin

Role required: sn_si.analyst

The available implementations are listed. Select the implementation(s), after you select them only the supported records will be submitted against each selected implementation(s).

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.
3. Go to **Investigation** tab of the workspace.
   The investigation tab with the entry points lists is displayed.

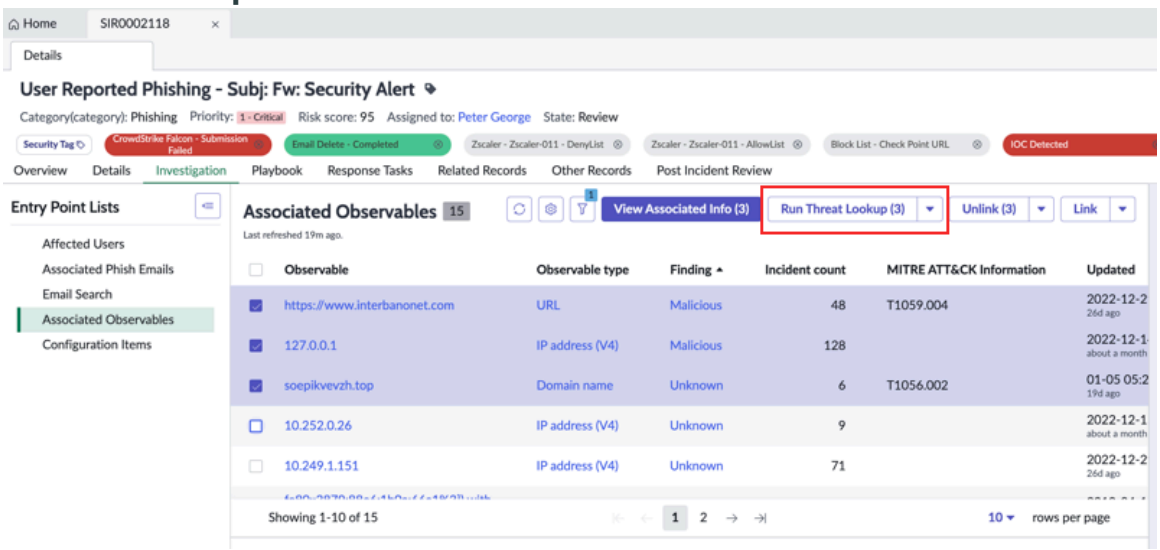


4. Select the associated observable from the entry point lists.
   For example, select **Associated Observables** related list. The corresponding observables records are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can select an implementation to perform a lookup on the selected observables, or you can perform the lookup by selecting all implementations.

Run Threat Lookup

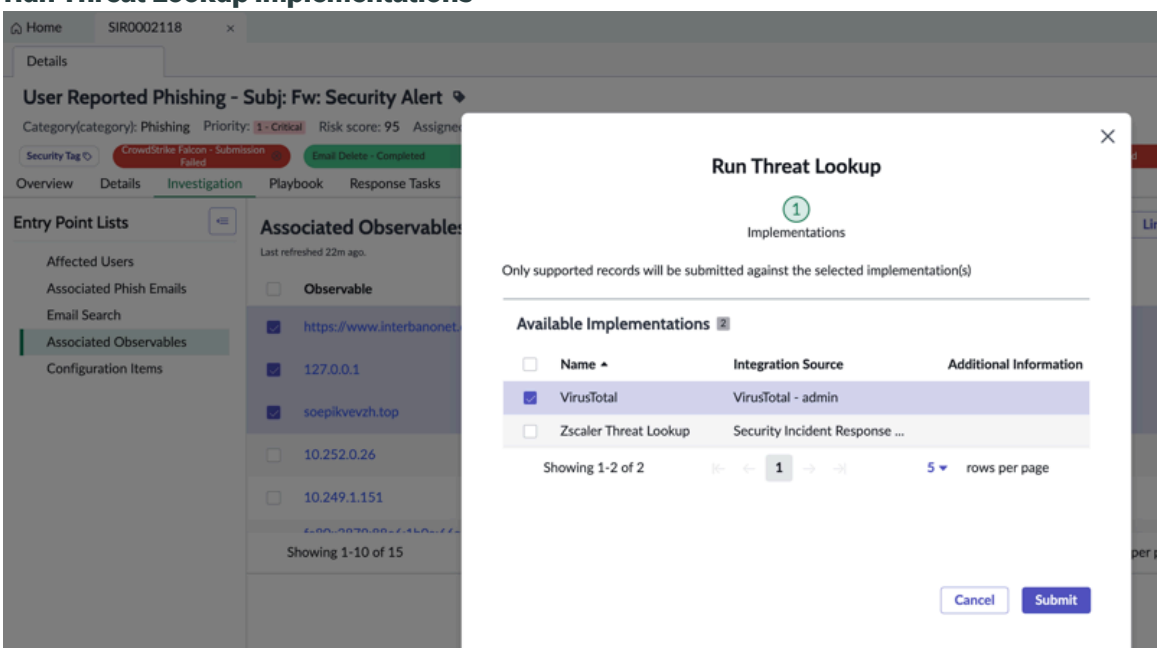


5. Select any observable check box that you wish to perform the threat lookup.
6. Navigate to the related lists actions drop down that is displayed on top of the related lists page.
7. Select **Run Threat Lookup** to perform threat intel related integration capabilities action.

Note: The Run Threat Lookups capability performs threat intelligence lookups to determine whether one or more observables are associated with any known security threats.

The **Run Threat Lookup Implementations** modal screen is displayed.

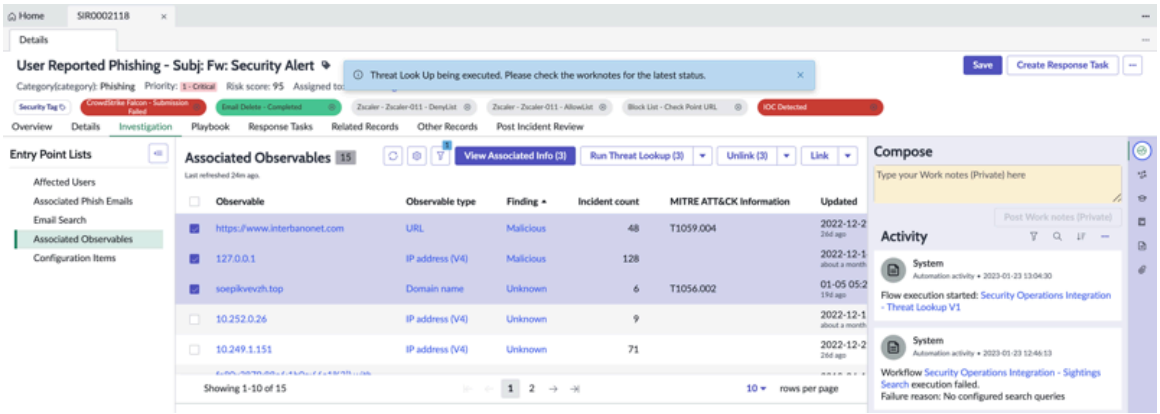
Run Threat Lookup Implementations



8. Select one or more implementations from the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Click **Submit**.
   After the selected records are submitted, a message is displayed that the lookup is being executed. Once the implementation is processed in the backend, the results are displayed in the **Threat Lookup Results** related list section. Also, the respective implementation activity is displayed in the **Activity** section. Two activities are displayed, one is when the implementation execution is started and the second one is when the execution is completed.



Note: The **Threat intel** related lists such as the associated observables related lists are displayed in the **Threat Lookup Results** section, and the **Sightings Search** related lists are displayed in the **Sightings Search Results** section under the Related Records.

Example 2: Common Inputs: Sighting Search

The example below demonstrates the common inputs capability action.

You can perform **Run Sighting Search** related integration capabilities action using the **Investigation** tab from the SIR Workspace.

1. On the **Investigation** tab, navigate to the **Entry Points Lists** section displayed on the left side of the page.
2. Select the respective entry point and run the integration capability action.

Note: You can also navigate to the **Related Records** tab on the workspace to perform the integrations capabilities action.

Add common inputs to an implementation

Add common run time inputs that apply for all the selected implementations as applicable.

Before you begin

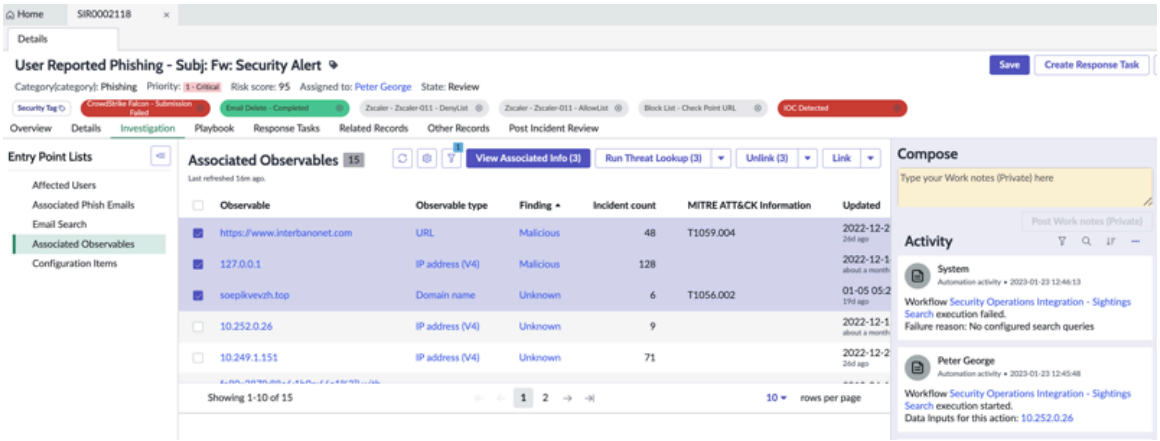
Role required: sn_si.analyst

The available implementations are listed. Select the implementation(s), after you select them only the supported records will be submitted against each selected implementation(s).

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.
3. Go to **Investigation** tab of the workspace.
   The investigation tab with the entry points lists is displayed.

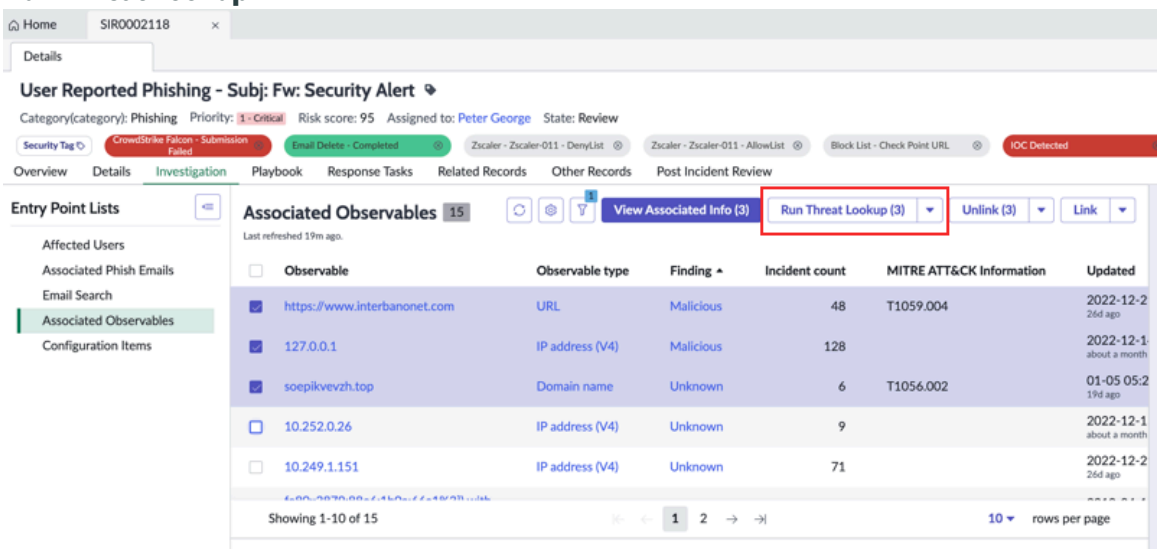
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Select the associated observable from the entry point lists.
   For example, select **Associated Observables** related list. The corresponding observables records are displayed.

   Note: You can select an implementation to perform a sighting search for the selected observables, or by selecting multiple implementations.

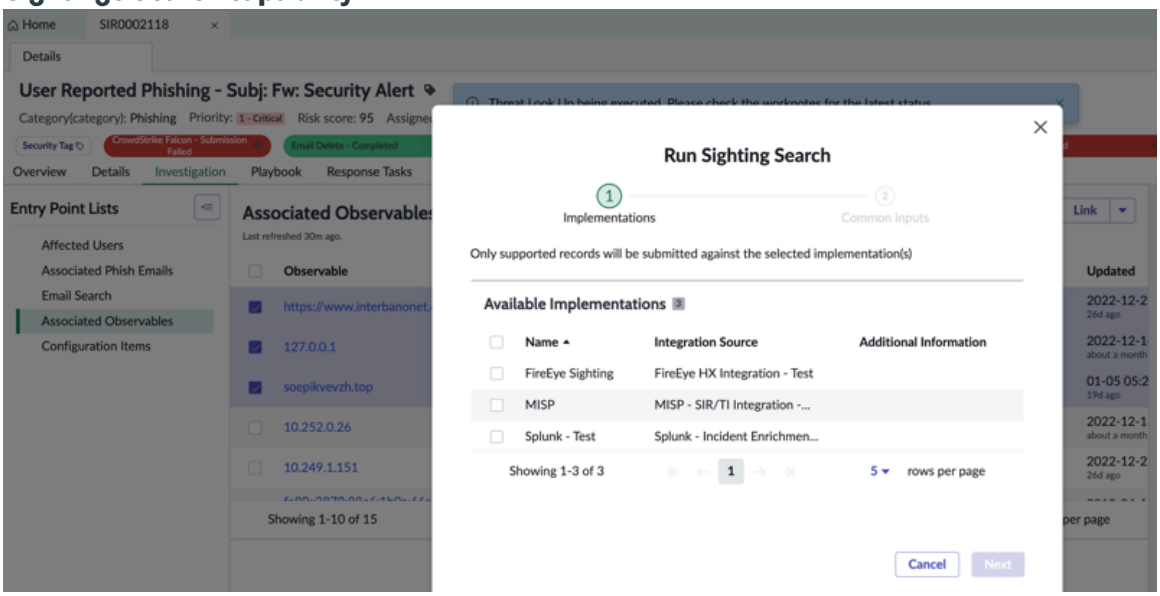
   Run Threat Lookup



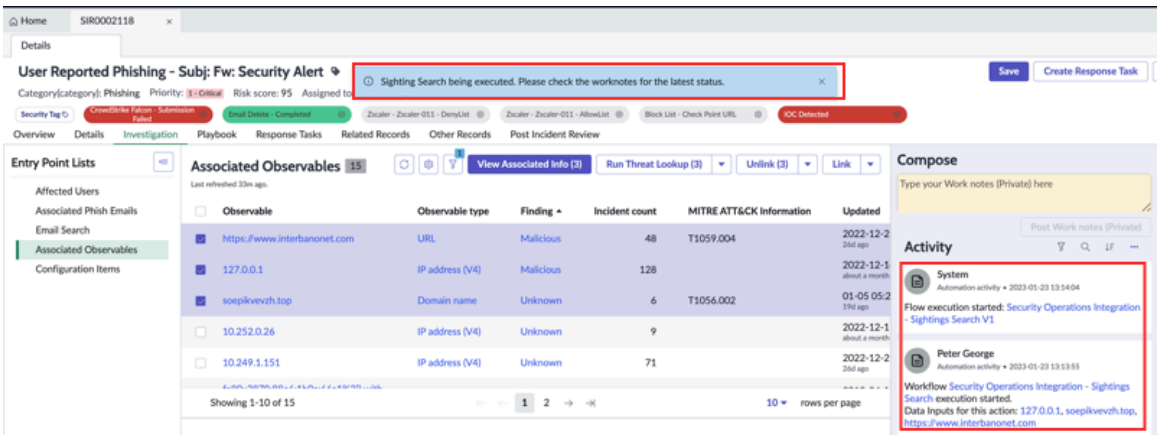
5. Select any observable check box that you wish to perform the threat lookup.
6. Select **Run Sighting Search** to perform email search.
   The Run Sighting Search Implementations modal dialogue box is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

An example that shows on how to add common runtime inputs by selecting Sightings Search capability



7. Select one or more implementations from the list.
8. Click **Next**.
   After the selected records are submitted, a message is displayed that the Sighting search is being requested. Once the implementation is processed in the backend, the results are displayed in the **Sighting Search** related list section. Also, the respective implementation activity is displayed in the Activity section. Two activities are displayed, one is when the implementation execution is started and the second one is when the execution is completed.
9. Select the common run time input value.
10. Click **Submit**.



After the selected records are submitted, a message is displayed that the Sighting search is being requested. Once the implementation is processed in the backend, the results are displayed in the **Sightings Search Results** related list section. Also, the respective implementation activity processing status is displayed in the **Activity** section.

Example 3: Add specific runtime details inputs to an implementation: Run Additional Actions

Add specific runtime details inputs to an implementation, Run Additional Actions.

You can perform **Run Additional Actions** related integration capabilities action using the **Investigation** tab from the SIR Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. On the **Investigation** tab, navigate to the **Entry Points Lists** section displayed on the left side of the page.
2. Select the respective entry point and run the integration capability action.

> **Note:** You can also navigate to the **Related Records** tab on the workspace to perform the integrations capabilities action.

Add specific inputs to an implementation

Add specific run time inputs for each of the selected implementation as applicable.

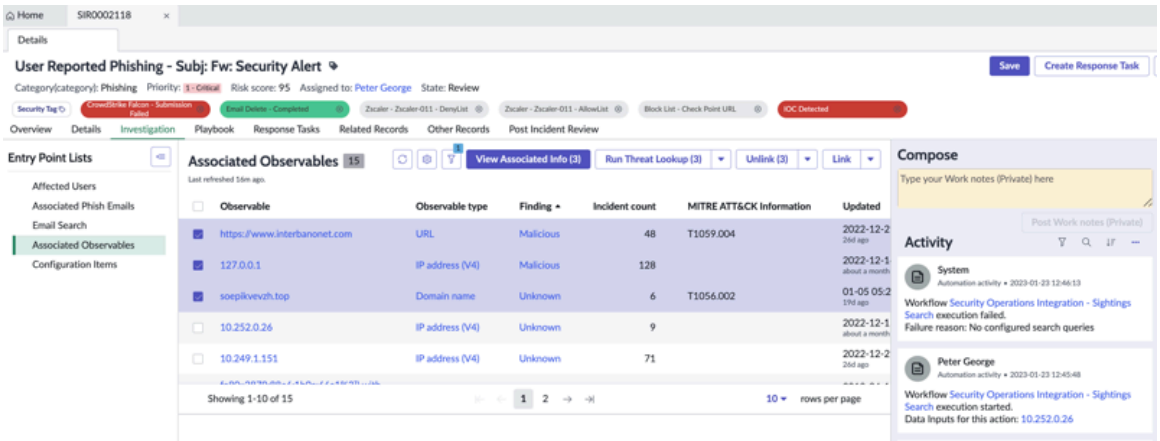
Before you begin

Role required: sn_si.analyst

The available implementations are listed. Select the implementation(s), after you select them only the supported records will be submitted against each selected implementation(s).

Procedure

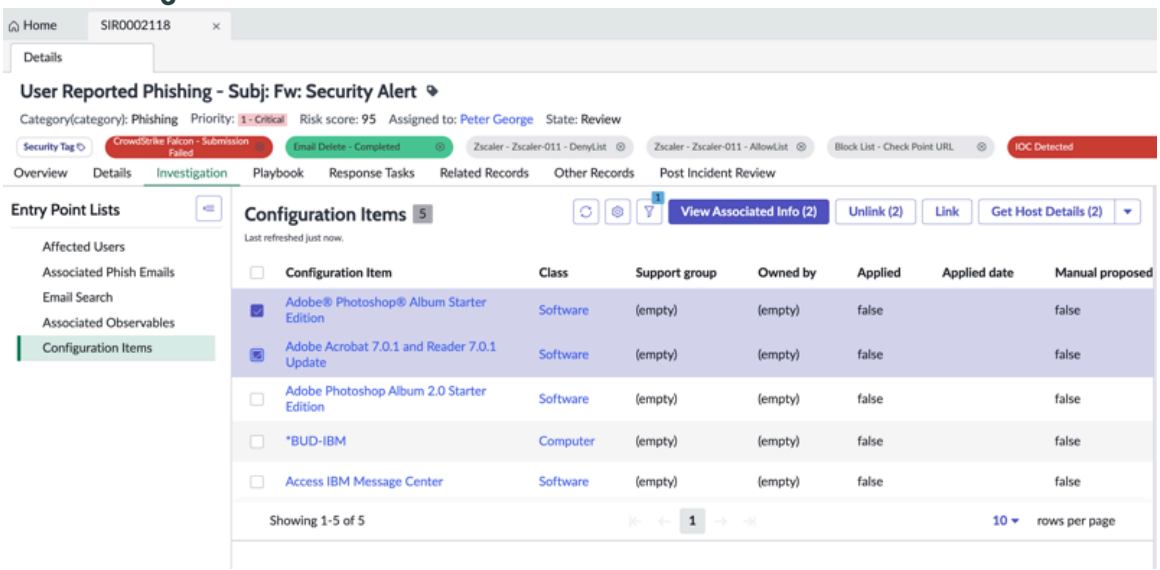
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.
3. Go to **Investigation** tab of the workspace.
   The investigation tab with the entry points lists is displayed.



4. Select the configuration item from the entry point list.
   For example, select **configuration Item** entry point list. The corresponding configuration items records are displayed.

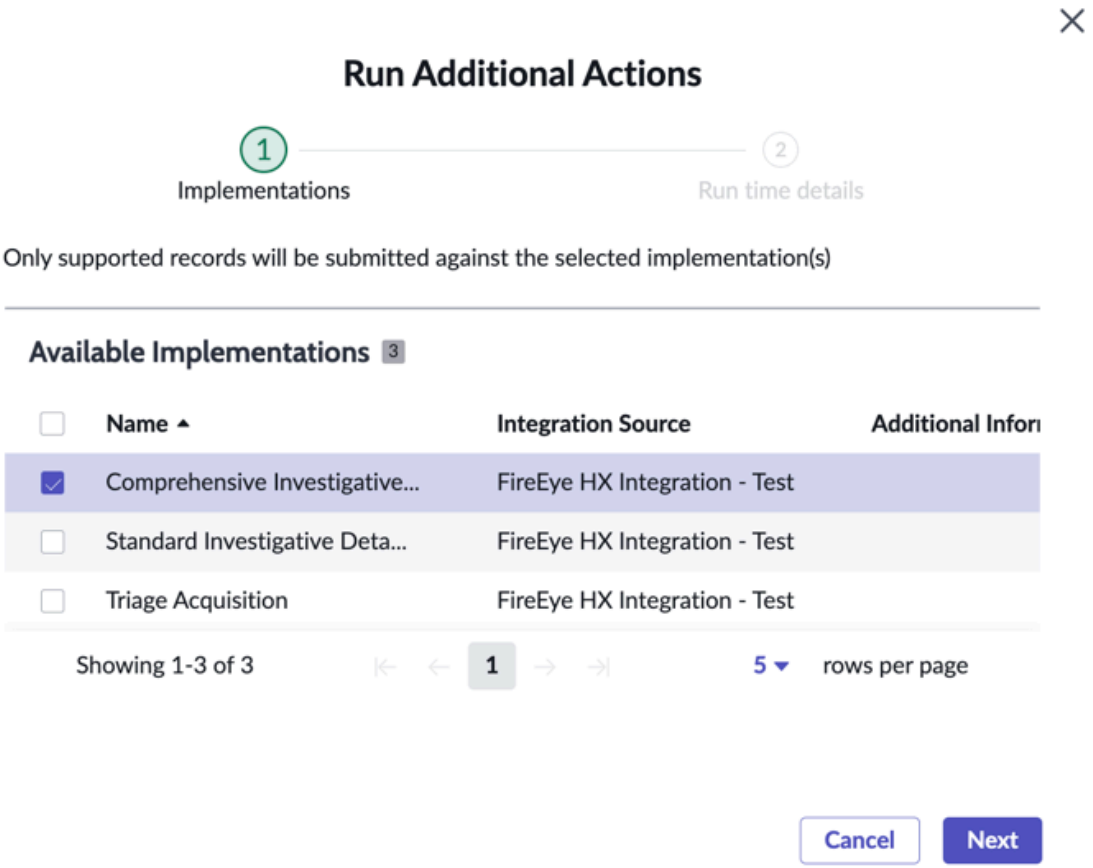
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select Configuration Item

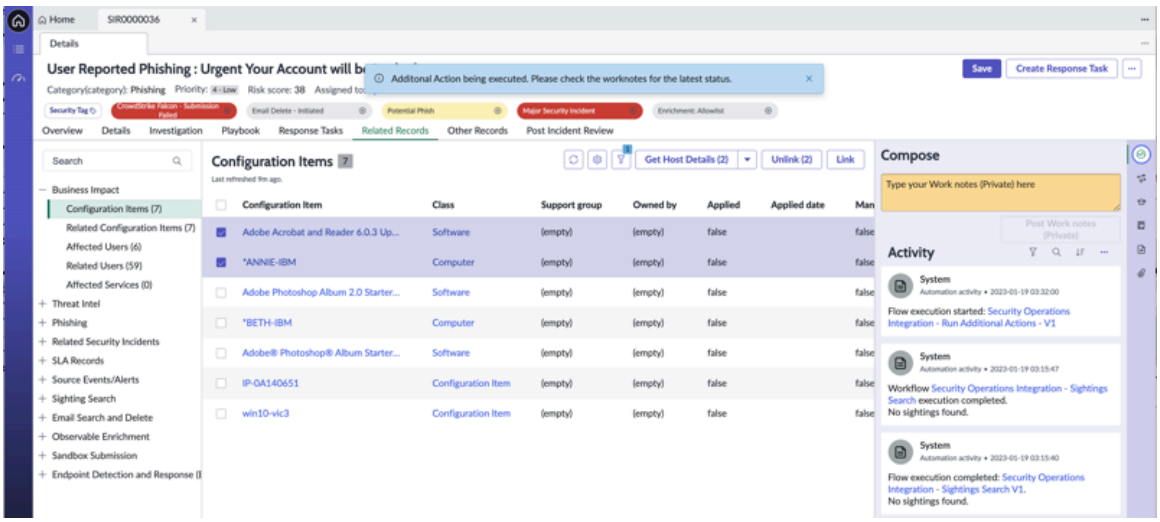


5. Select any **Configuration Item**.
6. Navigate to the related lists drop down that is displayed on top of the page.
   For security incident configuration item (CI), the drop down lists contains the following list of capabilities actions. The listed CI actions collect the results and store them as enrichment data on a security incident:
   - Get file: This capability performs the action to get files with a specific hash value or a file name.
   - Isolate Host: This capability restricts system connections to other devices.
   - Get Host Details: This capability retrieves the host details, details of logged-in users, and other enrichment capabilities.
   - Run Additional Actions: This capability runs the additional actions beyond the standard actions.
   - Get Network Statistics: This capability retrieves the network statistics for an affected resource.
   - Get Running Process: This capability retrieves a list of running processes on a configuration item (CI) from a host.
   - Get Logged on Users: This capability gathers the data of logged on users and relates it to the security incident.
7. Select **Run Additional Actions** to perform threat intel related integration capabilities action.
   The Run Additional Implementations modal dialogue box is displayed.
8. Select one or more implementations from the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Click **Next**.
   You will now be moved to the next step to add the run time details.
10. Enter a comment to associate with the action.
11. Click **Submit**.



After the selected records are submitted, a message is displayed that the Additional Action request is being executed. Also, the respective implementation action progress is displayed in the **Activity** section.

12. View the results from the EDR related list section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

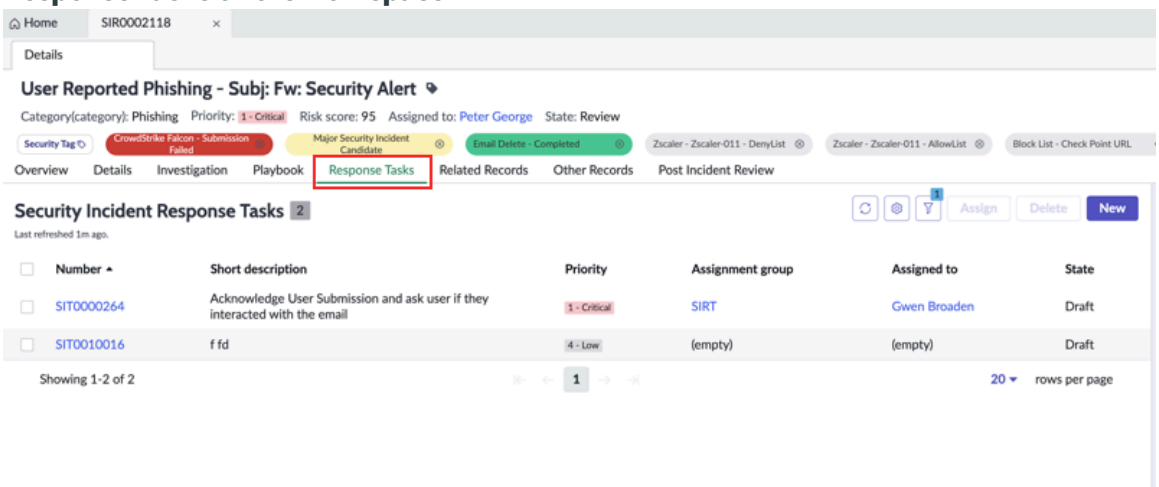
Security Incident Response Tasks

All the response tasks associated with a security incident are displayed within the Response Tasks section.

The analyst will be able to:

- create a new response task
- assign response tasks to self or others
- delete response tasks

Response Tasks on the workspace



Note: To make any quick edits to the response tasks. Select the response task and a list of response tasks are displayed, select the record and make changes and save the response task.

Create a Response Task

Create response tasks to track separate actions to be performed to respond to the security issue.

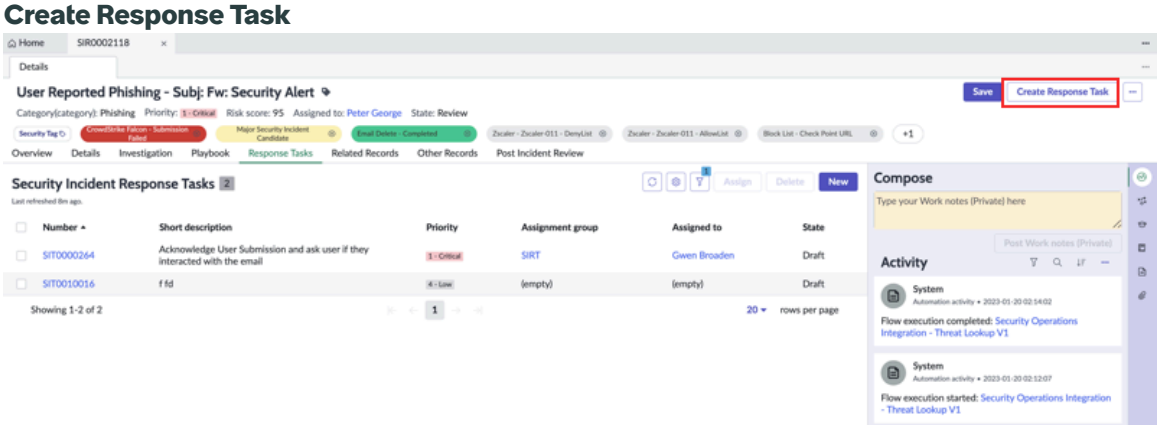
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Click the **Create Response Task** from the UI actions.

Create Response Task

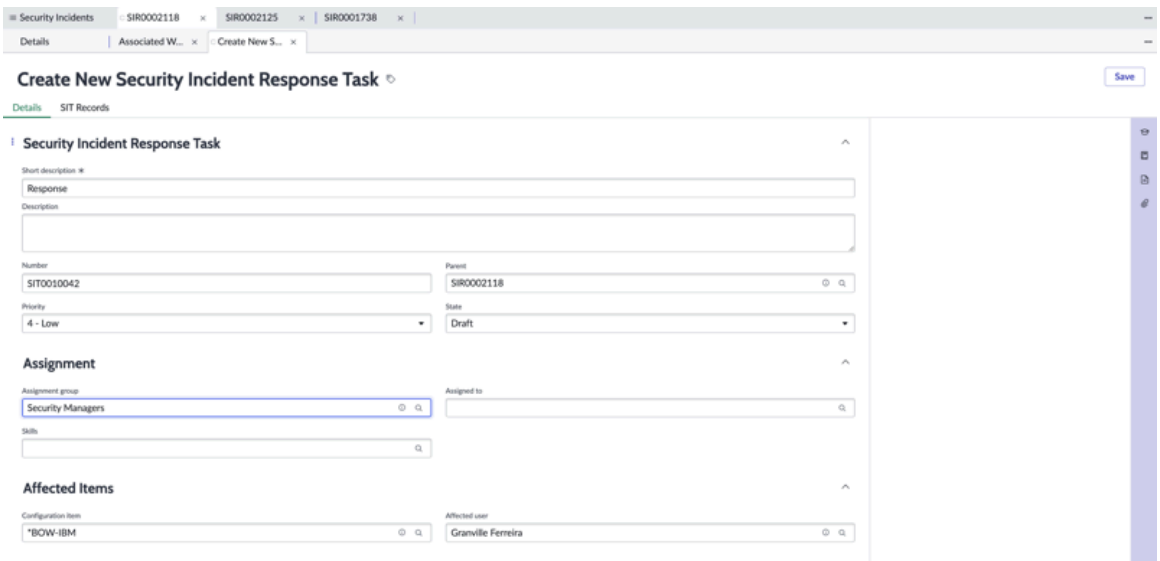


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Fill in the fields on the form, as appropriate.

Security incident

Field	Description
Short description	A description of the Security Incident Response task.
Description	A description for the selected task.
Number	Unique number that is automatically generated for a security incident.
Parent	The number of the related security incident.
Priority	The priority used to determine when this task is performed.
State	The current state of the security response task. By default, the initial state is **Draft**.
Assignment group	The assignment group from which the assigned worker is selected.
Assigned to	The individual assigned to perform the task.
Skills	The skill required to perform this task. Search from the lookup and select the skill required.
Affected Items	The affected items by the security issue.
Configuration Item	The configuration item affected by the security issue.
Affected User	The person affected by the security issue.



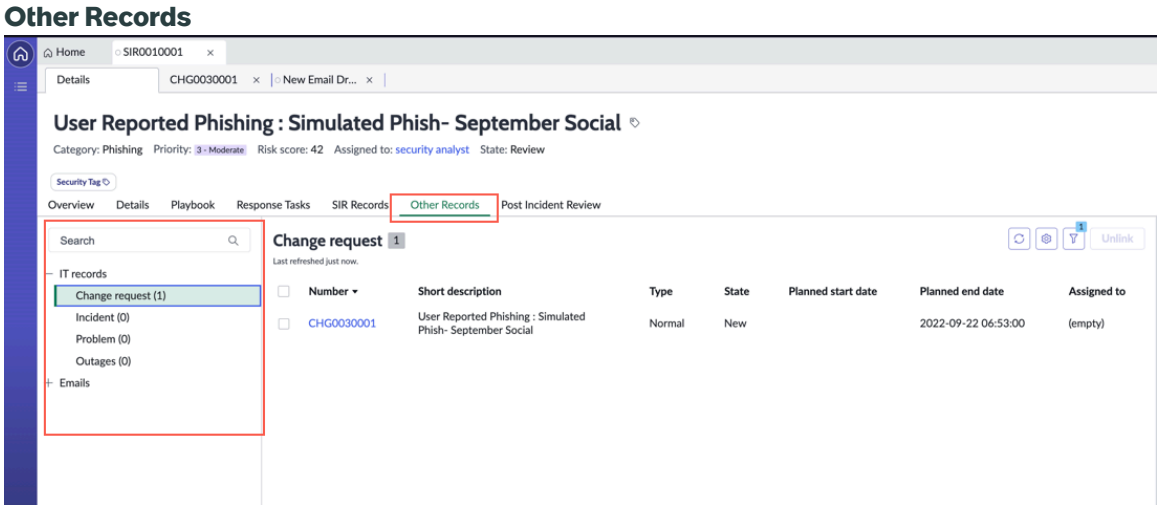
4. Click **Save**.
   The new Response Task (SIT) gets created.

Security Incident Response Other Records

This section displays the other records such as IT related records and email records. Under IT records, Incident, Change Request, Problem and Outages are displayed.

Under Email, Draft, Sent Emails and Received Emails are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Create an incident

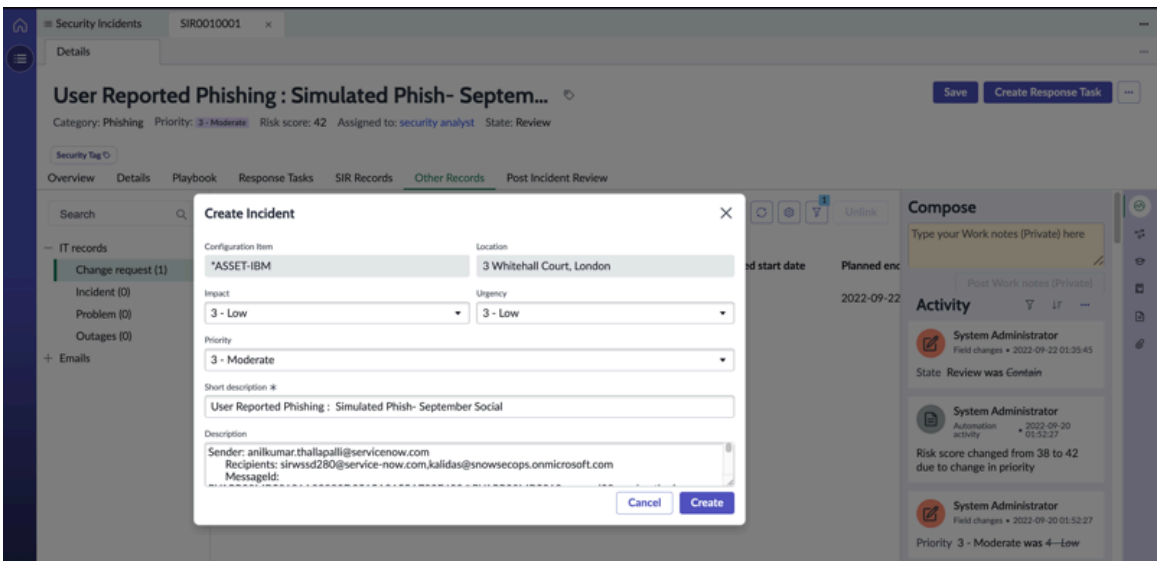
Create an incident within a security incident.

Before you begin

Role required: sn_si.analyst.

Procedure

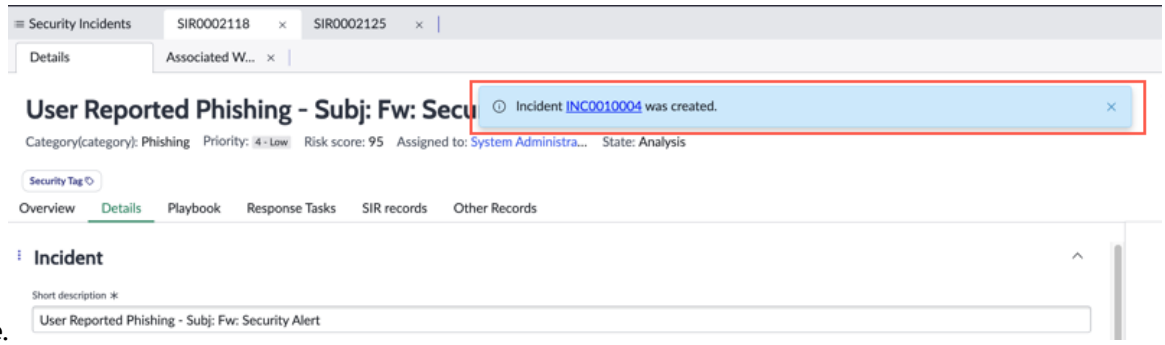
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any incident record.
3. Click **Create Incident**.



4. Enter the details such as Configuration Item, Impact, Urgency, Location, Priority, and Short Description.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Create**.



6. An incident gets created.

Link multiple ITSM incidents, problems or change requests to a security incident

Link related multiple IT Service Management (ITSM) incidents, problems or change requests to a security incident.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select the Security Incidents icon .
3. Open the incident record.
4. Select the **Other Records** tab.
5. Under **IT records**, select **Incident** or **Problems** or **Change Requests**.
6. Select **Link**.
7. Select the ITSM record you want to link to the selected security incident.
8. Select **Link**.

Result

The selected ITSM records are listed in the IT records section of the selected security incident record.

Create a problem task

Create a problem task.

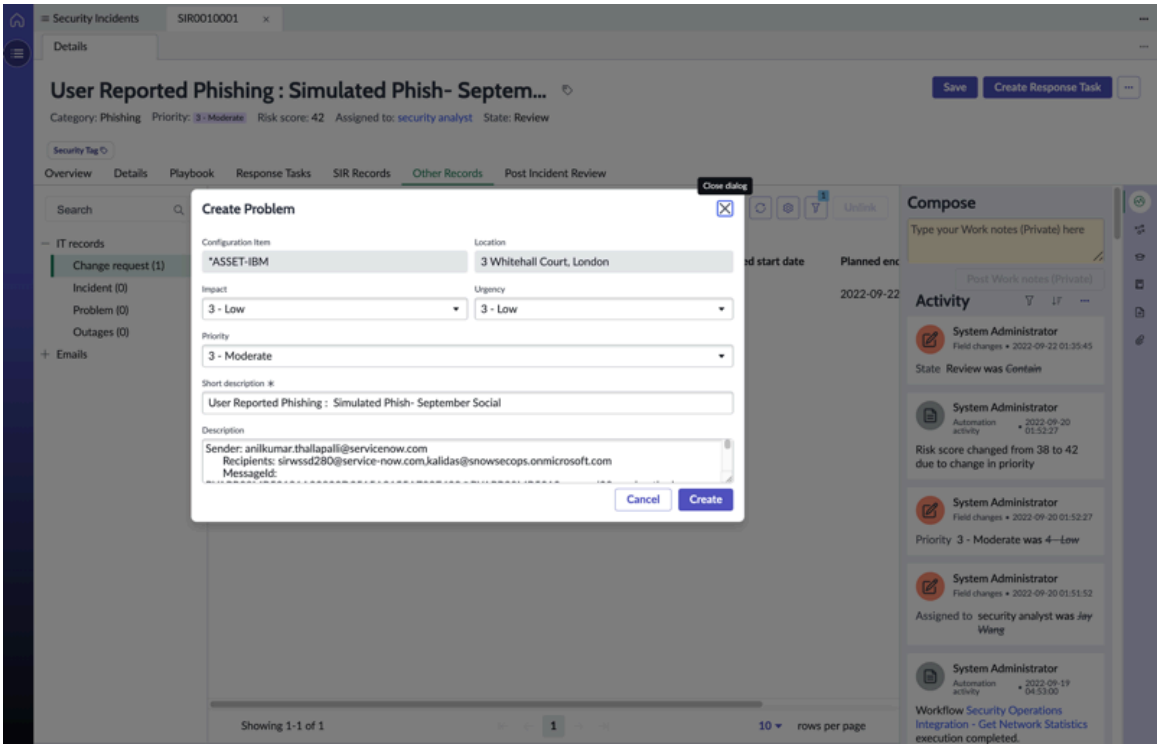
Before you begin

Role required: sn_si.analyst

Procedure

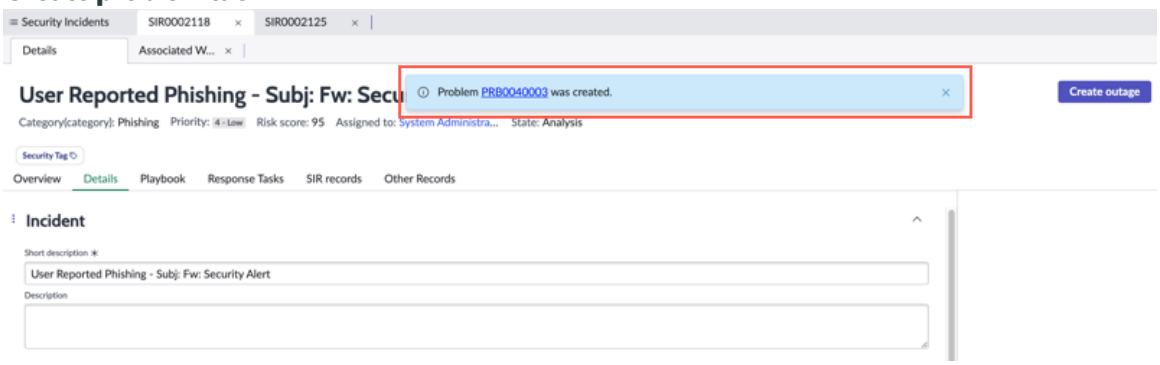
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any incident record.
3. Click **Create Problem**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Fill in the details such as Configuration Item, Location, Impact, Urgency, Priority, and Short description.
5. Click **Create**.

Create problem task



6. A problem task gets created.

Create a change request

Create a change request.

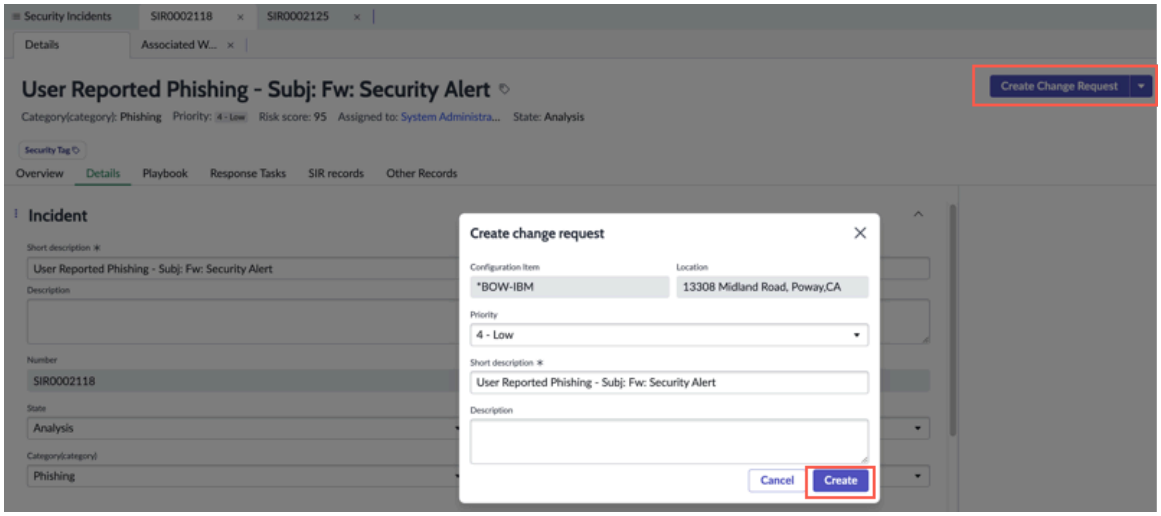
Before you begin

Role required: sn_si.analyst.

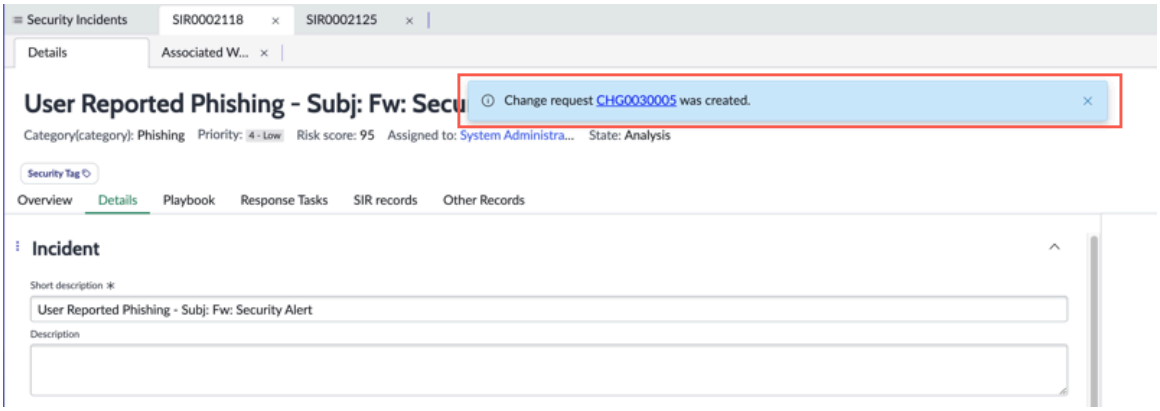
Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any incident record.
3. Click **Create Change Request**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter the details such as Configuration Item, Location, Priority, and Short description.
5. Click **Create**.



6. A change request gets created.

Create outage

Crete an outage from an incident to track the down time of a configuration item.

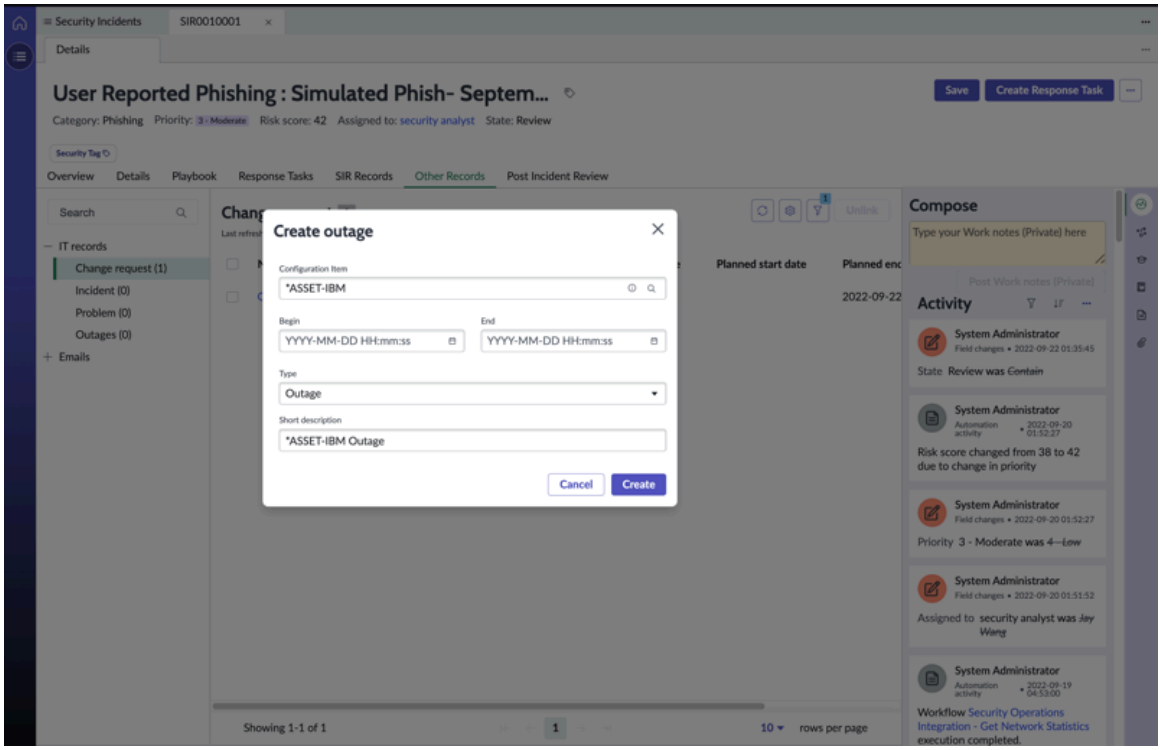
Before you begin

Role required: sn_si.analyst

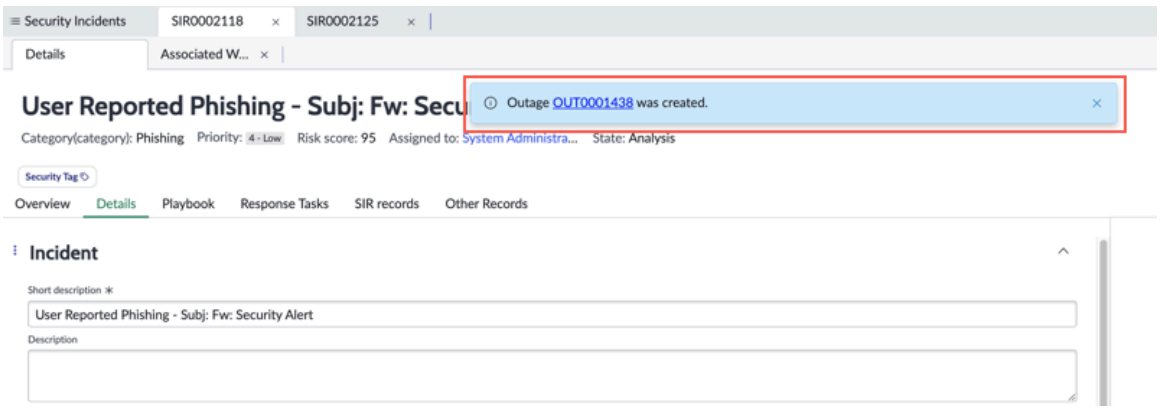
Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any incident record.
3. Click **Create outage**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter the details such as Configuration Item, Begin date, End date, Type, and Short description.
5. Click **Create**.



Compose Emails

As an analyst, you can compose emails directly from security incidents.

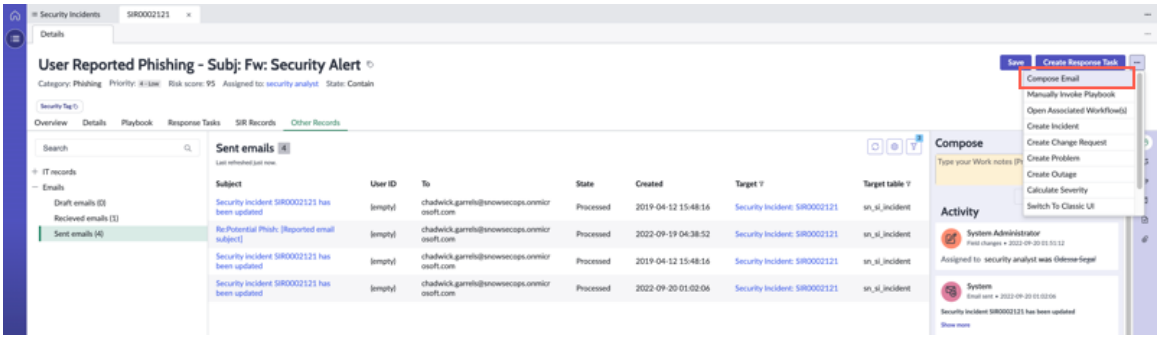
Before you begin

Role required: sn_si.analyst

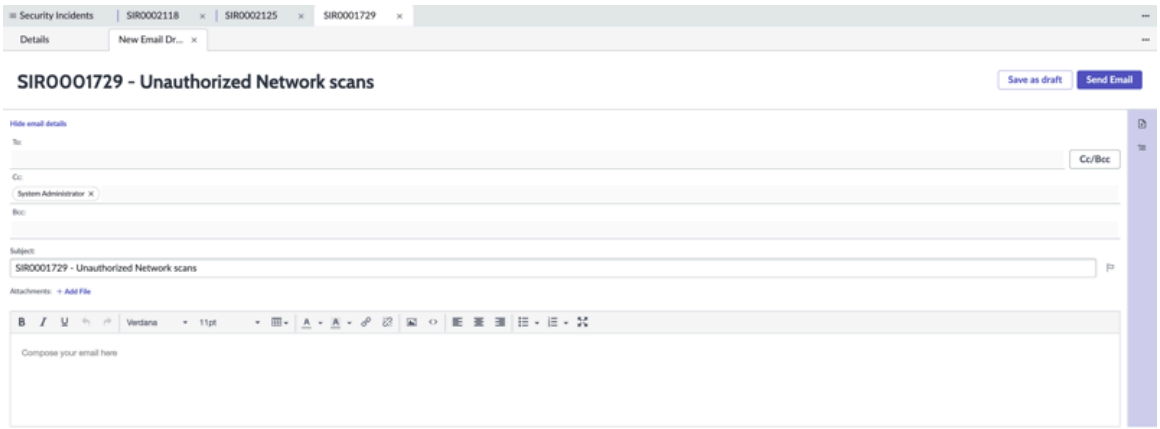
Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select and open the incident for which you want to compose an email.
3. Click the overflow and select **Compose Email**.

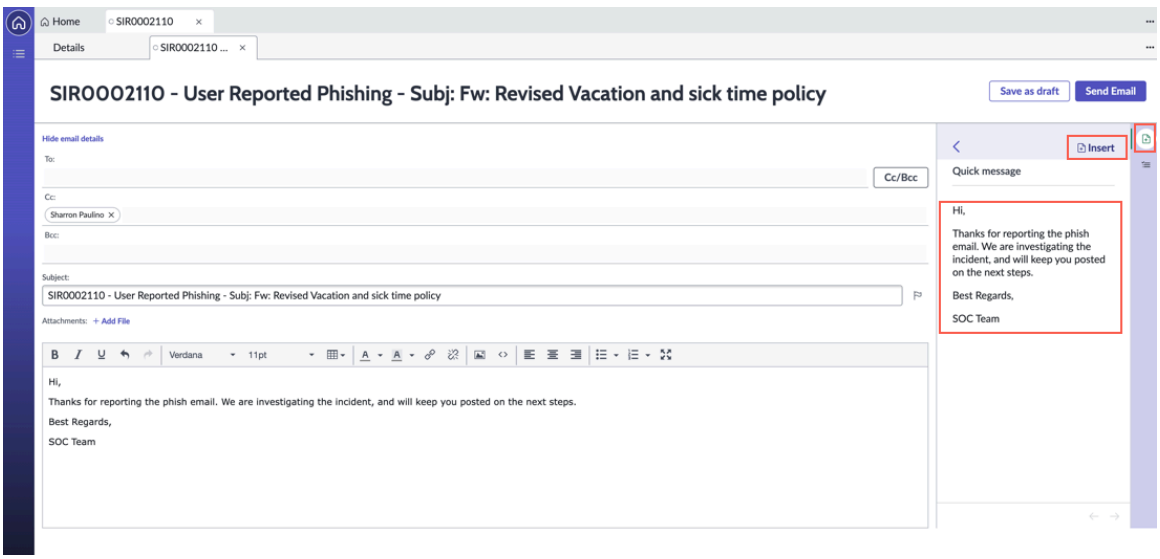
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter the **To** and **CC** field.



5. **Add** attachments, if any.
6. Within the Email form, click **Quick Messages** to view the quick messages which is displayed on the right side of the **Compose Emails** section.
   The available quick messages are displayed. Select the message and click **Insert**. The messages gets inserted in the body of the email.



7. Compose your email and click **Send Email**.

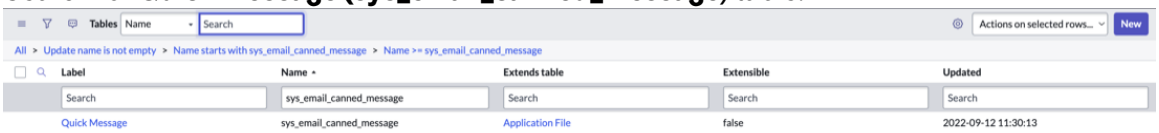
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can save an email as a draft. These draft emails will be available under the Other records tab.

How to configure Quick Messages:

a. Navigate to **System Definitions** > **Tables**.

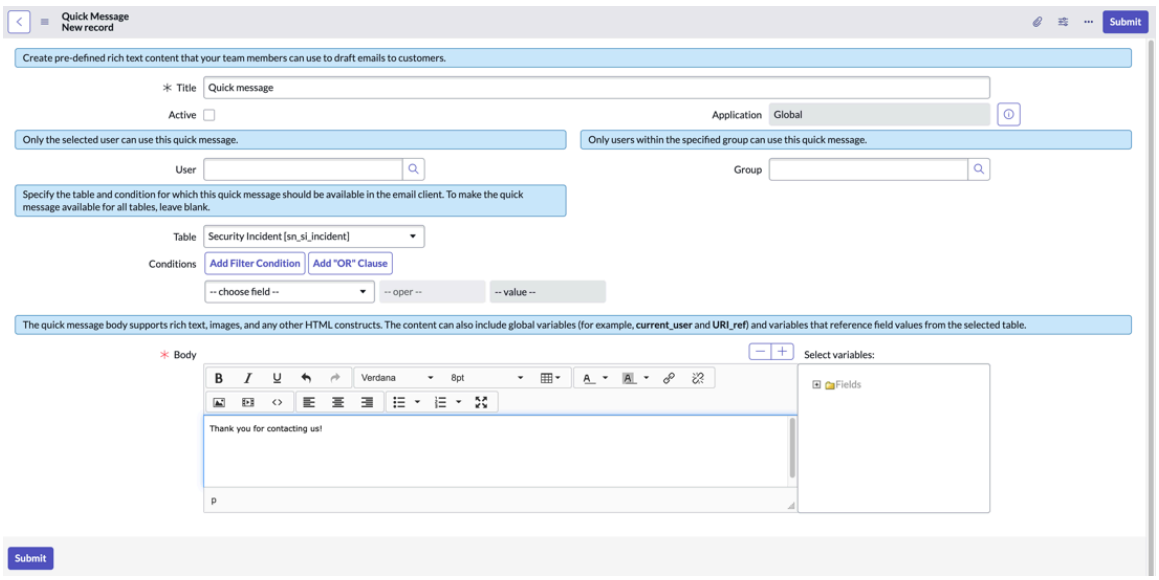
b. Search for **Quick Message (sys_email_canned_message)** table.



c. Go to **Related Links** > **Show List**.

d. Create **New**.

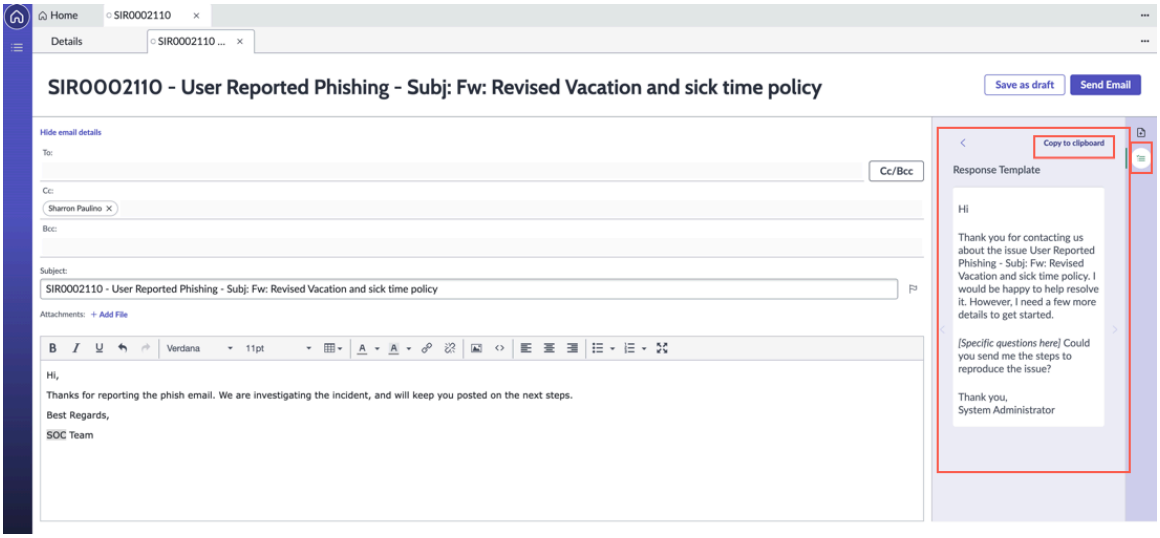
e. Enter the **Title**, **body of the message**, select the **Table: Security Incident (sn_si_incident)** and **Active** check box.



f. Click **Submit**.
After a new entry is created within the table, the quick message appears in the contextual menu.

8. Click **Templates** to add any template if required.
9. Select the **Response Template** and click **Copy to clipboard** and apply the template, if required.

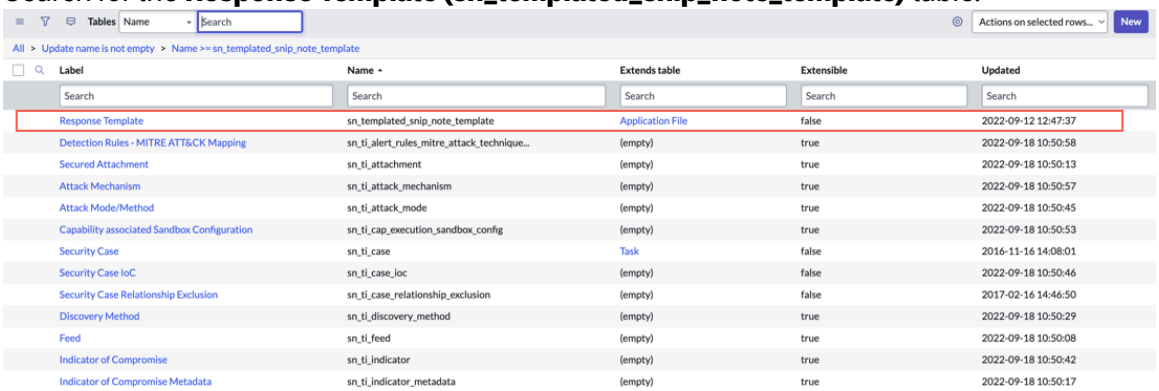
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



How to configure Response Templates:

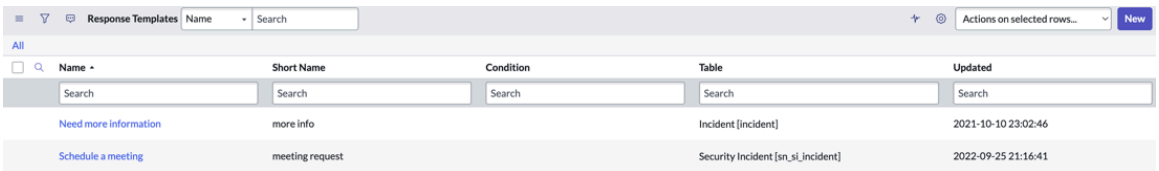
a. Navigate to **System Definitions** > **Tables**.

b. Search for the **Response Template (sn_templated_snip_note_template)** table.



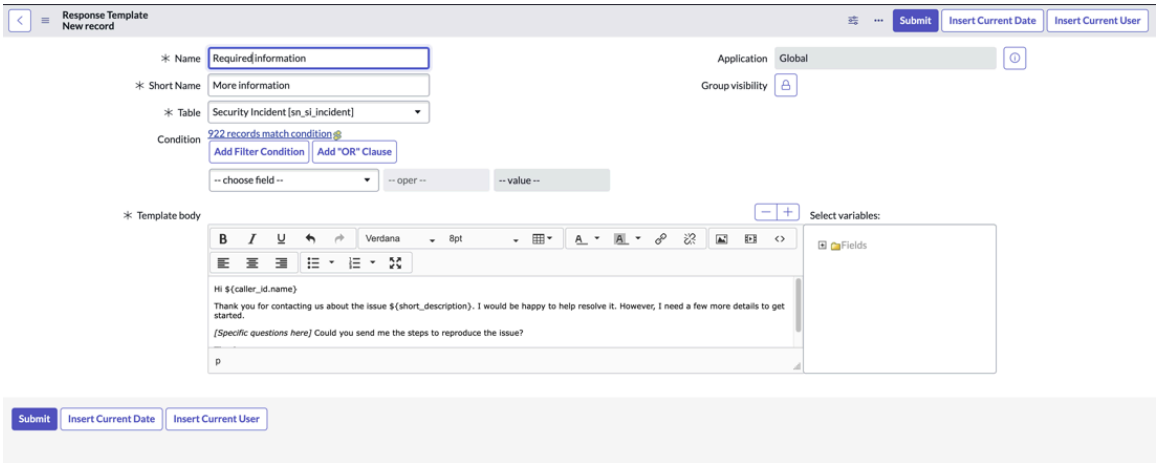
c. Go to **Related Links** > **Show List**.

d. Create **New**.



e. Enter the **Name**, **Short Name**, select the **Table: Security Incident (sn_si_incident)** and **Template body**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



f. Click **Submit**.
After a new entry is created within the table, the new template appears in the contextual menu.

Security Incident Response Post Incident Review

Post incident review appears when an incident is moved to a Review state.

For more detailed information on the conducting the post incident activities, see Post incident review report

The Post incident review consists of the following sections:

1. Assessments
2. Reports

From the Security Incident Response workspace, you will be able to request and take assessments using these new two UI actions.

Name	Description
Assessments	Assessment displays all the assessments that are associated with the security incident other assessments. The analyst will be able to take assessments and request assessments. • **Take assessments**: Click on **Take assessments** to take the assessments (if applicable) and complete the assessment. Before completing the assessment, the security incident state is Ready to take and Due date of the incident is indicated in Red. • Request assessments: Click on **Request assessment** for any additional assessments

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	and you can add the new users whom you want to request. **Note:** Users who had already requested will not appear in this section. Any assessment for this incident has been configured based on the conditions set on the Post Incident Review, it be either mandatory or optional.
Reports	Modify the runtime configurations and generate the report. Select the Report instance, modify the filters and save the report. The analyst can preview and download the PIR report.

Edit Related Records in list view

Edit related records for a security incident directly from the Related Records list view. This allows security analysts to quickly update the records without leaving their current context.

Before you begin

Use cases:

- Analyst can update the severity and confidence levels of multiple IP address observables directly within the incident workspace.
- Analyst can manage multiple findings by updating status and assignee inline from the workspace view. This enhances SOC team coordination during active investigations.
- Analyst can enrich observables with updated descriptions and attributes as new information becomes available instantly.

Limitations:

- Complex field dependencies may still require accessing the full form for accurate updates.
- Certain advanced field types, such as **Modified**, are not supported for inline editing.
- Bulk editing is restricted for non-compatible field types and logically grouped items.

Note: The following are the example steps for updating the associated observables records of a security incident. You can refer this to update any record in the **Related Records** tab.

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident.
3. Select the **Related Records** tab.
4. Select **Threat Intel** and then select **Associated Observables**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select the fields to update.
6. Update the value of the fields as required.

Result
The updated field values are saved.

TISC integration within SIR Workspace

The following section includes information about the Threat Intelligence Security Center integration from within the SIR workspace context.

Send data from SIR Workspace to TISC

Learn how the data is collaborated and shared between the Threat Intelligence Security Center (TISC) and Security Incident Response (SIR) Workspaces by following the procedures explained in the following sections.

System properties to send data

Review the system properties for TISC integrations to combine with SIRW. You can configure these properties to control how both applications manages the integrations.

Key considerations

The system properties for TISC integrations provide advanced configuration options on how the application handles observables and enrichments.

1. To set TISC integrations system properties within SIRW, navigate to the **System Properties** for Threat Intelligence and access the [sys_properties] table.
2. The system properties control and handles the behavior of each individual data push operation.
3. When the property is enabled then the data is pushed automatically when the observables or enrichments data is generated in the SIR Workspace.
4. If the property is disabled, then the data is pushed manually and allows the users to push data using the UI actions from the SIR Workspace.

The following lists shows the system properties for TISC - SIR integration:

- Push observables data both automatically and manually from SIR: Enable sn_ti.allow_observable_and_enrichment_records_push property to push the data either automatically or manual. If disabled, this property will disable both automatic and manual mode for all the data push from SIR.
- Push threat lookup results: Enable this sn_ti.automatic_push_threat_lookup_results system property to push threat lookup data automatically to TISC. If disabled, security analysts can still push the threat lookup data manually.
- Push sighting search results to TISC: Enable sn_ti.automatic_push_sighting_results_to_tisc this system property to push sighting search data automatically to TISC. If disabled, security analysts can still push the sighting search data manually.
- Push observables: Enable sn_ti.automatic_push_observable_to_tisc this system property to push observables data automatically to TISC. If disabled, security analysts can still push the observables data manually.
- Push enrichment results: Enable sn_ti.automatic_push_enichment_results this system property to push enrichment results data automatically to TISC. If disabled, security analysts can still push the enrichment results data manually.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add security incident to TISC case

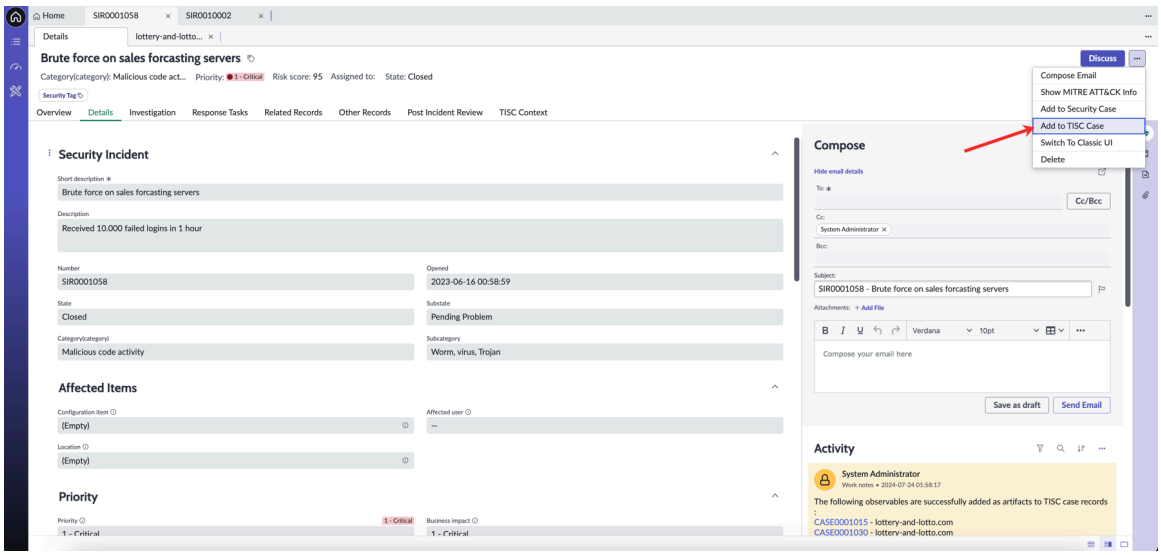
Add security incidents to TISC case records.

Before you begin

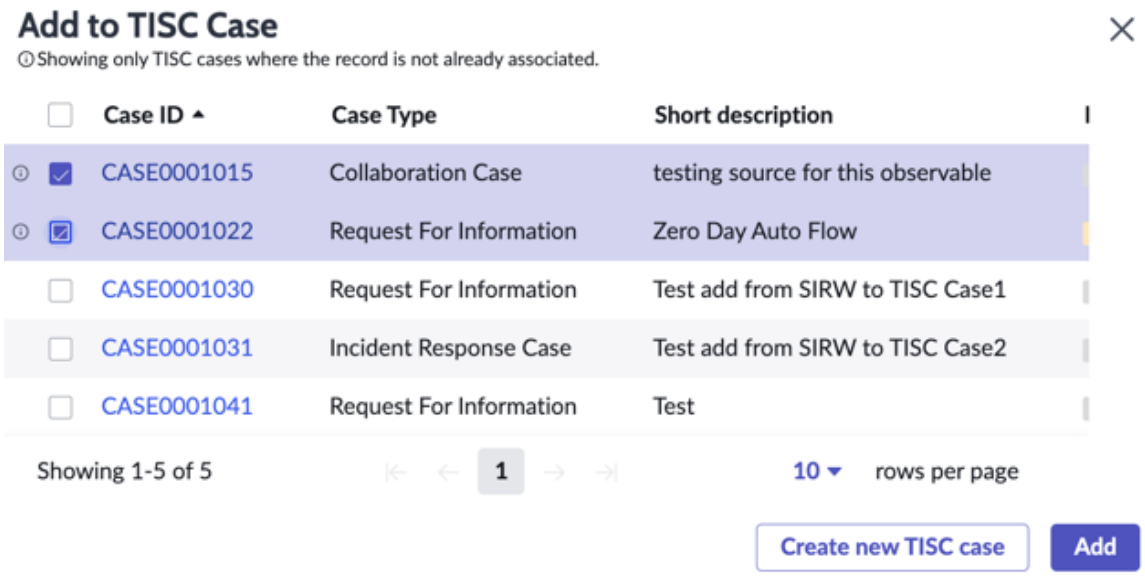
Role required: sn_si.analyst, sn_sec_tisc.case_write

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **All**.
2. Locate and open any specific security incident that you are investigating.
   This can also be done by searching for the incident ID or browsing from Quick Filters section or filtering through incident state.
3. Click on **More actions** icon.
4. Click **Add to TISC Case** action.
   Add to TISC Case dialog box displays and this only shows those TISC cases where the incident is not already associated.



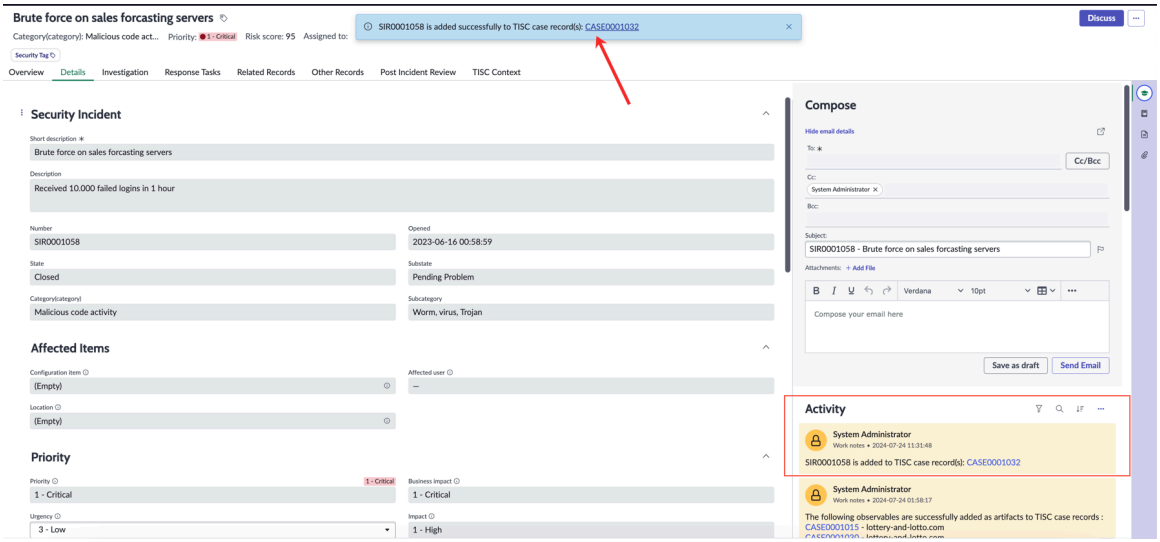
5. Select the case(s) from the **Add to Case** dialog box.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Create a new TISC case if there no case records. For more information on how to create case(s), see Creating cases using Threat Analyst Workbench.

6. Click **Add**.



7. Click the Case record to view the case in TISC from the information message displayed or from the **Activity** stream.

Note: To view the linked security incidents, click on the particular case record from the security incident **Activity** stream. By clicking on this will take you to the case record in TISC workspace and the security incidents will get added under **Artifacts** tab of the Case Management module.

Add observables to TISC Case

Add observables to TISC case records.

Before you begin

Role required: sn_si.analyst, sn_sec_tisc.case_write

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **All**.
2. Locate and open any specific security incident that you are investigating.
   This can also be done by searching for the incident ID or browsing from Quick Filters section or filtering through incident state.
3. Click on the **Related Records** tab on the workspace.
   You can perform the action of adding observables to TISC case(s) using various tabs from the Security Incident Response Workspace.

Note: You can navigate to the

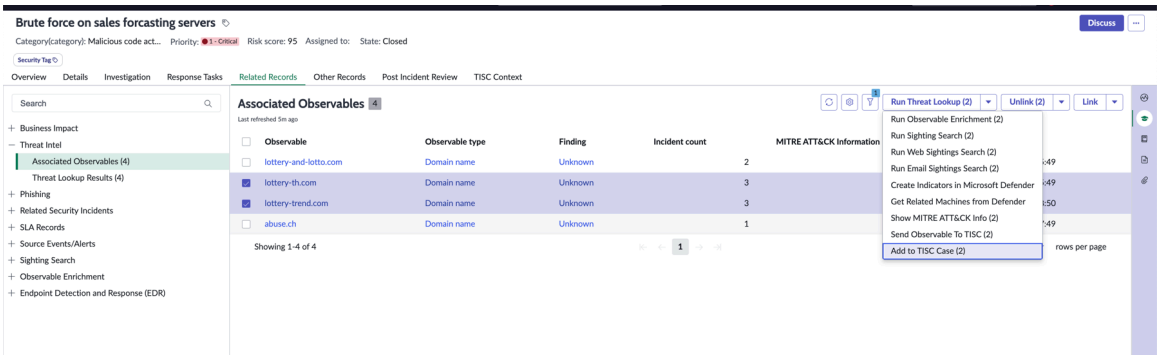
- Observables details page from the Related Records tab.
- **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to add observables to TISC case.

4. For example, select **Threat Intel** > **Associated Observables**.
5. Select one or multiple observable(s) to add the selected observables to case records.

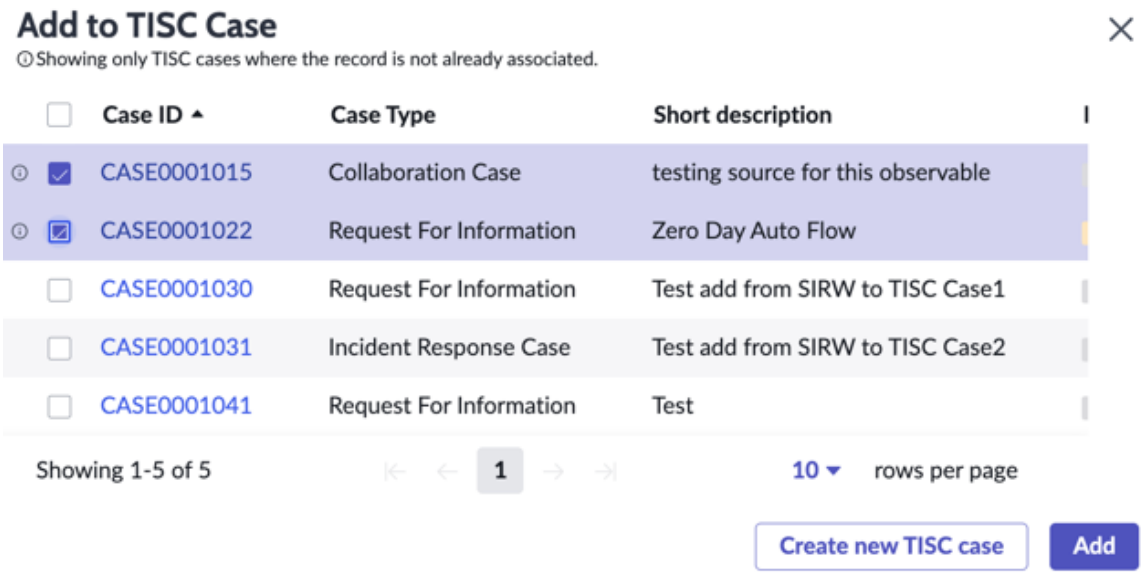
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can also click on any of the Observable record and it opens Observables details page in a different tab and you can add case records from here by clicking on Add to TISC Case.

6. Click the **Capability actions** split button.
7. Select **Add to TISC Case**.



8. Select the case(s) from the **Add to Case** dialog box.



Note: Create a new TISC case if there no case records. For more information on how to create case(s), see Creating cases using Threat Analyst Workbench.

9. Click **Add**.
10. Click the Case record to view the case in TISC from the information message displayed or from the **Activity** stream.

Note: If the observable does not have a corresponding TISC Observable, then the selected observable in SIR workspace will be sent to TISC automatically and will subsequently gets added to the selected TISC case record(s). To view the linked observables, click on the particular case record from the **Activity** stream. By clicking on this will take you to the case record in TISC workspace and the observables will get added under **Artifacts** tab of the Case Management module.

Result

You have successfully send the observables data to Threat Intelligence Security Center case management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Send Observables to TISC

Using this feature the security analyst can push the observables data from SIR to TISC. Using the TISC Context, you can check if the observables are present in TISC, if not security analyst can push the data whenever required.

Before you begin

Role required: sn_si.analyst

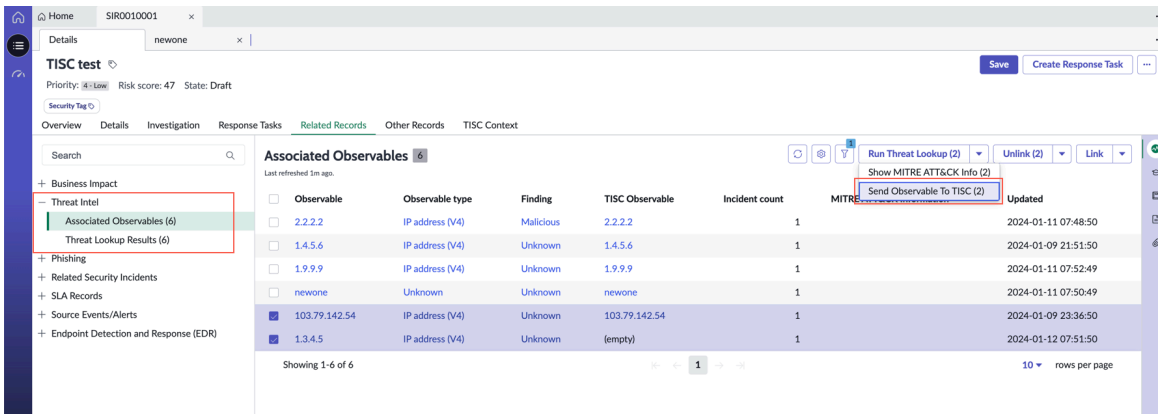
Procedure

1. Navigate to the **Related Records** tab on the SIR workspace to perform the TISC integration capability action.

Note:

- You can also navigate to the **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to perform the push operation.
- On the **Investigation** tab, click **View Related Info** to view all the associated threat lookup, sighting search, and enrichment data for the selected observable. For more information, see Explore Investigation Canvas.

2. For example, select **Threat Intel** > **Associated Observables** to perform the push operation and manually push the data into TISC.
3. Select one or more observable record to perform **Send Observable to TISC** operation to push the data.

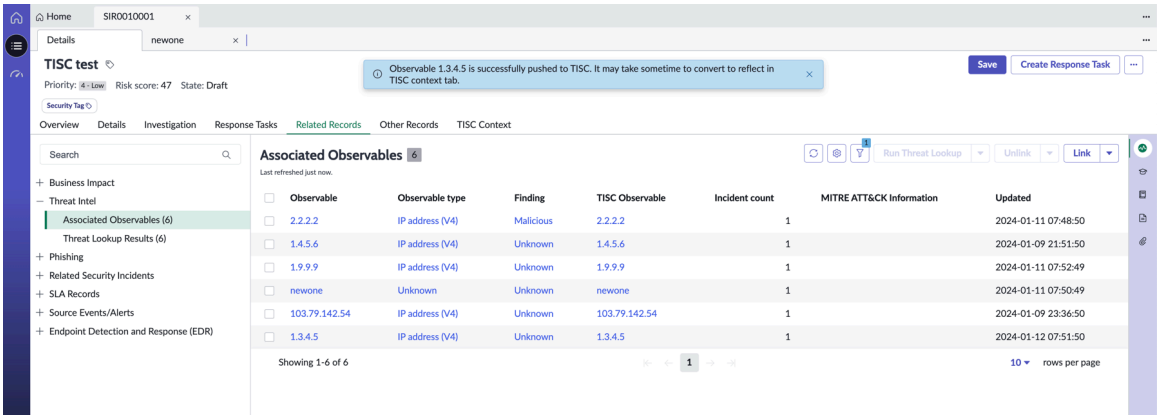


4. Click **Send Observable to TISC**.

Note:

- If the selected observable isn't present in TISC, then first the observable will be created as observable source and then once source observable creates TISC observable record, the observable record will be automatically associated with the newly created observable.
- Once the observable push operation is performed, then an information message is displayed that `Observable 0.0.0.0 is successfully pushed to TISC. It may take sometime to convert to reflect in TISC context tab.`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

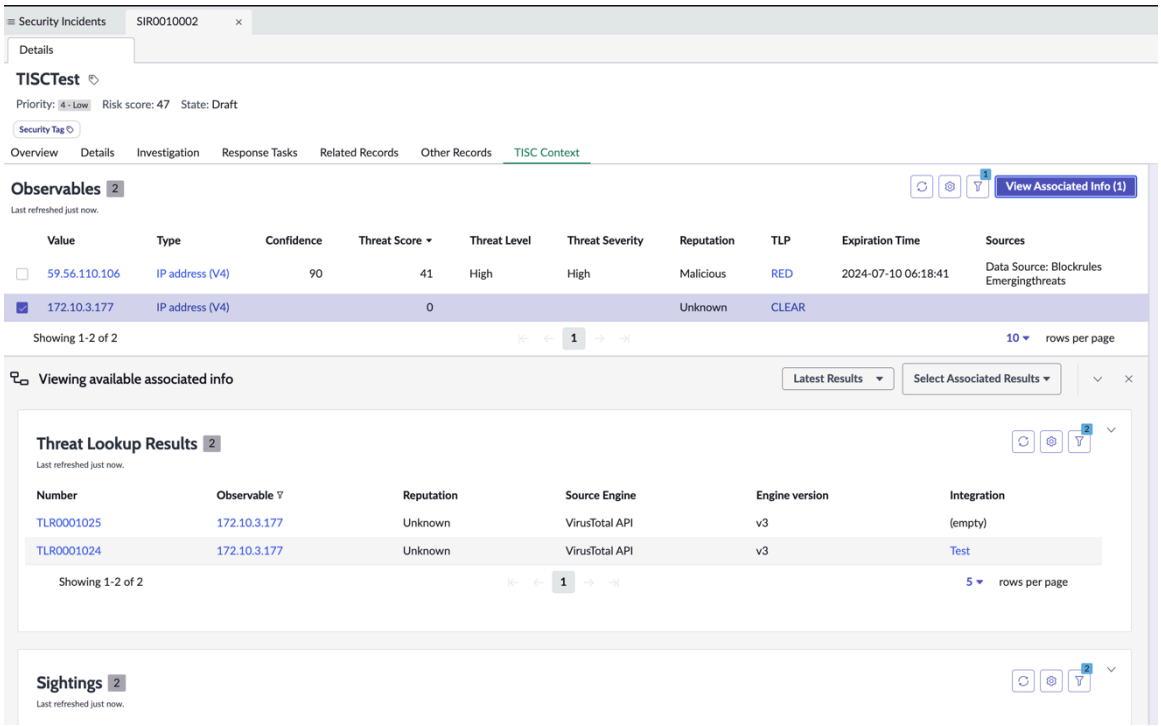


5. Select **TISC Context**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: :

- You will now see the observable that is pushed to TISC from SIR application.



- **In a manual push operation**: The observable data can only be pushed if they are linked to the security incidents. Once the observable is pushed from SIR then that data can be identified using sources which will have reference to security incident linked to the observable.
- **In an automatic push operation**: The observable or enrichment data will be pushed automatically when it is associated to security incident.
- **TISC Context** shows all the SIR associated observable which are also present in TISC.
- Using TISC context, the SIR analysts can see all the TISC Enrichment data including Threat Lookups, Sighting Search, and Observable Enrichment Results.
- **View Associated Info** will show all the associated observable enrichment data of the selected observables.

6. View the results.

Send Threat Lookup to TISC

Using this feature the security analyst can push the threat lookup data from SIR to TISC. Using the TISC Context, you can check if the threat lookup results are present in TISC, if not security analyst can push the data whenever required.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

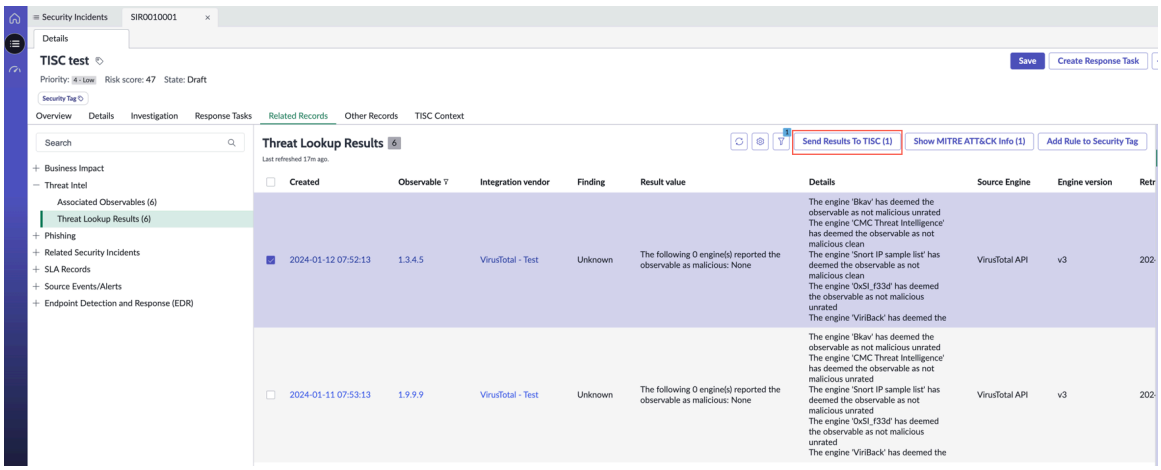
Procedure

1. Navigate to the **Related Records** tab on the SIR workspace to perform the TISC integration capability action.

   Note:

   - You can also navigate to the **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to perform the push operation.
   - On the **Investigation** tab, click **View Associated Info** to view all the associated threat lookup, sighting search, and enrichment data for the selected observable. For more information, see Explore Investigation Canvas.

2. Select **Threat Intel** > **Threat Lookup Results** to perform the push operation and manually push the data into TISC.
3. Select one or more Threat Lookup Results record.
4. Click **Send Results to TISC**.



   Note:

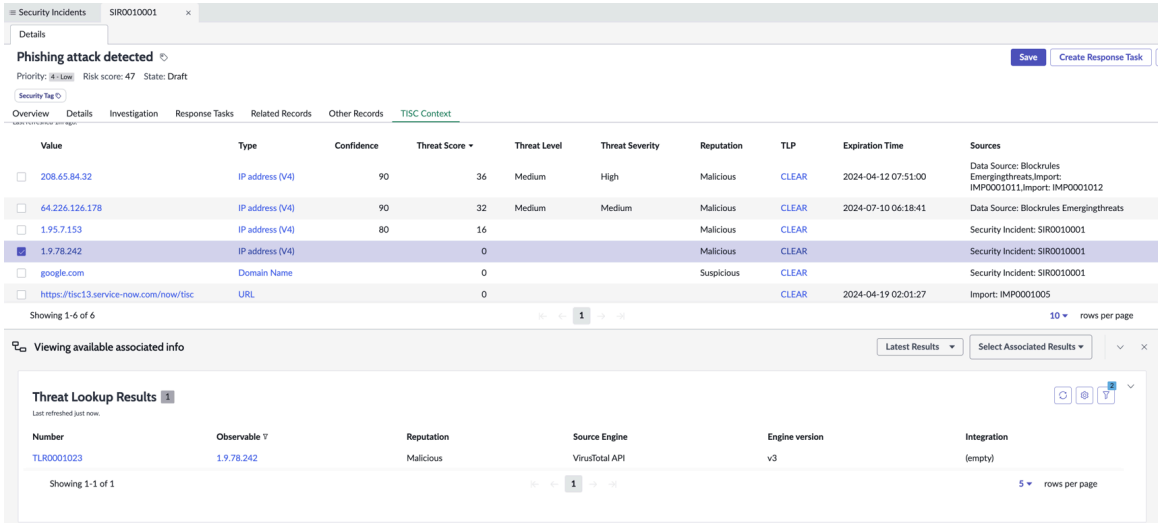
   - If the selected Threat Lookup observable isn't present in TISC, then in manual mode first the observable is created as observable source and then once source observable creates TISC observable record, the observable record will be automatically associated with the newly created observable. Also, selected threat lookup will also be pushed to the newly created threat lookup observable in manual mode.
   - In an automatic mode, the observables will not be pushed if the observable is present, then the threat lookups will be pushed automatically. If the observables are not present, then the threat lookups will not be pushed.

5. A confirmation message is displayed that `The observable (1.9.78.242) for the selected threat lookup record does not exist in TISC. It will take sometime to create observable and to automatically associate the observable threat lookup record in TISC.`
   Once this is processed and pushed, you can see the results.
6. Select **TISC Context**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: :

- You will now see the observable that is pushed to TISC from SIR application.

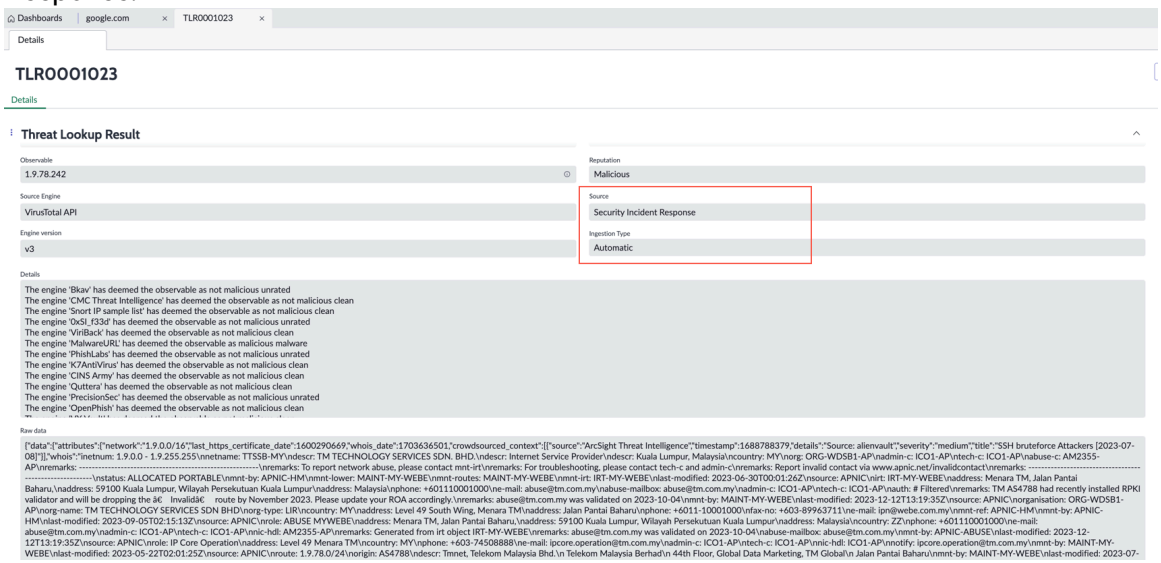


- **In a manual push operation**: The observable data can only be pushed if they are linked to the security incidents. Once the observable is pushed from SIR then that data can be identified using sources which will have reference to security incident linked to the observable.
- **In an automatic push operation**: The observable or enrichment data will be pushed automatically when it is associated to a security incident.
- **TISC Context** shows all the SIR associated observable which are also present in TISC.
- Using TISC context, the SIR analysts can see all the TISC Enrichment data including Threat Lookups, Sighting Search, and Observable Enrichment Results.
- **View Associated Info** will show all the associated observable enrichment data of the selected observables.

7. The list view displays all the threat lookup results, however select any record and click on **View Associated Info** button.
8. View the threat lookup results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Click on any threat lookup results record to view the record in the form view, which also shows the push or **Ingestion Type** (automatic or manual) and **Source** will be Security Incident Response.



Send Sighting Search to TISC

Using this feature the security analyst can push the sighting search data from SIR to TISC. Using the TISC Context, the analyst can check if the sighting search data is present in TISC, if not the security analyst can push the data whenever required.

Before you begin

Role required: sn_si.analyst

Procedure

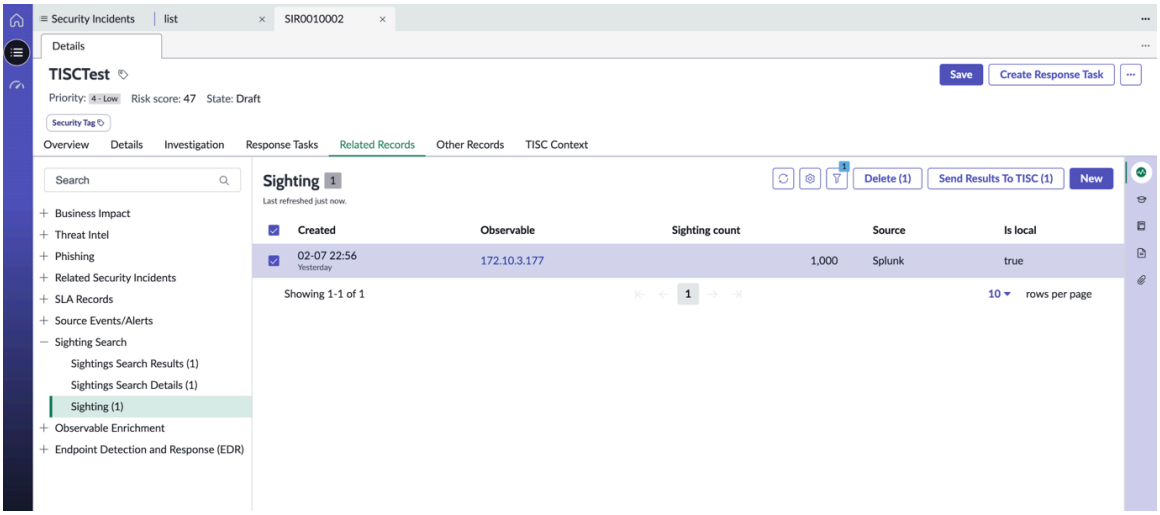
1. Navigate to the **Related Records** tab on the SIR workspace to perform the TISC integration capability action.

   Note:

   - You can also navigate to the **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to perform the push operation.
   - On the **Investigation** tab, click **View Associated Info** to view all the associated threat lookup, sighting search, and enrichment data for the selected observable. For more information, see Explore Investigation Canvas.

2. Select **Sighting Search** > **Sighting Search Results** to perform the push operation and manually push the data into TISC.
3. Select one or more Sighting Search Results record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

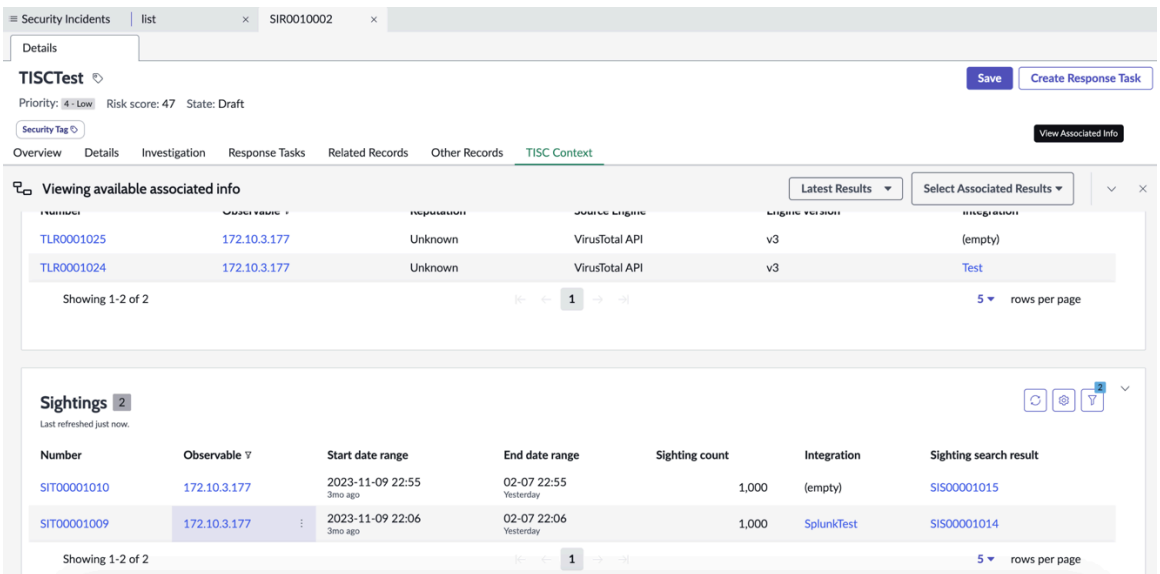


4. Click **Send Results to TISC**.

Note:

- If the selected sighting search observable isn't present in TISC, then in manual mode first the observable is created as observable source and then once source observable creates TISC observable record, the observable record will be automatically associated with the newly created observable. Also, selected sighting search will also be pushed to the newly created threat lookup observable in manual mode.
- In an automatic mode, the observables will not be pushed if the observable is present, then the threat lookups will be pushed automatically. If the observables are not present, then the threat lookups will not be pushed.

5. Select **TISC Context**.

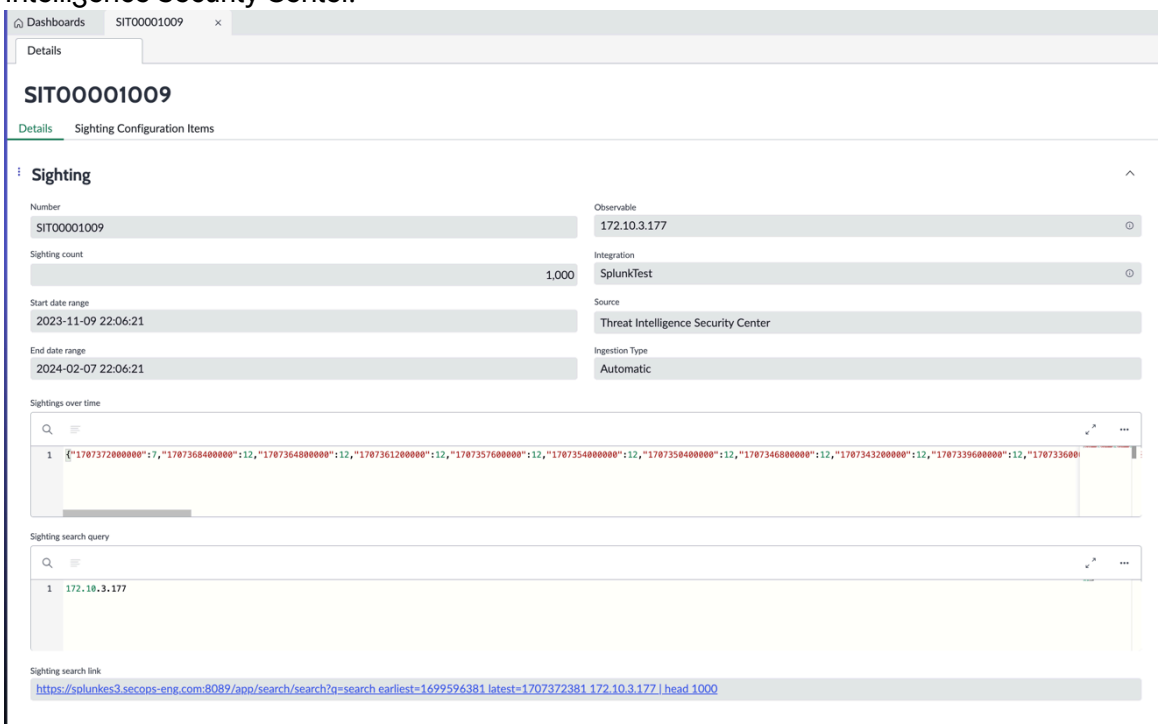


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: :

- You will now see the observable that is pushed to TISC from SIR application.
- **In a manual push operation**: The observable data can only be pushed if they are linked to the security incidents. Once the observable is pushed from SIR then that data can be identified using sources which will have reference to security incident linked to the observable.
- **In an automatic push operation**: The observable or enrichment data will be pushed automatically when it is associated to security incident.
- **TISC Context** shows all the SIR associated observable which are also present in TISC.
- Using TISC context, the SIR analysts can see all the TISC Enrichment data including Threat Lookups, Sighting Search, and Observable Enrichment Results.
- **View Associated Info** will show all the associated observable enrichment data of the selected observables.

6. Once the record is processed, select the record and click **View Associated info**.
7. View the results.
8. Click on any sighting search results record to view the record in the form view, which also shows the push or **Ingestion Type** (automatic or manual) and **Source** will be Threat Intelligence Security Center.



Send Observable Enrichment to TISC

Using this feature the security analyst can push the sighting search data from SIR to TISC. Using the TISC Context, the analyst can check if the sighting search data is present in TISC, if not the security analyst can push the data whenever required.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

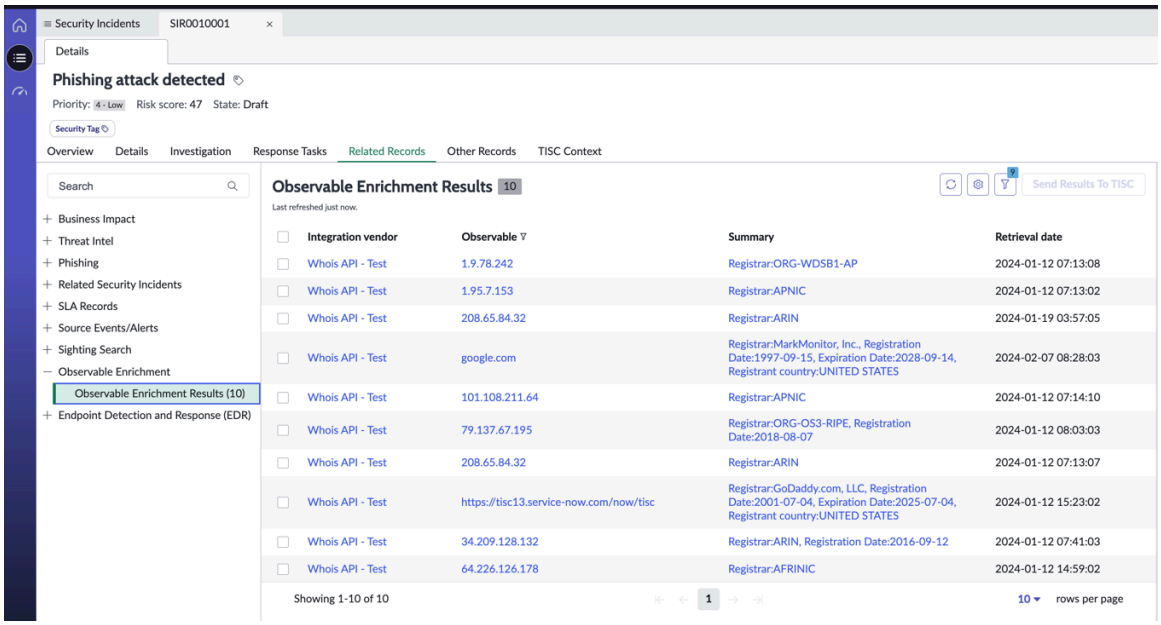
Procedure

1. Navigate to the **Related Records** tab on the SIR workspace to perform the TISC integration capability action.

   Note:

   - You can also navigate to the **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to perform the push operation.
   - On the **Investigation** tab, click **View Associated Info** to view all the associated threat lookup, sighting search, and enrichment data for the selected observable. For more information, see Explore Investigation Canvas.

2. Select **Observable Enrichment** > **Observable Enrichment Results** to perform the push operation and manually push the data into TISC.
3. Select one or more observable record to perform **Send Results to TISC** operation to push the data.



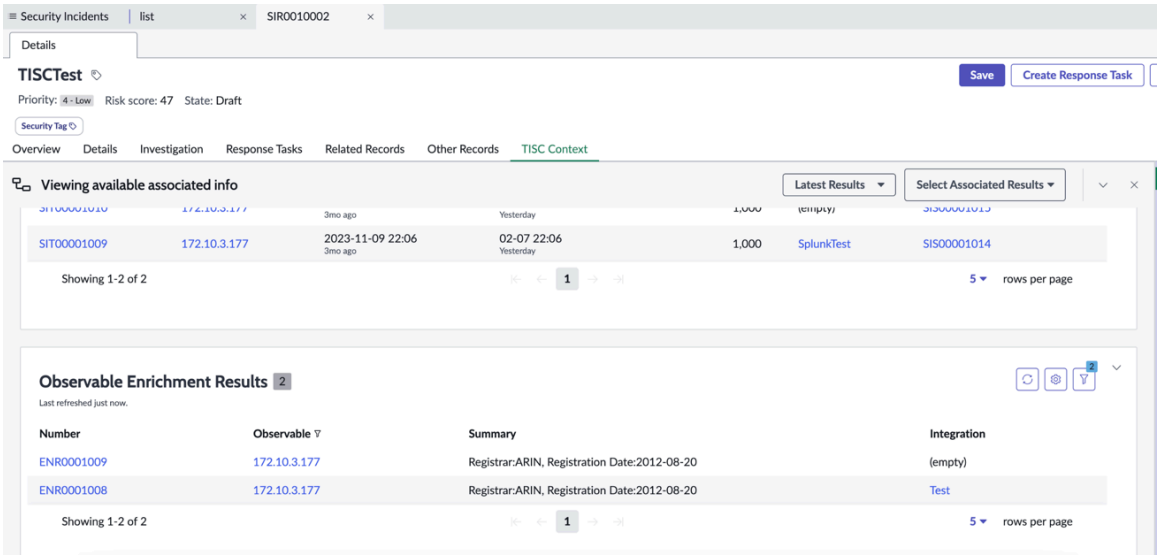
4. Click **Send Results to TISC**.

   Note:

   - If the selected observable isn't present in TISC, then first the observable will be created as observable source and then once source observable creates TISC observable record, the observable record will be automatically associated with the newly created observable.
   - Once the observable push operation is performed, then an information message is displayed that `Observable 0.0.0.0 is successfully pushed to TISC. It may take sometime to convert to reflect in TISC context tab.`

5. Select **TISC Context**.

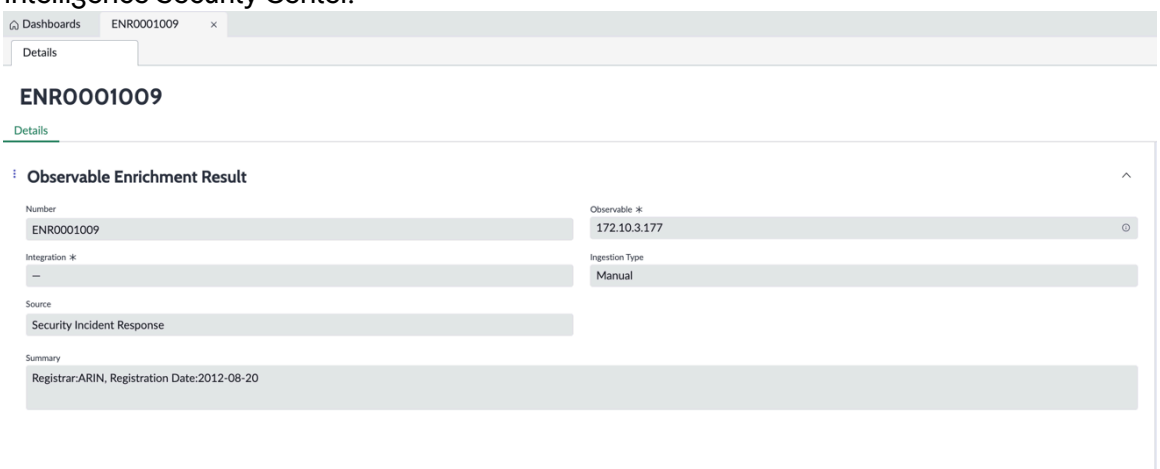
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: :

- You will now see the observable that is pushed to TISC from SIR application.
- **In a manual push operation**: The observable data can only be pushed if they are linked to the security incidents. Once the observable is pushed from SIR then that data can be identified using sources which will have reference to security incident linked to the observable.
- **In an automatic push operation**: The observable or enrichment data will be pushed automatically when it is associated to security incident.
- **TISC Context** shows all the SIR associated observable which are also present in TISC.
- Using TISC context, the SIR analysts can see all the TISC Enrichment data including Threat Lookups, Sighting Search, and Observable Enrichment Results.
- **View Associated Info** will show all the associated observable enrichment data of the selected observables.

6. View the results.
7. Click on any observable enrichment results record to view the record in the form view, which also shows the push or **Ingestion Type** (automatic or manual) and **Source** will be Threat Intelligence Security Center.



View TISC Context in SIR Workspace

View TISC Context under an incident in SIR workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.analyst, sn_sec_tisc.sir_enrichment_data_writer

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s) record.
3. View the **Source** column.
   After the TISC Context is set in SIR, the **Source** observables that are linked to the security incident and the same is displayed under the Source column.
4. Alternatively, click on the pushed observable record, which will take you to the Enrichment Results section for the TISC records.
5. View the **Enrichment Results** tab.
   The **Enrichment Results** tab displays the TISC integrations enrichment results.

Note:

- As the enrichment data is only in context to observable and not Security incident, you will only see source as security incident response.
- The enrichment data generated from TISC will have TISC as source.
- Using ingestion type column we can identity if the record is pushed manually or automatically.

Enrichment Name	Description
Threat Lookup Results	Lists all the associated threat lookup results for an observable enrichment record.
Sightings	Lists all the associated sightings for an observable.
Observable Enrichment Results	Lists all the associated observable enrichment results for an observable.

Working with TISC Context

TISC context facilitates viewing threat intelligence data such as observables within the security incident response workspace.

This helps security analysts to detect, investigate, and respond to security incidents more effectively from the workspace.

TISC Context in Security Incident Response workspace allows the security analysts to add security incidents or observables to TISC Case(s) directly from the workspace, also view the enrichment results, and view observables related information which are related threat actors, attack patterns, campaigns, and so on.

Using this section, you can do the following:

1. Associate observables to a TISC case.
2. View associated observables information.
3. View observables enrichment results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more detailed information and procedure, see the following sections, and for more information on how the integration works between TISC and SIR workspaces, see TISC integration with SIR Workspace in Threat Intelligence Security Center.

Add observables to TISC Case

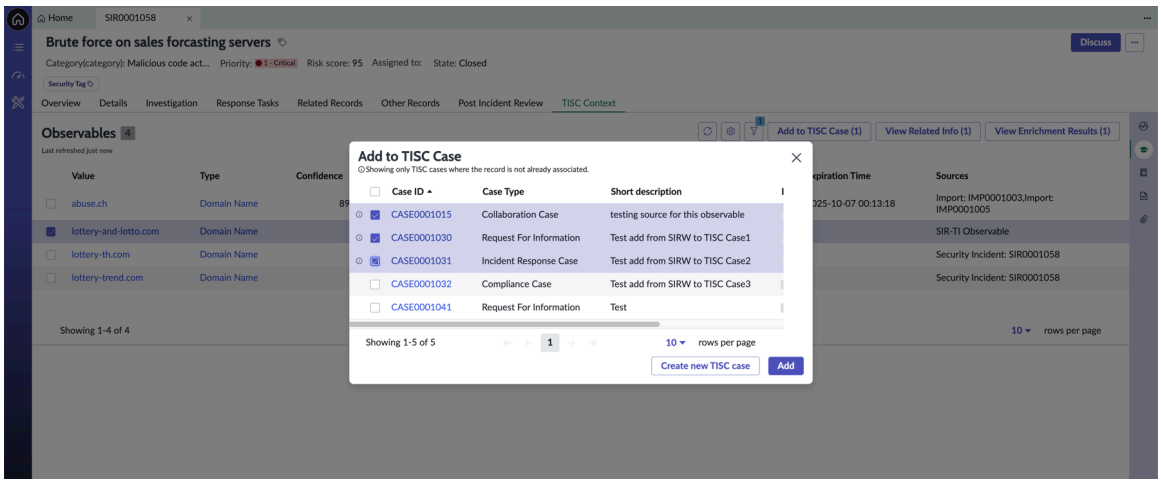
Use this section to add security incidents or observables to a TISC case.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **All**.
2. Locate and open any specific security incident that you are investigating.
   This can also be done by searching for the incident ID or filtering using Quick Filters section or browsing through an incident state.
3. Select **TISC Context** tab.
4. Click **Add to TISC Case** button.
   Add to TISC Case dialog box displays and this only shows the TISC cases where the record is not already associated.
5. Select the observables.
6. Select case(s) and click **Add** to add the cases to the observables and associate them to the security incident.



Note: You can also create a new case by clicking on **Create new TISC Case**, in case if you don't have any existing cases.

The following confirmation messages are displayed:

- The following observables are added as artifacts successfully.
- The following observables are sent to TISC and will be subsequently be added to the selected TISC case(s) records.

Note: The processing and association of the observables activities are posted in the activity stream as and when the association is completed.

7. View the associated case records by logging into Threat Intelligence Security Center Workspace for further steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information see, TISC integration with SIR Workspace.

Note:

From the Security Incident Response workspace, you can also associate observables to case records from the **Investigation** and **Related Records** tabs.

Note: To associate observables from **Investigation**, follow the below procedure and to associate from **Related Records** explained here Add observables to TISC Case.You can also navigate to the **Investigation** tab, and navigate to the **Entry Points Lists** section displayed on the left side of the page and select **Associated Observables** to add observables to TISC case.

View related info from TISC

Use this section to view the related info such as related threat actors, attack patterns, campaigns, and cases from TISC in SIR workspace.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **All**.
2. Locate and open any specific security incident that you are investigating.
   This can also be done by searching for the incident ID or browsing from Quick Filters section or filtering through incident state.
3. Once the incident is open, navigate to **TISC Context** tab.
   Viewing View Related Information:

   Within the incident details, you can view related information in several sections.

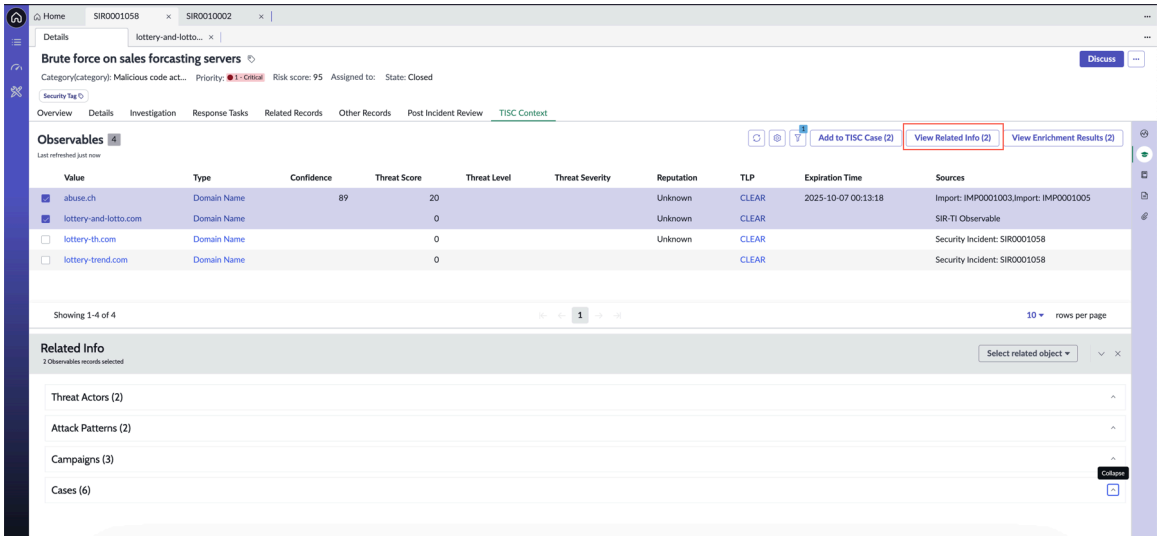
   a. Select one or more observables.

   b. Click on **View Related Info** button.
   This section displays the associated information that are related to the selected observables.

Name	Description
Threat Actors	Shows information from TISC for Threat Actors related to the selected observables.
Attack Patterns	Shows information from TISC for Attack Patterns related to the selected observables.
Campaigns	Shows information from TISC for Campaigns related to the selected observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
Cases	Shows information from TISC for TISC cases related to the selected observables.



View Enrichment Results

Use this section to view the observables enrichment results such as Threat Lookup Results, Sightings, and Observable Enrichment Results from TISC in SIR workspace.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **All**.
2. Locate and open any specific security incident that you are investigating.
   This can also be done by searching for the incident ID or browsing from Quick Filters section or filtering through incident state.
3. Once the incident is open, navigate to **TISC Context** tab.
   Viewing Enrichment Results:

   Within the incident details, you can view related information in several sections.

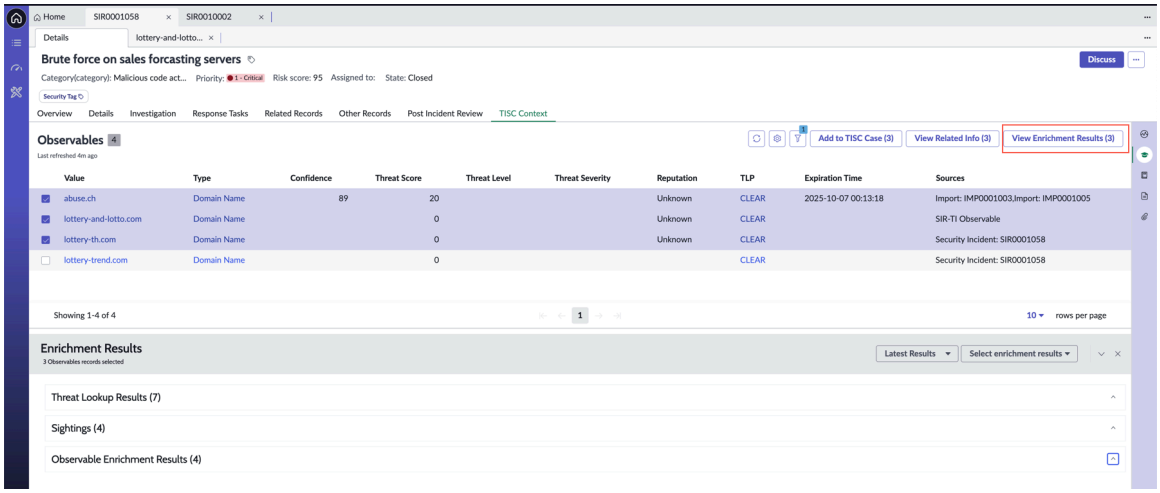
   a. Select one or more observables.

   b. Click on **View Enrichment Results** button.
   This section displays the details that are related to the selected observables.

Name	Description
Threat Lookup Results	Lists all the associated threat lookup results for selected TISC observables.
Sightings	Lists all the associated sightings for selected TISC observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
Observable Enrichment Results	Lists all the associated observable enrichment results for selected TISC observables.



Reports in Security Incident Response

All the reports associated with a security incident are available within the Reports section for analysis and sharing.

The analyst will be able to:

- Create a report
- Edit a report
- Delete a report

Create a report

Analysts can create a report in Security Incident Response to include the status of an incident and share it via email.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident.
3. Select **Reports**.

   The **Report** page displays a list of all the reports created for the selected incident.
4. Select **New**.
   The **Select Template** page appears with a list of all the published templates. The list of templates is available only when the admin has published reports templates. For more information, see Create a Report Template in Security Incident Response.
5. Select a report template.
   The report opens in edit mode with the incident data as configured in the template.
6. Select **Expand** and insert/remove the desired fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Common SIR Fields**: The list of most used fields for an incident.
- **All SIR Fields**: All the fields related to an incident. For example, when you are generating a incident report and want to add a field called Short description then you can select that field from the **All SIR Fields**. When you add a field, the short description if the incident is displayed in the report.
- **Related Records**: The related records of a particular incident. For example, if you want to add any associated observables in the report, you can add it to your report. These related records are displayed in the table format
- **Scripts**: To add the date and time of the report, you can add the Current Date Time script to your report. This will add the Report Created Date and Time in report.

7. Select **Preview** to view a preview of the report.
8. Select **Save Content** to save the changes.
9. **Optional:** Select the edit report details icon to update the report name and description.
10. Select **Publish** to publish the report.
11. Select the share report in email icon.
    a. Enter the recipient's emails in the **To** and **Cc/Bcc** fields.
    b. Update the email **Subject and Email Body**.
    c. Select **Send** to share the report over email.

Edit a report

Analysts can modify an unpublished report in Security Incident Response and share it via email.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident.
3. Select **Reports**.

   The **Report** page displays a list of all the reports created for the selected incident.

4. Open the report to update.
   The report opens in edit mode with the incident data as configured in the template.
5. Edit the report as required.
6. Select **Preview** to view a preview of the report.
7. Select **Save Content** to save the changes.
8. **Optional:** Select the edit report details icon to update the report name and description.
9. Select **Publish** to publish the report.
10. Select the share report in email icon  .
    a. Enter the recipient's emails in the **To** and **Cc/Bcc** fields.
    b. Update the email **Subject and Email Body**.
    c. Select **Send** to share the report over email.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Delete a report

You can delete a report in Security Incident Response which is in published or draft state.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident.
3. Select **Reports**.

   The **Report** page displays a list of all the reports created for the selected incident.
4. Open the report to delete.
5. Select **Delete**.
   A confirmation messages appears.
6. Select **Delete** to delete the report.

Collaborate using conference call or chat in Security Incident Response

You can collaborate with analysts and affected users to resolve or discuss about an incident in Security Incident Response application.

Related topics

Start a conference call in Security Incident Response

Start a Sidebar chat in Security Incident Response

Start a conference call in Security Incident Response

Using conference call, security analysts can collaborate with other analysts and affected users in real-time. These calls facilitate the exchange of information to help resolve incidents.

Before you begin

Make sure you've done the installed and activated the following apps and plugins:

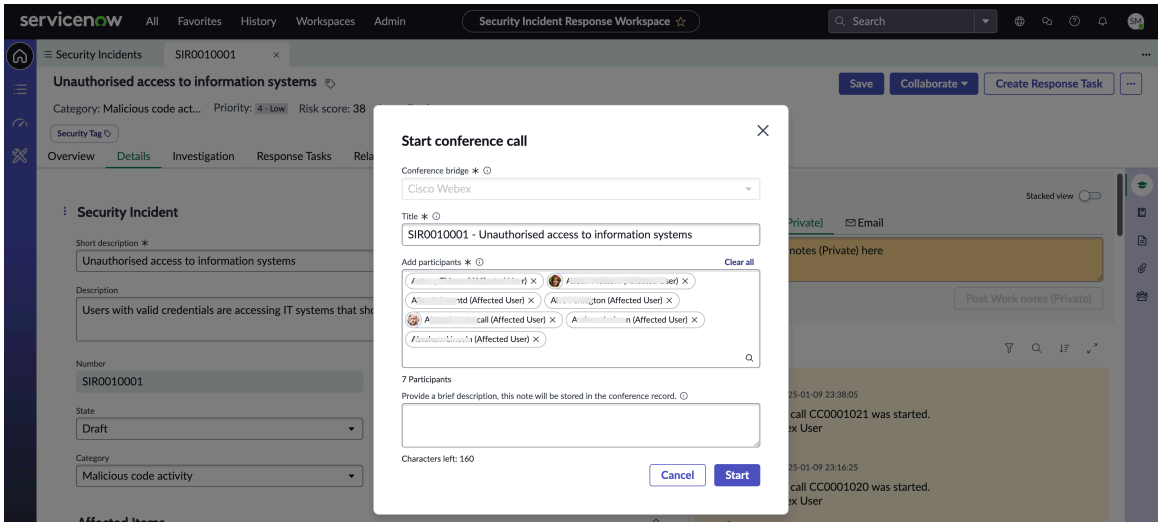
- Notify plugin (com.snc.notify).
- Notify UI Components for Configurable Workspaces app.
- Visual Task Board plugin (com.devsnc.snb_vtb)

Role required: sn_si.analyst or sn_si.manager

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident for which you want to initiate a conference call.
3. Select **Collaborate**, and then select **Start a Call**, or you can select the conference call icon  and then select the + icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Start conference call pop-up appears.

4. Select a conference bridge in the **Conference bridge** field.
5. Provide a title for the conference call in **Title**.

   Note: By default, the title of the incident is populated as the title of the call. You can modify the default title.

6. Add or remove call participants in **Add participants**.

   Note: Based on the configuration in Conference Call settings, a pre-populated list of participants is added to **Add participants** or a **Recommendations** list of participants is available. For more information, see Manage Conference Call users and groups.

7. Provide a brief description for starting the conference call.
8. Select **Start**.

   The conference call starts in the selected conference bridge. All the participants receive notification through email and through the conference bridge. The participants can use the link or notification to join the call.

9. Open the associated incident in Security Incident Response application to view the conference call details.
10. **Optional:** Select **Copy invite** to add participants in an active call.
11. Select **End call**.
    When the final participant leaves the conference call, the call ends
12. **Optional:** To restart a conference call, navigate to the **Completed** section and select the **Reinitiate** option of the required conference call.

Add participants to active Conference Call

You can add participants to an active conference call if you have not added them before starting the conference call.

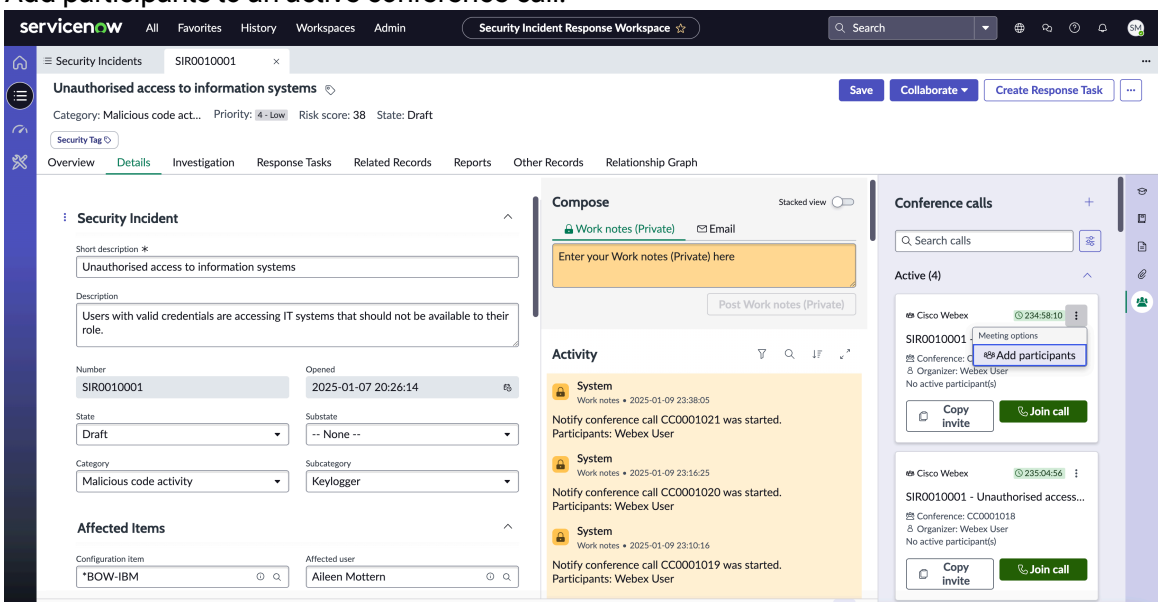
Before you begin

Role required: sn_si.analyst,sn_si.manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open the security incident for which you want to initiate a conference call.
3. Select the conference call icon to the view the details of the conference calls.
4. Add participants to an active conference call:



   - Select the meeting options icon ⋮ for the active conference call and select **Add participants**.
   - Select **Copy invite** on the **Conference calls** section, and share the invite with the required participants.

Start a Sidebar chat in Security Incident Response

Using Sidebar, security analysts can collaborate with others in real-time based on a Workspace task-based or interaction-based record. These Sidebar discussions facilitate the exchange of information and knowledge to help resolve issues faster and with higher-quality outcomes.

Before you begin

Role required: sn_si.read

Verify that you have activated the Omni-Experience Standard Feature Set plugin. For more information, see Installing Sidebar.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select the List view icon.
3. Open a security incident for which you want to initiate a sidebar discussion.
4. Select **Collaborate**, and then select **Start Chat**.
   The Start a Sidebar discussion dialog box appears.

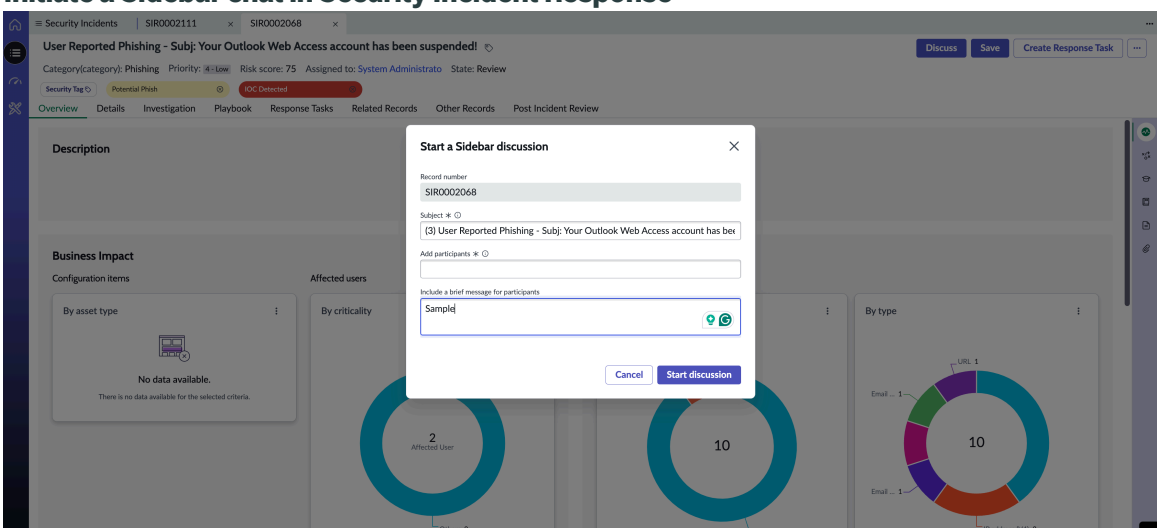
> **Note:** Sidebar's integration with Microsoft Teams enables Sidebar users and Microsoft Teams users to communicate with each other from their respective platforms. For more information, see Sidebar and Microsoft Teams.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. On the Start a Sidebar discussion dialog box, fill in the fields.

Field	Description
Record number	The task or incident number associated with the Sidebar discussion.
Subject	Provide a title for the sidebar discussion.
Add participants	Option to add participants for the sidebar dis cussion. If you have integrated sidebar chat with Microsoft Teams, you can also add partic ipants from Microsoft Teams. **Note:** ○ You need to add at least one partici pant to create a new discussion. ○ If Sidebar and Microsoft Teams are in tegrated, Microsoft Teams users are differentiated from Sidebar users with a Microsoft Teams icon. ○ By default, all users who have read ac cess to the SIR records will also have access to sidebar chats, but this can be controlled using member query. For more information, see Configuring
Include a brief message	Provide a brief summary about the issue to be discussed in the sidebar discussion.

Initiate a Sidebar chat in Security Incident Response



6. Select **Start discussion**.

7. You can perform additional configuration like quick actions.
To limit the action usage, you can use the **Apply to group** field on the quick action page. For more information, see Creating a quick action .

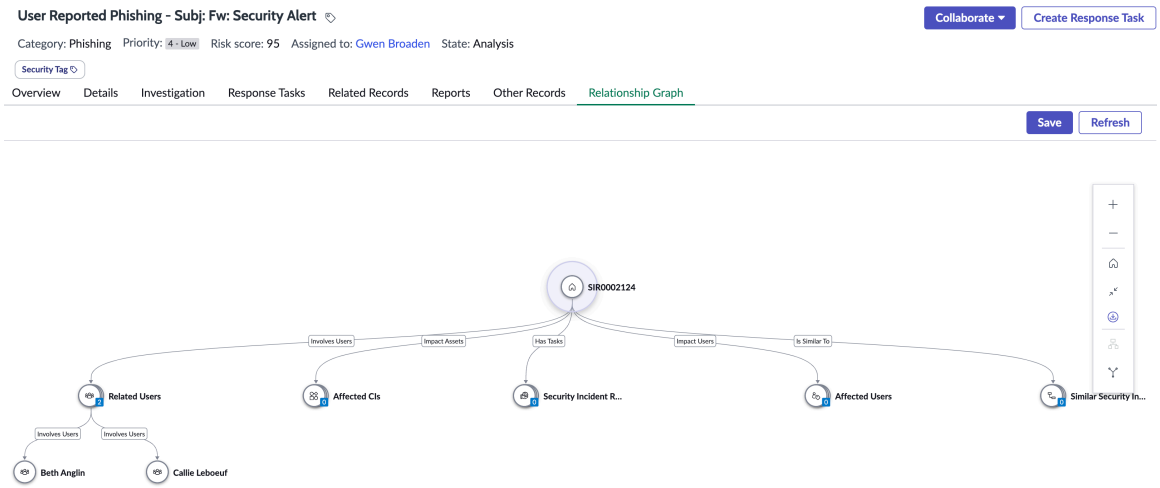
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing incident details with a relationship graph

Relationship graphs in the Security Incident Response workspace visually display the connections between a security incident and its related items to help you analyze the full context of a security incident.

Items related to a security incident could include associated observables, configuration items (CIs), similar security incidents (SIRs), response tasks, and other related lists.

The following relationship graph example displays details for a security incident.



When you open a relationship graph for a security incident, the available configurations are visible by default. You can interact with the graph as follows:

- Zoom into any object fit into the screen and drag the nodes.
- Add subnodes for each node, if available, and view details of the subnodes.
- Hide any node or subnode from the graph.
- View details of a subnode.

Customize a relationship graph

Visualize and analyze security incidents and their associated data in a relationship graph.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspaces** > **Administration**.
2. Select **Relationship Graph**, and then **Relationship Graph Configurations**.
3. Select **New**.
4. On the form, fill in the fields.

Relationship graph configurations

Field	Description
Related Table Name	The table from which you want to fetch the security incident observable data, such as the Associate observable [sn_ti_observable]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	table or Security Incident [sn_si_incident] table.
Node Label	The node label for the observable that appears on the relationship graph. The automatically supplied value depends on the selected related table.
Active	Option to enable the configuration.
Data Node Label	The primary label and secondary label to display on the node for the selected related list.
Default Visible	Option to display the data node label.
Relationship Label	The relationship between a node and link node to display on the relationship graph.

5. Select **Save**.

Create a relationship graph for an incident

Create a node relationship graph in Security Incident Response so you can better analyze a security incident by correlating it with malicious observables, configuration items (CIs), similar security incidents (SIRs), response tasks, and other related information.

Before you begin
Role required: sn_si.analyst

About this task
For information about how to create a customized relationship graph rather than using a predefined graph, see Customize a relationship graph.

Note: Changes to the relationship graph aren't saved automatically.

Procedure
1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open a security incident.
3. Select the **Relationship Graph** tab.
4. In the relationship graph, select and hold (or right-click) the parent node, and then select **Add Nodes**.
5. Select one or more category nodes to display in the relationship graph, such as Related users, Affected CIs, similar security incidents (SIRs), or Affected Users.

   Note: You can select multiple category nodes.

6. Select and hold (or right-click) a category node and select **Link Nodes** to add data associated with the category node.

   Note: You can apply filters to reduce the number of items in the list.

   A list of all related records for the selected category node appears. For example, if you select **Affected Users** from the node category, a list of all the users affected by this incident displays.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select the desired records from the list and select **Add**.
8. Select **Add**.
9. **Optional:** Clear changes if necessary by selecting **Refresh**.
10. Select **Save**.

> **Note:** Changes to filters are also saved when you save the relationship graph.

11. **Optional:** Display the details of a subnode.
    a. Select a subnode.
    b. Select **Show Details**.
12. **Optional:** Download the map to your system.

    a. If only a portion of the map is visible on the screen and you want the whole screen to be included in the PDF, select the Fit to screen icon ( ).

    > **Note:** Only the portion of the map that appears on the screen is included in the PDF file.

    b. Select the export map icon ( ).

Example: Video showing how to edit a relationship graph to add category nodes and subnodes

https://player.vimeo.com/video/1095955062?h=593c16e2b6&badge=0&autopause=0&player_id=0&app_id=58479

MITRE attack and defend technique graph

The MITRE attack and defend technique graph provides security analysts with an interactive, node-based visualization of attack techniques, defense techniques, and associated artifacts for a security incident.

MITRE attack and defend technique graph Overview

The MITRE attack and defend technique graph enables analysts to explore relationships between security threats and defensive measures, helping them understand the complete attack and defense landscape for an incident. The graph uses a hierarchical structure with the SIR record as the root node, branching out to display attack techniques, defend techniques, and their associated artifacts.

Analysts can interact with nodes to view details, establish associations, and manage the visibility of information based on their investigation needs. The visualization only appears when MITRE attack and defend technique data has been ingested into the system. Without ingested data, the MITRE attack and defend technique tab remains hidden from the SIR workspace.

Graph structure

The graph consists of the following node types arranged in a hierarchical structure:

- SIR node (root): The central node representing the Security Incident Response record.
- Attack technique nodes: First or second-level nodes representing specific attack methods.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Defend technique nodes: First or second-level nodes representing defensive measures.
- Artifact nodes: Second or third level nodes representing specific artifacts related to defend techniques.

Nodes at the same hierarchical level can have cross-references, creating connecting edges when the same node relates to multiple parent nodes.

Available actions

The graph provides different actions depending on the node type being interacted with.

SIR node actions

- **Show attack technique:** Display all attack techniques associated with the SIR.
- **Show defend technique:** Display all defend techniques associated with the SIR.
- **Associate attack technique:** Open a modal window to associate new attack techniques with the SIR.
- **Associate defend technique:** Open a modal window to associate new defend techniques with the SIR.

Attack technique node actions

- **Show details:** Opens a panel displaying the details of the selected node.
- **Show defend techniques:** Display all defend techniques associated with this specific attack technique.
- **Hide node:** Temporarily remove a node from the graph view. A **Show hidden nodes** option becomes available to restore hidden nodes.

Defend technique node actions

- **Show details:** Opens a panel displaying the details of the selected node.
- **Show defend artifacts:** Display all artifacts associated with the selected defend technique. Artifacts shared across multiple defend techniques appear as a single node with multiple connecting edges. Edge labels indicate the relationship between the defend technique and artifact.
- **Hide node:** Temporarily remove the defend technique node from the graph view. A **Show hidden nodes** option becomes available to restore hidden nodes.

Graph-level actions

- **Save**: Preserve the current graph view state. Saved views persist when users return to the tab. Includes node visibility, expanded sections, and layout preferences.
- **Refresh**: Update the graph with the latest data from the backend. Updates node labels if names have changed, removes associations that have been deleted from the backend, and displays newly associated techniques not currently visible in the graph. Maintains the saved view structure while refreshing the data.
- **Find on map**: Search for specific nodes by name. Highlights and centers the selected node in the graph. Useful for locating nodes in complex graphs with many techniques.
- **Show hidden nodes**: Restore all nodes that have been hidden from view.

Association actions

When associating attack or defend techniques:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Select technique:** Choose from available techniques in the modal window.
- **Save association:** Confirm and create the association. Newly associated nodes appear at the end of the graph. Use the **Find on map** function to locate newly added nodes.
- **Cancel:** Close the modal without creating an association.

The association modal uses the same interface experience as the MITRE-ATT&CK technique functionality.

Node relationships and edges

The graph displays relationships between nodes using connecting lines (edges):

- Direct associations: Lines connect parent nodes to their directly associated child nodes.
- Shared relationships: When a defend artifact relates to multiple defend techniques, a single artifact node connects to multiple parent nodes via separate edges.
- Cross-level references: When nodes at the same hierarchical level share relationships, connecting lines appear between them.
- Edge labels: Labels on the edges between defend techniques and artifacts indicate the relationship type (sourced from MITRE-ATT&CK data).

Security Incident Playbook

Invoke the security incident playbook flow automatically or manually.

A Playbook is visible only if at least one playbook is associated with a security incident. The playbook component works only for the Process Automation Designer (PAD) built processes and not for the flow designer-built flows. For the existing flow designer enabled flows, it will continue to work, and the activities will be continuing to be rendered as response tasks.

There are two ways of associating playbook with the security incident:

- Automatically invoke playbook
- Manually add playbook

Invoke playbook automatically

For a Playbook to be invoked automatically, a process needs to be defined using **Process Automation Designer (PAD)**, and when the trigger condition is met then automatically the playbook tab is rendered with the playbook activities being displayed.

Add playbook manually

For a Playbook to be invoked manually, navigate to the Form UI action drop down and select **Add Playbook**. For more information see, Add Playbook

Note: If there is already a playbook available then the new playbooks added will run in parallel to the existing playbooks.

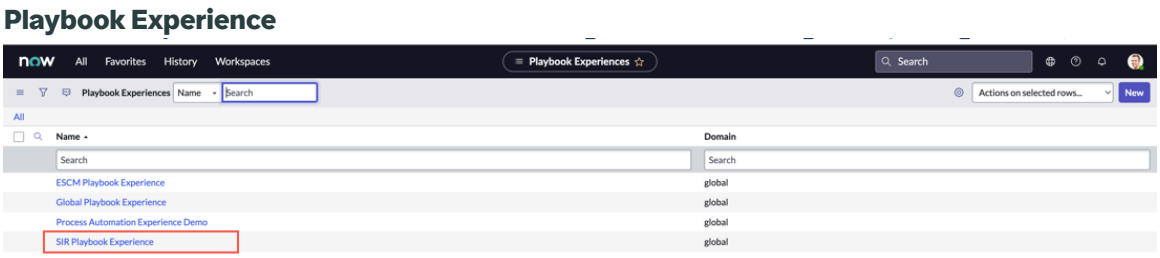
- Within the playbook, the analyst can filter the playbook cards by status.
- The analyst can cancel a playbook by selecting it from the ellipse icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

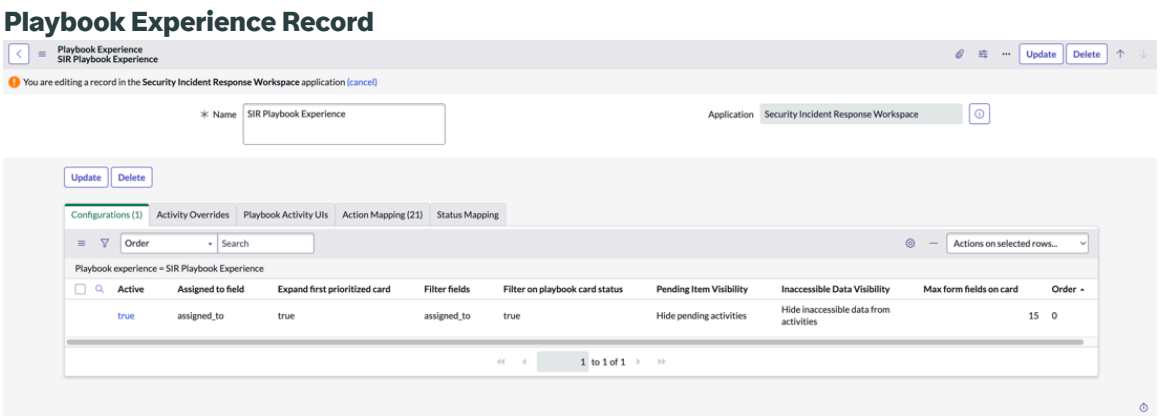
- Within each activity, the analyst will be able to perform the actions defined within the activity cards such as Skip, Mark as complete, Cancel, or Orchestration actions such as Submit to sandbox, Search Emails and so on.
- Each of these actions are defined within the activity definition, and the complete card visible is customizable at the time of building the activity definition itself.

Note: All the future activity definitions and the next steps to be performed are displayed with a lock icon and are in read-only mode to the user. The playbook display mode is controlled by a configuration as explained below.

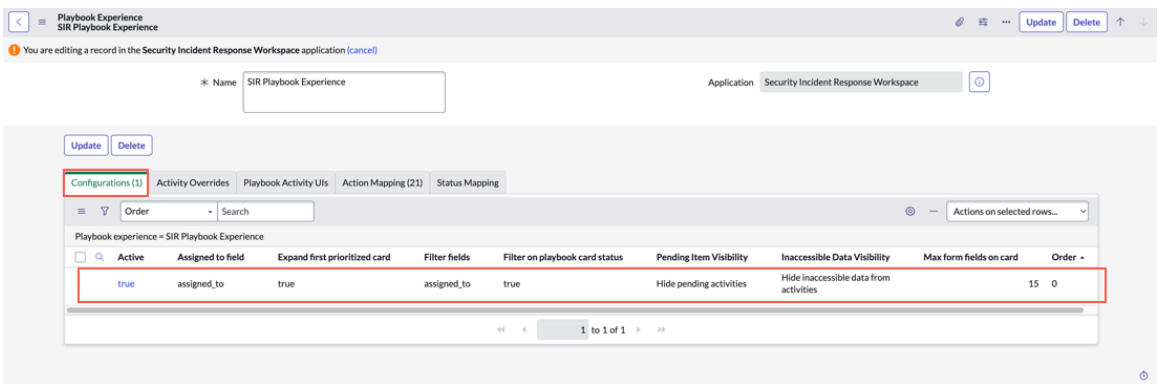
1. Navigate to **All** > **Playbook Experiences**.
2. In the Playbook Experiences page, select an **SIR Playbook Experience**.



The **Playbook Experience SIR Playbook Experience** page is displayed.



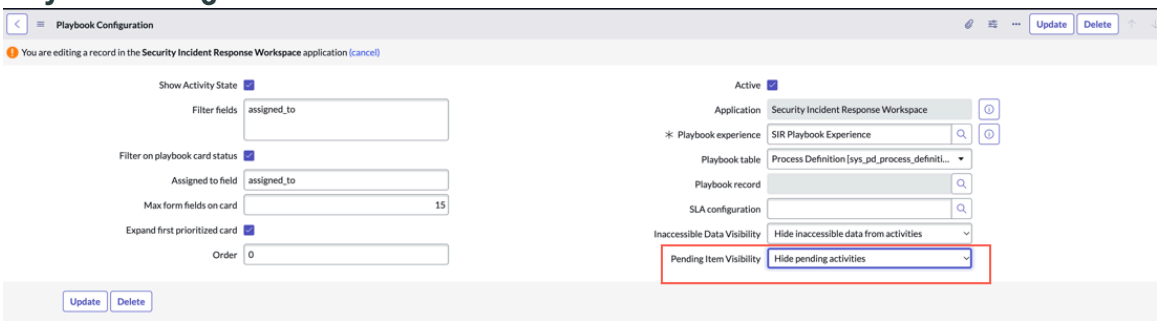
3. Click on the **Configuration** record.



4. In the Configuration tab, click the SIR Playbook Experience Configuration.

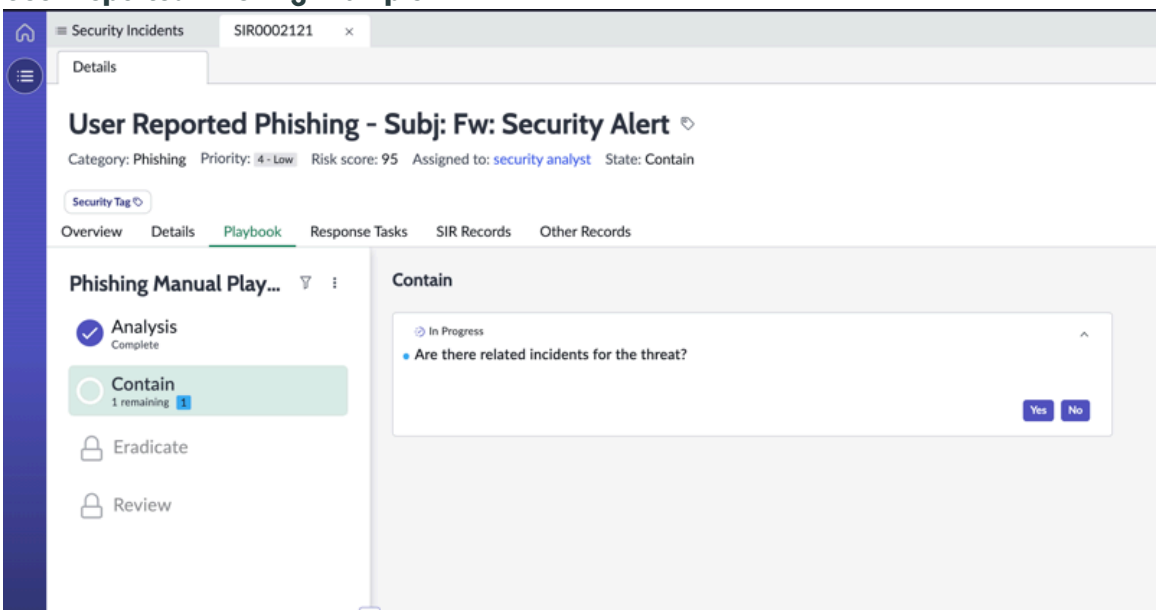
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Playbook Configuration



5. Navigate to the **Pending Item Visibility** field's drop down list, select the desired option and save the record. Choose from the following options:
   - **Hide pending activities**: Select this option to hide the pending activities that you would like to see on the playbook section of the workspace.

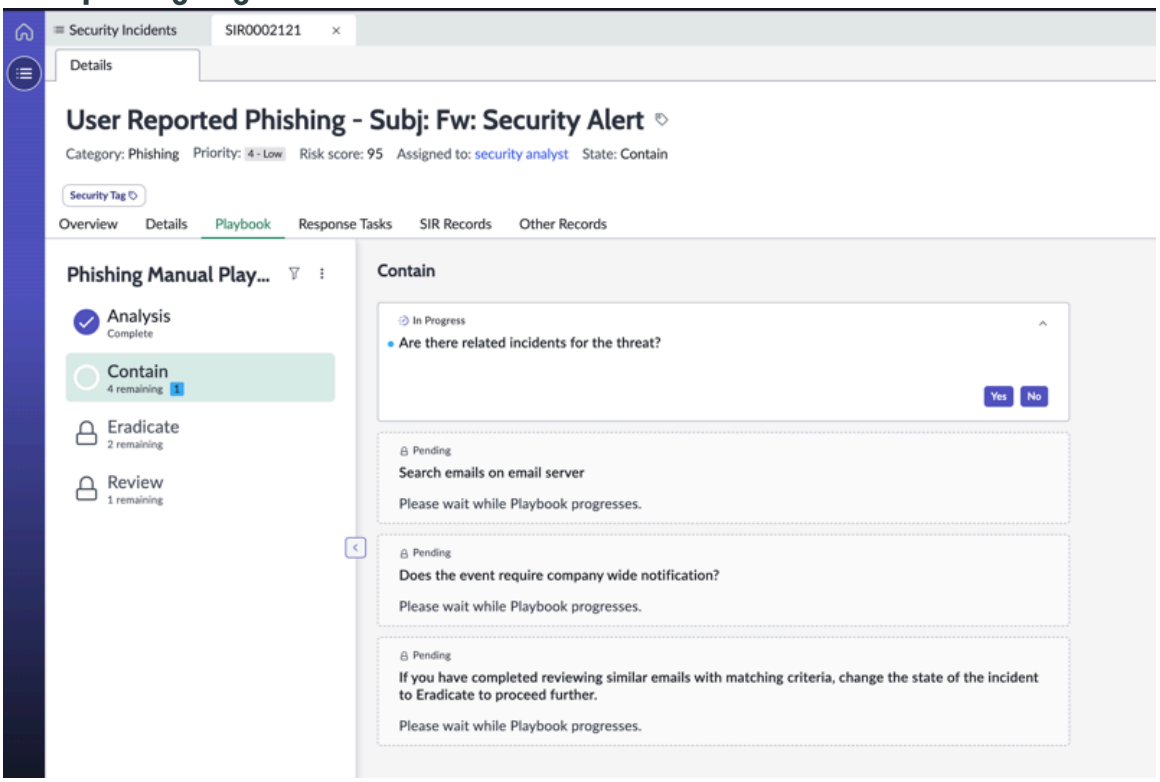
User Reported Phishing Example



   - **Show pending stages and activities**: Select this option to show pending stages and activities that you would to like to see on the playbook section of the workspace.

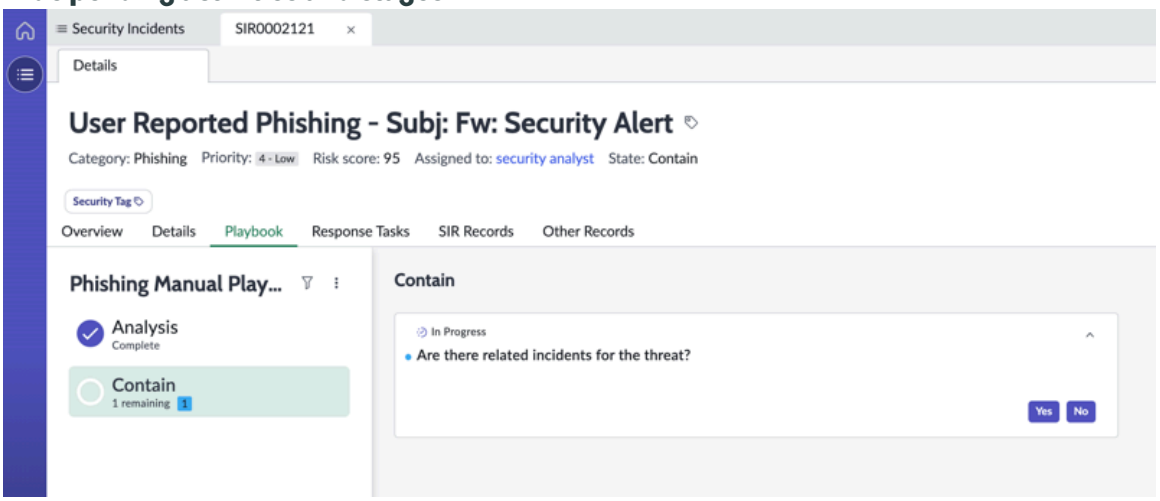
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Show pending stages and activities



- **Hide pending activities and stages**: Select this option to hide pending activities and stages,that you would like to see on the playbook section of the workspace.

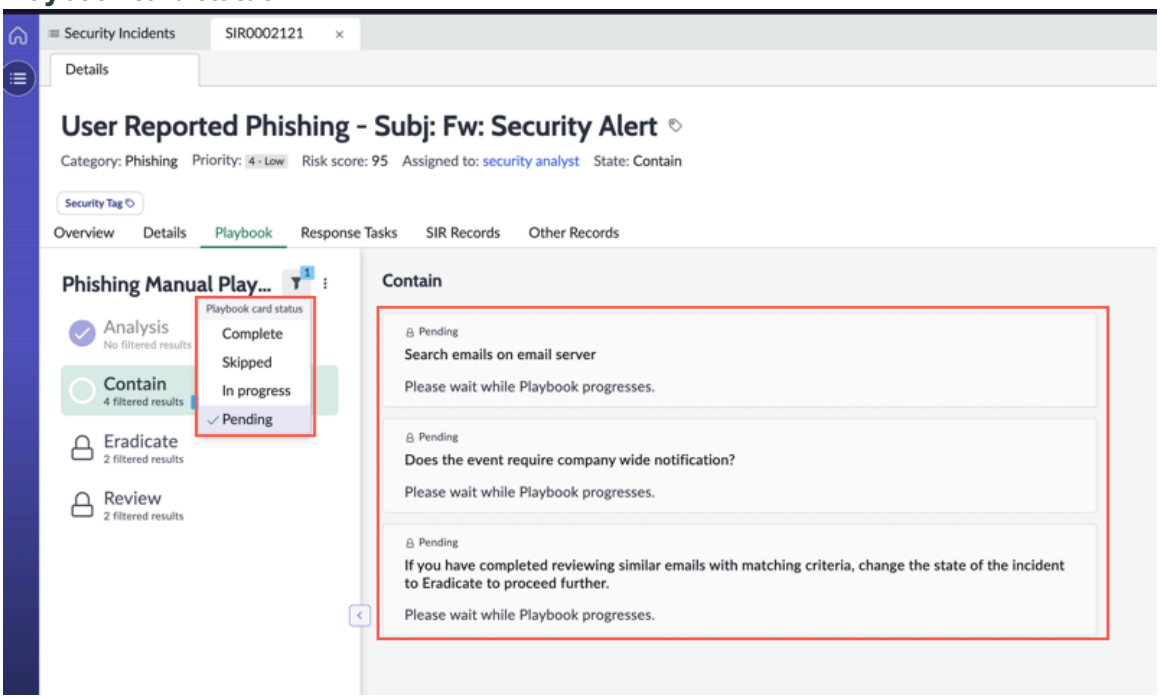
Hide pending activities and stages



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. On the Playbook section, use the filter option to filter the activities by Playbook card status (activity definition).

Playbook card status



Add Playbook

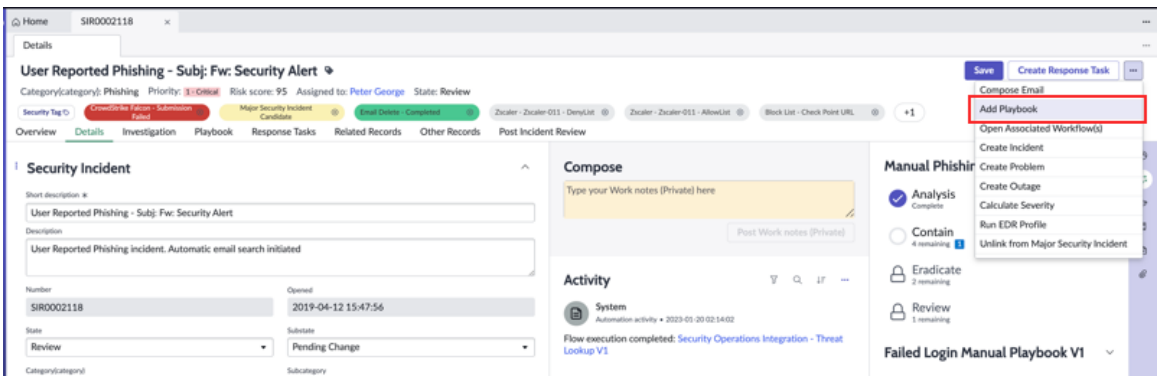
Use this section to add playbook manually.

Before you begin

Role required: sn_si.analyst

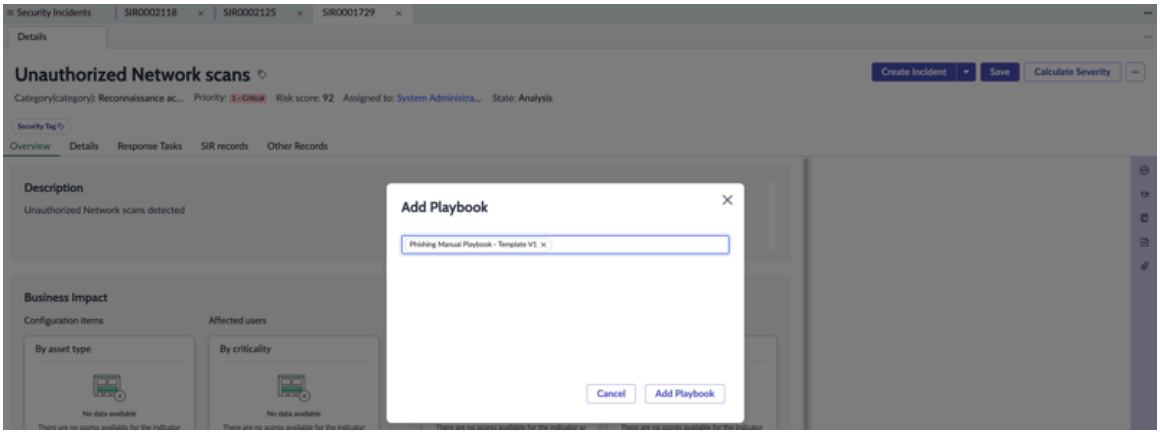
Procedure

1. Navigate to **All** > **Security Incident** > **Security Analyst Workspace**.
2. Open an incident record.
3. Click **Add Playbook**.

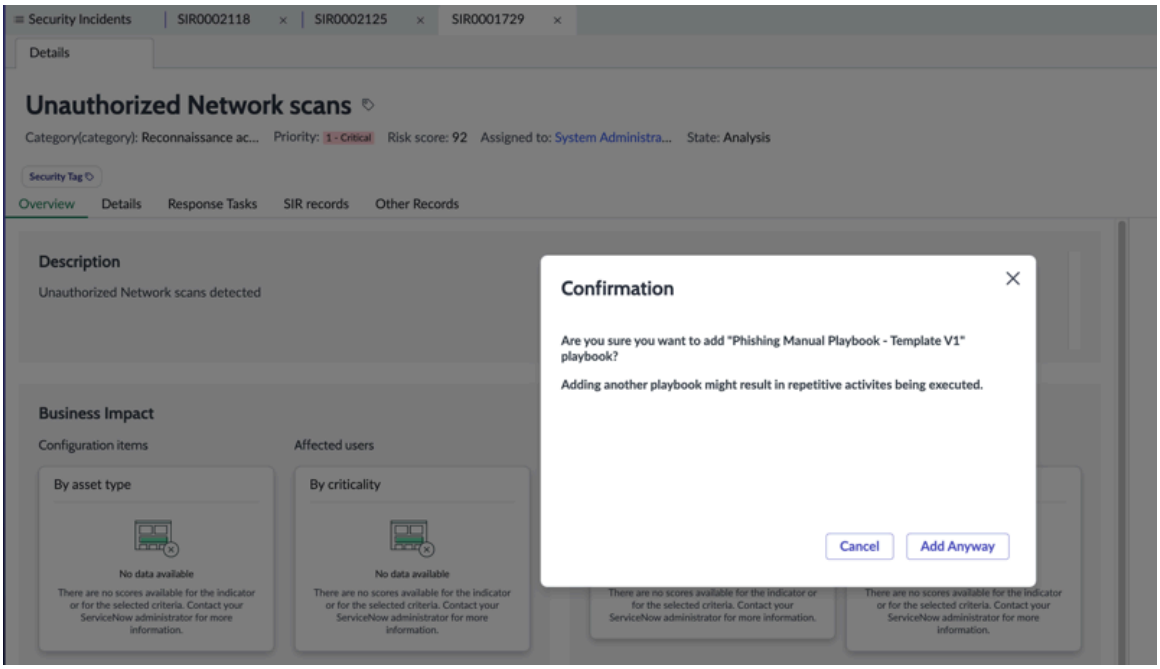


The **Add Playbook** dialogue box is displayed.

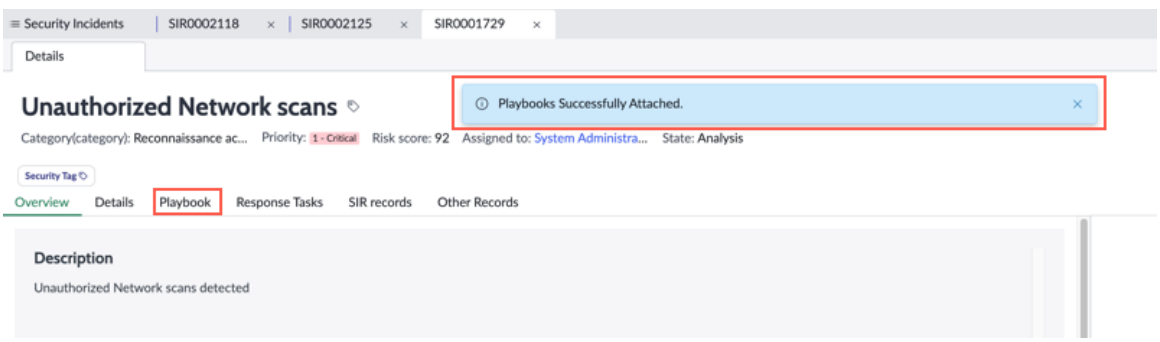
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Select the playbook template.
5. Click **Add Playbook**.
   A confirmation message dialogue box is displayed for you to confirm.
6. Click **Add Anyway**.

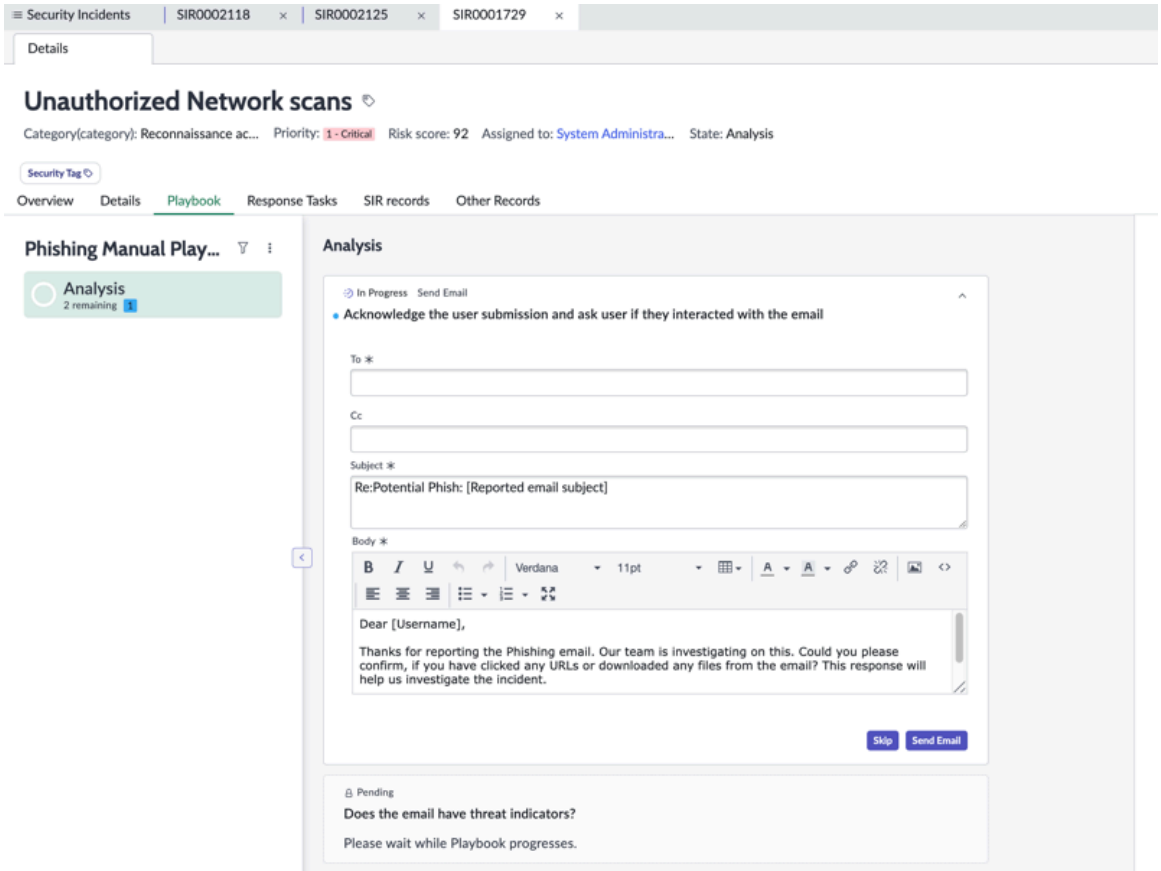


7. The **Playbook** gets added next to the **Details** tab.



8. Click the **Playbook** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Perform the series of activities as listed to move to the next level.

> **Note:** If a Security incident is associated with a playbook, until the associated playbook gets closed or cancelled the user cannot again associate the same playbook to the same security incident.

Prerequisites for the Playbooks

You need the following roles and plugins to build the Playbooks.

Role required: admin.

- Enable the Process Automation Designer (PAD) [com.glide.pad.license] plugin.
- Enable the following plugins for a playbook experience:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Enable Security Operations spoke to access flows [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Commons.

Make sure that you have read the platform documentation on Exploring playbooks and Process Automation Designer before you start with this guide.

Rebuilding existing playbooks in Workflow Studio

You can't convert existing flows directly into playbooks in Workflow Studio. Each flow designer step that creates a response task to guide the analyst must be broken down into separate actions or subflows.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You are not allowed to convert existing flows directly into playbooks in Workflow Studio. Each flow designer step that creates a response task to guide the analyst must be broken down into separate actions or subflows. By using these granular subflows or actions, you must create activity definitions. After you build these activity definitions, they get added as activities within stage in the process definition. You can reuse activity definitions across multiple playbooks.

You can customize each activity to render the required actions within them and how the card should look while building the activity definition. The activity can show email clients, tables, actions, KB articles, URLs, and so on. You can define how the activity definition and underlying action or subflows are created.

For more information, refer to the following sections.

- Activity definitions
- Process Automation Designer

Activity Definitions

The ServiceNow AI Platform provides a few activity definitions within the base system. In addition, for the playbooks that SIR Workspace base system, there are a few activity definitions defined in the base system under Enterprise Security Case Management PAD Commons application.

Role required: sn_si.admin.

Here's the list of activity definitions that are a part of the base system:

Activity Definition	Table	Description	Application
Wait For Condition with No Experience	Global[global]	Wait for Condition with no experience	Enterprise Security Case Management PAD Commons
Submit to CSF X Sandbox	Security Incident [sn_si_incident]	Submit to sandbox	Enterprise Security Case Management PAD Commons
Send Email	Security Incident [sn_si_incident]	Send email activity for SIR playbooks.	Enterprise Security Case Management PAD Commons
Search Email	Security Incident [sn_si_incident]	Search emails on email server	Enterprise Security Case Management PAD Commons
Update Task State	Security Incident [sn_si_incident]	Update the task state	Enterprise Security Case Management PAD Commons
Delete Email	Security Incident [sn_si_incident]	Delete emails	Enterprise Security Case Management PAD Commons
Yes No Outcome	Task [task]	Expected outcome	Enterprise Security Case Management PAD Commons

Example Activity Definition: Send email

The following is an example of Send email activity definition.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Basic

The basic details capture the name (label), application, description, table, and from all the applications it's accessible from.

Add the Automation plan, Activity experience and submit. After submitting, edit the document to add more details against each tab.

Automation Plan

The Automation Plan associates the backend action or subflows built using the flow designer. This example uses: **Send Email - ESCM Activity** subflow.

This subflow enables sending an email. It has the core logic to send an email. It has all the input fields and output fields defined.

All the input fields are shown within the automation plan section. Each input field can be enabled to be visible only for the admin, in the standard modal, in the standard modal and the configuration panel:

- **Admin visibility only**: when set to admin, only admin can view it.
- **Include in standard model**: when set to view in the standard modal, it appears only in the properties modal.
- **Include in standard model and configuration panel**: when set to view in the standard modal and the configuration panel, it appears in the PAD configuration panel as well as in the properties modal. For more information, see Activity definitions

You can define the input fields at the time of activity definition itself, provided you don't have any need to change these values at the time of configuration. This helps the business process owner save time while configuring an activity within a process.

Activity Experience

The activity experience tab defines how the activity card is rendered at run time. The base system provides the following experience types:

- Approval
- Catalog Item
- Create Record
- Instructional
- Knowledge
- List
- Notification
- Record

Based on the type of experience you select, the further fields are populated. For more information, refer the ServiceNow AI Platform documentation.

In this example, **Record** type is selected.

Note: For example, if you want to render a table, you can choose list as the experience type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Associated Record

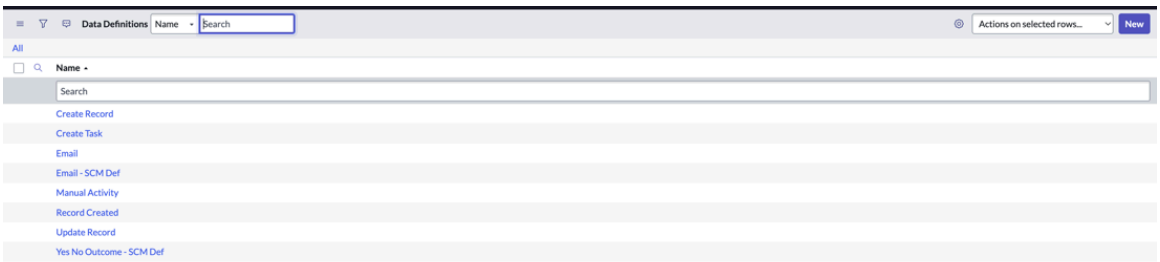
Use this record to store the associated data pertaining to the current activity. This would capture the run time data, as well the status of the experience.

- Associated table: Flow Data
- Associated Record: VL
- Experience status table: Flow Data
- Experience Status record: VL

In this example, Flow data table is used to capture the run time data. The run time data can vary based on the use case. In this example, the run time data are fields like To, cc, Subject, and body. For each use case, a flow data definition needs to be created to define the type of the run time data.

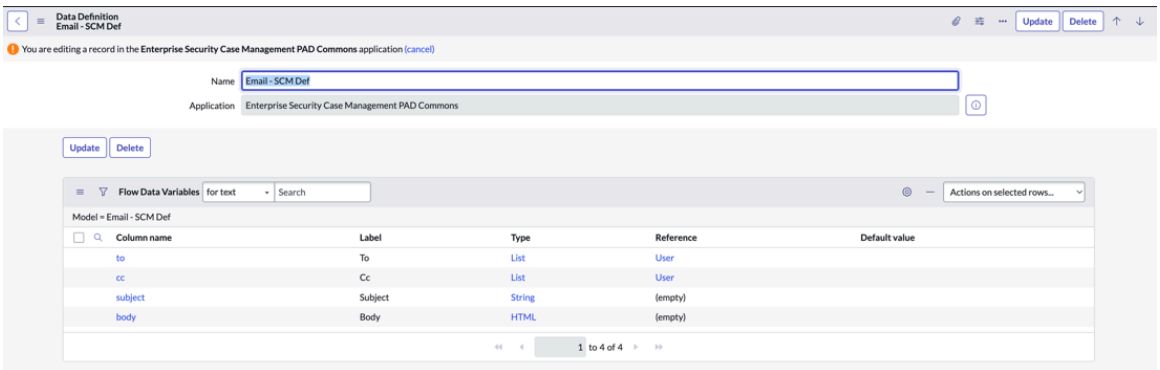
1. Navigate to the left pane and enter **sys_flow_data_definition.list**. It displays the list of definitions created for the flow data table.

Associate record



2. Open **Email - SCM Def** to view the definition related to this example.

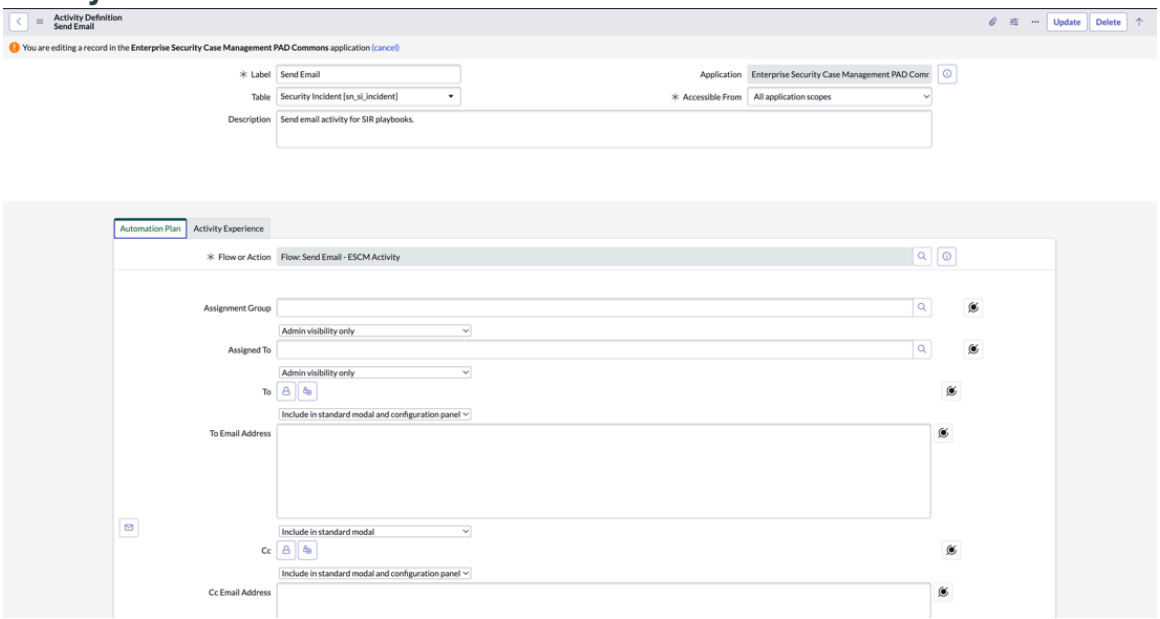
Email - SCM Def



This flow data definition must be used by the subflow or the action that is associated with this activity definition (Refer automation plan) to capture the run time data.

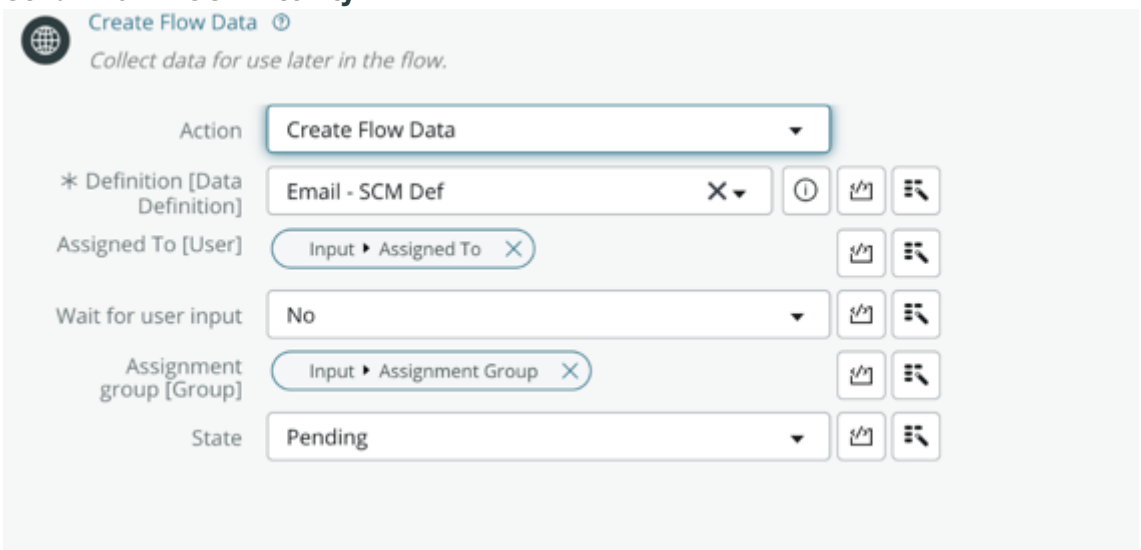
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activity Definitions



3. In this example, open the subflow: **Send Email - ESCM Activity**. Under **Create Flow Data** step, the flow data definition you created is mapped against the **Definition** field. This flow data record is used across the subflow. In this example, the activity card status (experience status) is captured in the flow data table.

Send Email - ESCM Activity



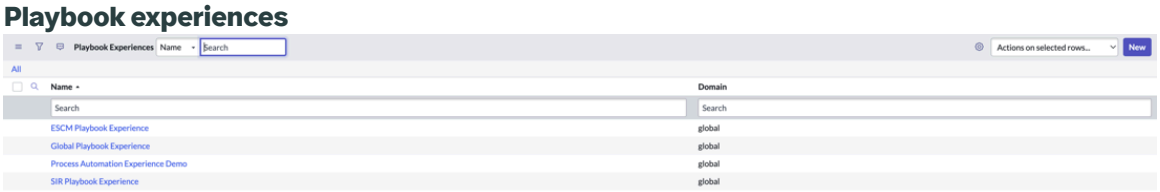
Note: If you want to capture the runtime data in a different table record other than flow data table, say for example in a response task. You can select the associated table as Response task table. The associated record should be set to response task record created by the subflow.

Similarly, experience status table captures the status of the activity card. In the base system, the state field of the flow data table is mapped to the activity card status. So, when flow data table is used to capture the experience status, it automatically updates the activity card status. You could also use a different table other than flow data table to capture the experience status.

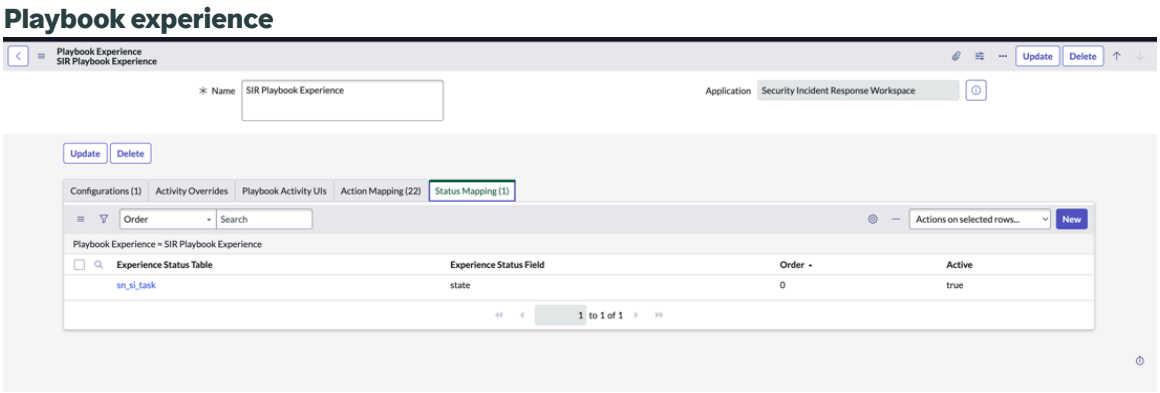
For example, if you would want to map the response task status to the activity card status then that is possible. To do so:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to **All** > **Playbook Experiences**.



2. Open **SIR Playbook experience**.
3. Open **Status Mapping** related list.

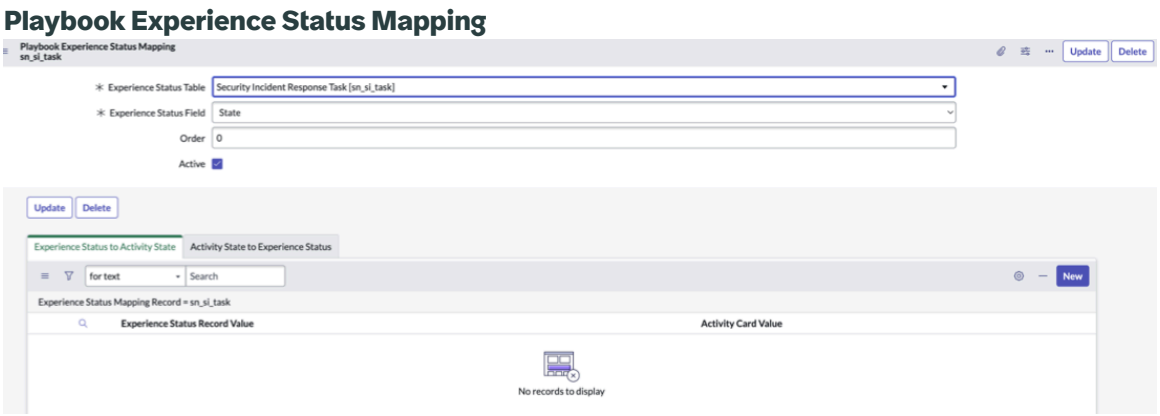


4. Enter the **Response Task** against Experience Status Table field.
5. Enter the **State** against Experience Status field.

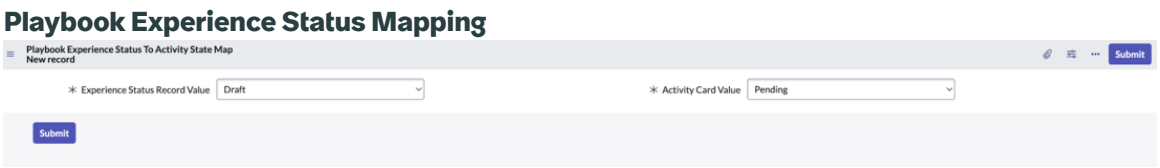


6. Click **Submit**. The record is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Under Experience Status to Activity State, map the states of response task to activity card status.
8. The left side shows the states of the Response Task, and the right side shows the activity card status.



9. The mapping can be bi-directional. Under Activity State to Experience related list as well, map the statuses correctly. This step is the reverse of the previous step. In this case, the left side shows the activity card status, and the right side shows the response task status.



Details

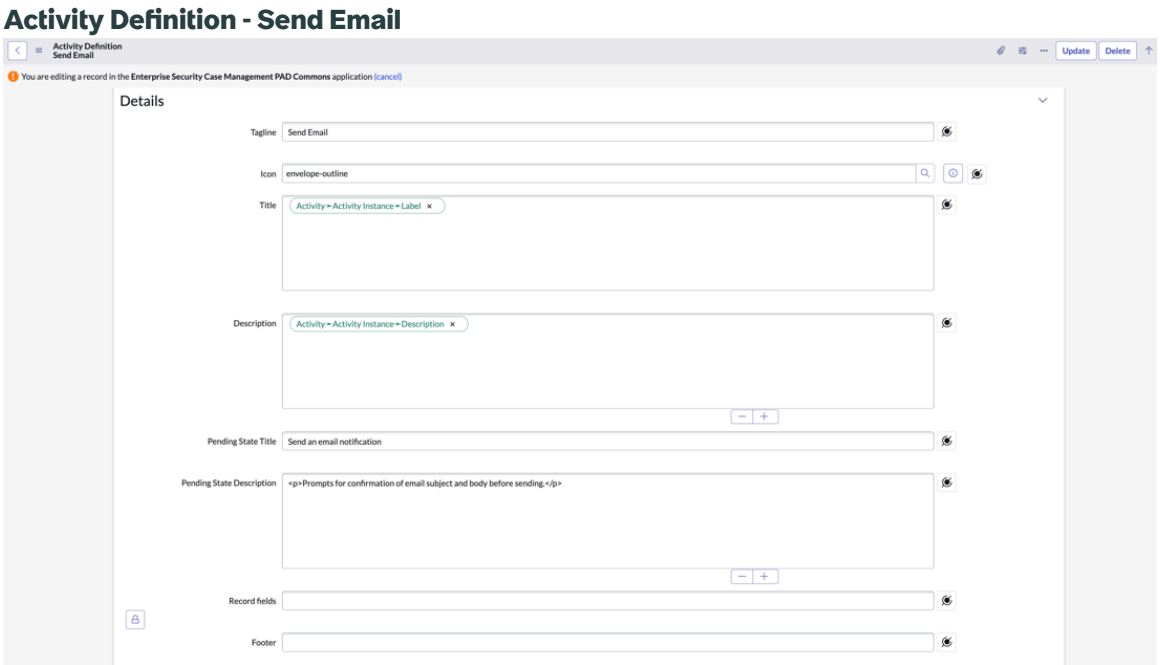
- Tag Line: Send Email
- Icon: Envelope outline (not shown in the user interface)
- Title: **Activity** > **Activity Instance** > **Label**. Here we have selected the activity instance's label. This dot-walking will replace the label value as the title dynamically at run time.
- Description: **Activity** > **Activity Instance** > **Description**. Here we have selected the activity instance's description. This dot-walking will replace the label value as the title dynamically at run time.
- Pending State Title: Send an email notification. This is the title when the activity is in Pending status.
- Pending State Description: Prompts for confirmation of email subject and body before sending. This is the description of the activity card when the status is pending Record Fields: There are record fields selected in this example.

  Record Fields are comma-separated list of field names to display for the associated record in a name-value pair list. Data is pre-fetched on the server, dot-walking is supported and #**canRead()**#permissions are evaluated on each field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Footer: There's no footer defined for this example.

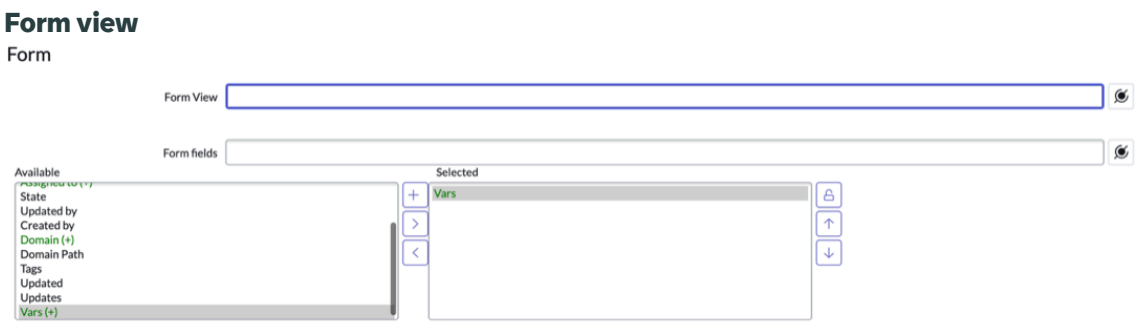
  Footer is a text in a gray area of the card footer. You can add any meaningful information to shown.



Form

- Form View: collect_data
- Form Fields:

This example uses collect_data view to show the fields that must be presented to the user to enter inputs. Collect_data view is a platform provided view corresponding to flow data table. Alternatively, you could leave Form View as empty, and select Vars from the list of values available against Form Fields. (click the lock icon to open the list of available values).



Attachments

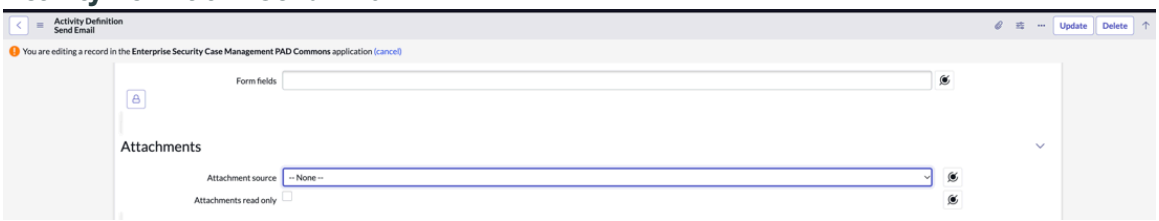
In this example:

- Attachment Source is empty.
- Attachment Read only not selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Attachment Source - Drop down. What attachments to show on the card: Those attached to the Parent Record, the Associated Record, or none.
2. Attachment Read only - True or False. Prevent the user from renaming or deleting the existing attachments.

Activity Definition - Send Email



Features

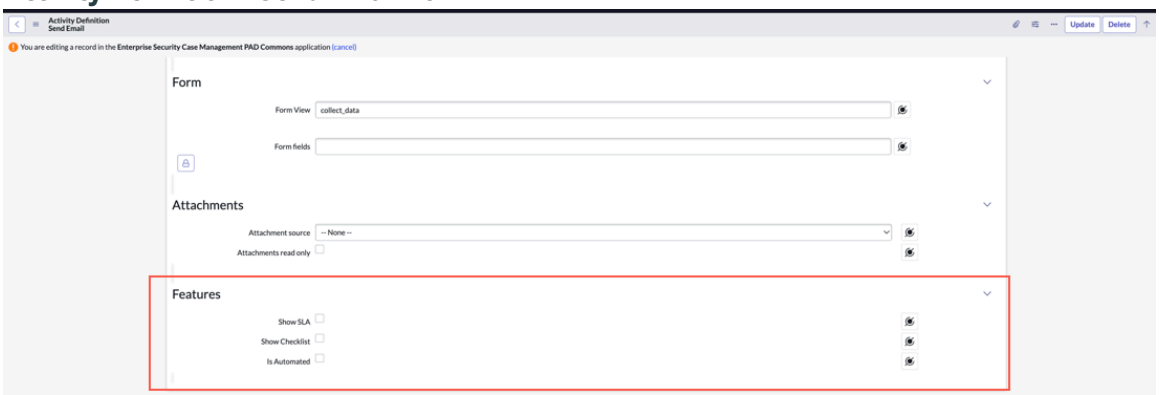
In this example,

- Show SLA - Cleared
- Show Checklist - Cleared
- Is Automated - Cleared

Show SLA: True / False. Renders an SLA timer in the header of the card for the Associated Record. The SLA is chosen according to the SLA Configuration record specified in the Playbook configuration.

1. Show Checklist# True or False. Renders any checklist that is attached to the Associated Record. The checklist is editable and changes are saved without requiring a Declarative Action.
2. Is Automated - True or False. If true, then the#**tagline**# and#**icon**#will be overridden with the text **Automated Task** and an automated icon.

Activity Definition - Send Email Form



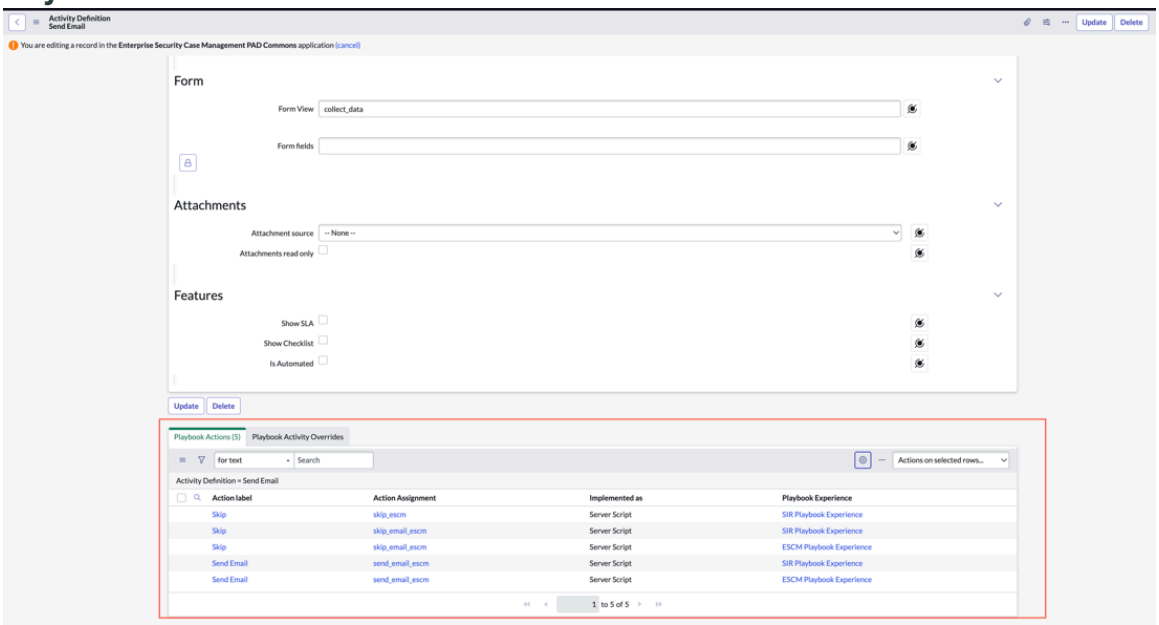
Playbook Actions in Activity Definition

This section has the actions that will be rendered on the activity card. This example has **Skip**, and **Send Email** as actions.

To add a new action to the activity card, you must create a record in the **Playbook Actions** related list present at the bottom of the page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Playbook Actions



1. Click **New**.
2. Select existing activity action against Action Assignment field.
3. Select **SIR Playbook Experience** against Playbook Experience field.

Create an Activity Action

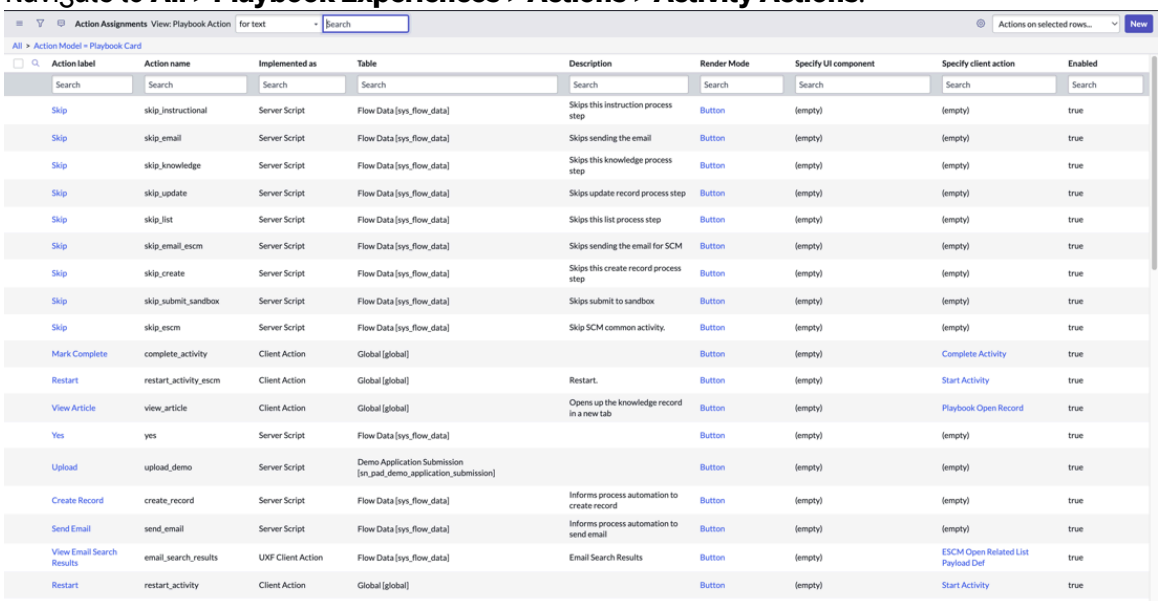
Following is procedure to create an activity action.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Playbook Experiences** > **Actions** > **Activity Actions**.



2. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Refer to the ServiceNow AI Platform documentation to know how to create these actions. In this example, Skip is implemented as a server script.

3. **Playbook override:**

   You can also override the existing activity experience type. For more information, see ServiceNow AI Platform documentation. No Playbook overrides are added in this example.

Submit to CSF X Sandbox

Submit to CSF X Sandbox is an example of an activity definition process.

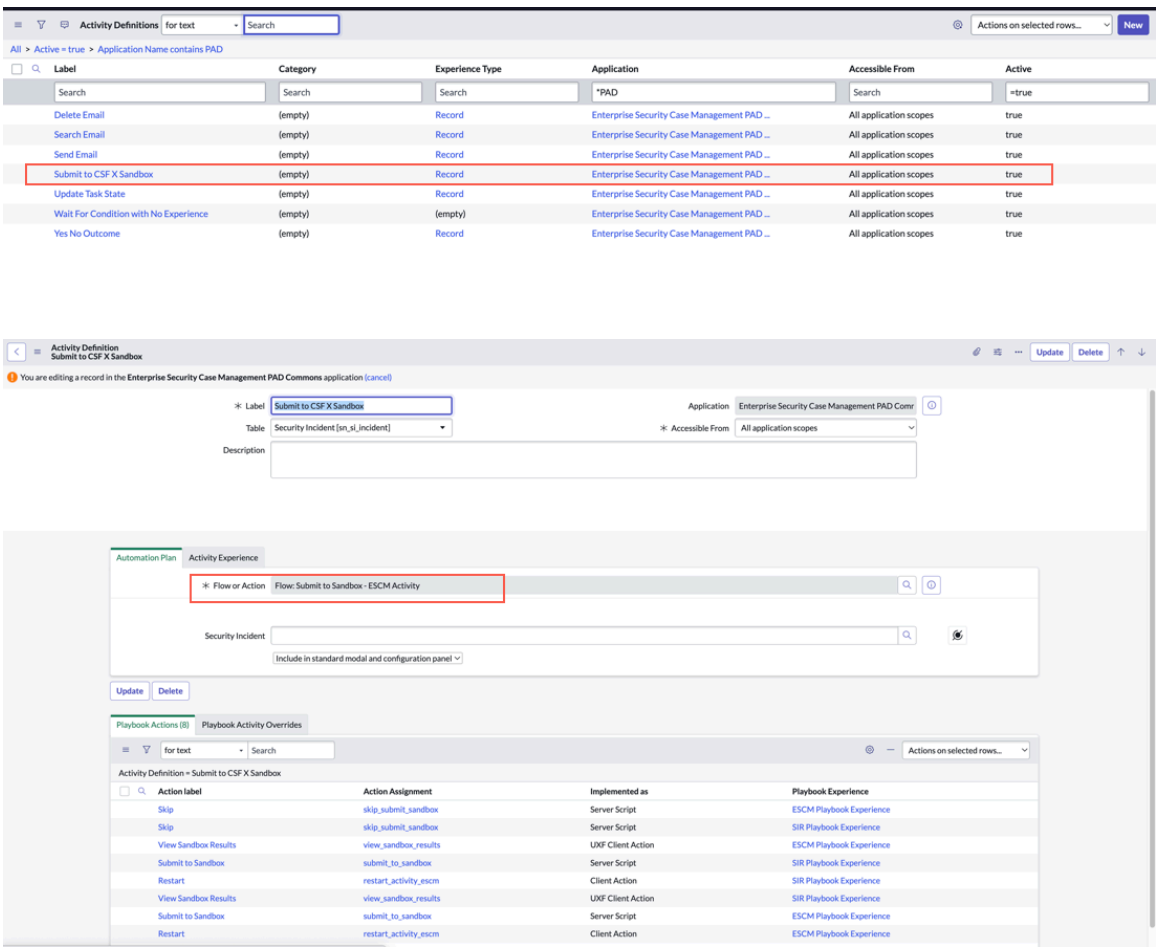
Basic

The basic details captures the name (label), application, description, Table, and from which all applications it is accessible from.

Add the Automation plan, Activity experience and submit. Once submitted, edit the document to add more details against each tab.

Automation Plan

The Automation Plan associates the backend action/subflow built using the flow designer. This example uses **Submit to Sandbox - ESCM Activity**sub-flow.



This sub-flow enables submitting the malicious observables to sandbox. It has all the input fields and output fields defined.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident is the input field.

Activity Experience

In this example, **Record** type is selected.

Associated Record

Associated record is to store the associated data pertaining to the current activity. This would capture the run time data, as well the status of the experience.

- Associated table: Flow Data
- Associated Record: VL
- Experience status table: Flow Data
- Experience Status record: VL

Details

- Tag Line: Send Email
- Icon: Envelope outline
- Title: **Activity** > **Activity Instance** > **Label**. Here we have selected the activity instance's label. This dot walking will replace the label value as the title dynamically at run time.
- Description: VL (Sub-flow output is mapped)
- Pending State Title: blank
- Pending State Description: blank
- Record Fields
- Footer

Form

- Form View: blank
- Form Fields: blank

Attachments

In this example:

- Attachment Source - None
- Attachment Read only - Unchecked

1. Attachment Source - This is a drop down. What attachments to show on the card: those attached to the Parent Record, the Associated Record, or none.
2. Attachment Read only - This is a True / False. Prevent the user from renaming or deleting the existing attachments.

Features

In this example,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Show SLA - Unchecked
- Show Checklist - Unchecked
- Is Automated - Unchecked

Playbook Actions in Activity Definition

This section has the actions that will be rendered on the activity card.

This example has Skip, View Sandbox Results, Submit to Sandbox, and Restart actions.

To add a new action to the activity card, you need to create a new record in the Playbook Actions related list present at the bottom of the page.

Playbook override

No Playbook overrides for this example.

Sample Playbooks for SIR Workspace

You can create or configure playbooks for SIR Workspace quickly and easily without writing complicated code. You can use these playbooks to resolve security threats in a step-by-step manner. You can invoke the security incident playbook flow automatically or manually.

The Security Incident Response provides the following playbooks with the base system:

- Playbook for Manual Phishing
- Playbook for Automated Phishing
- Playbook for Manual Malware
- Playbook for Automated Malware
- Playbook for Failed Login Manual

Working with MSI Records

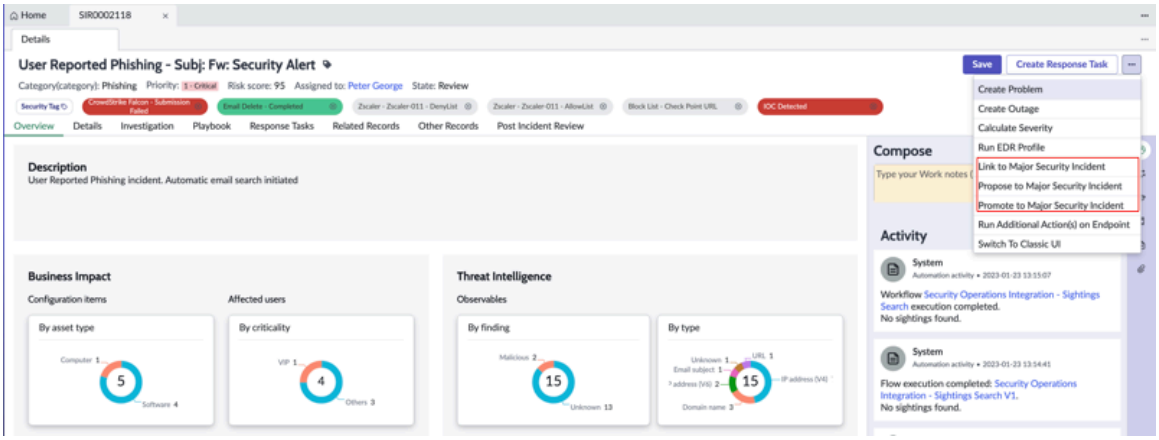
Using the Security Incident Response workspace, you can propose, promote, or link security incidents as major security incidents when the incidents are identified as critical threat to the organization.

After you install Major Security Incident Management (MSIM) on your ServiceNow AI Platform instance, you can then handle the transition of security incidents to major incidents.

The Major Security Incident Management (MSIM) UI actions are displayed on the top right of the security incident form banner of the SIR workspace. Select the UI action as applicable.

Note: Some actions are contextual. For example, Unlink action is available only when the security incident is already proposed or promoted or linked to a major security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Propose as Major Security Incident

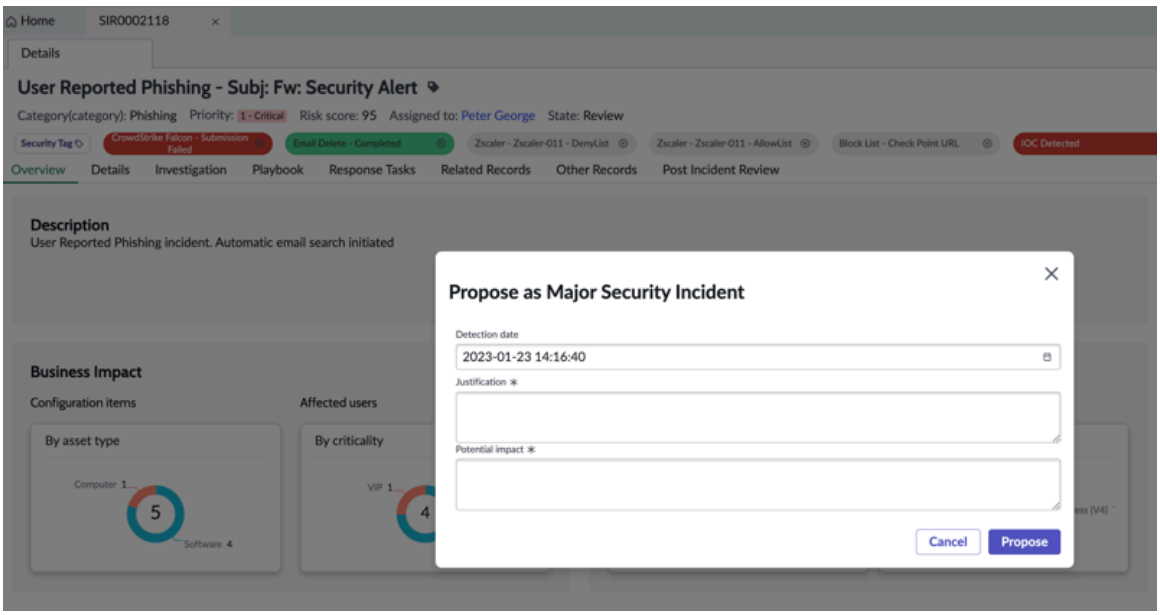
Propose a security incident as a Major Security Incident (MSI).

Before you begin

Role required: sn_si.analyst.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.
3. Click **Propose to Major Security Incident**.



4. On the form, fill in the fields such as Detection date, Justification, and Potential impact.
5. Click **Propose**.
   The incident record is proposed as a major security incident candidate.
   After the incident record is proposed as a major security incident candidate, **Major Security Incident Candidate** tag is applied and displayed on the security incident form banner.

> **Note:** Click **Unlink from Major Security Incident** to unlink the incident if you don't wish to propose or doesn't have any critical impact. The incident will be unlinked and lists under the list view to the security analyst for remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Promote to Major Security Incident

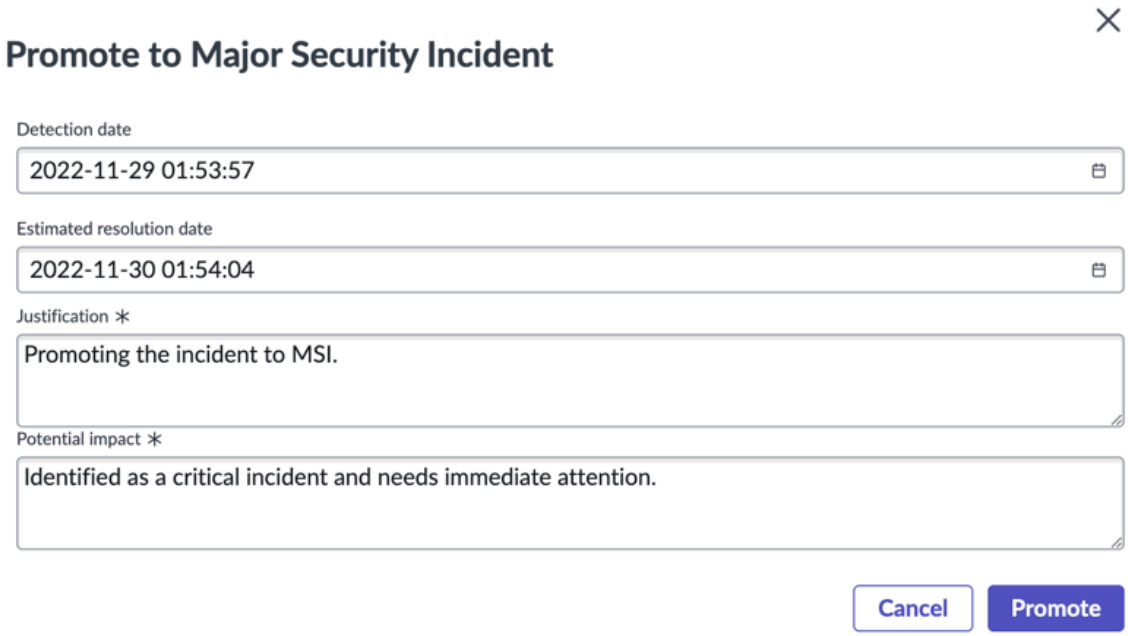
Promote a security incident to major security incident.

Before you begin

Role required: sn_si.analyst.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.
3. Click **Promote to Major Security Incident**.
4. On the form, fill in the fields such as Detection date, Estimated resolution date, Justification, and Potential impact.



5. Click **Promote**.
   The incident record is promoted as a major security incident.
   After the incident record is promoted as a major security incident, **Major Security Incident** tag is applied and displayed on the form banner.

> **Note:** You can also unlink the major security incident if the incident is not critical, the incident will then be unlinked and lists under the list view for the security analyst remediation.

Link to Major Security Incident

Link a security incident to a major security incident as child security incident(s).

Before you begin

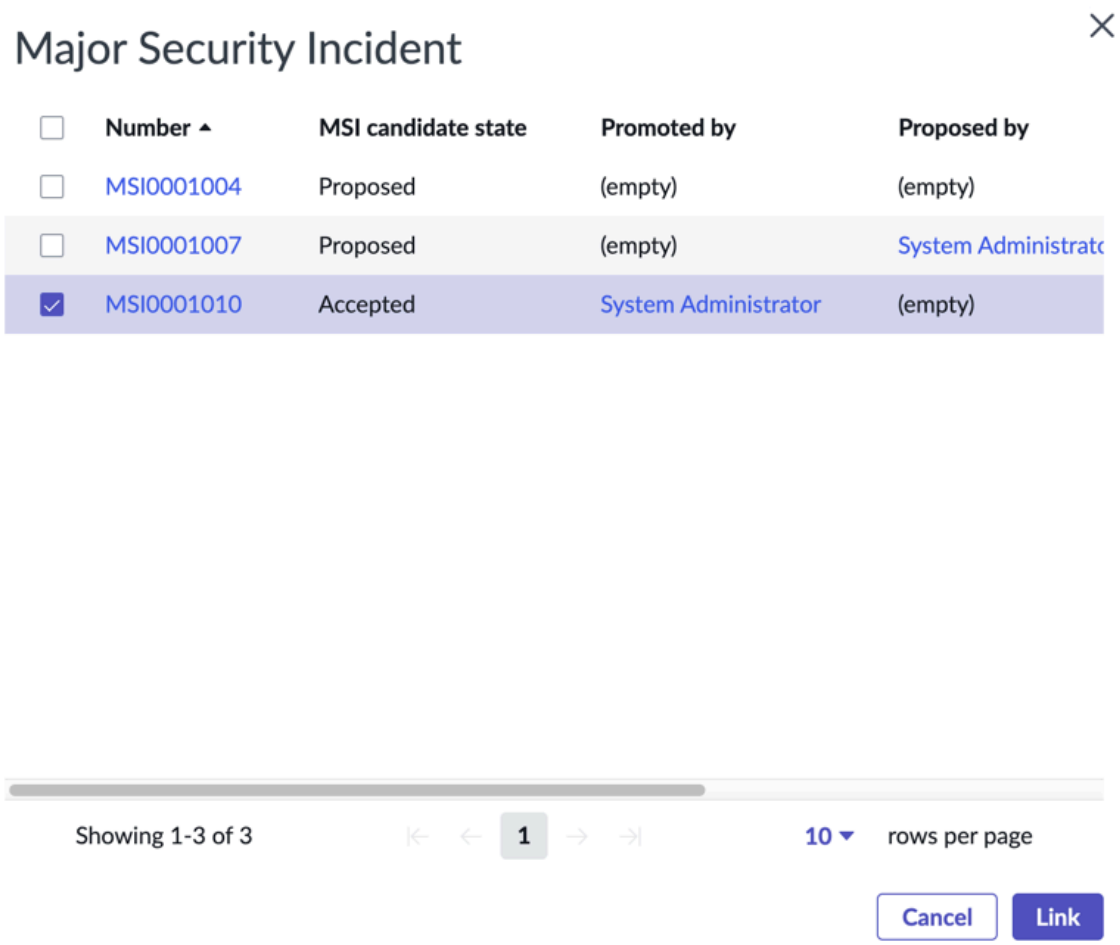
Role required: sn_si.analyst.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Open any security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Link to Major Security Incident**.



4. Select the incident(s) to link to a major security incident.
5. Click **Link**.
6. The incident record is linked as a child incident of the major security incident.
   After the incident is linked as a child incident to a major security incident, **Major Security Incident** tag is applied and displayed on the form banner.

Working with Form UI actions

Following are the UI actions that are displayed on the security incident form.

To navigate to the form UI actions:

1. Go to **Workspaces** > **Security Incident Response Workspace**.
2. Select any security incident from the list view.
3. All the UI actions are present in the top-right corner of the security incident form.

Workspace Form UI actions

Field Name	Description
Discuss	Create or start a sidebar discussion for the security incident.
Save	Save or update the Security Incident Response record after making any changes.

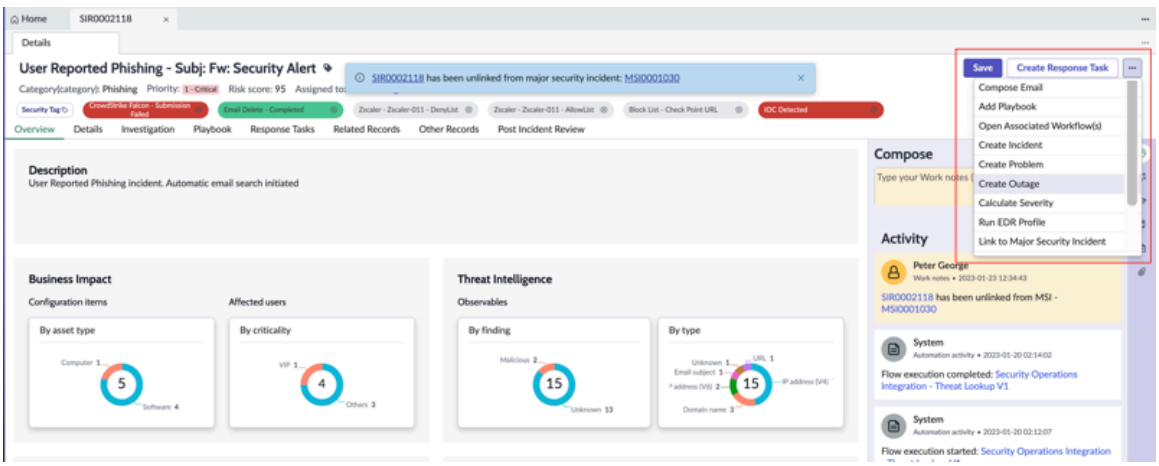
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
Create Response Task	Create a response task for the security incident.
Compose Emails	Compose emails for the security incident.
Add Playbook	Add the playbook manually for the security incident.
Create Incident	Create an incident within the security incident.
Create Customer Service Case	Create a customer service case for the security incident that will be tracked by the Customer Service Management (CSM) team. **Note:** This option is available only when Customer Service Management (CSM) is installed.
Open Associated Wokflow(s)	Open any workflow(s) context associated with the security incident. This option would be visible only if there are any workflows.
Create Change Request	Create a change request within the security incident.
Create Problem	Create a problem within the security incident.
Create Outage	Create an outage within the security incident.
Calculate Severity	Calculate the severity of a security incident using predefined calculators. The severity is calculated based on the predefined rules in the calculators. The severity of an incident is based on the Risk score, Business Impact, and Priority.
Run EDR Profile	Select and run the EDR Profile for the required integration. **Note:** This option is available only when any integrations are installed.
Link to Major Security Incident	Link a security incident to a major security incident.
Report risk event	Report this security incident as a risk event to the Risk Management team. The Risk Management team analyzes the event and ensure that such events and the associated losses don't reoccur. **Note:** This option is available only when Risk Management is installed.
Unlink from Major Security Incident	Unlink from major security incident.
Propose as Major Security Incident	Propose a security incident as a major security incident.
Promote to Major Security Incident	Promote a security incident as a major security incident.
Run Additional Action(s) on Endpoint	Run additional actions on the endpoint. **Note:** This option is available only when Endpoint integrations are installed. For example: FireEye HX

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
Create a new Event in MISP	Create and modify events in MISP automatically or manually. **Note:** This option is available only when MISP integration is installed.
Associate MITRE ATT&K Technique	Associate MITRE ATT&K Techniques to the security incident. **Note:** This option is available when MITRE ATT&K is installed.
Show MITRE ATT&K info	Shows the MITRE ATT&K information associated with the security incident. **Note:** This option is available when MITRE ATT&K is installed.
Add to Security Case	Add the security incident to an existing or new security case. **Note:** This option is available when Threat Intel is installed.
Switch to Classic UI	Enable the analyst to switch between classic and new UI so that the analyst can also work on the existing functionalities that aren't available on the new workspace yet.
Cancel	Cancel a security incident. After you select **Cancel** all the related records such as response tasks, child security incidents will also get canceled.
Delete	Delete a security incident record.

4. Click on a security incident number to view the security incident record. You can see the UI actions on the top of the page.



Security Incident Closure workflow

Close the security incident by updating the incident state.

Before you begin

Role required: sn_si.analyst

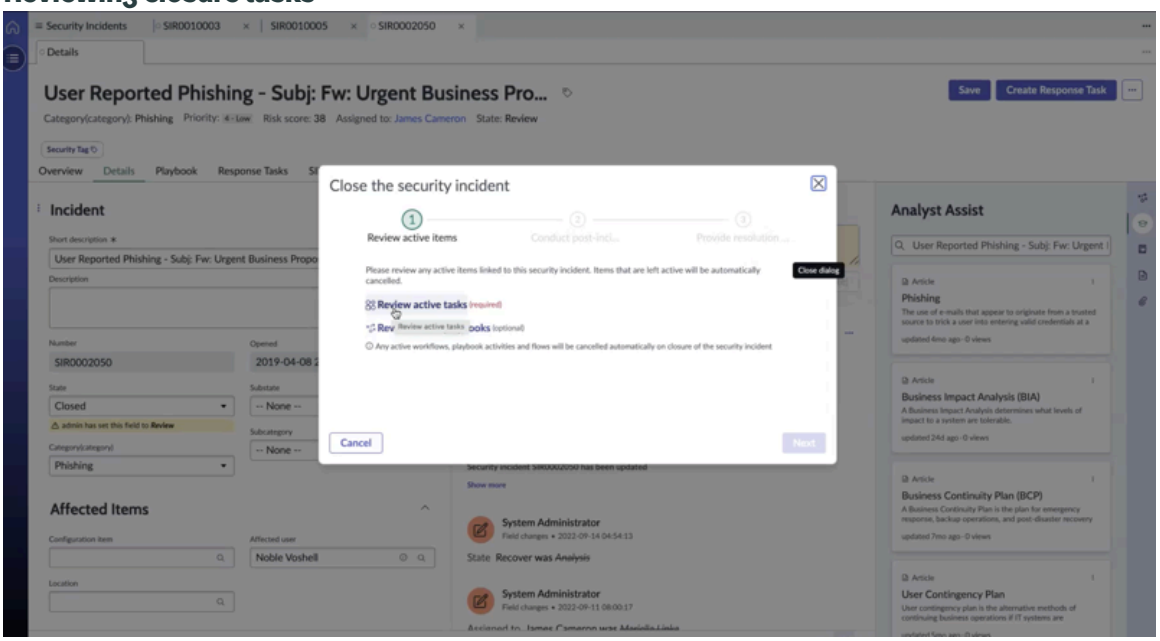
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. For example, go to **Lists** > **Security Incidents** > **Open incidents**.
3. Open an incident that you want to close.
4. Go to the **Details** tab.
5. Drill down to the incident state and select **Close**.
6. Perform the closing activities.

   - This is a mandatory step to review any task before closing a security incident. Any response tasks must be reviewed by the analyst and closed or canceled before closing as security incident. When the Analyst clicks on **Review active tasks**, it takes the user to the **Response Tasks** tab. A session message is displayed prompting that you are in the process of closing a security incident. Click **continue**.
   - Click **Continue**. The first step – review active tasks in closing the security incident is complete.

Reviewing closure tasks

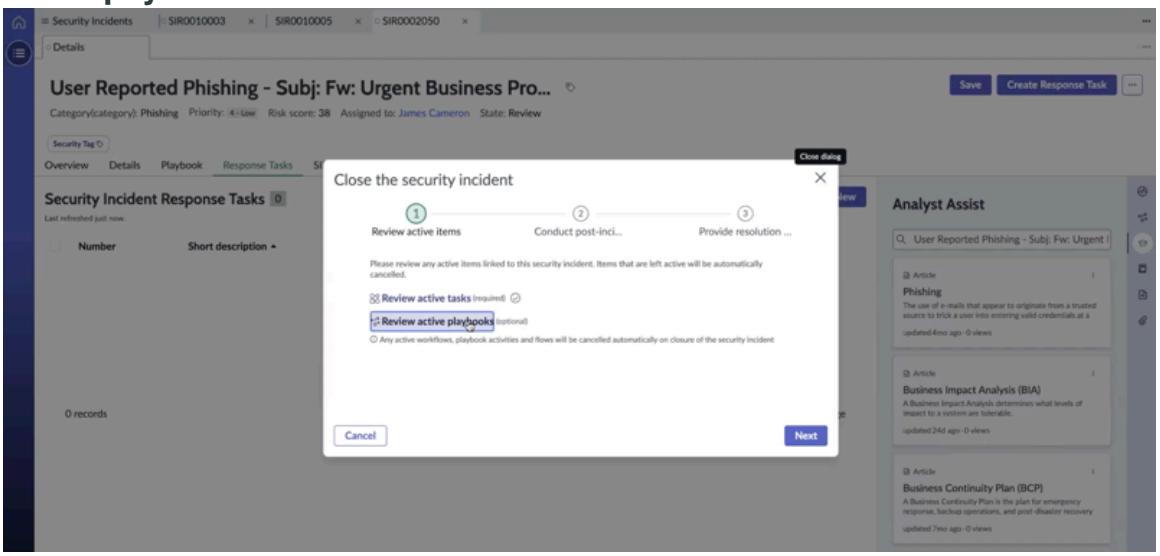


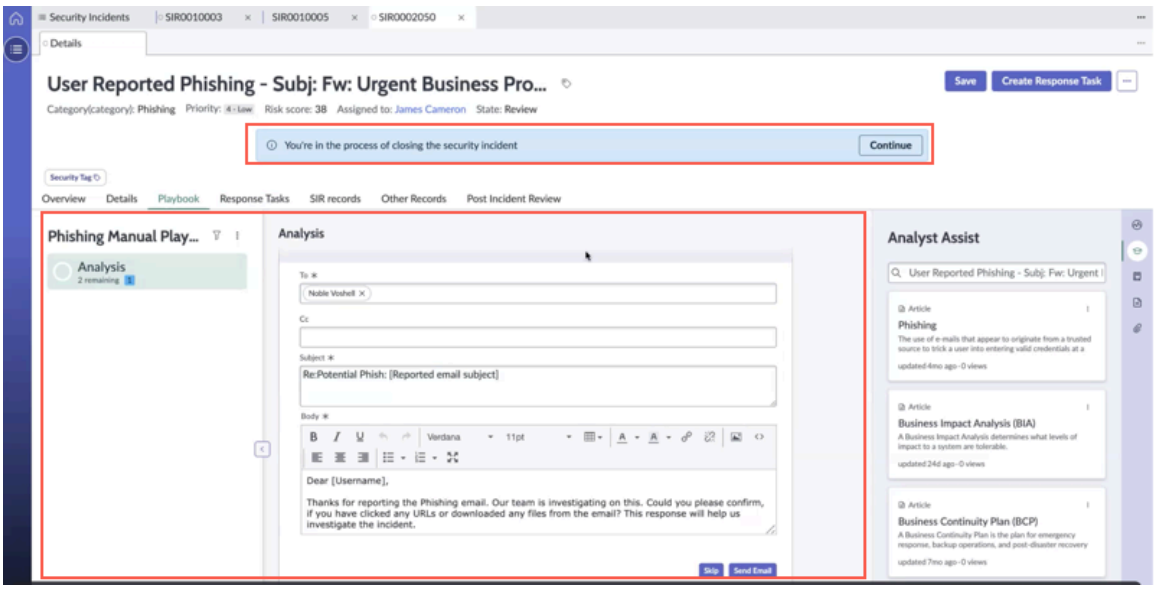
   - Move to the next step to review the active playbooks for the analyst to review, which is an optional step. You can click the link to review the active playbook task and close them as required.

> **Note:** Any active workflow(s), playbook activities, and flows will be automatically cancelled on closure of the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Review playbook tasks

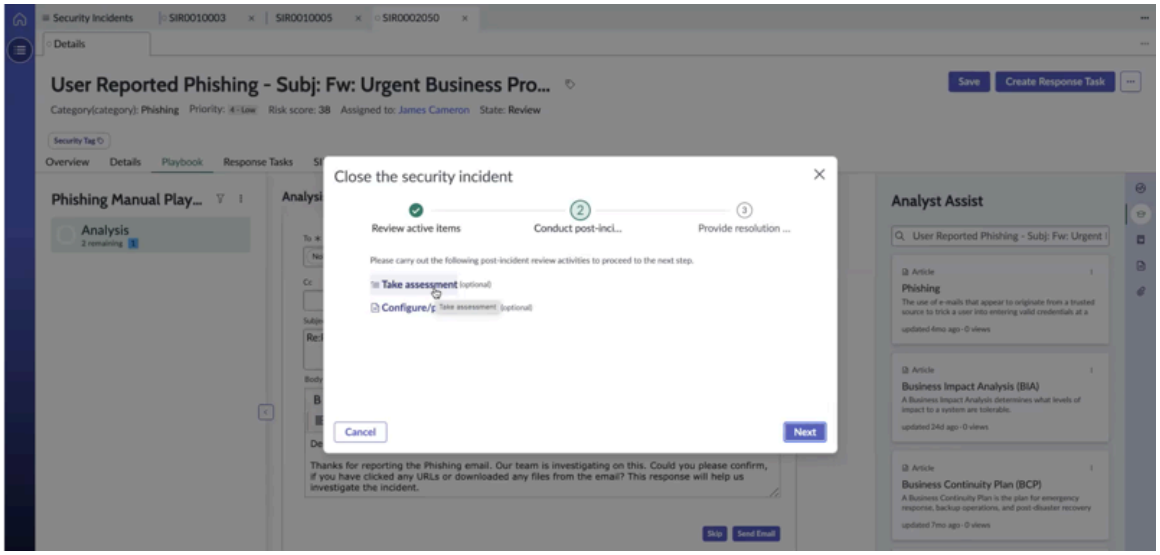


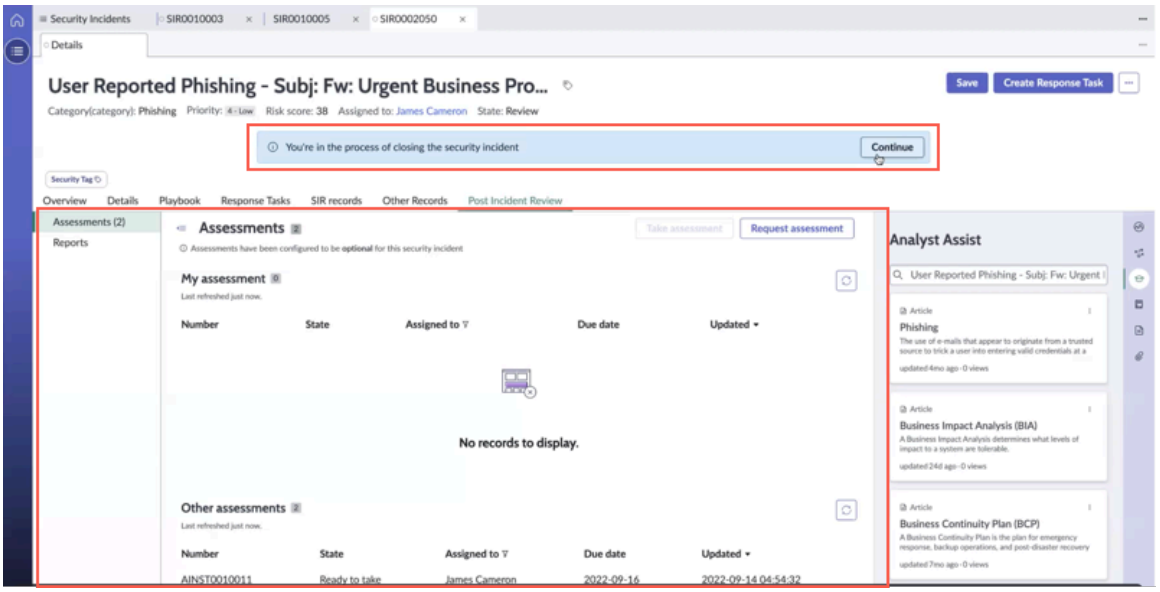


- Post-incident review report: You will now be moved to review the post-incident activities to proceed further with the closure. If the assessment is optional then skip the step or if the assessment is mandatory then take the assessment and complete it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

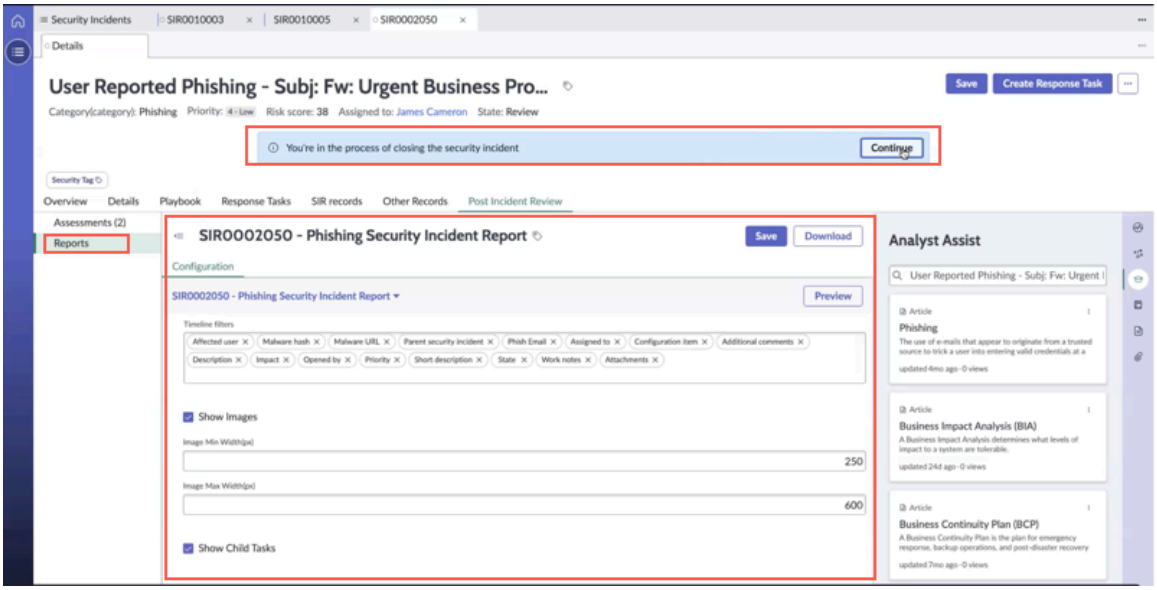
Review/Take assessment



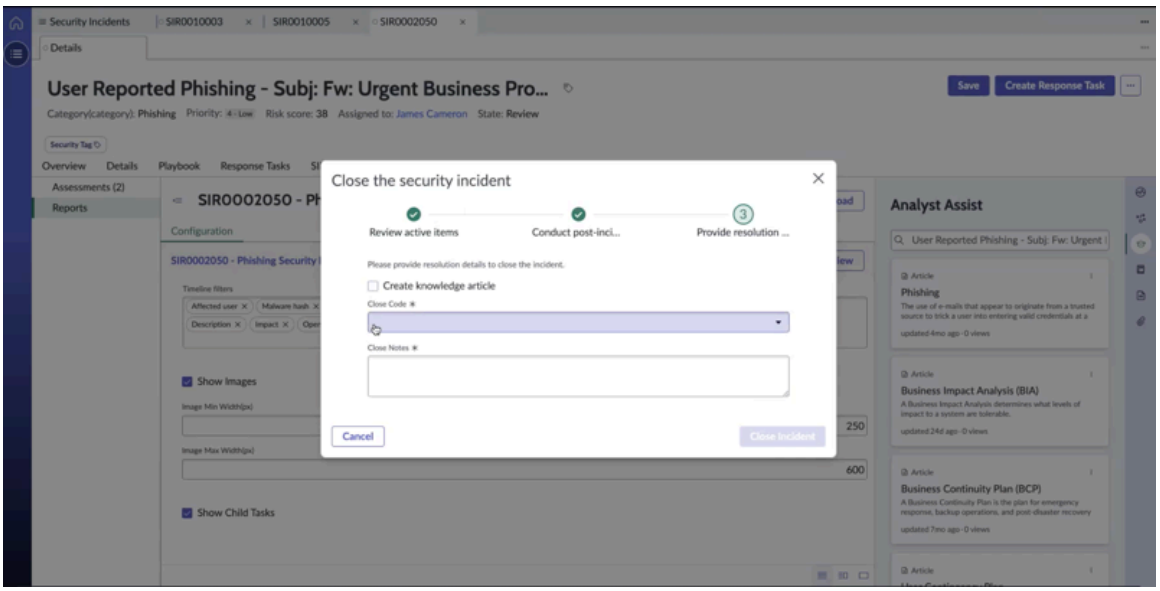


- Configure/preview report: This is again an optional step, click the link to review report and proceed to **Next** step.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- Provide Resolution details: The analyst can select the check box to create knowledge articles automatically.
- Provide the Closure code, Closure notes and click **Close incident**.



Note: By any chance if the analyst cancels the **Close the security incident** dialogue box, then the analyst can navigate to the **Details** tab and change the incident state to **close** to continue with the closure.

Handle security incidents using AWA

Using AWA, security analysts can handle the security incidents assigned to them, which are available in the inbox folder of SIR Workspace.

Before you begin

Role required: sn_si_analyst and awa_agent

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace**.
2. Select the **Inbox** button.
3. Select your presence state using the **Status** field.
   Available presence states are:
   - **Available**: Analyst is available and can accept security incidents. Incidents are available for picking only to agents whose status is available.

     Note: If auto-assigned is configured, security incidents are directly assigned to you.

   - **Away**: Analyst isn't available. Incoming incidents and not assigned.
   - **Offline**: The analyst is offline. Incoming incidents and not assigned. This is the default option.

   If your status is available, based on the configured service channel, queues and assignment rules, the incoming incidents are assigned to all the available security analysts including you. These incidents are either listed for you to accept or reject (if configured) or are auto-assigned to you.
4. You can **Accept** or **Reject** a security incident.

   Note: Reject option is only available if rejection handling is enabled in AWA. If rejection handling isn't enabled in AWA, incident is assigned to you on the basis of the configured service channel, queues, assignment rules, and your availability.

   When you accept a security incident, it's assigned to you. When you reject a security incident, you have to select the reason for rejecting the security incident.

Viewing SIR Workspace Dashboards

This section present the important metrics to analyze your Security Incident Response process such as new security incidents or the average age of open security incidents.

In the Classic UI, there are few standard dashboards available under homepage and Performance Analytics Dashboards that are available when Performance Analytics for Security Incident Response plugin is installed. All of these will now be available in the new workspace under the **SIR Dashboards** section.

Standard Dashboards under homepage:

- Security Incident Response Overview
  - Analyst Overview
  - Manager Overview (supported in future releases)
  - CISO Overview (supported in future releases)
- **Platform Analytics for** *`Security Incident Response`*
  - Security Incident Explorer
  - CISO Dashboard (future release)
  - Security Incident Management
  - Security Incident Management Premium KPIs
  - Security Operations Efficiency
  - Context Sensitive Analytics – SI Dashboard

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: There might be some repetition of dashboards across standard and platform analytics for security incident response dashboards such as CISO Dashboard. When the plugin is installed, there will be additional content in these dashboards and will not be available as duplicate.

Users need to install the plugin for the dashboards listed under Platform Analytics for Security Incident Response Dashboards to be present in the workspace. Otherwise, only the standard dashboards will be available.

In the current version of the SIR Workspace, the following dashboards are available under the **SIR Dashboards** section. The other dashboards that are missing will be available in later releases.

Security Incident Response Dashboards

Dashboard	Description
Standard Dashboard	
Security Analyst Overview	With this dashboard, security analysts can view security incidents summarized based on analyst's critical priority work, high priority work, security Incidents that are assigned to the analyst, tasks assigned to the analysts, and incident count.
Performance Analytics (PA) for Security Incident Response Dashboards	
Security Incident Explorer	With this dashboard, security managers and analysts can view security incidents summarized and grouped by category, subcategory, location, priority, and business impact. These views let managers and analysts quickly gain insight into the frequency in which attacks are occurring and which business services are affected.
Security Incident Management	With this dashboard, security managers can easily track the volume, performance, and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.
CISO Dashboard	Proposed to support in future release.
Security Operations Efficiency	With this dashboard, managers and analysts can view overall efficiency metrics and measure the performance of the SOC.
Security Incident Management Premium KPIs	With this dashboard, security managers can track and view the volume, performance, and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.
Context Sensitive Analytics – S	With this dashboard, managers and analysts can view the open security incidents, the average age of open Security Incidents, the average close time of security incidents, the percentage of security incidents that were

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response Dashboards (continued)

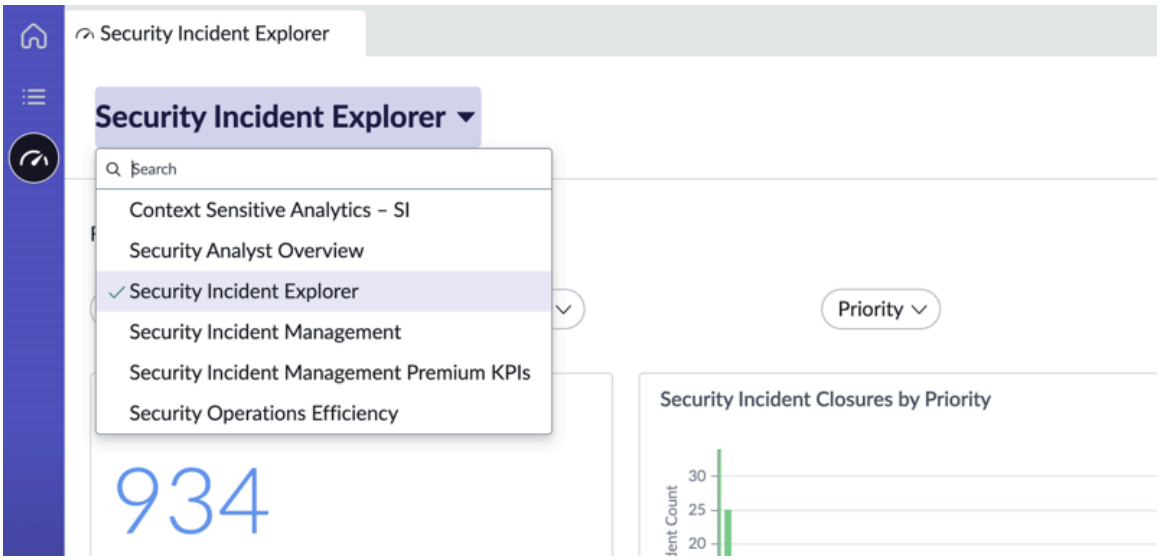
Dashboard	Description
	opened and closed on the same day, and the percentage of the incidents that were not updated in the last 5 days and 30 days.

Access SIR and PA Dashboards

The **SIR Dashboards** icon displayed on the left side of the workspace home page.

Note: Users with sn_si.manager or sn_si.admin access can edit the dashboards. The users must be within the same scope of the dashboards that the user is trying to make edits. For example, security analyst overview dashboard is available in the SIR workspace, then the user should also be in the same SIR workspace scope to make the edits to the dashboard.

1. Navigate to **Workspaces** > **Security Incident Management Workspace**.
2. Click on the **SIR Dashboards** icon.
3. Select the desired Dashboard from the drop down list.



You can edit the dashboards, add new elements to the dashboards, and create your own dashboards. For more information on how to use dashboards, see Working with responsive dashboards

View Security Analyst Overview dashboard

With this dashboard, security analysts can view security incidents summarized based on analysts' critical priority work, high priority work, security Incidents that are assigned to the analyst, tasks assigned to the analysts, and incident count.

Before you begin

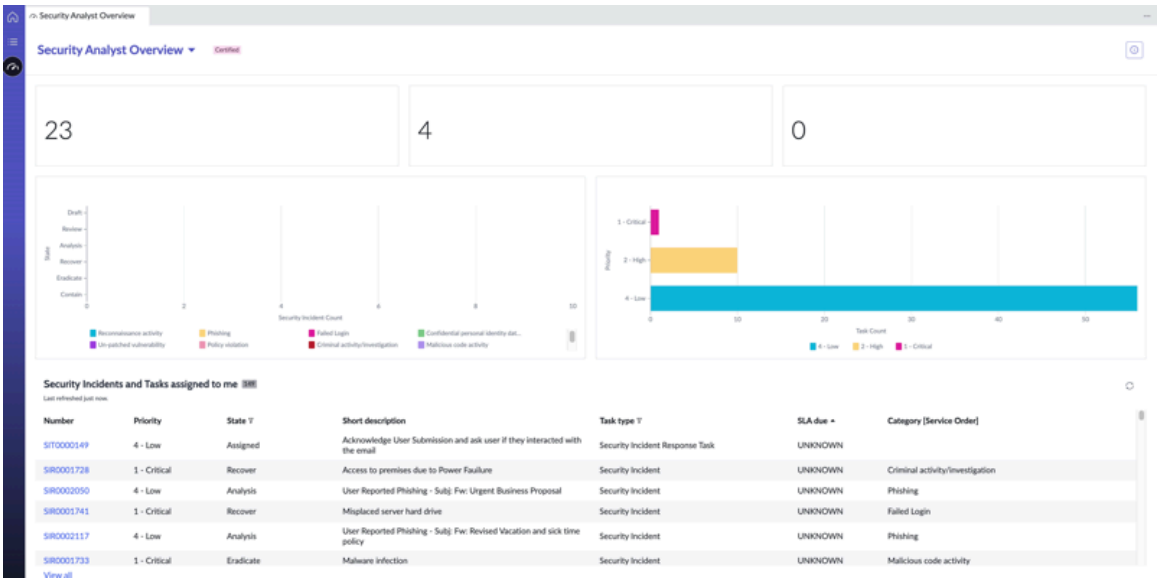
By default, the Security Analyst Overview dashboard is displayed for the users with sn_si.analyst access.

Role required: sn_si.analyst (Read), sn_si.manager or sn_si.admin (Write)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Security Analyst Overview** from the drop down list.



View the Security Analyst Overview dashboard for further action. For detailed information on Security Analyst Overview dashboard, see Security Incident Response Platform Analytics Solutions.

View Security Incident Explorer dashboard

With this dashboard, security managers are able to view security incidents summarized and grouped by category, subcategory, location, priority and business impact.

Before you begin

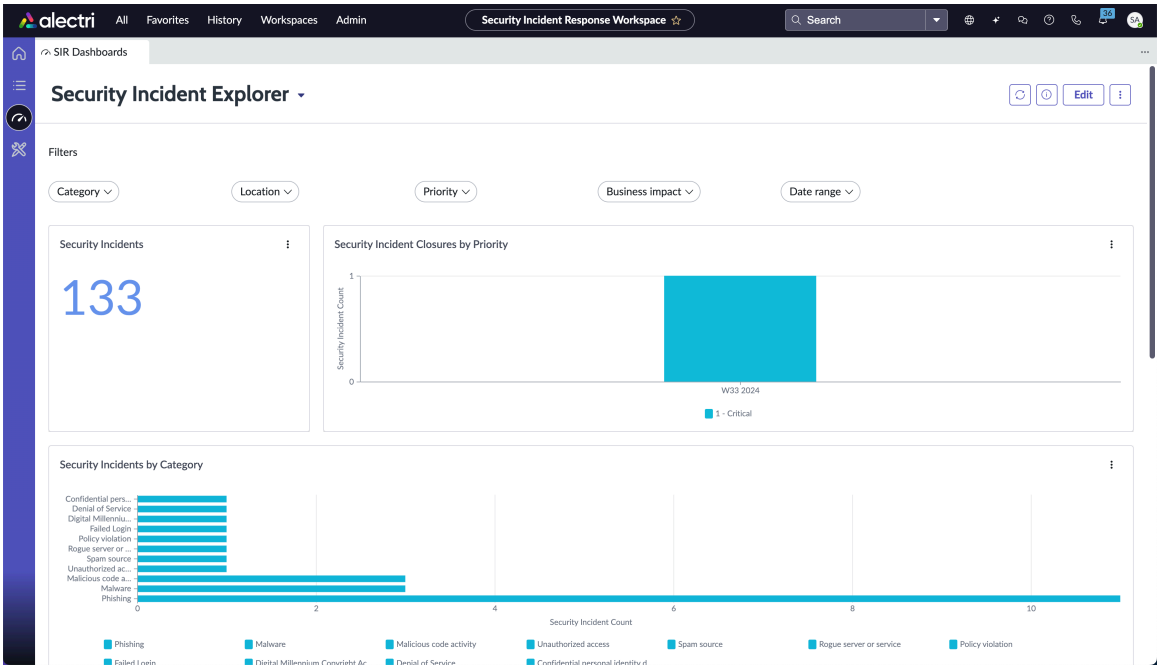
By default, Security Incident Explorer dashboard is displayed for the users with sn_si.manager access.

Role required: sn_si.analyst (Read), sn_si.manager or sn_si.admin (Write)

Procedure

1. Navigate to **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Security Incident Explorer** from the drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



View the Security Incident Explorer dashboard for further action. For detailed information on Security Incident Explorer dashboard, see Security Incident Explorer dashboard

In the current release, the following list of reports is not supported in the Security Incident Explorer dashboard:

- Security Incident Assignment HeatMap - HeatMap visualisation is not available.
- Security Incident Map - Map visualisation is not available.

View Security Incident Management dashboard

With this dashboard, security managers can easily track the volume, performance and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.

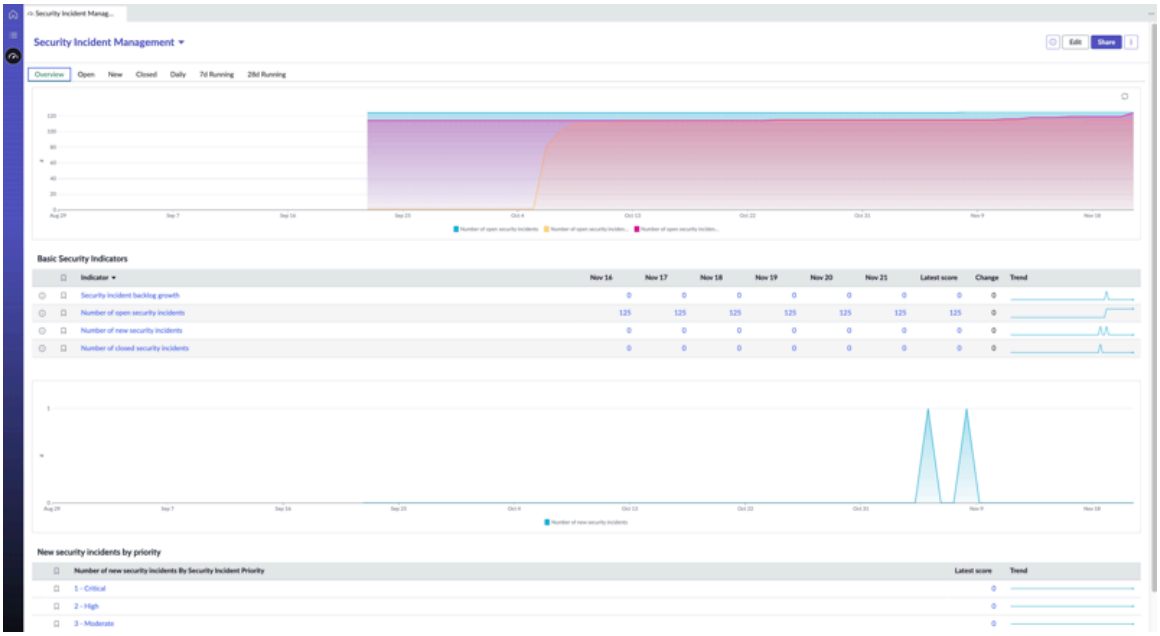
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Security Incident Management** from the drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



View the Security Incident Management dashboard for further action. For detailed information on Security Incident Management dashboard, see Security Incident Management dashboard

View Security Operations Efficiency dashboard

Security operations center (SOC) managers can view overall efficiency metrics and measure the individual performance of the SOC team members in the organization.

Before you begin

In the current release, the following report is not supported in the Security Operations Efficiency dashboard:

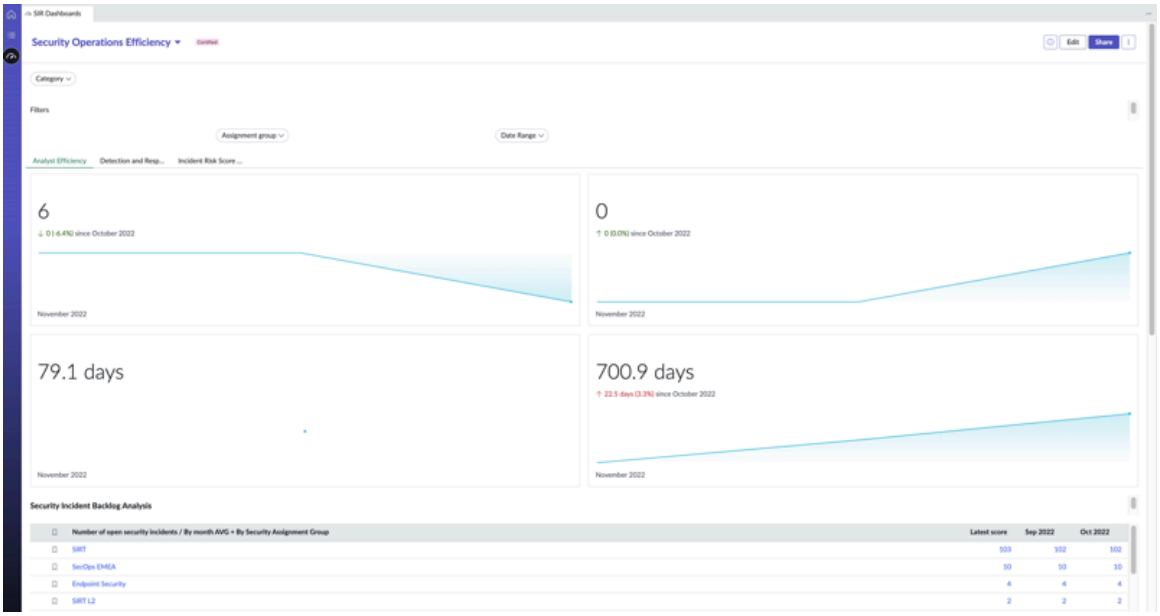
- Security Incident stage Analysis - Workbench is not available

Role required: sn_si.analyst (Read), sn_si.manager or sn_si.admin (write)

Procedure

1. Navigate to **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Security Operations Efficiency** from the drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



View the Security Operations Efficiency dashboard for further action. For detailed information on Security Operations Efficiency dashboard, see Security Operations Efficiency dashboard

View Security Incident Response Premium KPIs dashboard

With this dashboard, security managers can track and view the volume, performance, and progress of security incidents from initial analysis/detection to containment, eradication, and recovery.

Before you begin

In the current release, the following list of reports is not supported in the Security Incident Response Premium KPIs dashboard:

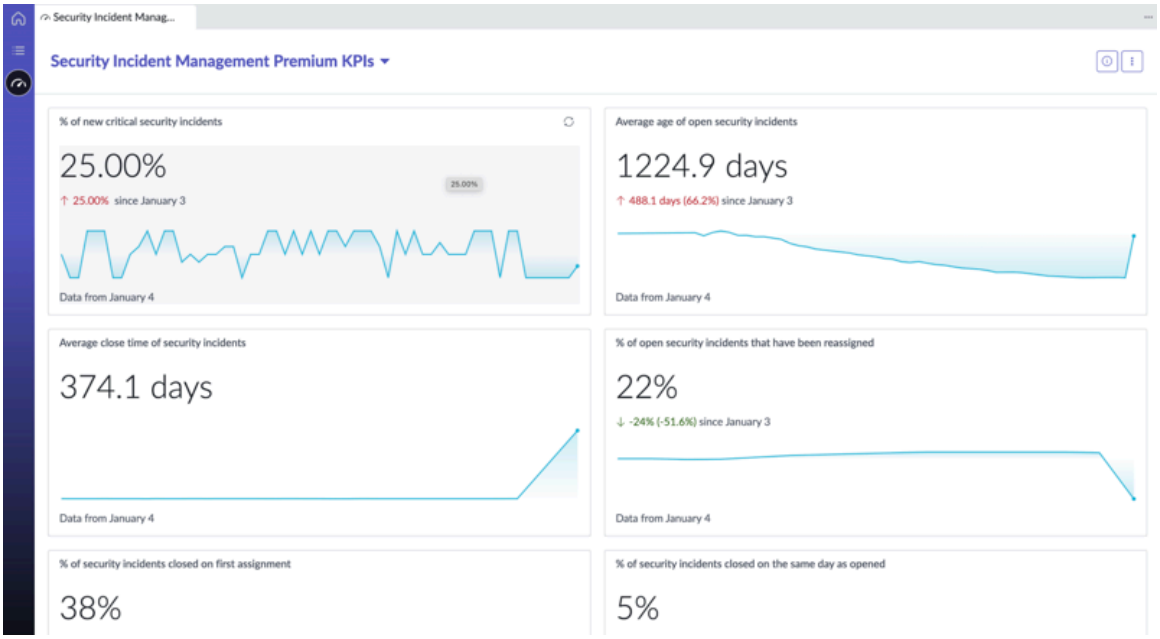
- Process by state - Workbench is not available
- Process by Age - Workbench is not available
- Security incidents open for more than 30 days by assignment group and state - HeatMap visualisation is not available.
- Security incidents not updated for more than 30 days by assignment group and state - HeatMap visualisation is not available.
- Security incidents with assignee that is not active - HeatMap visualisation is not available.

Role required: sn_si.analyst (Read), sn_si.manager or sn_si.admin (write)

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Security Incident Response Premium KPIs** from the drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. View the Security Incident Response Premium KPIs dashboard for further action.
   For detailed information on Security Incident Response Premium KPIs dashboard, see Security Incident Management Premium dashboard

View Context Sensitive Analytics - SI dashboard

With this dashboard, managers and analysts can view the open security incidents, the average age of open Security Incidents, the average close time of security incidents, the percentage of security incidents that were opened and closed on the same day, and the percentage of the incidents that were not updated in the last 5 days and 30 days.

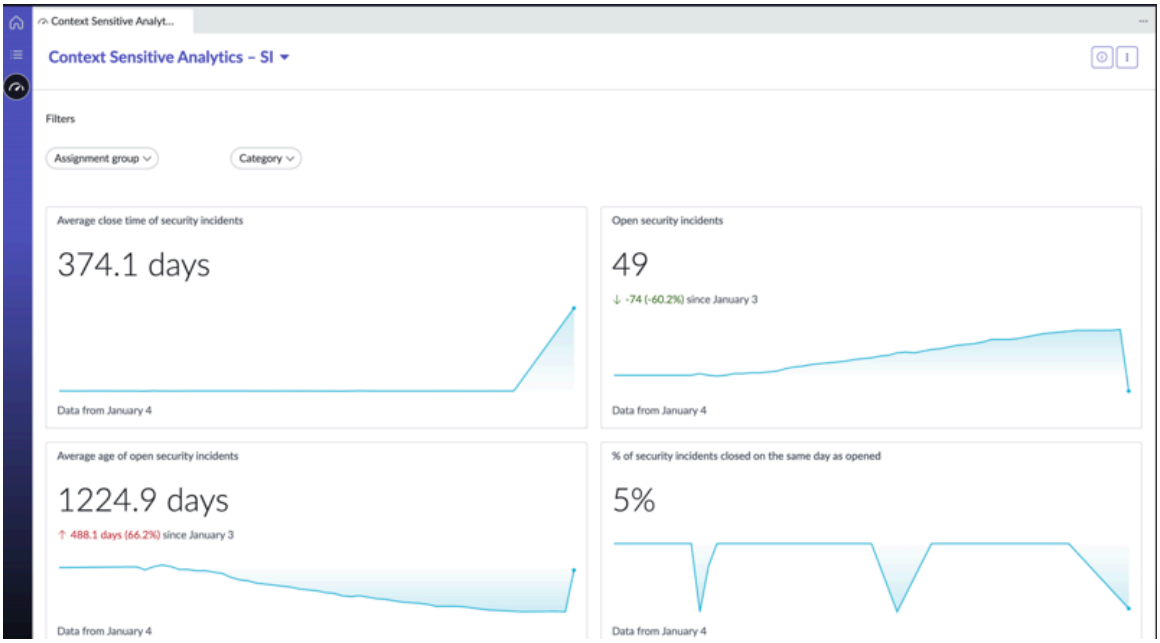
Before you begin

Role required: sn_si.analyst (Read), sn_si.manager or sn_si.admin (write)

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response**.
2. Click **SIR Dashboards** icon, displayed on the left side of the workspace home page.
3. Select **Context Sensitive Analytics – SI** from the drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. View the Context Sensitive Analytics – SI dashboard for further action.

View CISO dashboard

This dashboard provides the Chief Information Security Officers (CISOs) with a high-level overview of security incidents and weekly incidents trends on the instance in the form of graphical charts. These charts help you effectively view and analyze how the Security operations center (SOC) performs.

Before you begin

- Role required: sn_si.admin and sn_si.ciso - Edit and view incidents.
- Ensure that you have the Performance Analytics for Security Incident Response app installed.

About this task

Note: The CISO dashboard and CISO Overview dashboard were two different ones in the classic UI. But, now the capabilities of the two dashboards have been merged under the CISO dashboard.

The CISO dashboard provides key insights about your security incidents on a weekly basis. You can set up indicators and collect data snapshots of the incidents matching the conditions in the indicator properties. The collected data is then visualized using widgets in the dashboard.

You can visualize the weekly trends using the widgets in the CISO dashboard. The data or statistics for the trends of your security incidents are collected from the weekly incidents indicator properties that are defined by the organization. You can gain key insights by using the following charts:

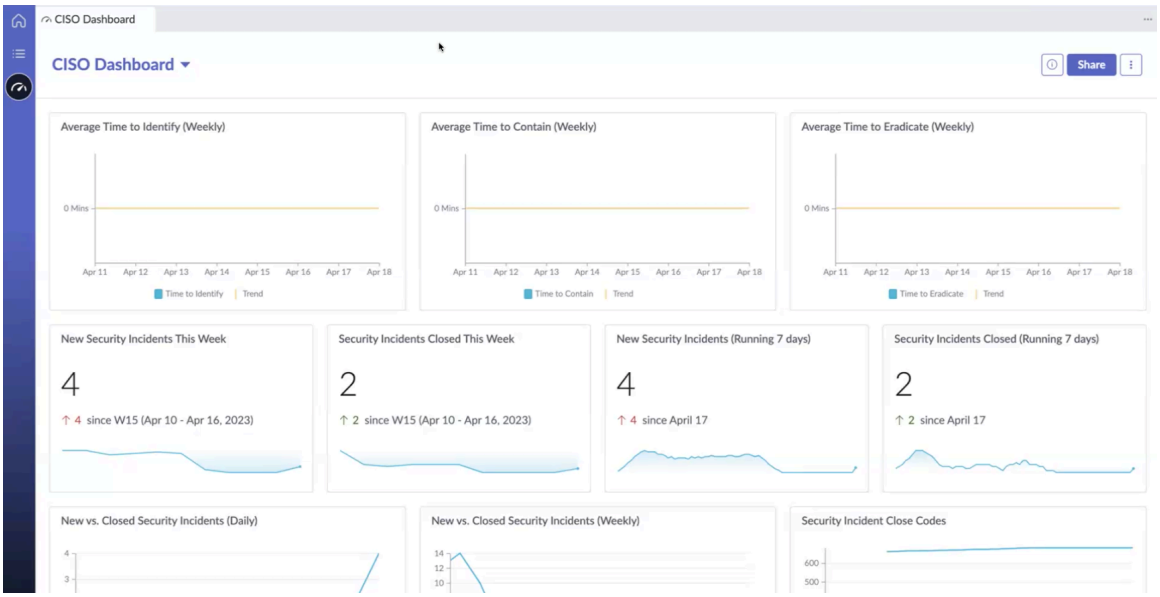
- **Average Time to Identify (Weekly)**: This chart illustrates the average weekly time taken to identify a security incident.
- **Average Time to Contain (Weekly)**: This chart illustrates the average weekly time taken to contain a security incident.
- **Average Time to Eradicate (Weekly)**: This chart illustrates the average weekly time taken to eradicate a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **New Security Incidents this Week**: This chart illustrates the number of new security incidents this week.
- **Security Incidents Closed this Week**: This chart illustrates the number of security incidents closed this week.
- **New Security Incidents (Running 7 days)**: This chart illustrates the number of new security incidents which are running for a week.
- **Security Incidents Closed (Running 7 days)**: This chart illustrates the number of new security incidents that are closed but are running for a week.
- **New vs Closed incidents (Daily)**: This chart illustrates the comparison between the daily new security incidents and daily closed security incidents.
- **New vs Closed incidents (Weekly)**: This chart illustrates the comparison between the weekly new security incidents and the weekly closed security incidents.
- **Security Incident Closed Codes**: This chart illustrates the closed codes of the security incidents.

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response**.
2. Click the **SIR Dashboards** icon on the left side of the workspace home page.
3. Select **CISO Dashboard** from the drop-down list.



4. View the CISO dashboard for further action.

View CISO Reporting Overview dashboard

This dashboard provides the Chief Information Security Officers (CISOs) with a high-level reporting overview of the security incidents and weekly incidents trends on the instance in the form of graphical charts. These charts help you effectively view and analyze how the Security operations center (SOC) performs.

Before you begin

Role required: sn_si.admin and sn_si.ciso - Edit and view incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

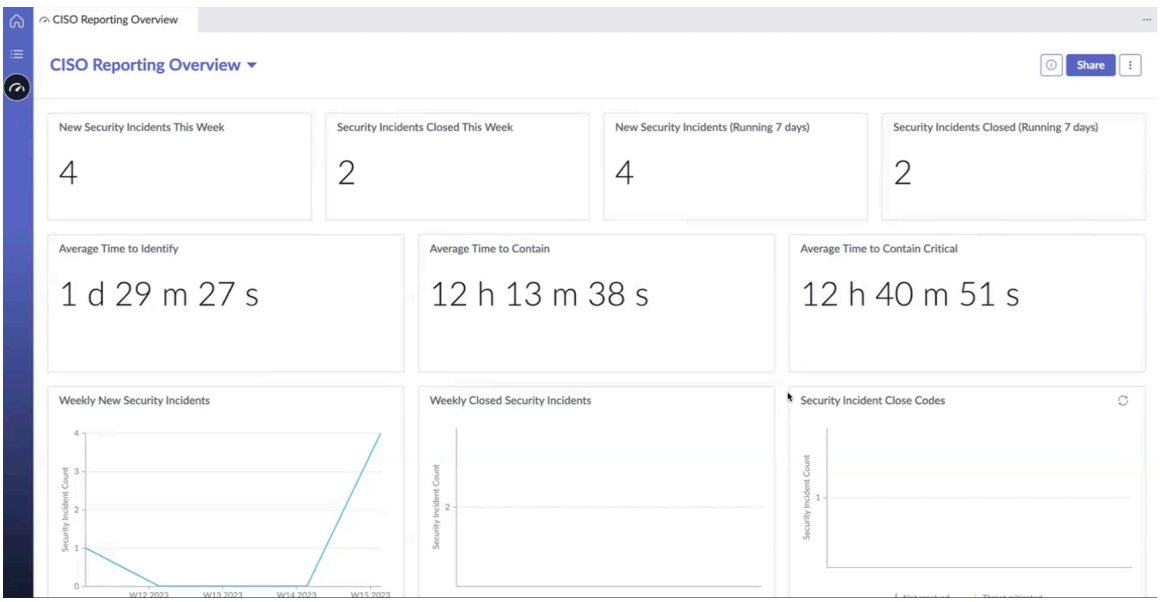
About this task

The CISO Reporting Overview dashboard provides key insights about the security incidents on a weekly basis, and you can visualize the weekly trends using widgets. You can gain key insights on the CISO Reporting by using the following charts:

- **New Security Incidents this Week**: This tile displays the report of the number of new security incidents this week.
- **Security Incidents Closed this Week**: This tile displays the report of the number of security incidents closed this week.
- **New Security Incidents (Running 7 days)**: This tile displays the report of the number of new security incidents which are running for a week.
- **Security Incidents Closed (Running 7 days)**: This tile displays the report of the number of new security incidents closed but are running for a week.
- **Average Time to Identify**: This tile displays the report of the average weekly time taken to identify security incidents.
- **Average Time to Contain**: This tile displays the report of the average weekly time taken to contain security incidents.
- **Average Time to Contain Critical**: This tile displays the report of the average weekly time taken to contain critical security incidents.
- **Weekly New Security Incidents**: This chart illustrates the report of the weekly new security incidents.
- **Weekly Closed Security Incidents**: This chart illustrates the report of the weekly closed security incidents.
- **Security Incident Closed Codes**: This chart illustrates the report of the closed codes of the security incidents.

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response**.
2. Click the **SIR Dashboards** icon on the left side of the workspace homepage.
3. Select **CISO Reporting Overview** from the drop-down list.



4. View the CISO Reporting dashboard for further action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View Security Incident Manager Overview dashboard

This dashboard provides managers with a high-level overview of the critical or high priority security incidents at a team level, SLAs that are about expire in 24 hours, and weekly incidents trends on the instance in the form of reports and graphical charts.

Before you begin

Role required:

- sn_si.admin - Edit and view dashboard.
- sn_si.manager - View dashboard.

About this task

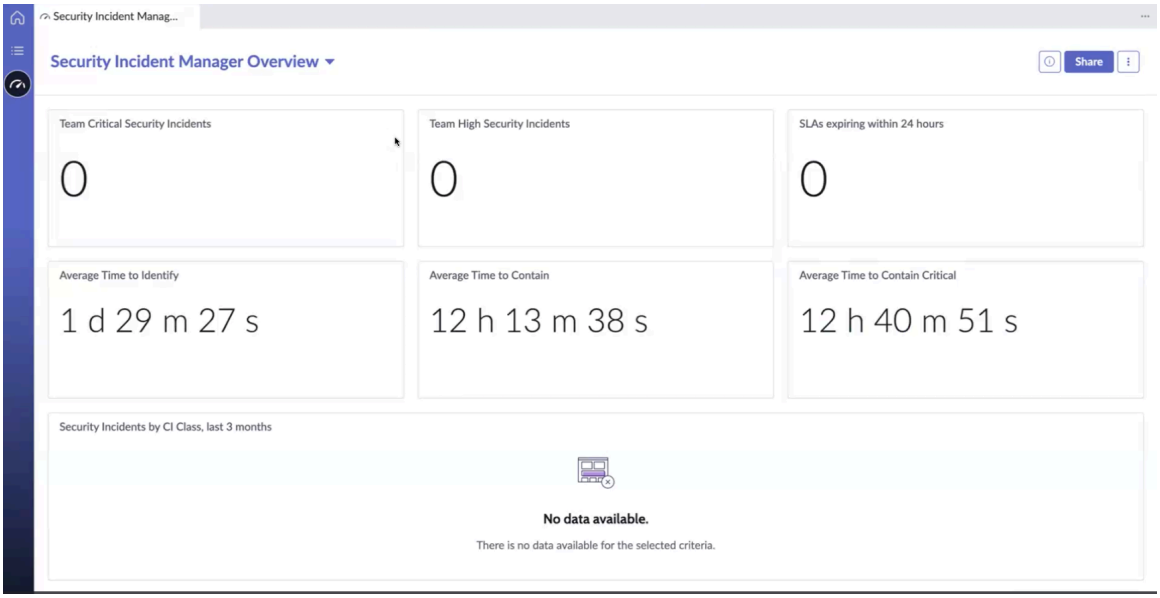
You can analyze the critical or high priority security incidents, or SLAs that needs immediate attention. You can also visualize the weekly trends using the widgets in the Security Incident Manager Overview dashboard. The data or statistics for the weekly or monthly trends of your security incidents are collected from the incidents' tables that are defined by the organization. You can gain key insights by using the following charts:

- **Team Critical Security Incidents**: This tile displays the number of critical security incidents for the team this week.
- **Team High Security Incidents**: This tile displays the number of high security incidents for the team this week.
- **SLAs expiring within 24 hours**: This tile displays the number of SLAs that will be expiring within 24 hours.
- **Average Time to Identify**: This tile displays the average weekly time taken to identify security incidents.
- **Average Time to Contain**: This tile displays the average weekly time taken to contain security incidents.
- **Average Time to Contain Critical**: This tile displays the average weekly time taken to contain critical security incidents.
- **Security Incident by CI Class, last 3 months**: This chart illustrates the trends of all the security incidents based on the CI Class for the last three months.
- **Trend of All Security Incidents by Category**: This chart illustrates the trends of all the security incident based on category.
- **Trend of All Security Incidents by Priority**: This chart illustrates the trends of all the security incident based on priority.

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response**.
2. Click the **SIR Dashboards** icon on the left side of the workspace homepage.
3. Select **Security Incident Manager Overview** from the drop-down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. View the Security Incident Manager Overview for further action.

View Security Incident Response Health dashboard

Security Incident Response Health dashboard feature provides a centralized view of critical aspects related to incident response process implementation, issues/errors encountered, and performance metrics. It serves as a vital tool for monitoring and optimizing the effectiveness of an organization's security incident response capabilities.

Before you begin

Role required: sn_si.admin, or sn_si.analyst, or sn_si.analytics_read - View dashboard.

About this task

You can monitor the health of the security incidents using the widgets and trend charts for each application. These statistics present a comprehensive health score detailing the configuration state and remediation effectiveness within the SIR applications. The Security Incident Response Health dashboard supports the following four tabs:

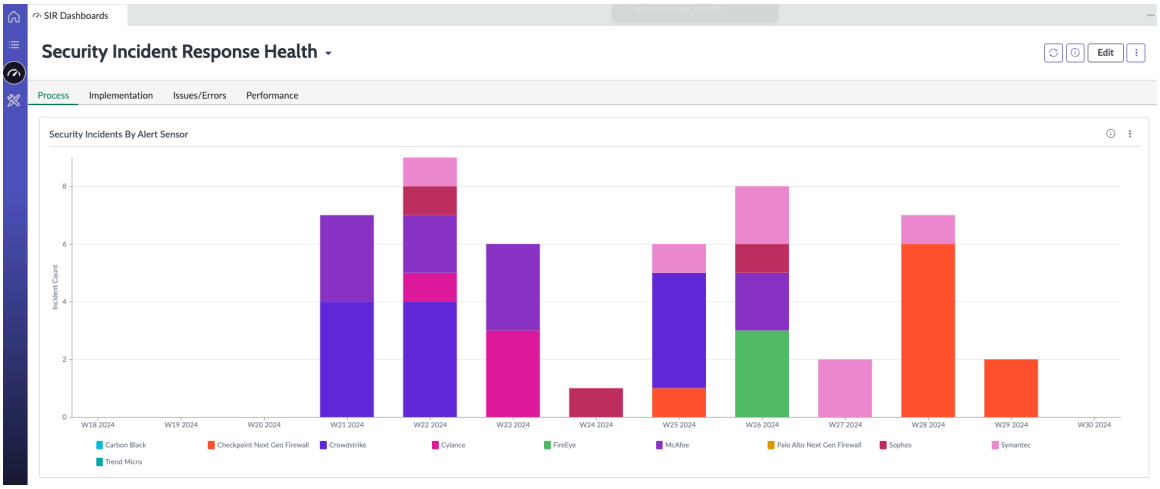
- **Process**: The tab displays a summary of all the incidents from various alert sensors grouped on a weekly basis.
- **Implementation**: This tab displays the customizations that the customers perform in their instances covering script includes, business rules, flows, and upgrades.
- **Issues/Errors**: The tab displays widgets highlighting errors in integration processes, discrepancies during the ingestion of raw incident data, outbound HTTP errors in SIR applications, and any issues arising during the execution of playbooks.
- **Performance**: This tab displays the performance issues in the SIR applications, including slowness in performance queries, business rules, and scripts.

Procedure

1. Navigate to **All** > **Workspaces** > **Security Incident Response Workspace**.
2. Select the **SIR Dashboards** icon on the SIR workspace homepage.
3. Select **Security Incident Response Health dashboard** from the drop-down list.
4. Select the **Process** tab to view the number of security incidents that were triggered on a weekly basis for each alert sensor on the chart.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Process tab



You can perform the following tasks:

a. Select an alert sensor on the chart to view the KPI details of the number of security incidents that triggered by alert sensors in a week.

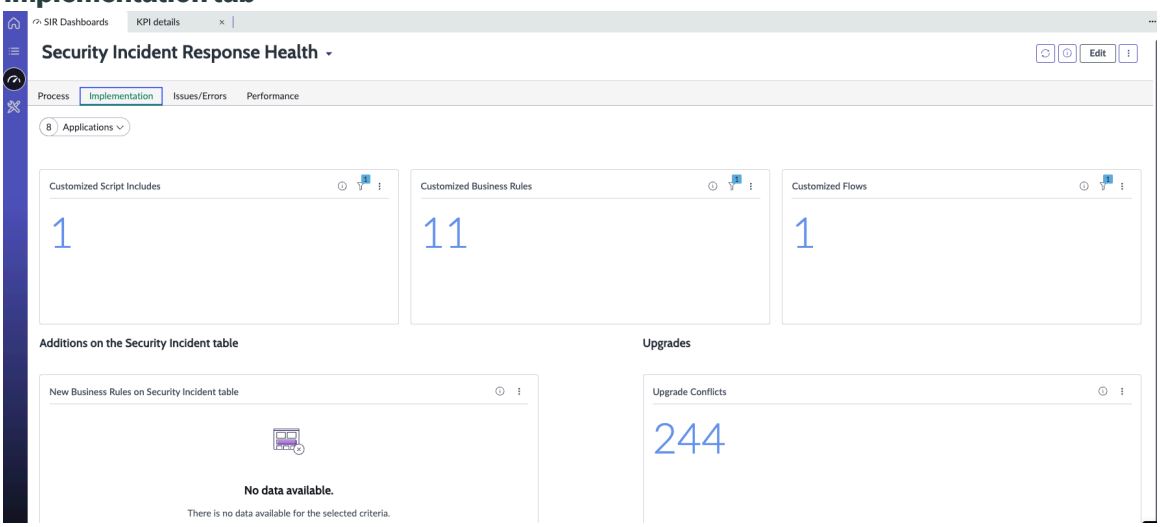
b. To get the KPI details for a particular week, use the **Calendar** option.

c. To compare the security incidents triggered by the alert sensor, select the **Compare Records** option.

d. To use the Chart type, Time series, or Analysis, select the **Chart Options**.

5. Select the **Implementation** tab to view the number of customizations that were created for the security incidents in the Security Incident Response applications.

Implementation tab



Implementation tab:

You can view the aggregated dashboard for the number of customizations that were created for each Incident Response application.

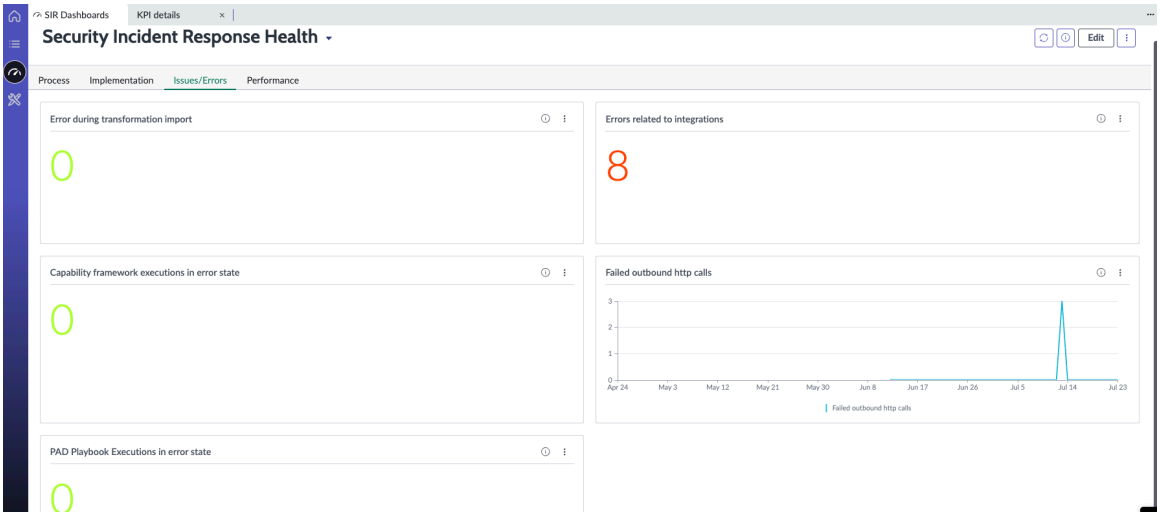
- **Customized Script Includes**: This widget displays the number of customized scripts that were added based on your requirements in the SIR applications.
- **Customized Business Rules**: This widget displays the number of customized business rules that were added based on your requirements in the SIR applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Customized Flows**: This widget displays the number of customized flows that were added based on your requirements in the SIR applications.
- **New Business Rule on Security Incident table**: This widget displays the number of business rules that were created on the Security Incident table.
- **Upgrade Conflicts**: This widget displays the number of conflicts that were triggered during upgrades in the SIR applications.

6. Select the **Issues/Errors** tab to view the number of issues or errors that were triggered in the Security Incident Response applications.

Issues/Errors tab



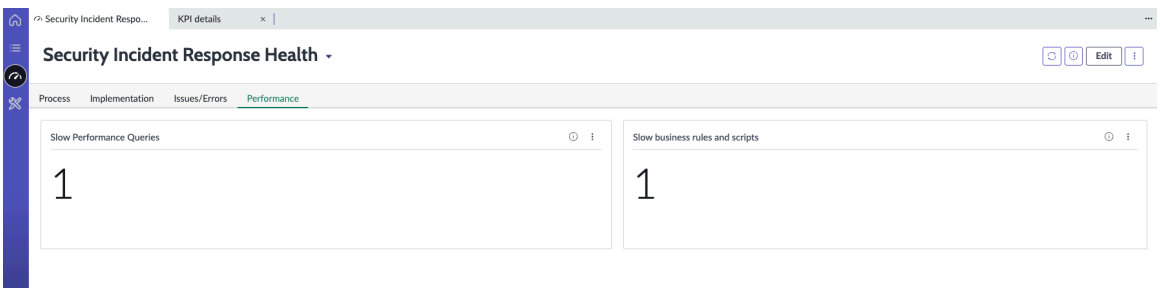
Issues/Errors tab:

You can view the aggregated dashboard for issues or errors in the Security Incident Response applications.

- **Errors during transformation import**: This widget displays the number of errors that were triggered during the transformation import in SIR applications.
- **Errors related to integrations**: This widget displays the number of errors that were triggered during the SIR integrations.
- **Capability framework executions in error state**: This widget displays the number of errors that were triggered during the capability framework executions in SIR applications.
- **Failed outbound HTTP calls**: This widget displays the number of failed outbound HTTP calls that were triggered in the SIR applications.
- **PAD Playbook executions in error state**: This widget displays the number of PAD Playbook execution errors that were triggered in the SIR applications.

7. Select the **Performance** tab to view the number of performance issues that were triggered in the Security Incident Response applications.

Performance tab



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Performance tab:

You can view the aggregated dashboard for performance issues in the Security Incident Response applications.

- **Slow Performance Queries**: This widget displays the number of performance queries in the SIR applications whose average execution time is greater than 10 ms and averaged on 1000 or more executions.
- **Slow business rules and scripts**: This widget displays the number of business rules and scripts in the SIR applications whose average execution time is greater than 10 ms and averaged on 1000 or more executions.

8. You can use the **Refresh** icon to refresh the data in the Security Incident Response Health dashboard.
9. You can use the **View dashboard details** icon to view the details of the Security Incident Response Health dashboard.
10. You can use the **Edit** option to modify the details of the Security Incident Response Health dashboard.
11. You can use the **More** option to perform additional actions on the Security Incident Response Health dashboard.

Security incident creation

Security incidents can be created manually from the form, or automatically via security events received from integrated third-party alert monitoring tools, such as Splunk.

Important: The latest features in Security Incident Response are exclusively available in the Security Incident Response Workspace. Install or upgrade to the latest Security Incident Response or Security Incident Response Workspace version to access and leverage features such as Shift-Handover, Risk Score Calculator, and so on.

If you have a security role, you can use any of the following methods to manually create security incidents.

Methods for manually creating security incidents

Method	Description
Manually created from the Security Incident list	On the Security Incident list, select **New** to create a new security incident.
Manually created from the Security Incident Catalog	You can create security incidents by selecting from categories of security threats defined in the security incident catalog.
Incident Management	On the Incident form in incident management, select **Create Security Incident** to create a new security incident. **Note:** You can avoid duplicate security incidents creation by enabling the `sn_si.disable_duplicate_security_incident` system property.
Manually converted from a security request	On the Security Request form, select **Convert to Security Incident** to create a new security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Methods for manually creating security incidents (continued)

Method	Description
Manually created from an Event Management alert	On the Event Management Alerts form, select **Create Security incident** to create a new security incident from an alert.
Manually created from an alert	On the Event Management Alert form, select **Create Security Incident** to create a new security incident.
Manually converted from a vulnerability record (if the Vulnerability Response plugin is activated)	On the Vulnerability Items form, select **Create Security Incident** to create a new security incident.

Automatic creation of security incidents

Generally, security administrators are responsible for setting up alert rules to automatically generate security incidents.

Security admin method for creating security incidents

Method	Description
Automatically created using alert rules	Security incidents can be created based on alert rules defined in the Event management in your data center application.

Security incident manual creation

You can create a security incident from the Security Incident form, as well as from several other forms.

You can create security incidents based on an existing record from the following forms:

- From any security incident list
- Incident form
- Event Management Alert form
- Vulnerable Items form
- Security Request form

Create a security incident from the Security Incident list

In addition to automatic methods for creating security incidents, you can create them manually, as needed.

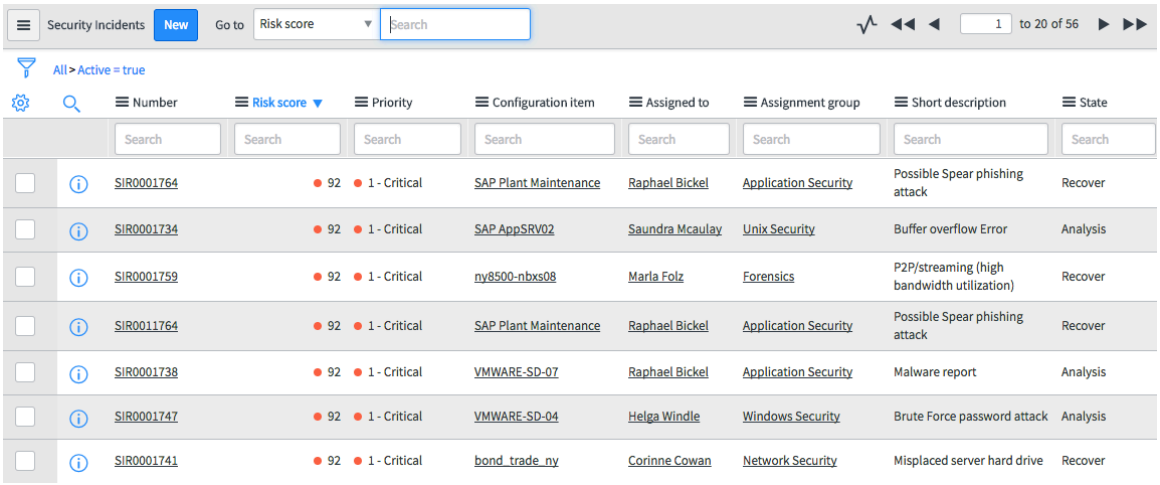
This video shows a visual overview of how you could create a security incident from the Security Incident list.

Before you begin
Role required: sn_si.basic

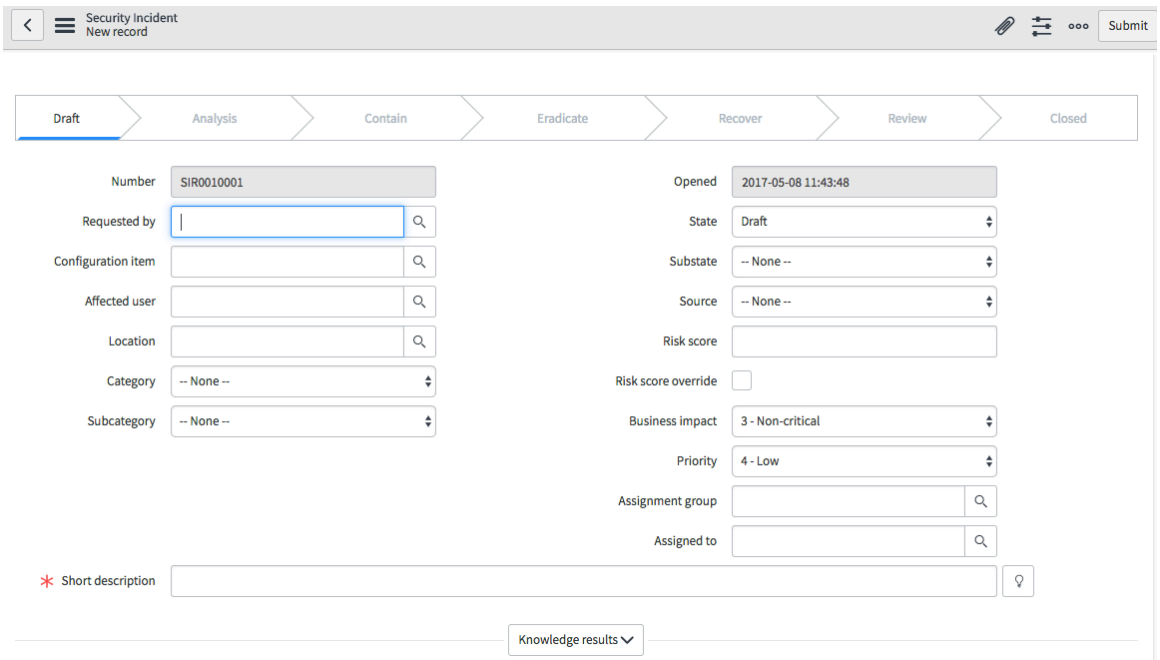
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to any security incident list (for example, **All** > **Security Incident** > **Incidents** > **Show All Incidents**).



2. Click **New**.



3. On the form, fill in the fields.

Field	Description
Select security tag	If needed, select a Security tag to add metadata to the record or identify who should have access to this security incident record. This field appears only after the security incident has been saved.
Number	[Read only] The security incident number.
Requested by	The person requesting the work to be performed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

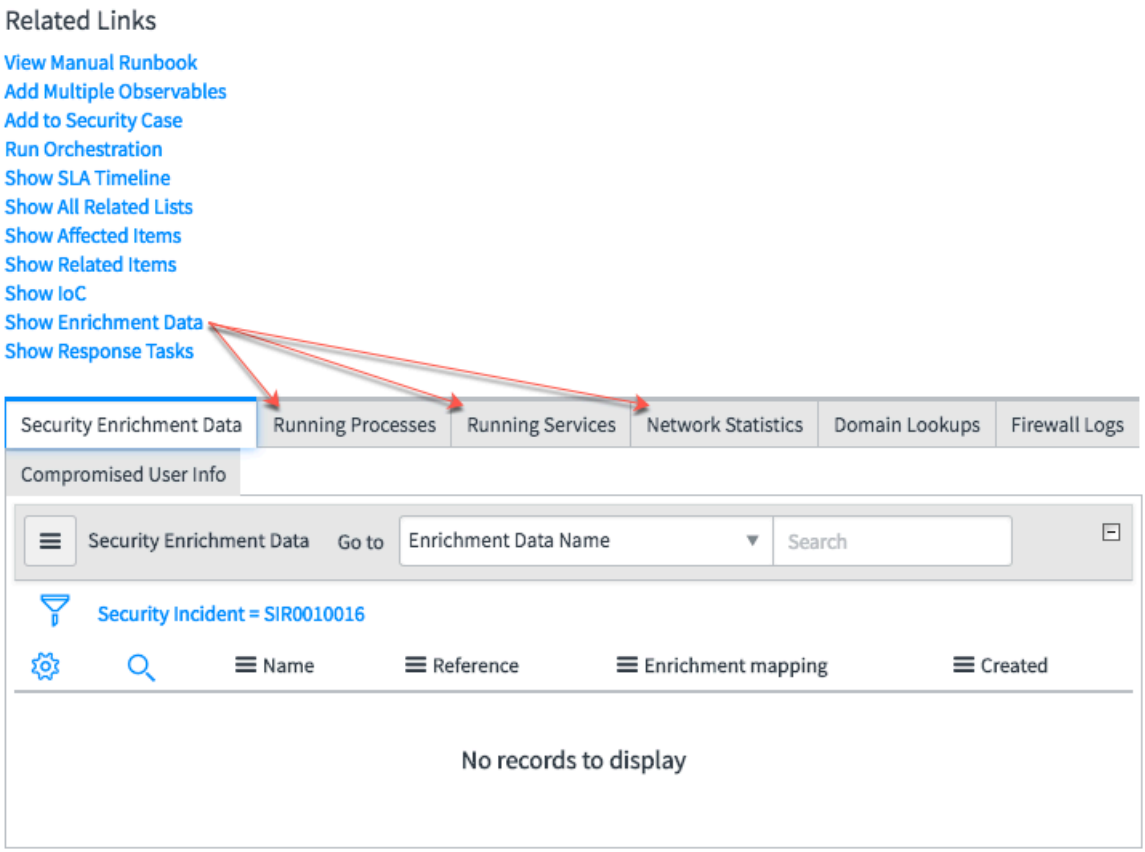
Field	Description
Configuration Item	The server, computer, router, or other configuration item affected by the security issue.
Affected user	The person affected by the security issue.
Location	The location of the requester or resource. If a **Configuration Item** is not selected, this field is pre-filled with the location of the requester.
Category	The category that identifies the type of security issue. If a category is selected, a workflow for analyzing this issue is executed when the record is saved. For example, if you select **Denial of Service**, the Security Incident - Denial of Service - Template workflow is executed.
Subcategory	The subcategory that further defines the issue.
Opened	[Read only] Displays the date and time the incident was opened.
State	The current state of the security incident. Upon security incident creation, this field defaults to **Draft**.
Substate	Identifies whether the security incident includes a pending problem or change.
Source	Identifies the source of the security incident, such as email, a phone call, or network monitoring.
Alert Sensor	Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee, and so on.
Alert Rule	The rule in the security product which triggered the creation of this security incident.
Risk score	Displays the risk score calculated for this security incident. The value is based on the priority of the security incident, the type of security incident (Denial of Service, Spear Phishing, or Malicious code activity), and the number of sources that triggered a failed reputation score on an indicator. The risk score aids in prioritizing security incident work for analysts. Three security incident properties allow you to further designate a color-coded dot to appear next to the risk score in list view to make them more easily identifiable. If you make changes to certain fields in the security incident, such as the **Business impact** or **Priority**, and save the record, the **Risk score** is automatically recalculated and displayed. The change is also reflected in the work notes and on the Risk Score Audits related list. **Note:** The risk score is also recalculated when affected users are associated with a security incident, affected services, or vulnerable items. You can also manually enter a new **Risk score**. This can be useful if you want to keep a particular security incident at the top of the list of security incidents you are analyzing. If you enter a new **Risk score**, the **Risk score override** check box is automatically selected. Regardless of the changes made in the security incident, a manually-entered risk score is not automatically recalculated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If you have upgraded your instance from a prior release, risk scores were calculated for all of your open security incidents. For more information, see Understanding security incident calculators.
Risk score override	Select this check box to override the automatic update of the risk score. The override will be reflected in the work notes.
Business impact	Select the importance of this security incident to your business. The default value is Non-critical. If, after the security incident record has been saved, you change the value in the **Priority** fand/or **Risk** fields, the **Business impact** is recalculated.
Priority	Select the order in which to address this security incident, based on the urgency. If this value is changed after the record is saved, it can affect the **Business impact** calculation.
Assignment group	The group to which this security incident is assigned.
Assigned to	The individual assigned to analyze this security incident. Assignments can be performed manually or automatically. For more information, see Assigning security analysts.
Short description	A brief description of the security incident.
Knowledge results	As you type the short description, links to related articles from the knowledge base appear. Scanning the information could solve your issue.

4. Right-click in the record header and select **Save**.
   If you added a new CI to the security incident, the following integration workflows are automatically executed:
   - Security Operations - Get Running Processes Flow. This workflow retrieves a list of running processes on a configuration item (CI) from a host or endpoint.
   - Security Incident Response - Get Running Services Flow. This workflow retrieves a list of running services from Windows-based CIs.
   - Security Operations Integrations - Get Network Statistics workflow. This workflow retrieves a list of active network connections from a host or endpoint.
5. To view the information retrieved by these workflows, click the **Show Enrichment Data** related link, and then click any of the indicated tabs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: Additional workflows are executed based on the third-party integrations you have activated as follows Security Operations Carbon Black Integration - Get Running Processes Flow

Related topics

Security Incident Response setup

Create a security incident from the Security Incident Catalog

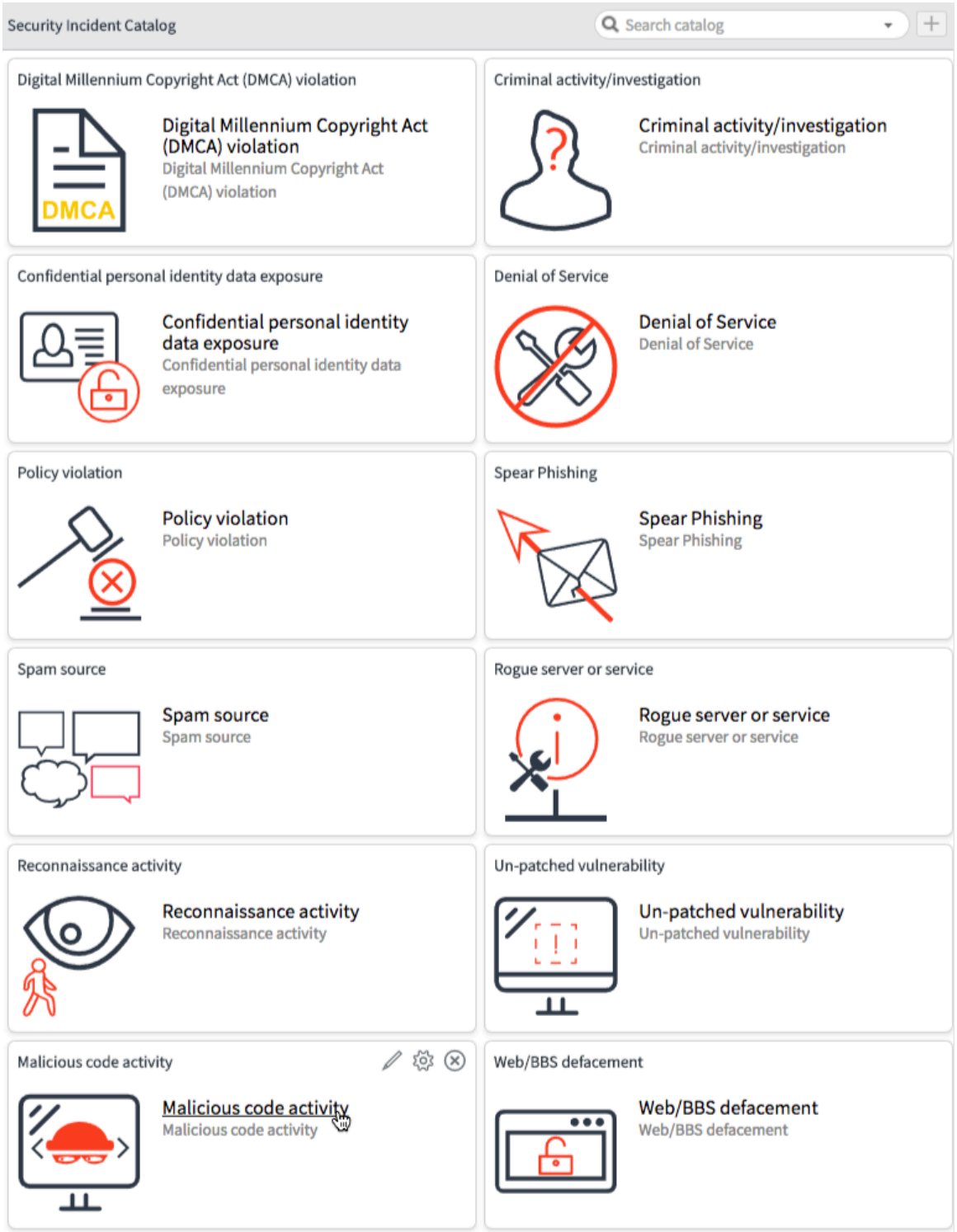
Users in your company can use the Security Incident Catalog to request various types of security-related analysis.

Before you begin
Role required: none

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

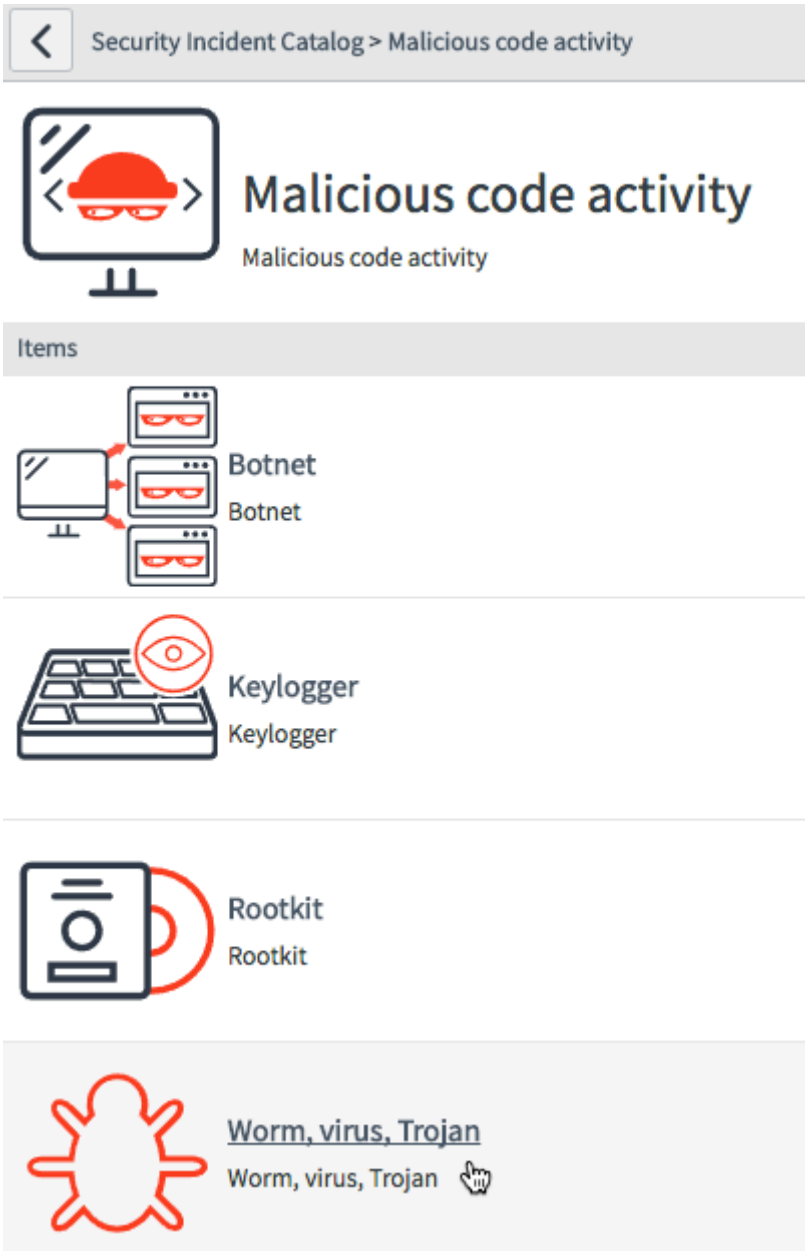
Procedure

1. Navigate to **All** > **Self-Service** > **Security Incident Catalog**.



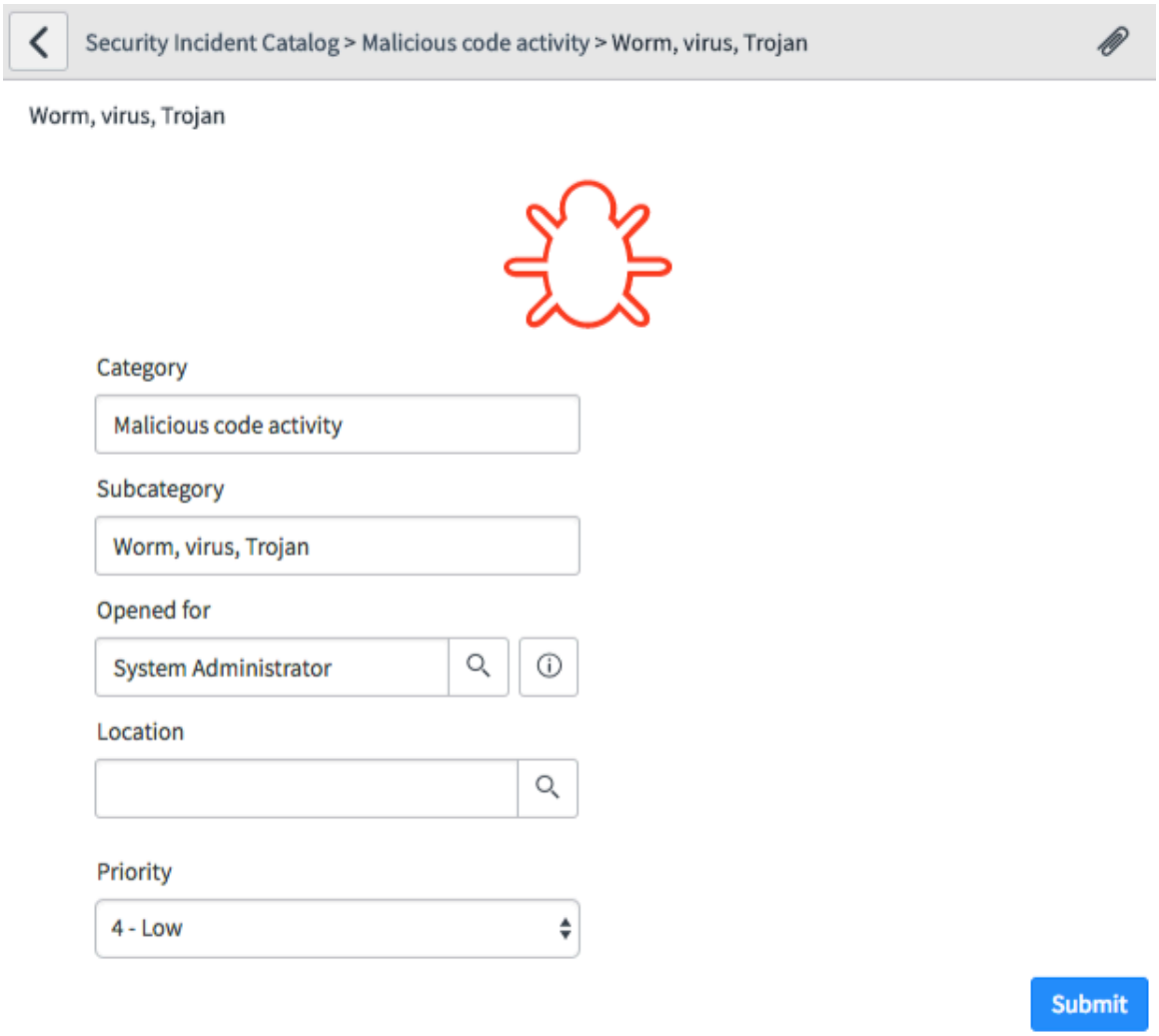
2. Click the catalog item for which you want to make a request.
   If the item you selected from the main catalog contains subcategories, the list is shown. In the following example, **Malicious code activity** was selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click the subcategory that best matches the type of request you want to make.
   In this example, the **Worm, virus, Trojan** subcategory was selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter the information for the request, and click **Submit**.
   The request is sent to your Security Incident department.
5. After you have submitted the request, you can track its progress by navigating to **Self-Service** > **My Requests**, and entering the request number.

Create a security incident from an Event Management alert

When Event Management is activated, you can manually create security incidents from the Alert form.

Before you begin

The Event Management plugin requires a separate subscription and must be activated by ServiceNow personnel. This plugin includes demo data and activates related plugins if they are not already active. The Service Analytics is activated automatically when Event Management is activated.
Role required: evt_mgmt_admin, evt_mgmt_operator, or evt_mgmt_user

Procedure

1. Navigate to **All** > **Event Management** > **All Alerts**.
2. Click the alert **Number**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Create Security incident**.
4. Click **Update**.

Security incident automatic creation

Third-party monitoring tools, such as Splunk, can be integrated with Security Incident Response so that security events imported from those tools automatically generate security incidents. You can also import data from third-party tools into security alerts.

To integrate alert monitoring tools to Security Incident Response, you must use the REST API to write to the Security Incident Import [sn_si_incident_import] table. Then, using the **Security Incident Transform** transform maps, the import set source table is mapped to fields in the target Security Incident [sn_si.incident] table.

If you attempt to import CI records that are not recognized by the transform map, the transform map script checks the record for the following (in this order) in an attempt to make a match:

- sys_id
- CI name
- fully qualified domain name
- IP address

Note: If you find that the **Security Incident Transform** transform map is not adequate for the third-party alert monitoring tool you are using, duplicate the transform map, create a new one, and edit the fields, as needed.

Security incidents created from events and alerts

As events are imported from alert monitoring tools, they are first processed by Event Management and grouped into alerts. These alerts can be used to create security incidents based on customizable alert rules, or manually reviewed to select those alerts to be investigated as a security incident.

You can find a sample alert rule called **Create security incidents from critical alerts** in the Alert Rules module of the Event Management application. This alert rule automatically creates security incidents when critical security-related events are received from within ServiceNow or from third-party monitoring applications. After the security incident has been created, it will be updated as new events are received. You can modify the task template in the alert rule to change the initial values for the security incident created by this alert rule. To handle each distinct variety of security incident that you would like to create, you can define other alert rules with different conditions.

Alternatively, if you are a user with the Security Admin role, you can manually create a security incident by clicking the **Create Security Incident** button from any suspicious alert.

It is important that the events received from external tools include the following information:

- The node set to the name, IP address, or sys_id of the CI that becomes the affected resource.
- The event classification is set to Security to distinguish them from other IT events.
- The event description, which populates the description of the security incident.
- The additional information can include any extra information that does not fit into the previously listed fields or other event fields, such as the category, attack vectors, return URL, or correlation ID. The format is a string that lists field names along with their values, using the following JSON format:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For each field and value pair, if the field in the security incident where the column name matches the fieldName is empty, it is set to the fieldValue. If the field in the security incident is not empty, it is not changed. In either case, the event and all the fields and values encoded in the additional information are recorded in a work notes entry describing the event. If nothing changes in the security incident, a work note entry is not created. Any fields in a security incident, including custom fields you add to the table, can be set.

Data imported into security alerts

When an event is created with more JSON-encoded data, that data is imported into any field with a name that matches the fieldName of that value in the JSON data.

If you have data in your third-party monitoring software (for example, Splunk) that is not common to the base system, you can add new fields to the Alert table to accommodate the data import. The JSON format for importing data into alerts is the same format used for creating security incidents from events and alerts:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

The only difference is that the data in the field is always overwritten with the fieldValue.

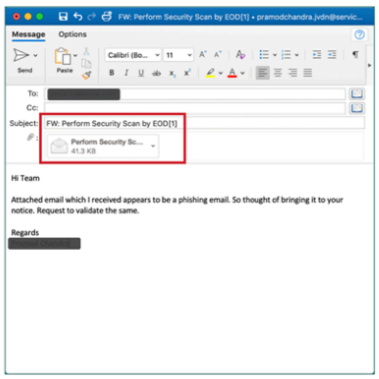
When the security event data is imported, it populates the fields in the Alert table with matching field names. If the alert is later turned into a security incident, the same additional information data populates matching fields in the security incident.

Create security incidents from User Reported Phishing emails

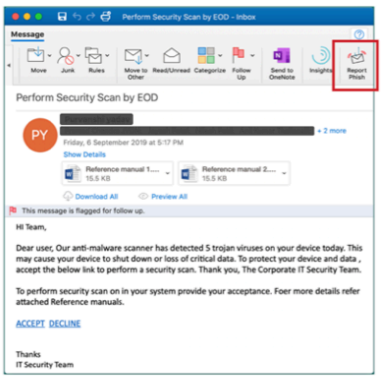
Use this feature to create security incidents from user reported phishing emails.

The enhanced User Reported Phishing functionality includes aggregation capabilities, email header extraction, and configuration.

- You can report phishing emails in multiple ways:
  - Emails can be forwarded as attachments.
  - If the **PhishAlarm** plugin (previously known as Wombat) is configured with the Microsoft Outlook client, you can:
    - Select the **Report Phish** button.
    - Forward phishing emails from a mobile device using the **Report Phish** option.



Desktop



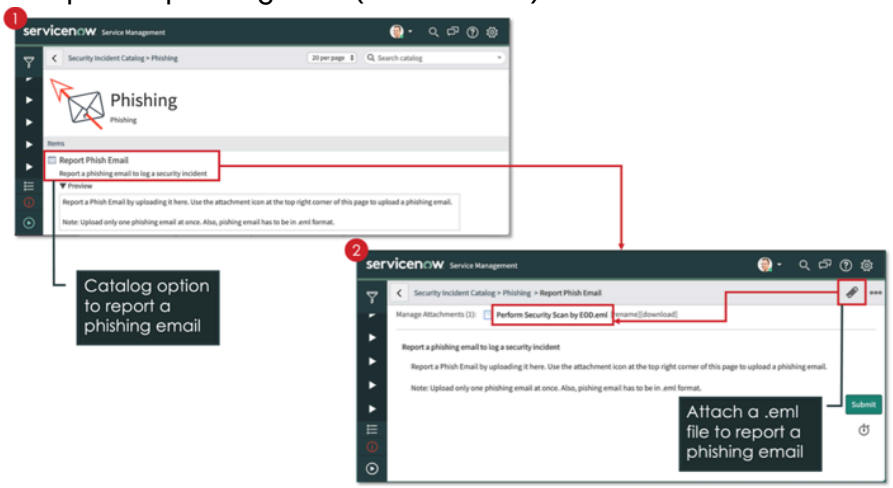
Desktop



Mobile

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can upload a phishing email (in .eml format).



- User reported phishing includes **aggregation business logic** that identifies duplicate phishing emails reported by users in an organization. Users can use this capability to:
  - Aggregate duplicate or similar user reported phishing incidents (company initiated phishing campaigns).
  - Avoid triaging duplicate user reported phishing incidents and reduce the manual effort involved in consolidating incidents.
  - Enable security analysts to work on a single user reported phishing incident.
- Provides phishing email headers within the user reported phishing incident.
  - Security analysts can scan for key email header information within the incident.
  - Manual effort in gathering header information from other sources is no longer required.
- The original phishing email submitted is stored as a **Phishing Email Record** in a new table.
- Security analysts can view details of the original phishing email like phishing email content, headers, origin.
- Security administrators can configure and make certain enhancements that include:
  - Configurations to extract email headers from the email body (**Report Phish** submissions).
  - Filters to capture selected headers.
  - Configurations to handle parent-child incident association when duplicate phishing email records are identified.
  - Flow Designer configurations to modify aggregation business logic based on the requirements.

Set up ingestion rules for user reported phishing

As a user with the `sn_si.admin` role, you can define email matching rules to filter user reported phishing emails based on specific criteria. For example, you can define a rule where all emails sent either directly or through the Report Phish button to *`security@acme.com`* are categorized as user reported phishing emails. For more information, see Set up ingestion rules for User Reported Phishing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define user reported phishing properties

Define the header information that needs to be captured from user reported phishing emails. For more information, see Define User Reported Phishing properties.

Phishing email records created from user reported phishing emails

User reported phishing emails are converted to security incidents based on the email matching rules that have been defined. For more information, see Phishing email records created from user reported phishing emails.

Transform phishing email to security incident

The Transform Phishing Email to Security Incident flow converts or transforms phishing email records to security incidents. For more information, see Transform user-reported phishing emails to security incidents.

Security incident records created from phishing email records

View the security incident record details including the Related Lists, Worknotes, and other important information. For more information, see Security incident records created from phishing email records.

Required components and plugins

The User Reported Phishing feature available is an enhanced version of the existing user reported phishing functionality available. See **Create rules to validate user-reported phishing attacks**.

Important Installation Instructions

This enhancement replaces the existing User Reported Phishing design. The new design includes the following updates:

- The existing **User Reported Phishing** email inbound actions (Type = Forward and Type = New) have been disabled.
- A new **Create Phishing Email** inbound action is now available.
- The Transform user-reported phishing emails to security incidents is a new flow that contains the security incident creation and aggregation business logic for the new design. You must activate this flow for the new design to take effect.
- The existing User Reported Phishing rules have been preserved during the upgrade.

Note: If you use custom email inbound actions and custom workflows for user reported phishing submissions, you must review both the old and new designs for conflicting or overlapping functionalities.

User Reported Phishing Enhancement details: The following are the details of the enhancement:

- Reporting the phishing email in multiple ways: See Create security incidents from User Reported Phishing emails for the details. The phishing email is then moved to the *sn_si_phishing_email* table.
- Creating phishing email records: If the email-matching rules are met (See Set up ingestion rules for User Reported Phishing), the **Create Phishing Email** inbound action creates a phishing email record. The parsed email headers are stored in the *sn_si_phishing_email_header* table and associated with the phishing email as a related list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Aggregating similar phishing records into a single security incident: The Transform user-reported phishing emails to security incidents flow creates security incidents from the phishing email records and aggregates similar records into a single incident. The aggregation conditions can be modified as required in this flow.

Note:

- The **User Reported Phishing** inbound actions available prior to the Security Incident Response 9.0 release are now disabled. Security incidents are no longer created through the disabled inbound actions.
- The Security Operations spoke application must be installed for the new design to take effect. This includes the Transform user-reported phishing emails to security incidents flow which is available in an inactive state by default. Activate this flow to create security incidents from the phishing email records.

The following image shows the differences between the old and the new designs:



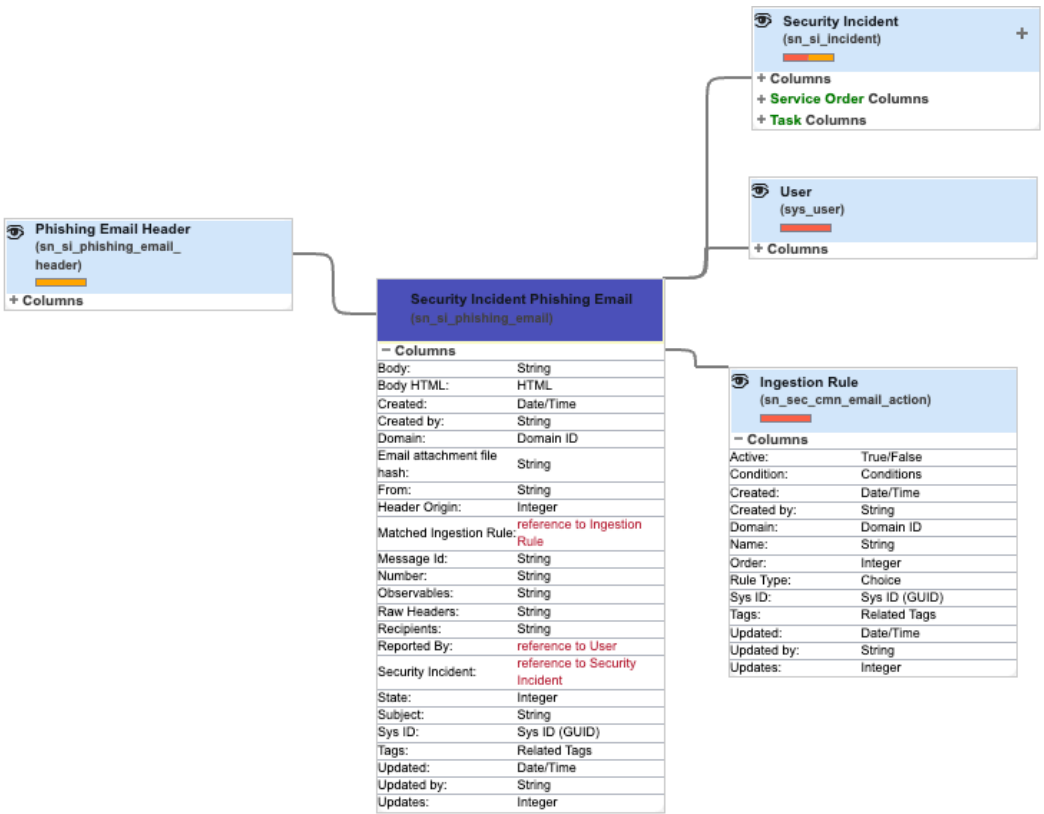
To use the enhanced User Reported Phishing feature, the following plugins and components are required:

- Security Support Common (*sn_sec_cmn*): Includes:
  - Inbound action
  - New EmailUserReportedPhishing script
  - Ingestion Rules table
- Security Incident Response (sn_si): Includes:
  - Security incident table (sn_si_incident)
  - Security phishing emails table (sn_si_phishing_email)
  - Security phishing email headers table (sn_si_phishing_email_header)
  - EML upload record producer
- Security Operations Spoke

  Flows and subflows for aggregating emails and transforming phishing emails to security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure shows the new phishing emails table with references to the matched URP rule and target security incident record (sn_si_incident).



Set up ingestion rules for User Reported Phishing

As a user with the `sn_si.admin` role, you can define email matching rules to filter user reported phishing emails based on specific criteria. For example, you can define a rule where all emails sent either directly or through the Report Phish button to *`security@acme.com`* are categorized as user reported phishing emails.

Before you begin

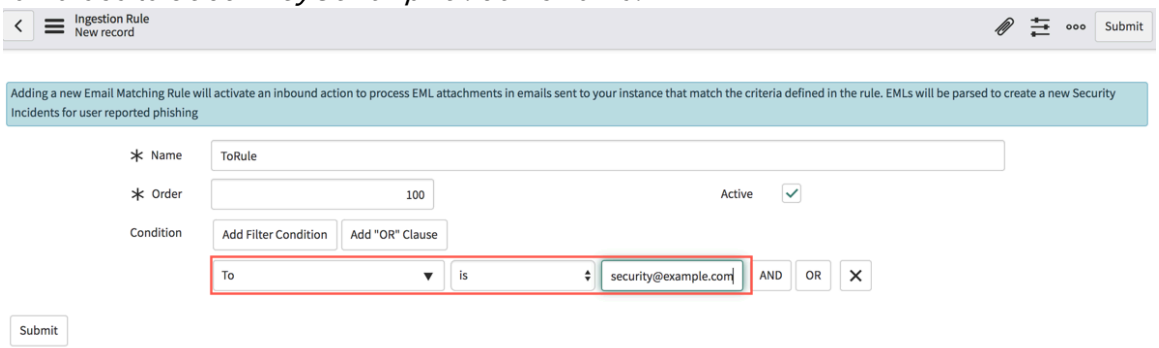
Role required: sn_si.admin

Procedure

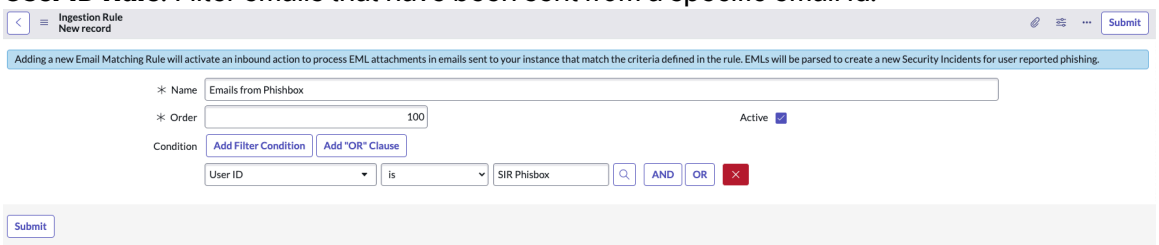
1. Navigate to **All** > **Security Operations** > **Email Processing** > **Ingestion Rules - User Reported Phishing**.
2. Click **New** to create a new Email Matching Rule.
3. Enter a name and define one or more conditions for the rule.
4. Click **Submit** to save the rule.
   The following are some sample rules:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **ToRule**: Filter emails that have been sent directly or forwarded to *security@example.com* email id.



- **User ID Rule**: Filter emails that have been sent from a specific email id.



Define User Reported Phishing properties

Define the header information that must be captured from user reported phishing emails.

Before you begin

Role required: sn_si.admin

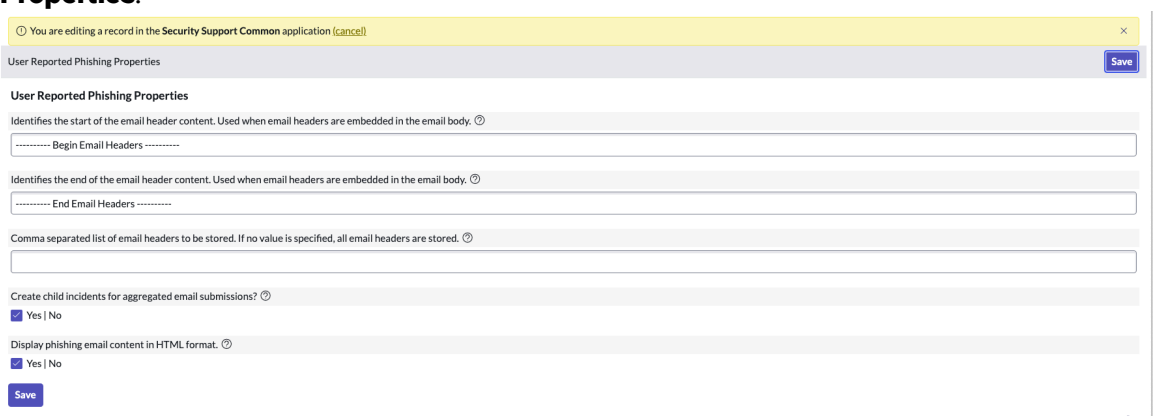
About this task

Use these options to configure the following user reported phishing settings.

- Configuration to extract email headers from the email body. (**Report Phish** submissions.)
- Filter to select headers.
- Enable or disable parent-child association.

Procedure

1. Navigate to **All** > **Security Operations** > **Email Processing** > **User Reported Phishing Properties**.



2. Specify the configuration for extracting email headers from the email body:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Enter a string that identifies the beginning of the email header.
- Enter a string that identifies the end of the email header.

> **Note:** Apply these settings only to headers captured as part of the email body of the phishing email. For instance, if the **PhishAlarm** plugin (previously known as Wombat) has configured with the Microsoft Outlook client, when the user clicks the **Report Phish** button, the email headers are captured as per the configuration defined here. The header information is not captured if the phishing email is forwarded as an attachment.

3. Specify filters to eliminate headers that are not required for investigating the security incident.

   Enter a comma-separated list of email headers that must be captured from the user reported phishing email. If you don't specify any value here, all the header information is captured.

4. Enable or disable parent-child association.
   By default, the **Yes** option is enabled. Select **Yes** to indicate that child security incidents must be created when user reported phishing emails are aggregated. If you select **No**, child security incidents are not created, but the user reported phishing emails are associated with the security incident and the security incident record is updated. See Transform user-reported phishing emails to security incidents for more information on how the child security incidents are created.
5. Enable or disable the option to display the phishing email content in HTML format.
   By default, the **Yes** option is enabled. Select **Yes** to display the phishing email content in HTML format. If you select **No**, the email content in HTML format will not be visible within a phishing record.

Phishing email records created from user reported phishing emails

User reported phishing emails are converted to security incidents based on the email matching rules that have been defined.

When a new phishing email is reported, the following actions take place:

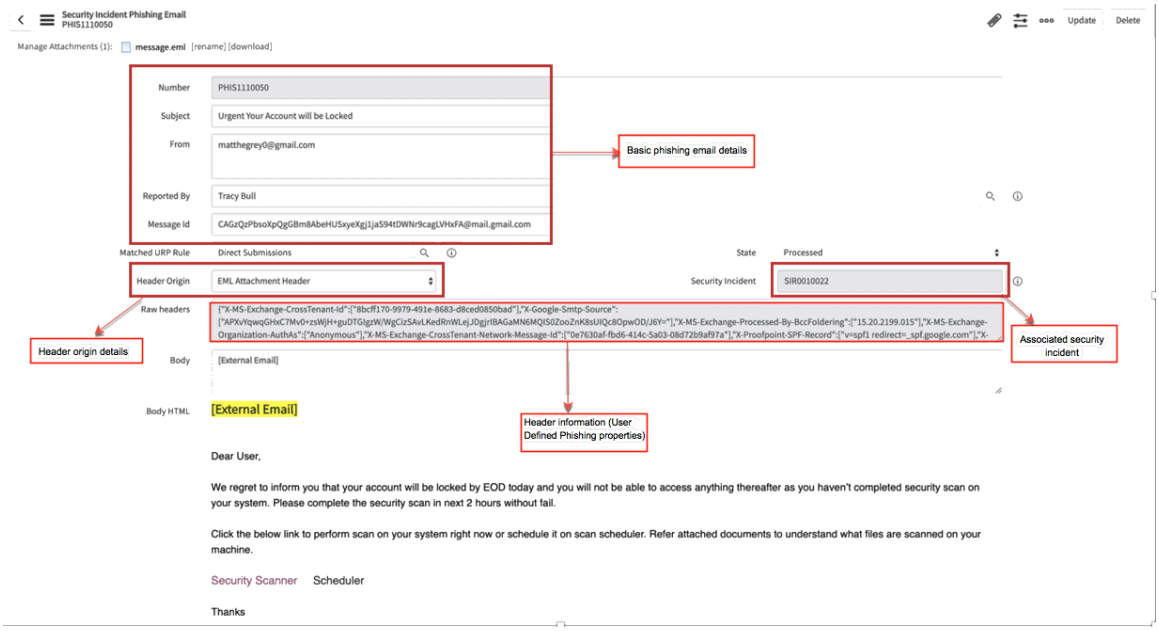
- An email record is created in the *sys_email* table.
- The **Create Phishing Email** inbound action runs on the email record and uses the Email Matching Rules (see Set up ingestion rules for User Reported Phishing) to determine if it is a phishing email.

> **Note:** The email is first verified with all the email matching rules where the **Rule Type** is set to **Deny**. If the email matches to the condition for any of the deny rule, an audit record is created in the `sn_si_phishing_email_deny_audit` table. A security incident isn't created for such email.

- When the email is identified as a phishing email, and it matches to an email matching rule where the **Rule Type** is set to **Allow**, a phishing email record is created in the `sn_si_phishing_email` table.
- Finally, the Transform user-reported phishing emails to security incidents flow is applied to convert the phishing email record to a security incident.

To view the email details, navigate to **Security Incident** > **Show All Phishing Emails**. A list of phishing email records are displayed. Select the date link in the Created column to view the email record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

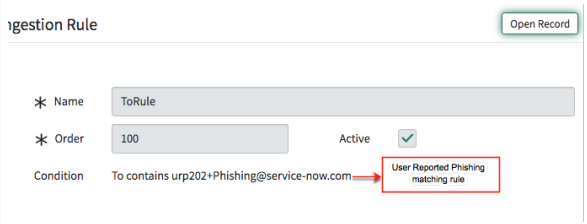


Security Incident Phishing Email Details

Field Name	Description
Number	The number assigned to the user-reported phishing email.
Subject	The subject of the email. The subject rule is useful in simulated phishing campaigns or tests. In this case, organizations send deceptive emails to their own staff to test their response to phishing and similar email attacks. In simulated phishing email tests, if the Microsoft Outlook email client with the **PhishAlarm** plugin (previously known as Wombat) is being used, the user can select the **Report Phish** button to report the phishing email. The email is sent to the Security Operations team with **Simulated Phishing** appended to the Subject of the email. This is used to identify the email as a simulated phishing email.
From	The email address from where this phishing email originated. This information is available if the phishing email is forwarded as an .EML file attachment or if the original headers are embedded in the email. If the user forwarded the phishing email directly, the From address may not be available.
Reported by	The email id of the user who reported this phishing email. Select the **Information** icon to view additional details.
Message id	The id assigned to the message.
Matched URP rule	The User Reported Phishing rule that is to be applied on this email. Select the Information icon to view additional details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Phishing Email Details (continued)

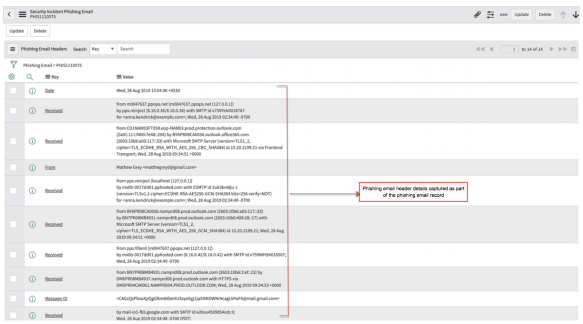
Field Name	Description
	 As you can see, in this example, the **Condition** field shows that the ToRule is applied on this email and a security incident is created. See Set up ingestion rules for User Reported Phishing for more information on defining email matching rules.
State	When a new phishing email record is created in the `sn_si_phishing_email` table, the State field is set to **New**. When this email record is converted to a security incident (see Transform user-reported phishing emails to security incidents), the State field is updated to **Processed**.

Header origin	This field indicates how the email headers originated or how the user reported the phishing email:
	• **Email Header**: The user forwarded the phishing email to the security operations team.
	• **Email Text Body:**
	  ○ The user selected the **Report Phish** option (if the **PhishAlarm** plugin (previously known as Wombat) has been configured with the email client).
	  ○ Based on the User Reported Phishing rule defined, the phishing email is forwarded to the security operations team.
	• **EML Attachment Header**:
	  ○ Attachment: The user forwarded the email as an attachment (.EML file).
	  ○ Service catalog submission: The user downloaded the email as a .EML file to the desktop and then uploaded it to a specified location. The security incident is then created from the email.
	• **EML Attachment Body**:
	  ○ The user selected the **Report Phish** option (if the **PhishAlarm** plugin (previously known as Wombat) has been configured with the email client).
	  ○ Based on the User Reported Phishing rule defined, the phishing email is forwarded as an attachment to the security operations team.

Security Incident	This field is blank when the user-reported-phishing email is first reported. When the Transform user-reported phishing emails to security incidents flow has been executed, this email is converted to a security incident record and the number of this record is displayed here.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Phishing Email Details (continued)

Field Name	Description
	Note: Security incident is only created for the emails, which matches to an email matching rule where the **Rule Type** is set to **Allow**.
Raw headers	This field shows the complete header information extracted from the email as defined in the Define User Reported Phishing properties page. The headers are parsed into key value pairs and displayed in the Phishing Email Headers list.
	
Body	Body of the user-reported phishing email.

Transform user-reported phishing emails to security incidents

The **Transform Phishing Email to Security Incident** flow converts or transforms phishing email records to security incidents.

Before you begin

Note: To enable the User Reported Phishing functionality, you must make a copy of the flow#and activate it. If you have created custom inbound actions and custom flows to handle user reported phishing submissions, the flow modifications suggested here aren't required.

- Role required: sn_si.admin
- Flow Designer spoke must be installed.

About this task

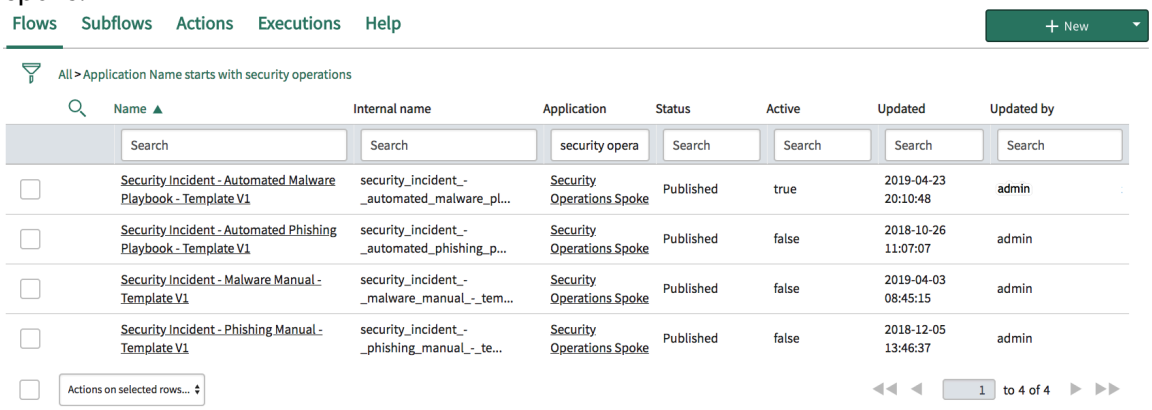
This flow is automatically launched when a user reported phishing email record with the State set to **New** is created. This flow contains the logic to:

- Aggregate security incidents.
- Update security incidents with relevant notes.
- Add header data.
- Create child incidents as required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

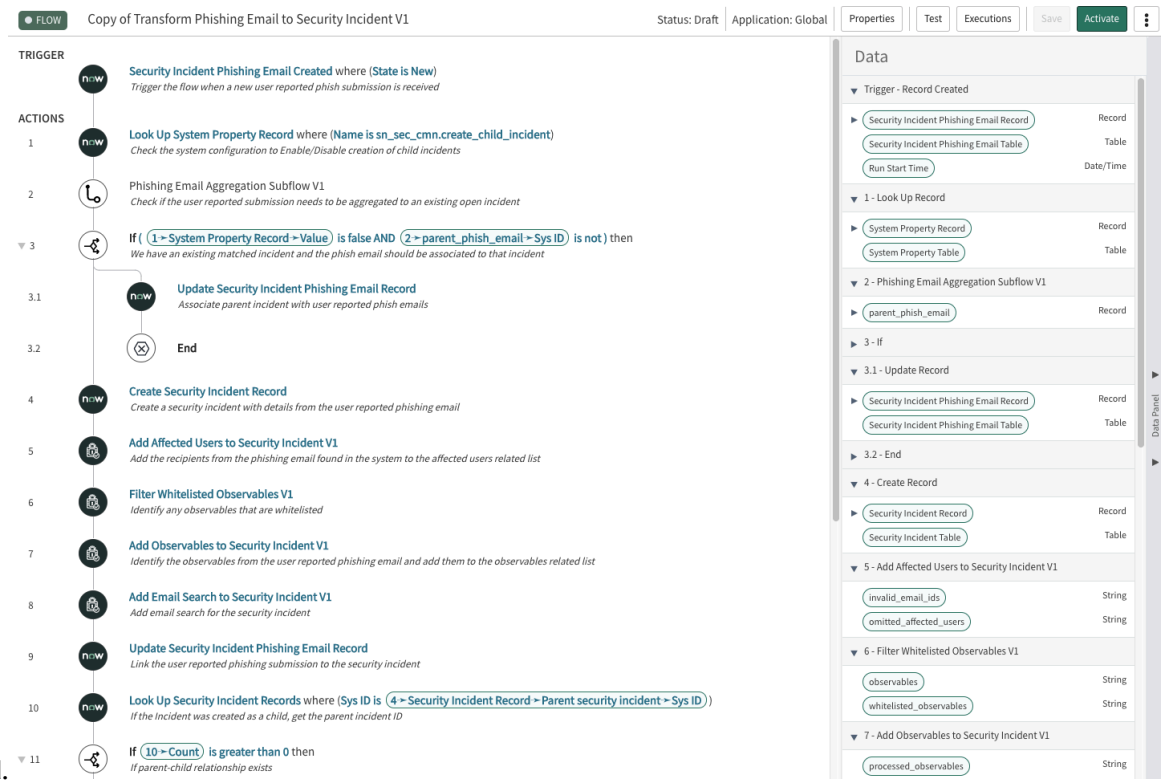
Procedure

- Navigate to **Flow Designer** > **Designer** to view the flows available with the Security Operations spoke.



- Select the **Transform Phishing Email to Security Incidents** link to view the flow.
- This flow is provided with the base system and is in **Read Only** mode and can't be used.

  Select the more icon , make a copy of the flow and open it for your use. You can now change your flow, such as modifying trigger conditions or actions, or adding and removing actions. After making the necessary changes, you must activate (See Activate a Security Incident Response flow) the flow so that it can be executed.

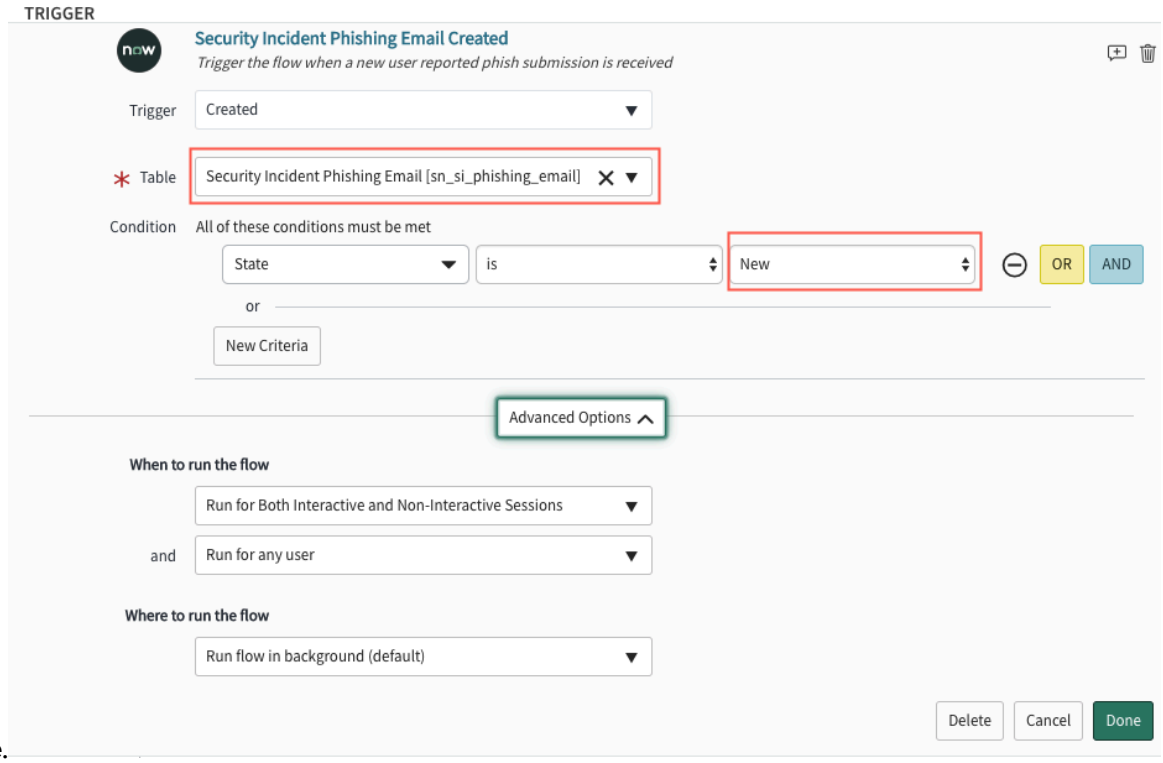


  This figure shows the trigger and the steps executed with the flow. The-right hand panel shows the data flow. Select on an icon to expand the step and view the details.

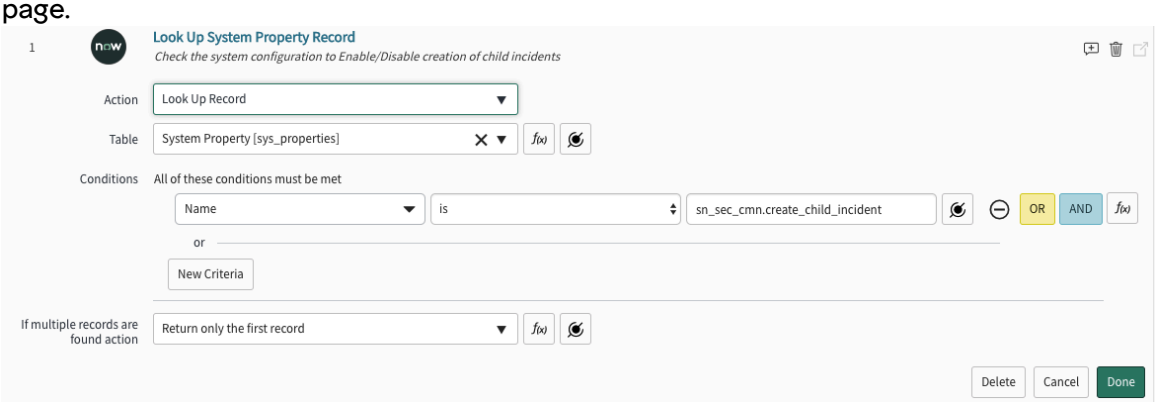
- Select the **Trigger** icon.
  In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and task to be performed when the conditions are met. This flow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

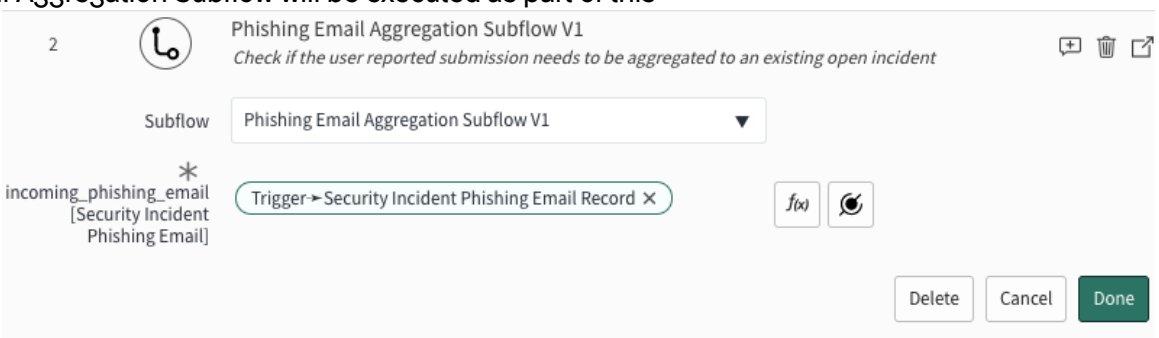
is initiated when a **New** record is uploaded to the `sn_si_phishing_email` table.



- In step 1, the flow verifies if the **Create child incidents for aggregated email submissions?** flag is enabled or disabled on the Transform user-reported phishing emails to security incidents page.

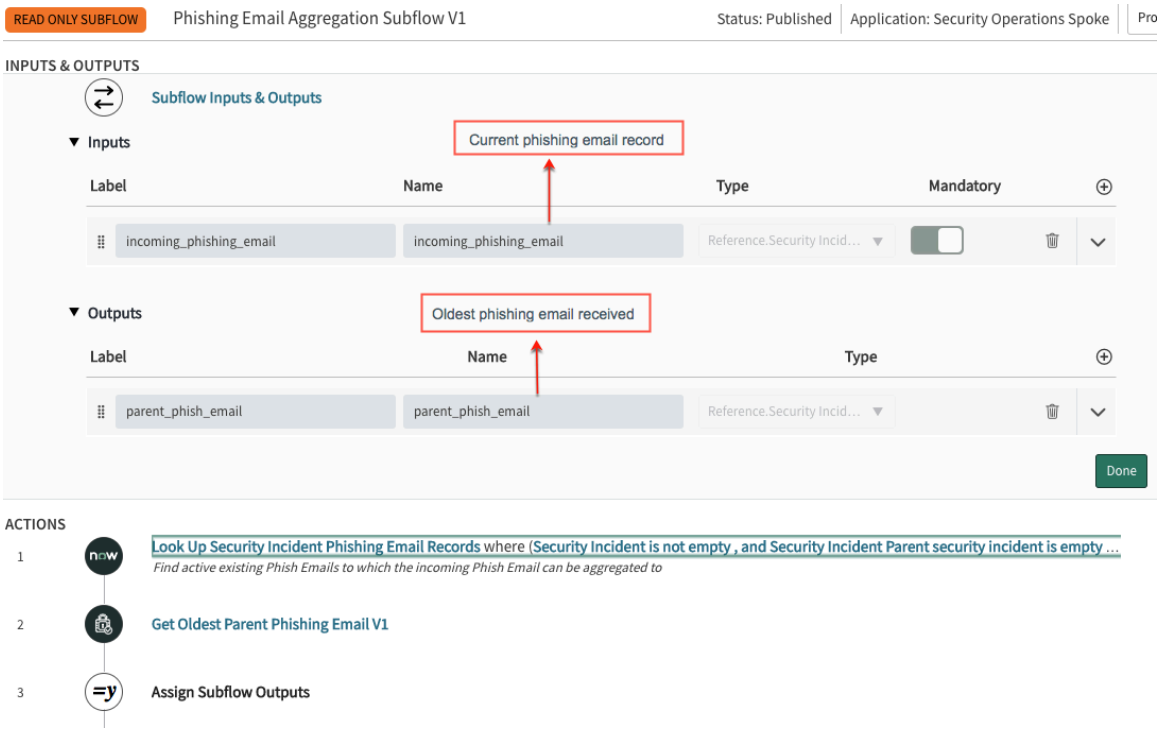


- In step 2, the oldest parent security incident is identified. Notice the icon in step 2. This indicates that the Phishing Email Aggregation Subflow will be executed as part of this step.

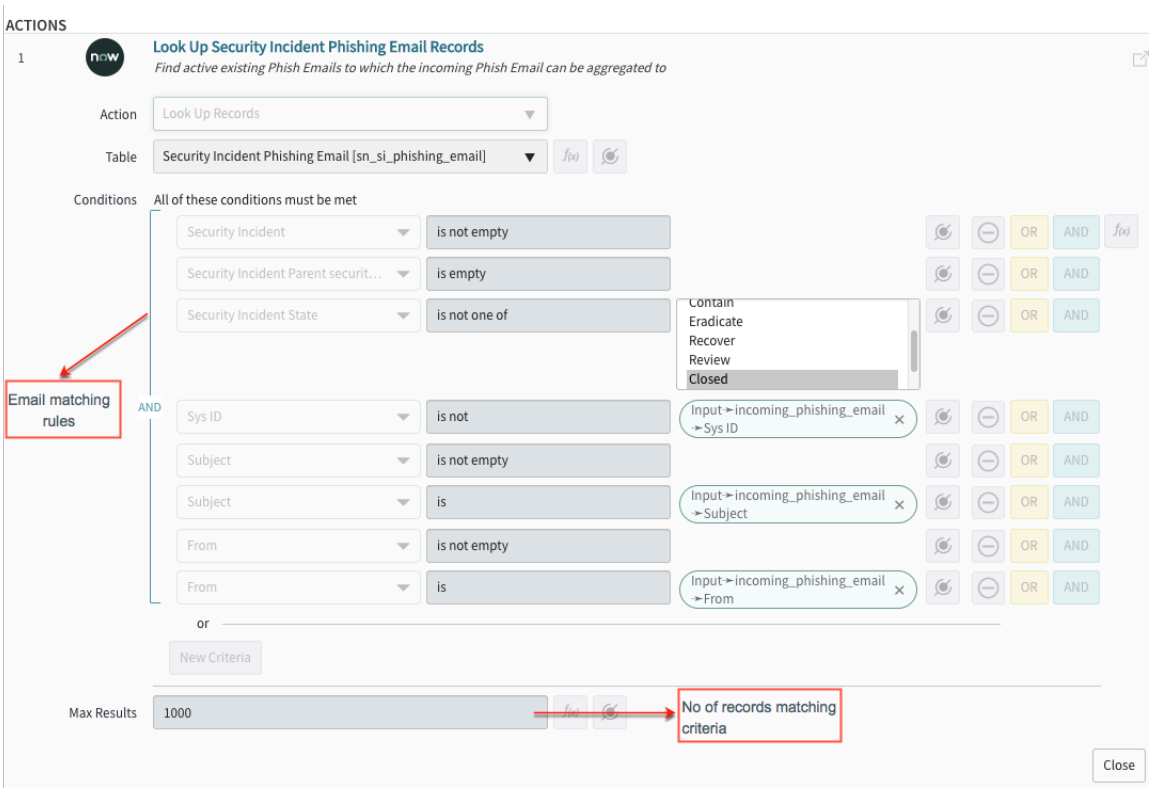


Select the action designer icon to see a detailed view of the action. This subflow checks the phishing email and matches it with an existing security incident based on the specified criteria.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



These two actions are performed when this subflow is executed. Select on the link of the first action to view additional details.



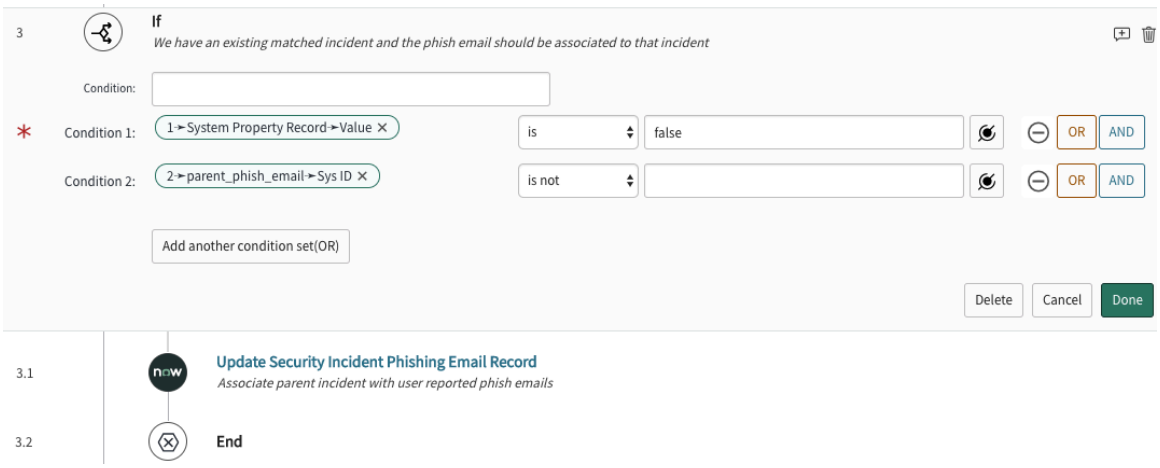
This action checks the emails that match the criteria for the new incoming email based on conditions such as:

- Security Incident State isn't **Closed**.
- Subject or From value match the email matching rule conditions defined (See Set up ingestion rules for User Reported Phishing).

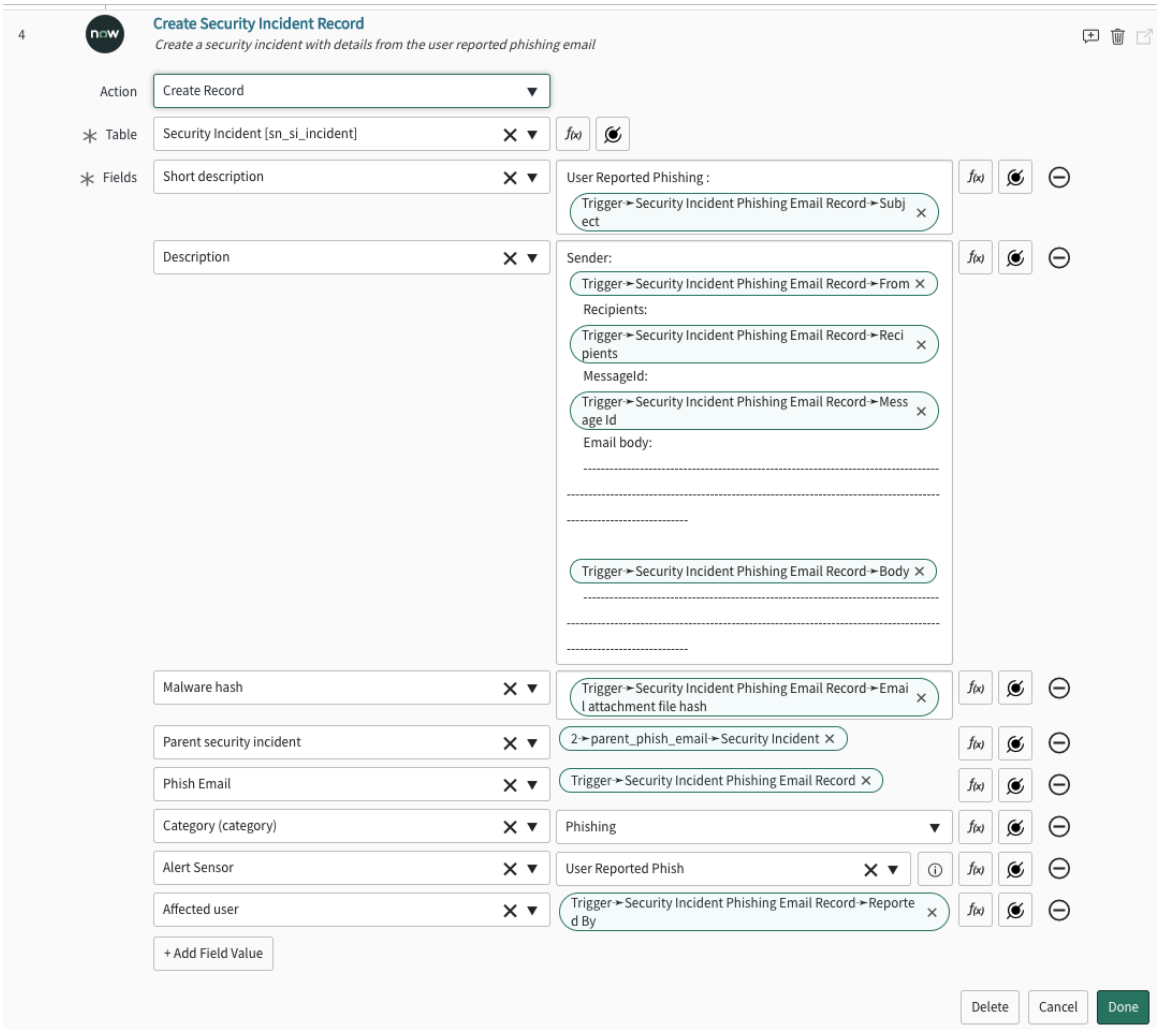
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If these conditions are met, you can see the number of records that match the criteria in the Max Results field. The oldest or the first record in the list is designated as the parent record against which the security incidents are aggregated.

- Step 3 is applicable only if the **Create child incidents for aggregated email submissions?** flag was set to **No** in the Transform user-reported phishing emails to security incidents page. In this case, the phishing email is associated with the security incident record and the flow ends.

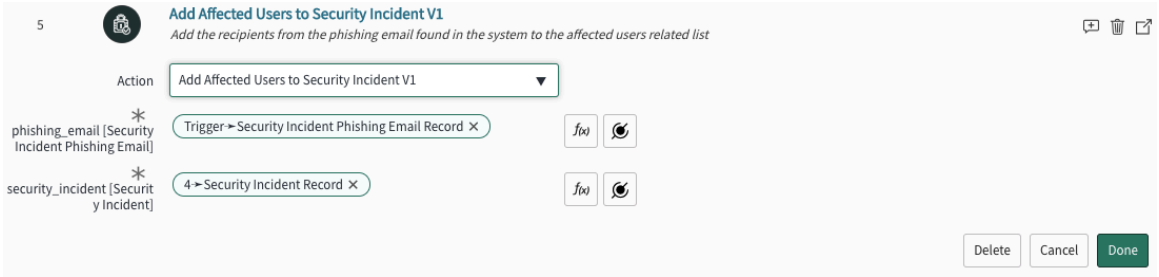


- If the **Create child incidents for aggregated email submissions?** is set to **Yes**, the flow continues to run and a new security incident is created based on the user-reported phishing email.

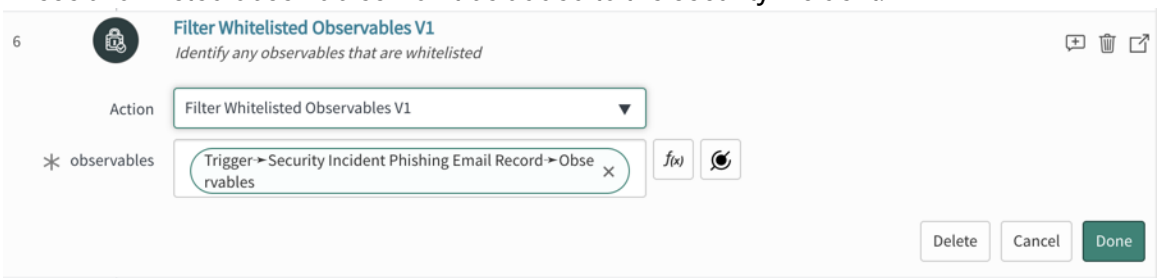


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

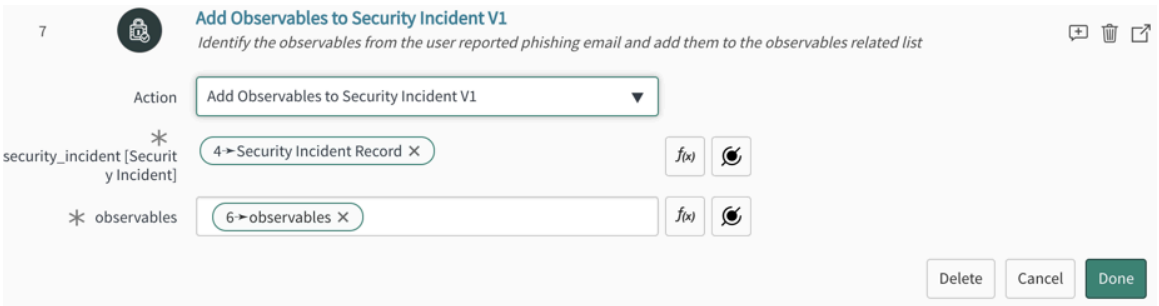
- In step 5, users who received the phishing email (employees in the To and CC list of the phishing email) are added to the Affected Users related list in the security incident record.



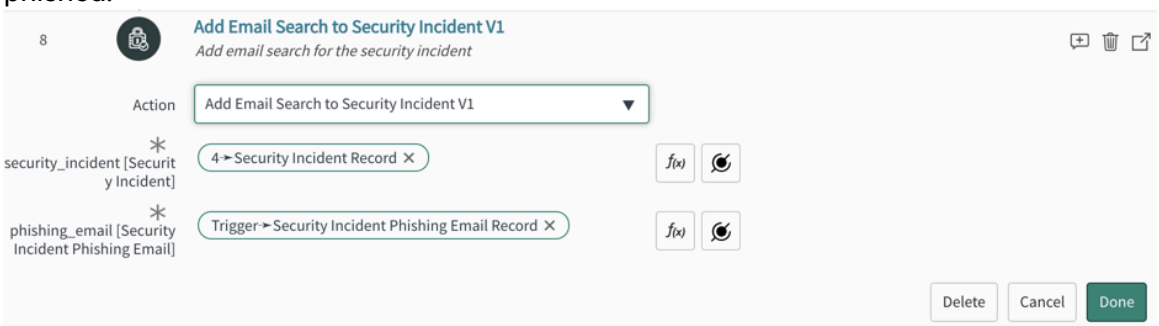
- In step 6, allow listed observables are filtered from the list of observables in the security incident.
  These allow listed observables won't be added to the security incident.



- In step 7, unknown observables from the user-reported phishing email are identified and added to the Observables related list.

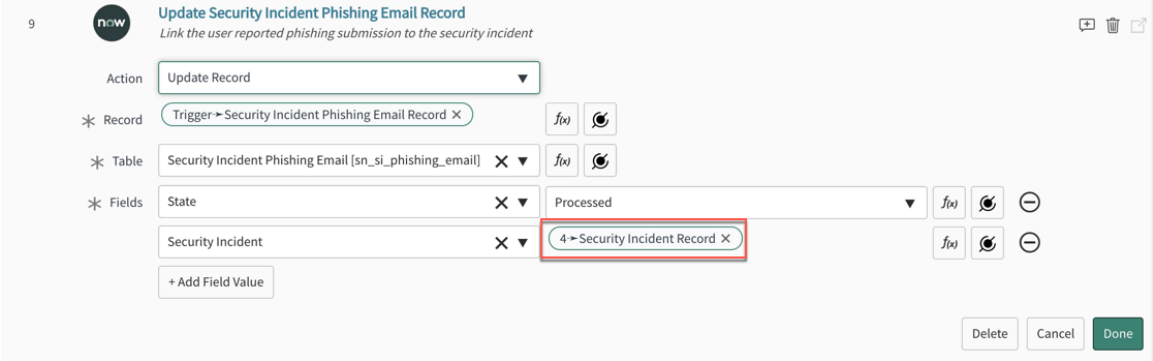


- In step 8, an email search query is generated which is a combination of the Subject and the From address of the email.
  This information is useful in identifying the employees in the organization who have been phished.



- In step 9, the user reported phishing email is associated with the security incident and the security incident record (created in step 4) is updated.

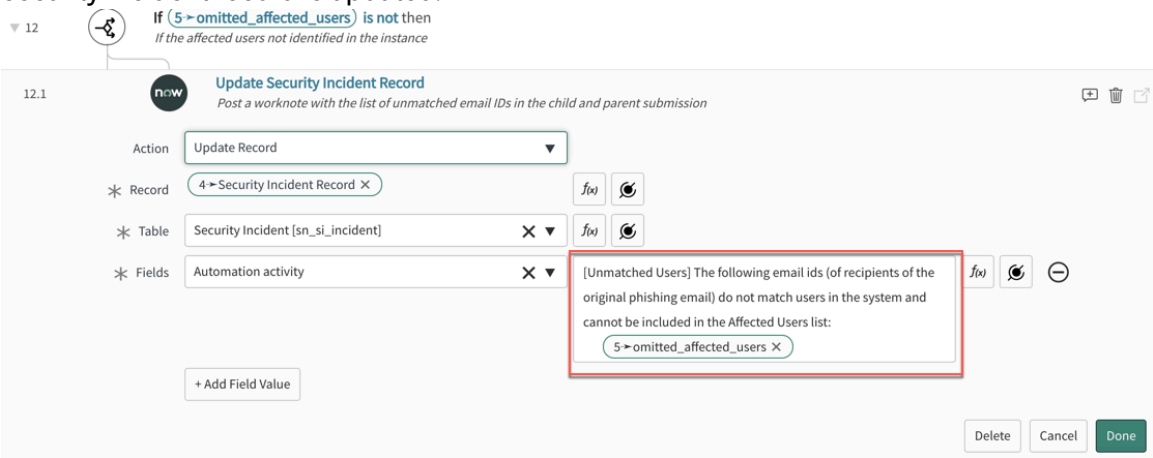
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- In step 10, the parent security incident is identified and a check is made to see if it's an open security incident record.

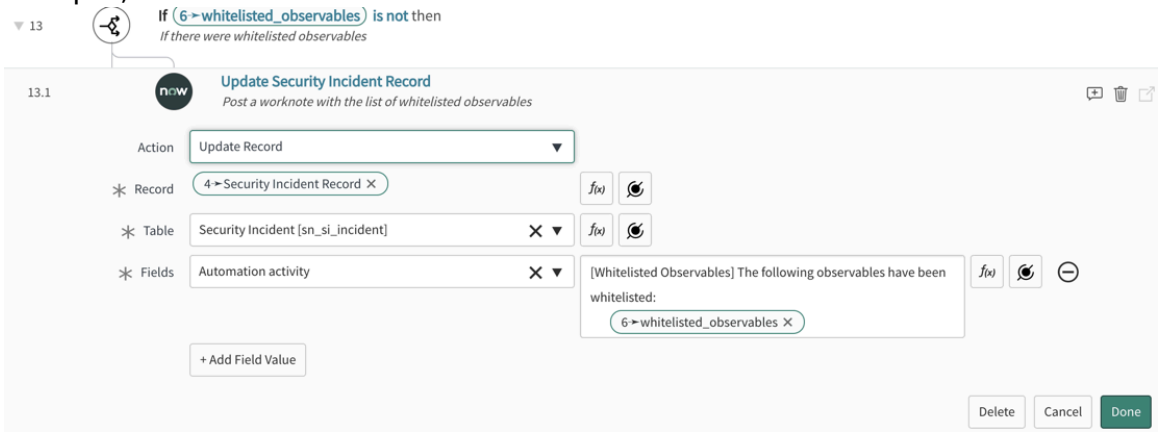


- If the parent security is active, notes are added to the child and the parent security incident records indicating how they're associated with each other.
- In step 12, if no Affected Users were found (in step 5 of the flow), a worknote is added and the security incident record is updated.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

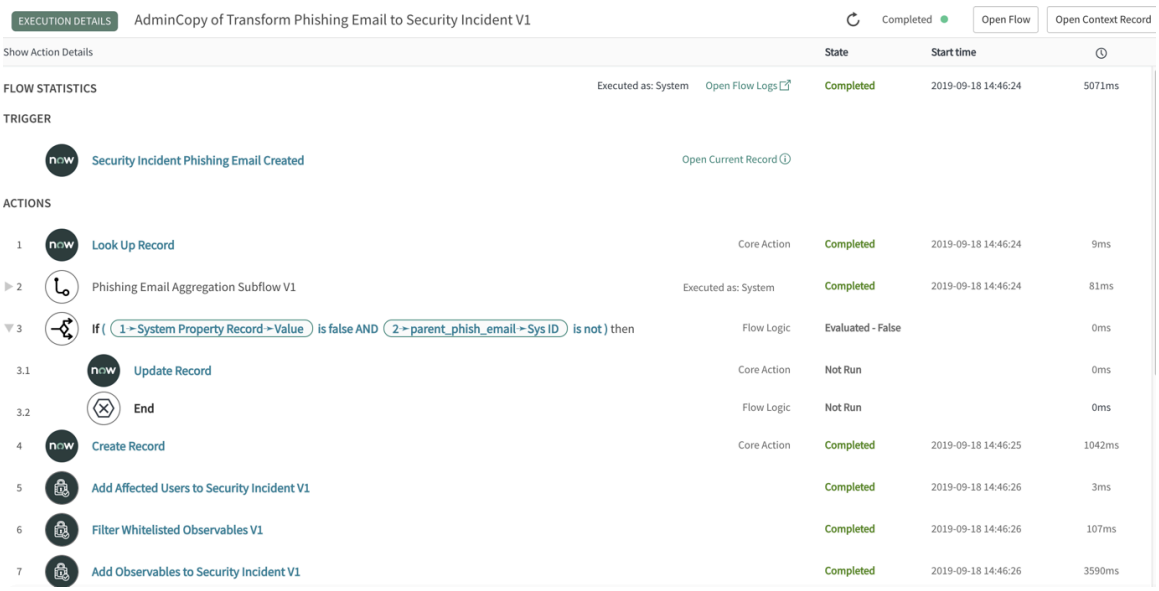
- In step 13, a worknote is added with the list of allow listed observables.



What to do next

You can select **Test** to simulate the actions in the flow before it is published. After testing the flow, select **Activate** to activate the flow so that it can be executed.

Select **Executions** to view the execution details of the flow.



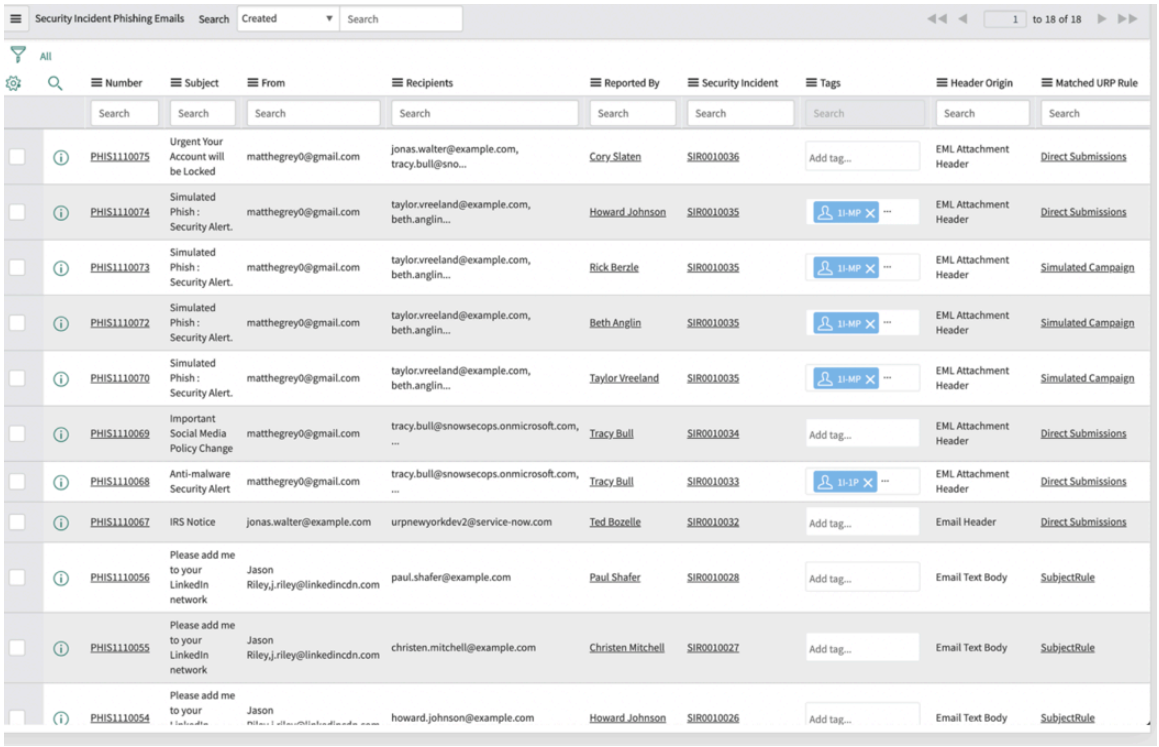
When the flow has been executed, the phishing email record is converted to a security incident. See Security incident records created from phishing email records.

Security incident records created from phishing email records

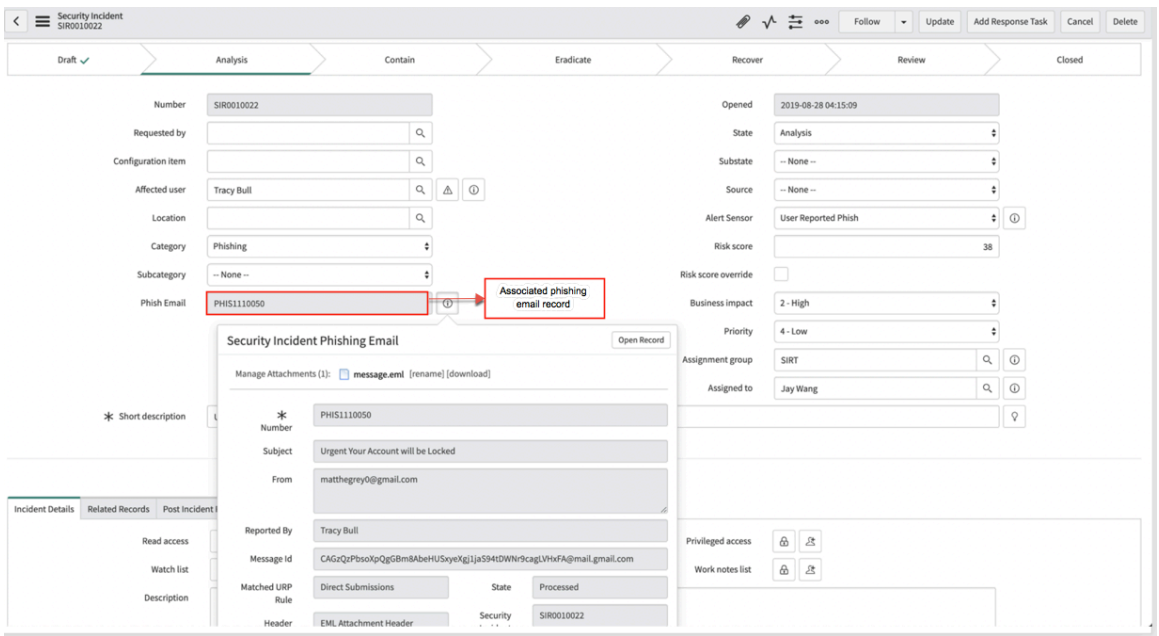
Phishing email records stored in the *sn_si_phishing_email* table are converted to security incidents records.

To view the security incident associated with the phishing email record, click **Security incident** > **Phishing Email** > **Show All Phishing emails**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Click the link in the Security Incident column associated with the phishing email record. The security incident details are displayed.



Related lists

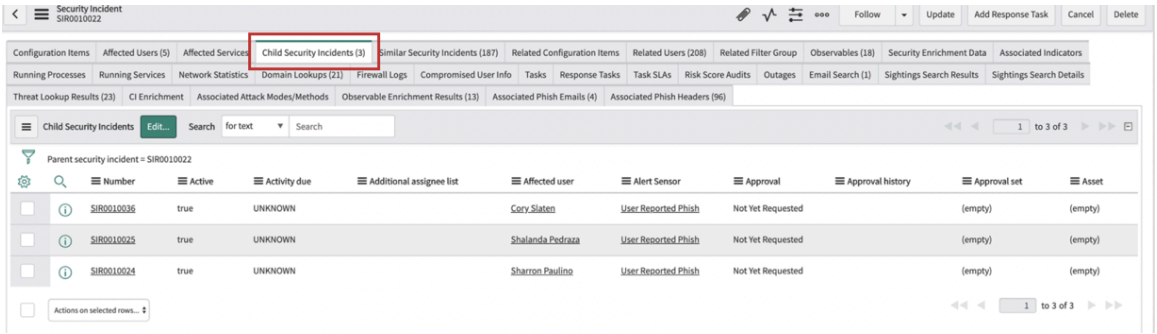
Scroll down to the Related Links section of the security incident and click **Show All related list**. View details like child security incidents, affected users, associated phishing emails.

Child security incidents

Click the **Child Security Incidents** tab. You can see a list of child security incidents associated with the parent security incident based on the aggregation logic that has been applied. For every child record added, an automated system activity is added (in the Worknote section) to the parent record. This notifies the security analyst about the aggregated child record.

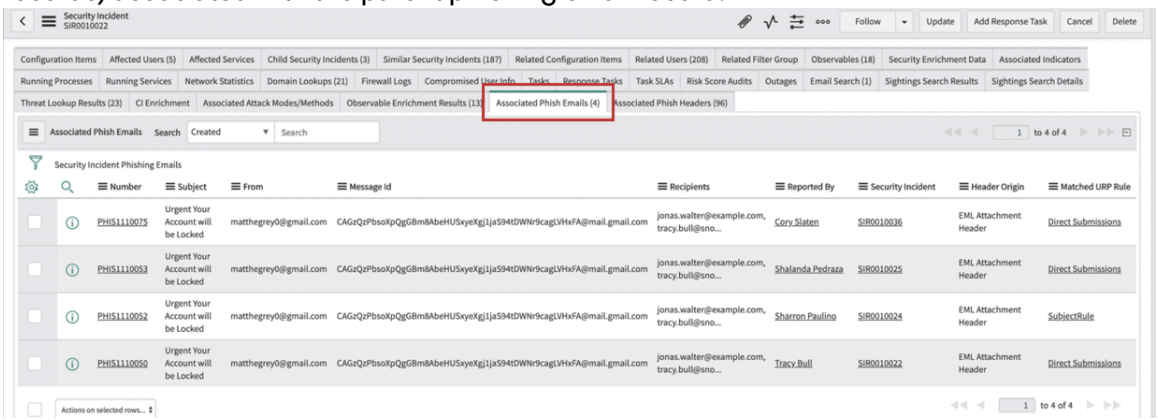
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can see the child security incidents here only if the **Create child incidents for aggregated emails submissions** flag is set to **Yes** in the User Reported Phishing Properties page. See Define User Reported Phishing properties for the details.



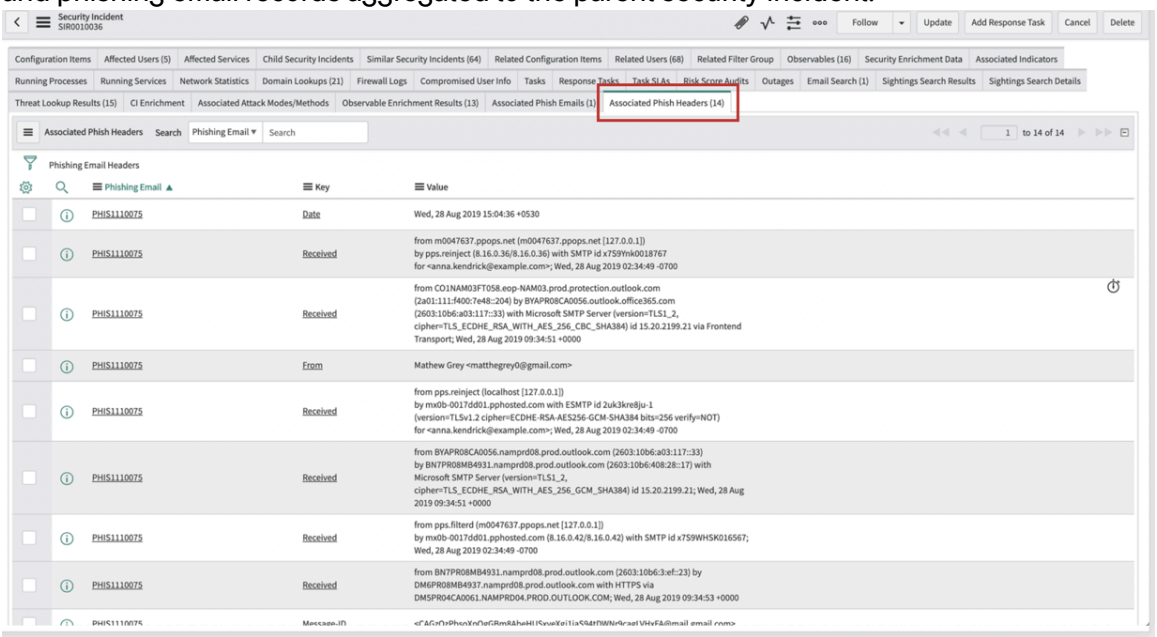
Associated phishing emails

Click the **Associated Phish Emails** tab. You see a list of phishing email records (duplicate records) associated with the parent phishing email record.



Associated phishing email headers

Click the **Associated Phish Emails** tab. You see the phishing email header details that have been captured as part of the security incident. You can view the rolled-up headers of all child records and phishing email records aggregated to the parent security incident.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Allowed list observables

As the Transform user-reported phishing emails to security incidents flow is being executed, you can monitor the status of the security incident. When certain observables are marked as allowed list observables, they aren't added to the Observables Related list. By marking the observables to the allow list, you can ensure that only the important details are displayed. For example, if www.google.com is one of the URLs that has been tagged as the allowed list, the following system message is displayed. Allowed list observables ensure that only the important observables are monitored.

Capturing unmatched users

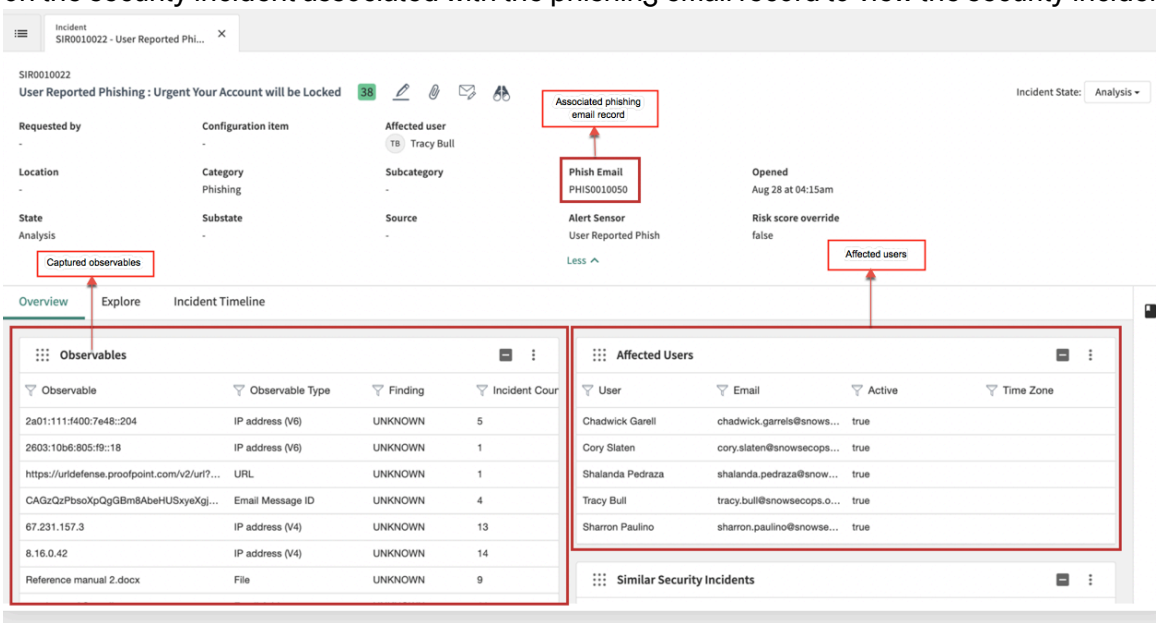
Some email ids in the To and CC list of the phishing email may not belong to users in the organization. These email ids are categorized as unmatched users and aren't included in the Affected Users related list. A worknote indicating that these are unmatched users is displayed.



User Reported Phishing in the Security Analyst Workspace

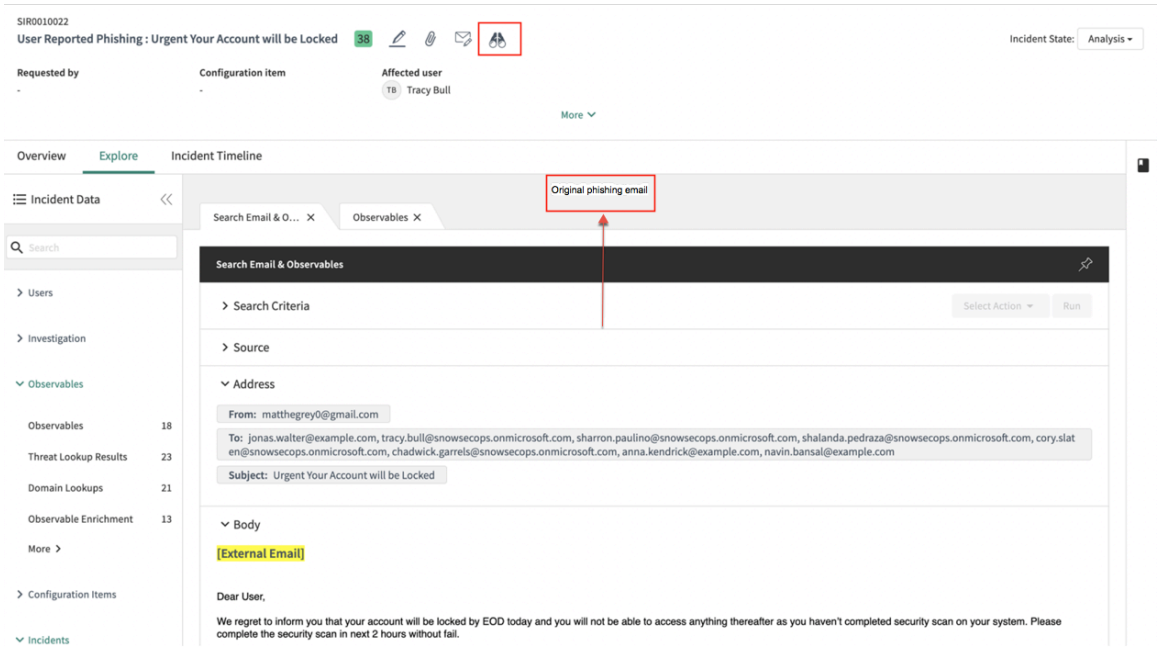
You can view security incidents associated with the phishing email records in the Security Analyst Workspace.

Navigate to **Security Incident** > **New UI**. The workspace opens in a separate browser tab. Select on the security incident associated with the phishing email record to view the security incident.

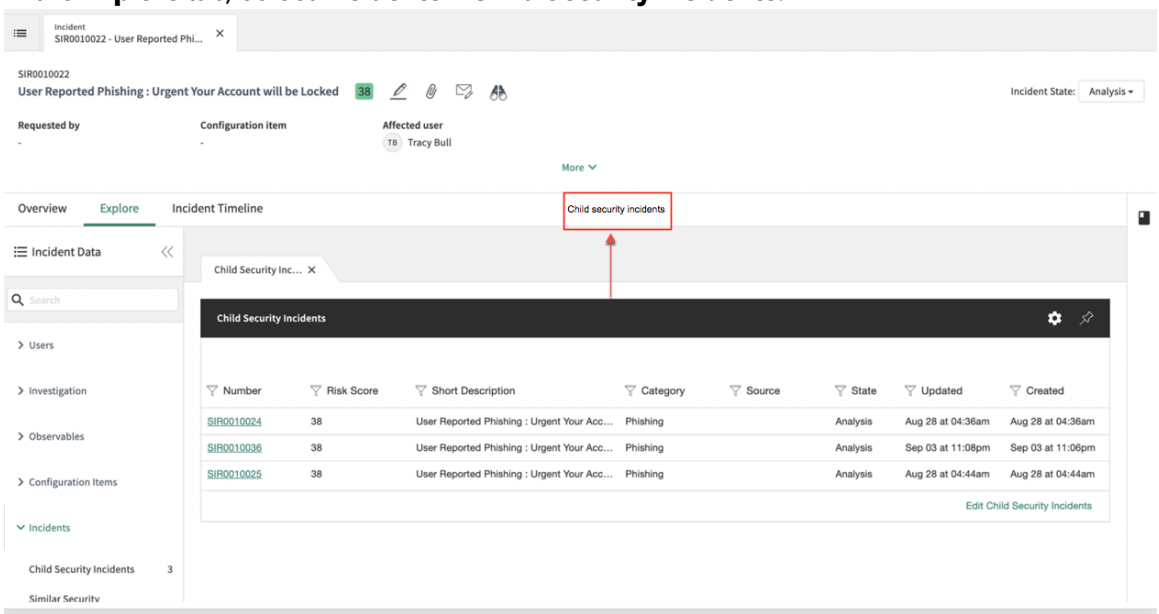


Select the binoculars icon. The original phishing email is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

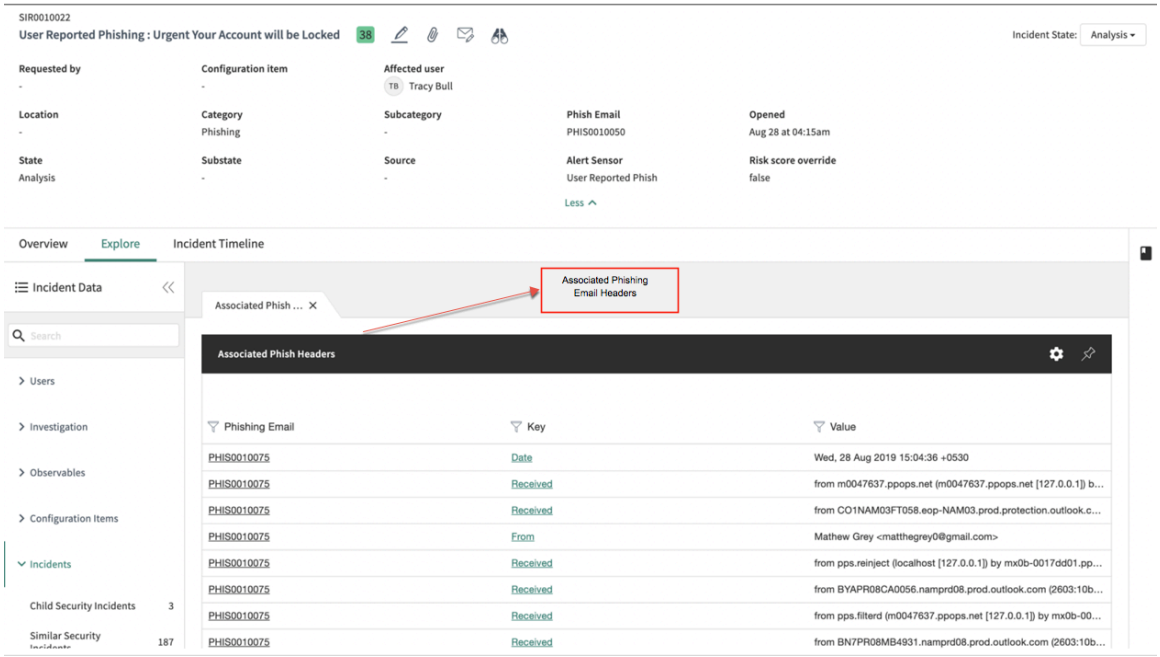


In the **Explore** tab, select **Incidents** > **Child Security Incidents**.

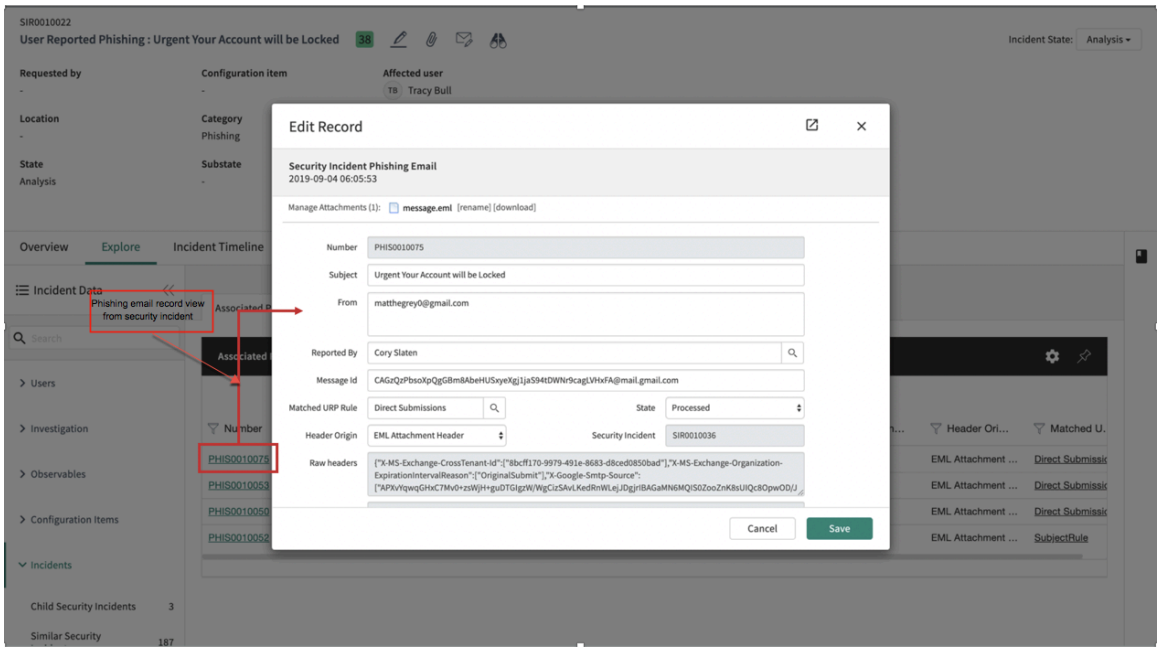


Select **Incidents** > **Associated Phish Headers** > . You can view the rolled up headers of all child records and phishing email records aggregated to the parent security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

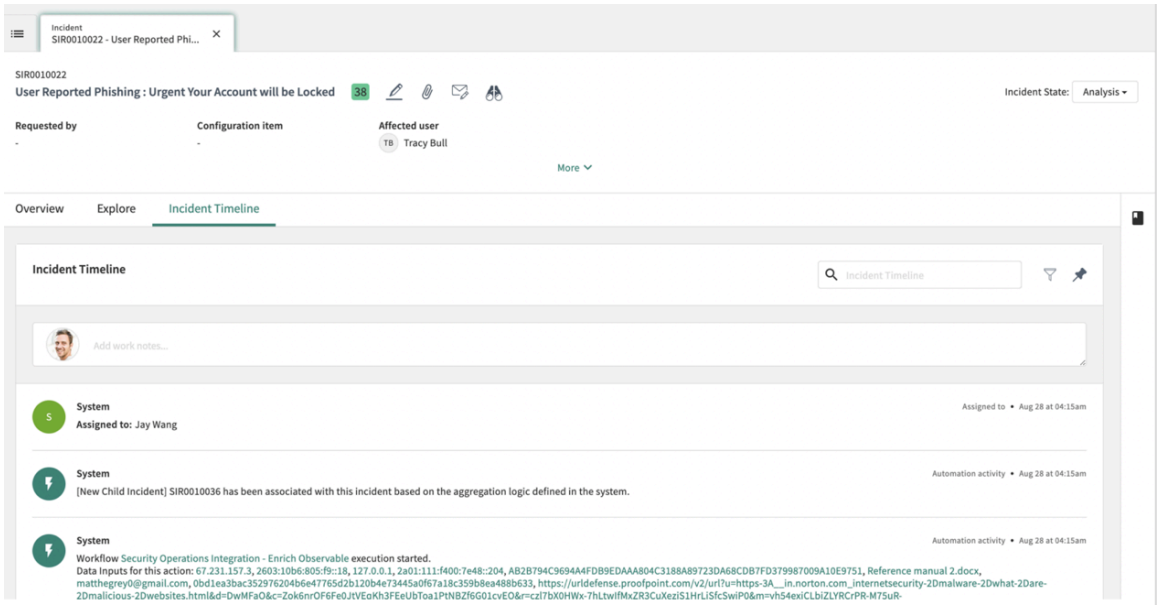


Select on the phishing email link to view the phishing email record associated with the security incident.



Select the **Incident Timeline** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can view the system updates that highlight:

- Identified duplicate child records.
- Allowed list observables.
- Unmatched users who received the phishing email but do not belong to the Affected Users list.

Frequently Asked Questions

This section covers some of the frequently asked questions about the enhanced User Reported Phishing feature.

1. I have installed the new Security Incident Response spoke but I cannot view any user reported phishing incidents.

   By default, the User Reported Phishing functionality has been disabled.

   To enable this feature, you must make a copy of the read-only Transform user-reported phishing emails to security incidents flow and activate it before use.

2. While ingesting phishing emails and converting them into security incidents, what precautionary measures are used to handle malicious links and attachments in the phishing emails?

   The ServiceNow anti-virus scanner scans such malicious attachments and links. However, to ensure that security analysts can investigate the incidents accurately, the Security Incident Response application captures all the artefacts that are part of a phishing email. But the User Reported Phishing functionality mutes the malicious links in the phishing email so that security analysts don't accidentally click these links. Regarding malicious attachments, security analysts must be cautious about downloading them.

3. Do we capture all malicious files that are part of the phishing emails for security incident enrichment?

   Yes, we capture all files from the phishing emails. You can view these details are available as part of security incident observables in the form of a file hash.

4. Do we send malicious files and links from phishing emails to a sandbox instance for investigation?

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Currently, we do not support out-of-the-box sandbox integrations for investigating malicious files and links.

5. Is there a time window or a trigger that defines the duration in which incoming duplicate phishing email records are associated with a parent security incident?

   Duplicate phishing email records are aggregated only to an active parent security incident. If the parent incident is closed or canceled, then the incoming new duplicate phishing email will be created as a new security incident. However, in this scenario, within the new security incident, you can view the closed or canceled parent security incident in the **Similar Security Incident** related list.

   Note: This behavior can be configured using the flow designer.

6. Does the User Report Phishing feature support the use of only the Microsoft Outlook **PhishAlarm** plugin (previously known as Wombat) to capture email header details?

   The User Reported functionality has been built to parse email headers and complies with RFC822 standards. So, similar to the **PhishAlarm** plugin (previously known as Wombat), all other Microsoft Outlook plugins that capture email headers based on RFC822 standards are supported.

Record creation from security incidents

After you have created and saved a security incident, you can create a change request (CHG), incident (INC), or problem (PRB) record from it. You can also create a customer service case from any security incident.

Create a change, incident, or problem from a security incident

After you have created and saved a security incident, you can create a change request (CHG), incident (INC), or problem (PRB) record from it.

Before you begin

Role required: sn.si_basic or higher

Procedure

1. Open a security incident using one of these methods.
   - Open an exiting security incident by navigating to **Security Incident** > **Unassigned** > **Incidents**, and clicking a security incident.
   - Create a security incident by navigating to **Security Incident** > **Unassigned** > **Incidents**, click **New**, fill out the form, and save the record.
2. Right-click in the security incident header bar and click one of the following:
   - **Create Change**
   - **Create Incident**
   - **Create Problem**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: This choice applies only if the popup property (sn_vul.popup) is enabled. When you click one of these buttons, a preview window opens to show you the information from the security incident that is used to create the change, incident, or problem. That is, the configuration item, its location, its priority, and the short and long descriptions. If you are creating a Change Request you can edit the **Priority**, **Short description**, and **Description** fields. If you are creating an Incident, you can edit the **Impact**, **Urgency**, **Short description** and **Description** fields. The fields in the associated security incident screen are not affected.

3. Click **Submit** to create the change, incident, or problem.

Create a Customer Service case from a security incident

Security Incident Response ships with a default field mapping that maps a security incident to a Customer Service (CS) case. You can create a CS case from any security incident, edit the **Priority**, and also add **Optional notes**.

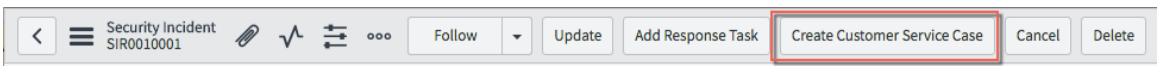
Before you begin

Role required: sn_si.basic and sn_customerservice_agent

Note: The Customer Service plugin must be activated to perform this task.

Procedure

1. Navigate to **Security Incident**.
2. Open the security incident that you want to add a CS case to.
3. Click **Create Customer Service Case** in the top header.

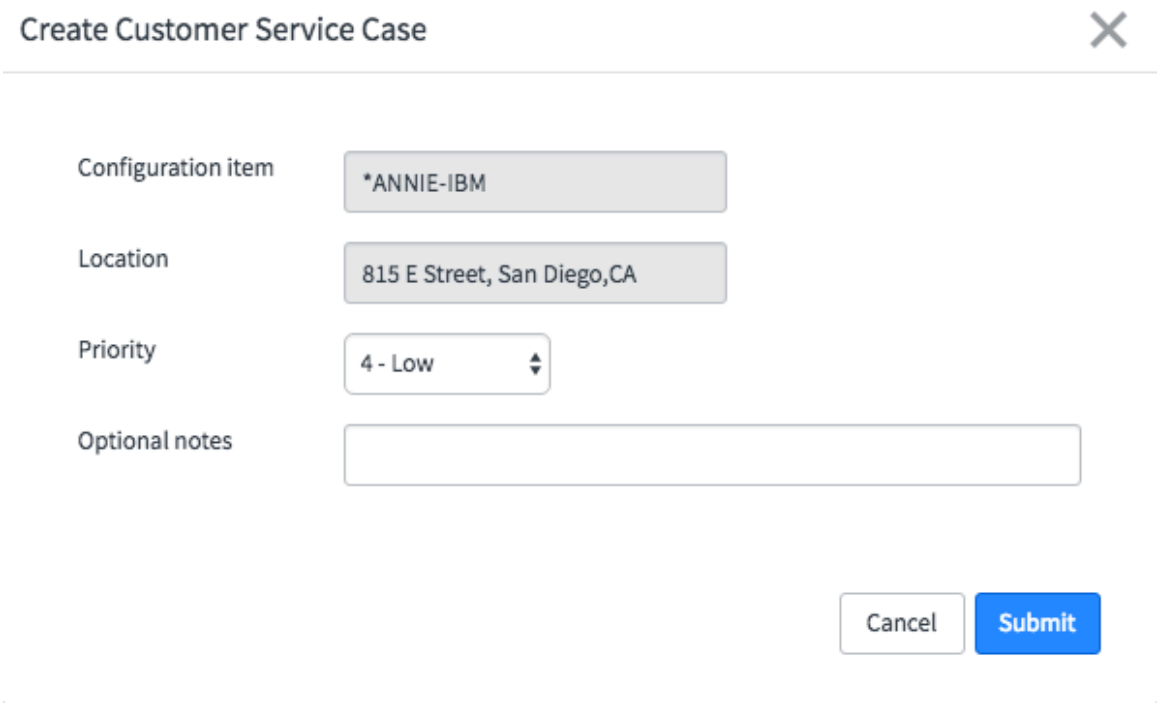


The pop-up window is prepopulated with information from the security incident based on your field mapping.

4. You can select a new **Priority** and add any **Optional notes**.

Note: The **Priority** field overwrites the default setting. The **Optional notes** are appended to the incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit.**
   A CS case is created and displayed in the Customer Service Cases related list in the security incident.
6. You can click the CS case link to follow up on the case.

Related topics

Customer service case management

Add a security incident to a security case

If you determine that a security incident requires a higher level of analysis, add it to a new or existing case.

Before you begin

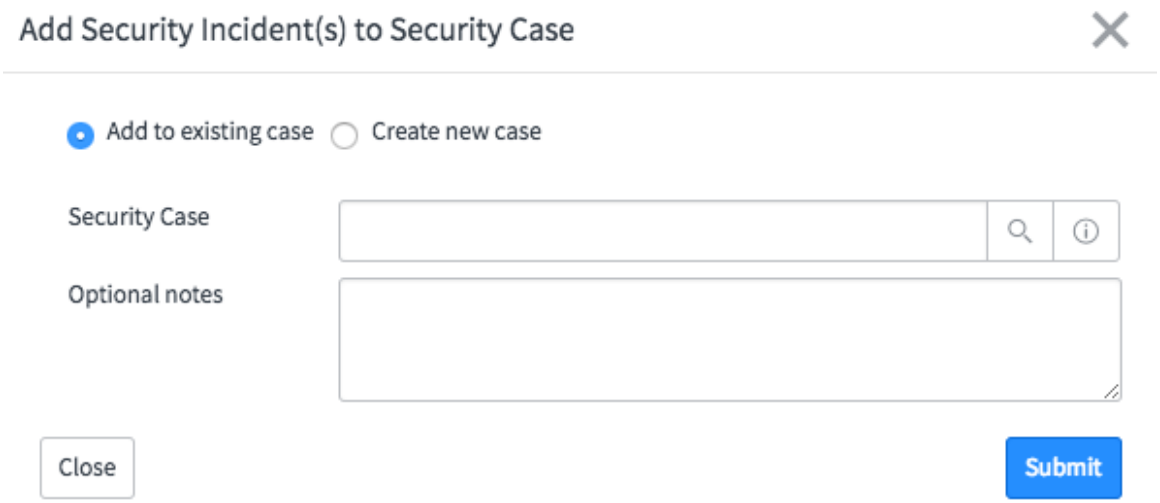
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_si.admin, sn_ti.case_user_write

Procedure

1. Navigate to the security incident that requires escalation by clicking **Security Incident** > **Incidents** > **Assigned to Me**, and open the security incident.
2. Click the **Add to Security Case** related link.
   The **Add Security Incident(s) to Security Case** dialog box opens.

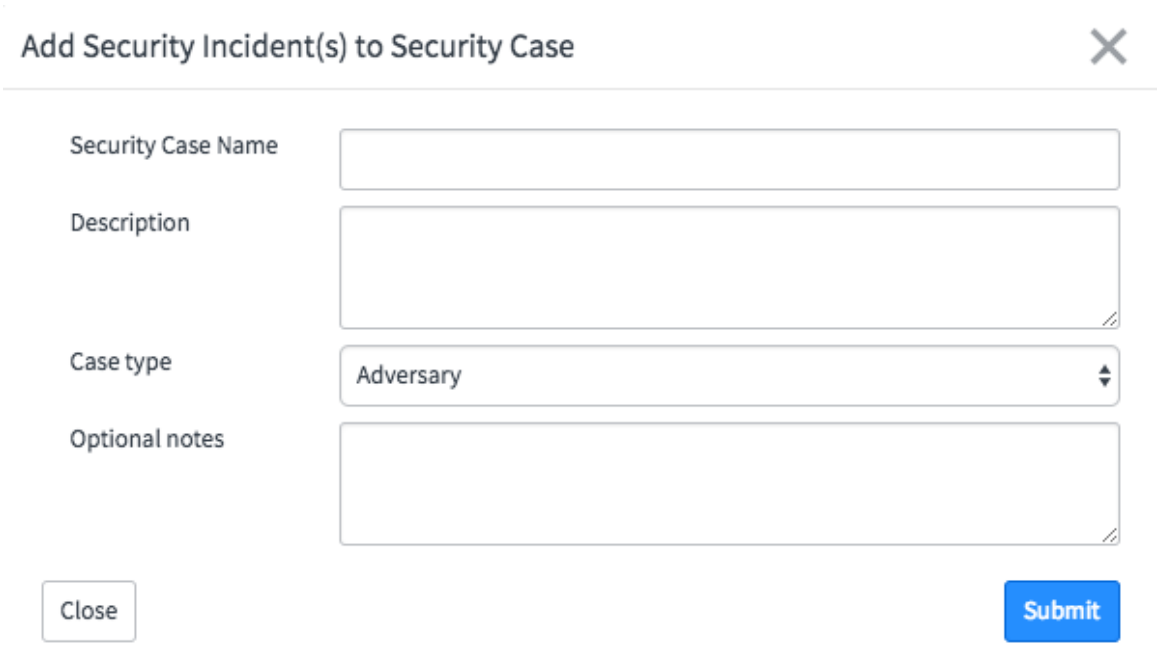
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. If you have a case assigned to you that you want to add this security incident to, fill in the fields as appropriate, then click **Submit**.

Field	Description
Security Case	Select the security case.
Optional notes	As needed, enter additional notes that would be of value to the case analyst.

4. If you have one or more cases assigned to you, but want to create a new case and assign the security incident to it, click **Create new case** to show additional fields.



Note: If you do not have any cases assigned to you, the screen above opens first.

5. Fill in the fields as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Security Case Name	Enter the name of the new security case.
Description	Enter a description for the case.
Case Type	Select the type of case being investigated.
Optional notes	As needed, enter additional notes that would be of value to the case analyst.

6. Click **Submit**.
   A message appears at the top of the security incident, along with a link to the new case.

Related topics

Security Case Management

Create response tasks

After a security incident has been created, you can create response tasks to track separate actions to be performed to respond to the security issue.

Before you begin

Role required: sn_si.basic

Procedure

1. Navigate to the appropriate location to open the security incident for which you want to create tasks.
   For example:
   - To create a response task based on a security incident assigned to you, select **Security Incident** > **Incidents** > **Assigned to Me**.
   - To create a response task based on a security incident assigned to your team, select **Security Incident** > **Incidents** > **Assigned to Team** > **Incidents**.
   - To create a response task based on an unassigned security incident, select **Security Incident** > **Incidents** > **Unassigned Incidents**.
2. Open the security incident for which you want to add response tasks.
3. Click the **Add Response Task** button in the form header.

   Note: To create any other task, click the **Tasks** tab in the incident Related List. For more information on creating other types of tasks, see Create a task.

4. Fill in the fields on the form, as appropriate.

Security incident

Field	Description
Select security tag	If you set up and activated security tags, you can select one or more tags to add metadata to the record or specify the degree of sensitivity of the response task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If you did not set up or activate security tags, this drop-down list is not displayed.
Number	[Read only] The automatically generated Security Incident Response number.
Parent	[Read only] The number of the related security incident.
Configuration Item	The configuration item (resource) affected by the security issue.
Affected User	The person affected by the security issue.
Priority	The priority used to determine when this task is performed.
State	The current state of the security response task. Upon task creation, this field defaults to **Draft**.
Skills	The skill required to perform this task. Click the lock icon and select the skill required. After you have completed your selections, click the lock icon again.
Assignment group	The assignment group from which the assigned worker is selected.
Assigned to	The individual assigned to perform the task.
Short description	A description of the Security Incident Response task.
Description	A description for the selected task.
Secure notes	The work notes that are encrypted and not visible to the customer.
Work notes	The work notes that are not visible to the customer.
Additional comments	Comments that you want to be visible to the customer.

5. When you have completed your entries, click **Submit**.

   Note: After you have created Security Incident Response tasks, you can view them using any of the following applications under the **Response Tasks** module:

   - **Assigned to Me**.
   - **Assigned to Team**.
   - **Show Open Tasks**
   - **Show All Tasks**
   - **Unassigned Tasks**.

Manage Predictive Intelligence for User Reported Phishing

The Predictive Intelligence for User Reported Phishing feature provides a significant solution in triaging and prioritizing user reported phishing emails.

This section describes the following:

- Predictive Intelligence for User Reported Phishing
- Required components and plugins

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Final verdict generation for User Reported Phishing
- Troubleshooting Predictive Intelligence for User Reported Phishing

Predictive Intelligence for User Reported Phishing

This feature assists security analysts in triaging and prioritizing user reported phishing emails.

The Predictive Intelligence framework provides solutions to train the system to predict, recommend, and organize data outcomes. For more details on predictive intelligence, see Predictive Intelligence. Using this framework, you can build models to automatically predict whether a user reported phishing email is suspicious or legitimate.

Using historical User Reported Phishing security incident data (email headers, email body and triage results captured through the security incident close codes), security analysts can train the system to classify the incoming user reported phishing submissions as ones that need to be further triaged (likely suspicious) and ones that are legitimate submissions.

By triaging incoming emails automatically, security analysts can easily prioritize the incident queue and focus on incidents that are likely to represent a risk to the organization first and foremost and spend less effort on emails that are very likely to be false positives. The prediction result also provides a confidence score on the classification to enable granular prioritization.

Required components and plugins

To use Predictive Intelligence for User Reported Phishing, you must install the following applications

Plugin name	Minimum version
Security Incident Response	9.0.1 or 10.0.2
Predictive Intelligence	Orlando version
Predictive Intelligence for User Reported Phishing	10.0.2

Note: The following new enhancements are available with Security Incident Response 10.4:

- The ability to choose close codes from custom fields for model training.
- The ability to explicitly activate predictions after model building.
- The ability to generate a final verdict on the User Reported Phishing submission using a decision table. (requires Security Operations Spoke 10.3.0)

To use the new enhancements, you must upgrade the following applications:

Plugin name	Upgrade to
Security Incident Response	10.0.4
Predictive Intelligence for User Reported Phishing	10.3.1

New and updated tables

- sn_sir_ml_urp_config (New): Contains the configuration for the URP ML application.
- sn_sir_ml_urp_feature (New): Records extracted from the sn_si_phishing email table.
- sn_sir_ml_urp_feature_import (New): Used to upload historical phishing email data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_si_incident (updated): The following new fields were added:
  - Prediction accepted
  - Prediction result
  - Confidence score
- **Script includes**
  - URPMLUtil: Retrieves configuration, run prediction job, and track prediction process.
  - URPMLProcessor: Extracts and processes data from the sn_si_phishing_email table.
  - URPMLAction: Executes flow to accept prediction result.

Final verdict generation for User Reported Phishing

Security Incident Response teams can now drive the finalized verdict for a user reported phishing record based on results from predictive intelligence and threat enrichment integrations.

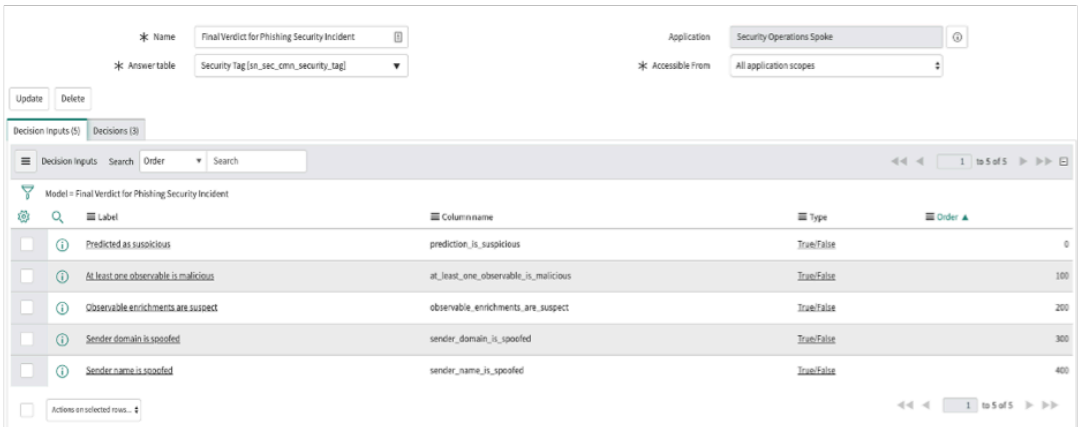
This final verdict generation is enabled through a decision table construct and leveraged within a flow.

Prerequisites

Ensure that all the plugins listed in Required components and plugins have been installed.

Navigate to **Predictive Intelligence for Phishing** > **Final Verdict** > **Final Verdict for Phishing Security Incident**.

The **Decision Inputs** tab shows the different conditions that were evaluated to arrive at the final verdict.



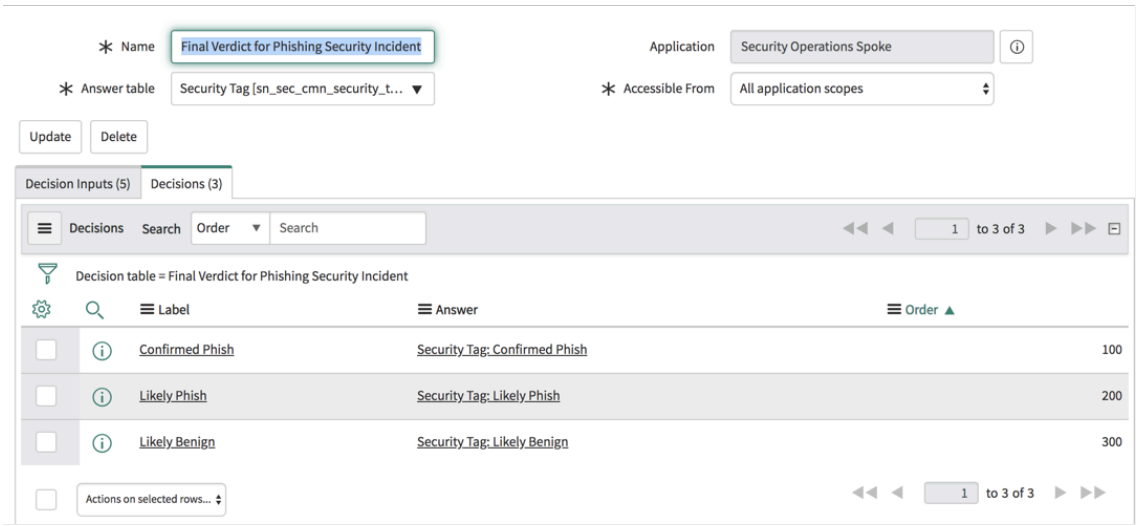
The following conditions are available with the base system:

- Predicted as suspicious: When predictive intelligence has classified the user reported phishing email as **suspicious**.
- At least one observable is malicious: When an observable involved in the security incident (For example, URL, Domain, IP, Hash) has been classified as **malicious** by threat intelligence sources.
- Observable enrichment are suspect: When enrichment on observables (For example, recency of phishing domain registration, country of phishing domain registration) are deemed to be suspect.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Sender domain is spoofed: When the phisher's email domain is suspected of spoofing a trusted domain.
- Sender name is spoofed: When the phisher's email address is suspect of spoofing an trusted employee of an organization.

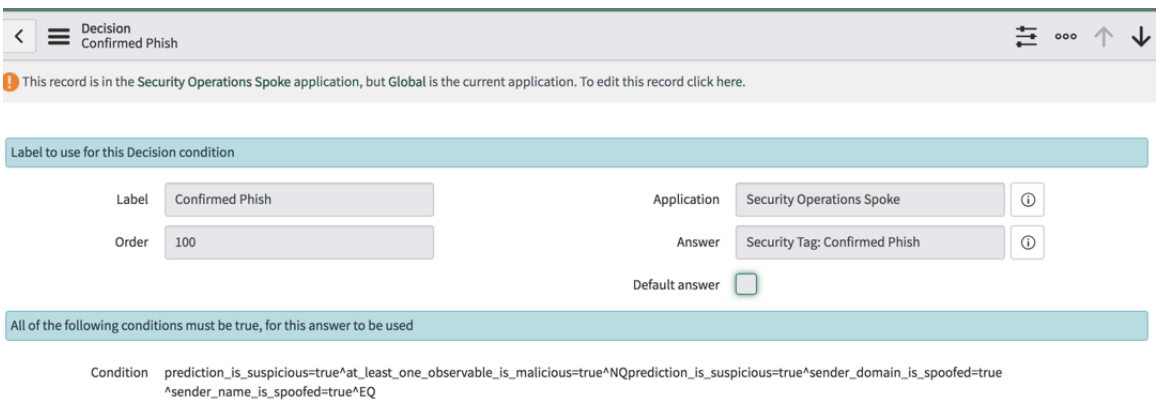
The **Decisions** tab shows the final verdict options that can be arrived at for a given security incident.



The following decisions are available with the base system:

- Confirmed Phish: When the conditions have led to the final verdict as being a confirmed phishing email.
- Likely Phish: When the conditions have led to the final verdict as a potential phishing attempt.
- Likely Benign: When the conditions have led to the final verdict as a benign submission.

You can see the conditions that were evaluated for each of the final verdict options. Click on the Label link to see the conditions.



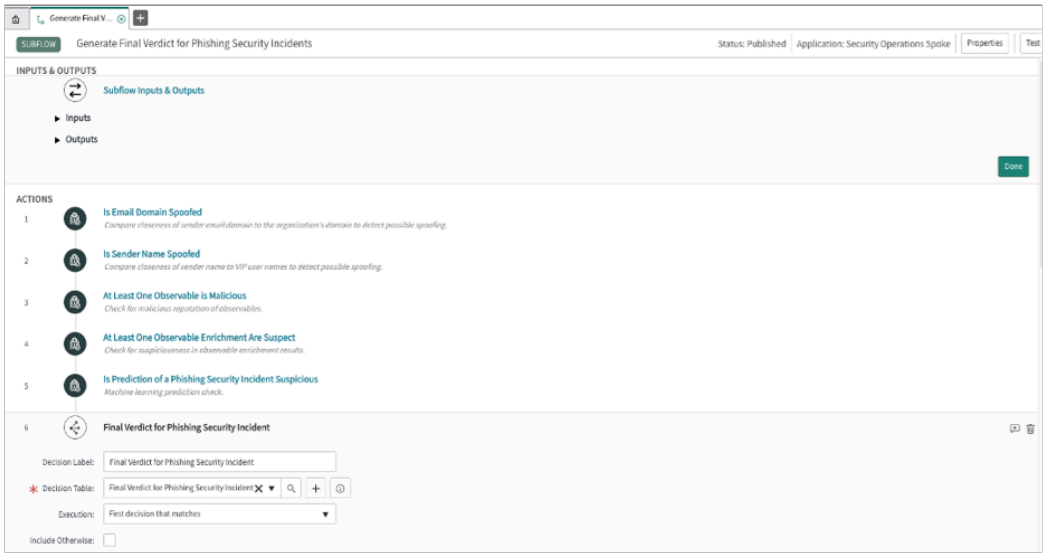
You can customize the decision table provided with the base system or create your own decision table. This decision table can be leveraged in security incident response playbooks. The **Generate Final Verdict for Phishing Security Incidents** subflow is available with the base system. This subflow automatically generates the final verdict for a phishing security incident and applies a security tag based on that decision. You can include this subflow as part of the **Automated Phishing** playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The inputs for this subflow are:

- incident_id: The sys ID of the phishing security incident.
- c_level_names: Comma separated list of names (For example, names of executives in the organization) likely being spoofed in the phishing attack.
- trusted_domains: Comma separated list of trusted email domains.
- enrichment_keywords: Comma separated list of keywords that indicate the maliciousness of the observable from enrichment results.
- sender_email (optional): The email address of the sender of the phishing email.

The output of this flow can be **Confirmed Phish**, **Likely Phish**, or **Likely Benign**.



Troubleshooting Predictive Intelligence for User Reported Phishing

This section covers a few common problem scenarios.

- Problem: I cannot modify the Predictive Intelligence configuration.

  Solution: Check if you have permissions to do so. You must login as a user with the ml_admin role to modify thresholds. Some scenarios may require even higher privileges, like, for example, you need to modify the training data limit. For such scenarios, you must contact Customer Support for assistance.

- Problem: The model training failed.

  Solution: Check if the URLs of the ML scheduler have been setup. Navigate to **System Properties** > **All Properties** and check if the *`glide.shared_service_scheduler.url`* property has been configured.

- Problem: Prediction results are not available on a security incident.

  Solution:

  - Check if the predictor URL has been set up in the *`glide.prediction_service.url`* system property and make sure the data center matches with the URL.
  - Check if the Predict User Reported Phishing Email scheduled job is active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure Predictive Intelligence for User Reported Phishing

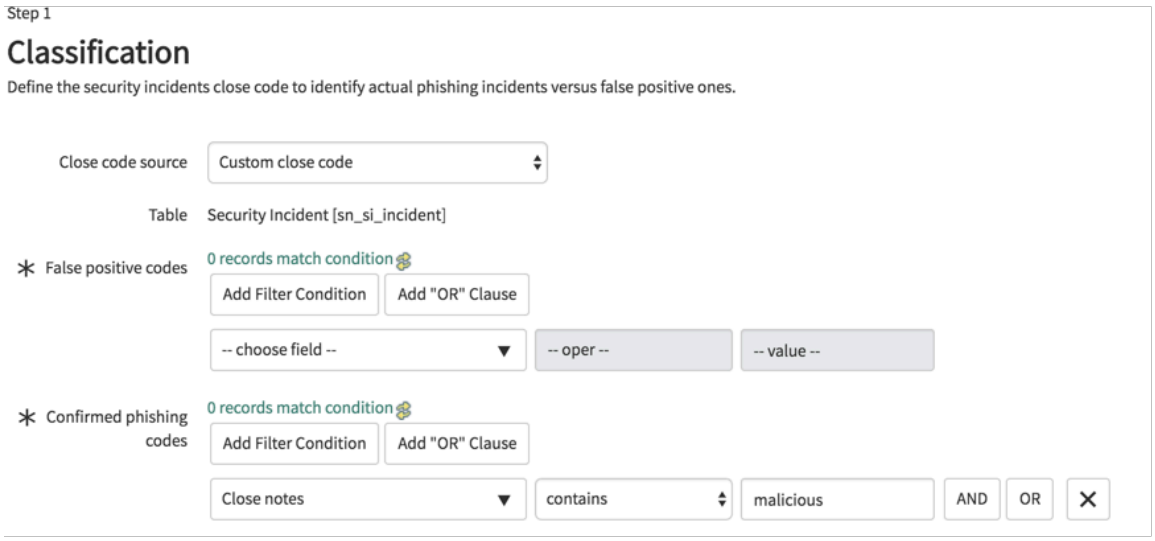
Configure and prepare the model to identify user reported phishing emails.

Before you begin

Role required: ml_admin

Procedure

1. Navigate to **All** > **Predictive Intelligence for Phishing** > **Configuration**.
2. In Step 1 of the configuration, select one of the following options from the Close code source list:
   - Default close code: Select this option to specify the default security incident close codes that must be used by the training model to identify malicious emails and legitimate ones. Click the lock icon and select one or more False positive codes or Confirmed phishing codes.
   - Custom close code: Select the Custom close code option if you want to define close codes from custom fields that may be used as part of your existing incident response procedures. To define a close code, select a field from the security incident table and specify one or more filter conditions.



3. In Step 2, import historical data that can be used to train the model.
   Select the Data Source for importing the historical data. This can be:
   - User reported phishing email table: You can see the number of records that can be imported as historical data. Select this option and click **Import**.
   - Custom data source: You can attach a single formatted CSV file that contains historical data records. Select the file and click **Import**.

   Note: The CSV file that you import must contain the following headers:
   - Label
   - Header
   - Body text

   Each record must contain a Malicious or Legitimate tag in the Label column in the CSV file.

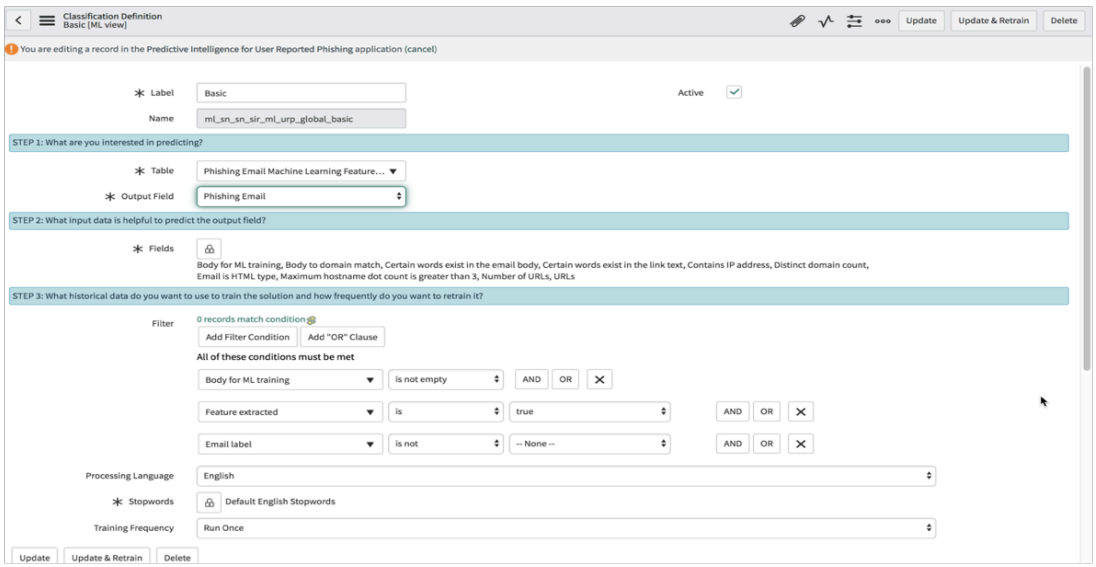
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Click **Cancel Import** to stop importing the data. The import process is canceled and all records that have been imported so far are deleted.

4. After you have imported the historical data, click the link to refresh the page.
   You can then either import more training data or continue with the next step.
5. In Step 3, verify if the number of records available for training meet the minimum threshold requirements.

   Note: The default values for maximum and minimum number of training records are displayed. These thresholds can be modified in the Platform Machine Learning Properties page. Contact Customer Support for assistance.

6. If the training data is sufficient, click **Train model**.
   You can update the inputs for training in the screen below.



7. Prediction inputs that you can modify include:
   - What are you interested in predicting?
   - What input data is helpful to predict the output field?
   - What historical data do you want to use to train the solution and how frequently do you want to retrain it?

   The default values for these inputs are displayed. You can modify them and click either of the following:

   - **Update**: Updates the training model definition.
   - **Update & Retrain**: Updates the training model definition and retrains the model (Triggers the **Train Model** function).
8. Finally, when you have completed training the model, click the **Activate Prediction** check box. Predictions are now provided on every user reported phishing record using that model. If you would like to stop providing predictions on the user reported phishing records, clear the **Activate Prediction** check box and click **Deactivate**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assigning security analysts

Depending on your settings in the SIR Administration Configuration screen, you can assign security analysts to security incidents manually; automatically by using a workflow; or automatically by using auto-assignment.

Manual analyst assignment

You can configure the Security Incident Response Administration Configuration screen to require that security analysts be assigned manually whenever someone or the SIR application creates a security incident or generates a security response task.

If a security incident or response task cannot be auto-assigned, you can set the SIR Administration Configuration screen to require the manual assignment of security analysts. This is a good choice if you have a limited number of security analysts for completing requests or if you simply do not want to auto-assign them.

Workflow-based security analyst assignment

You can configure the Security Incident Response Administration Configuration screen to use a selected workflow to assign the security analyst whenever someone or the SIR application creates a security incident or security response task.

In the Security Incident Administration configuration screen, you can choose to use a workflow to assign an analyst to each security incident or security response task. This option is a good choice for organizations that use a custom process for resolving security issues or otherwise have a process that can be automated.

Automatic security analyst assignment

You can configure the Security Incident Response Administration Configuration screen to auto-assign the security analyst whenever someone or the SIR application creates a security incident or security response task. Auto-assignment allows you to define, based on the needs of your organization, the criteria by which analysts are assigned automatically to security incidents.

Agent auto-assignment based on agent ratings

If auto-assignment is enabled and a security incident or a response task is created, the following actions occur:

- The available security analysts are evaluated based on the criteria defined in the configuration.
- An appropriate security analyst is automatically assigned to the task.
- The task is moved to the **Assigned** state.

If the configuration is set up to consider more than one set of conditions, such as skills, location, time zone, or group coverage area, the security analysts are evaluated based on the weighting property settings and other criteria. These configuration settings help you auto-assign agents based on optional properties. The calculated ratings are used to determine the best agent for the security incident or response task. Any combination of rating-based methods can be enabled in the application configuration screen.

When a task is created, a rating for each type of enabled selection criteria is calculated for each available agent. The agent whose total rating is highest is considered for auto-assignment.

The settings for the auto-assignment weighting properties, found in **Security Incident** > **Administration** > **Properties**, are included in the rating calculations.

These values help you prioritize which auto-assignment selection criterion is more important to your organization. Set the priority values between 1 (less important) and 10 (important).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For an example of how the weighting properties affect agent ratings, see Agent auto-assignment using multiple selection criteria.

On-call scheduling

The On-Call Scheduling application helps you to ensure that dedicated support team members are available to resolve issues as they arise. You can set up on-call schedules, roster rotations, and escalation policies, escalate notifications for a group, and determine the current contact for an escalation. The application identifies the assigned and available member of a support group, for example, when assigning an incident. See On-Call Scheduling for more information. On-call scheduling for Security Incident Response works the same way.

Agent auto assignment using location

Agents can be auto-assigned based on the home location in their user record and the location of the tasks.

Auto-assignment by location is performed when the **Auto-selection of agents will consider location of agents configuration** option is enabled.

When a task (security incident or response task) is created, the agent closest to the task location is considered for the task. If the application is configured so that only location is considered, the closest agent is auto-assigned the task.

When a task is created, agent locations are compared to the following ranges to determine each agent location rating.

Location rating calculation

Distance (mi.) from agent to task	Rating
0 to 0.1	1
0.11 to 0.5	0.9
0.51 to 5	0.7
5.1 to 10	0.5
10.1 to 20	0.4
20.1 to 30	0.3
30.1 to 40	0.2
40.1 to 100	0.1
>100	0

If the application is configured to use other selection criteria, such as skills, time zone, or schedule, the ratings of all selection criteria are weighted and summed up. The agent with the highest overall rating is auto-assigned for the task. See Agent auto-assignment using multiple selection criteria for details.

Agent auto-assignment using skills

Agents can be auto-assigned based on their skills and the skills required to perform the task. Assign skills to their user records using **Skills** > **Users**.

Auto-assignment by skills can be performed when the **Auto-selection of agents for tasks requires them to have skills** configuration option is set to **all** or **some**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When a task that includes skills is auto-assigned, an agent's skills are compared with the skills required to perform the task. A rating is calculated based on the skills configuration option. If the option is set to **some**, the agent with the closest skills match is auto-assigned the task. If the option is set to **all**, only agents who possess all the required skills are considered. If no agents possess all the skills required to perform the task, no one is auto-assigned.

A skills rating is calculated as:

Skills_agent/Skills_task

Where:

- Skills_agent is the number of skills possessed by the agent that match the skills required for the task.
- Skills_task is the total number of skills required for the task.

For example, if a task requires four skills, and Agent A possesses three of them and Agent B possesses two of them:

- Agent A skill rating = 3/4 or 0.75
- Agent B skill rating = 2/4 or 0.5

If the application is configured to use other selection criteria, such as location or time zone, the ratings of all selection criteria are weighted and summed up. The agent with the highest overall rating is selected for the task. See Agent auto-assignment using multiple selection criteria for details.

Agent auto-assignment using time zones

Agents can be auto-assigned based on the time zone defined in their user records and the time zone of the tasks.

If the **Auto-selection of agents will consider time zone for the task** configuration option is enabled, auto-assignment by time zone can be performed.

When a task is created, agents in the time zone closest to the task time zone are considered for the task. If the application is configured so that only time zone is considered, only an agent in the same time zone can be auto-assigned the task.

Note: It is important that the time zones for the agent and the task set correctly.

When a task is created, agents are rated based on the time zone of the task and the time zone of the agent using the following formula:

1 - [abs(Task_tz – Agent_tz) ÷ 12]

where:

- abs is the mathematical function to compute the absolute value.
- Task_tz is the offset between the time zone of the task and GMT.
- Agent_tz is the offset between the time zone of the agent and GMT.

For example, a task is created in New York City (GMT-4), and two agents are available to perform the task, one in Los Angeles (GMT-7) and one in Paris, France (GMT+1).

The rating of the agent in Los Angeles is calculated as:

1 - abs((-4) - (-7)) ÷ 12 or 0.75

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The rating of the agent in Paris is calculated as:

1 - abs((-4) - (+1)) ÷ 12 or 0.58

So if the auto-assignment of the task is based on the time zone alone, it's assigned to the agent from Los Angeles.

If the application is configured to use other selection criteria, such as skills or location, the ratings of all selection criteria are weighted and summed. The agent with the highest overall rating is selected for the task. See Agent auto-assignment using multiple selection criteria for the details.

Agent auto-assignment using group coverage areas

Agents can be auto-assigned based on the group coverage area defined in their user records.

Agent auto-assignment using multiple selection criteria

When a task is created, the agents ratings are calculated. For more information, see:

- Agent auto assignment using location
- Agent auto-assignment using skills
- Agent auto-assignment using time zones

Auto-assignment is based on the following calculation:

(Criteria_1 rating x Criteria_1 weight) + (Criteria_2 rating x Criteria_2 weight) + (Criteria_3 rating x Criteria_3 weight) / Number of criteria types used where:

Number of criteria types used = 1, 2, or 3 depending on the location, skill, and time zone settings used.

This example calculates agent auto-assignment based on location and skills. The example is based on the following assumptions.

- The **Auto-selection of agents will consider location of agents** configuration option is enabled for the application.
- The **Auto-selection of agents requires them to have some of the required skills for the task** configuration option is enabled for the application.
- The **Skills Weight** property is set to 10 for the application.
- The **Location Weight** property is set to 5 for the application.
- Agents A and B are available to perform a task, and the task requires four specific skills.
- Agent A location is 5 miles from the site of the task and possesses three of the four required skills.
- Agent B' location is one-quarter mile from the site, and possesses two of the required skills.

Auto-assignment for the agents uses this calculation: `[(Location rating x Location weight) + (Skills rating x Skills weight)]/ 2`

- The auto-assignment calculation for Agent A is: `[(0.7 x 0.5) + (0.75 x 1)]/ 2 = 0.55`
- The auto-assignment calculation for Agent B is: `[(0.9 x 0.5) + (0.5 x 1)]/ 2 = 0.475`

In this example, Agent A is auto-assigned the task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Agent assignment using Advanced Work Assignment (AWA)

You can configure Advanced Work Assignment to automatically assigns security incidents to your security analysts, based on their availability, capacity, and optionally, skills. AWA pushes work to qualified security analysts using work item queues, routing conditions, and assignment criteria that you define.

Process Mining Workspace for Security Incident Response

Process Mining scan through security incident audit logs and identify factors contributing to inefficiencies such as multiple reassignments, prolonged hold times, and periods of inactivity for security incidents. Organizations can use this information to address the inefficiencies.

With process mining, you can identify the following opportunities of improvements for your security incidents.

Opportunities with process mining

Opportunity	Description
Incidents with at least two assignment group changes	Incidents for which the assignment group changed for two or more times.
SIRT (Max repetitions is 2)	
Incidents took over 5 hours to escalate to high priority	Incidents for which the priority was escalated to a higher priority after five hours.
Incidents took more than 5 hours to analyze	Incidents that were in analysis state for more than five hours.
Incidents analyzed within 30 minutes	Incidents that were in analysis state for less than 30 minutes.
Review (Max repetitions is 2)	Incidents that were move to review state for two times.
Eradicate (Max repetitions is 2)	Incidents that were move to eradicate state for two times.

The Process Mining Content Pack for Security Incident Response adds a prebuilt project that includes a predefined process model definition for security incidents. To create a project, see Create process mining project for security incidents.

Note: To use the Process Mining in Security Incident Response, download and install the content pack. For more information, see Content pack for Security Incident Response.

Create process mining project for security incidents

Create a project in Process Mining Workspace using the pre-build process models definitions from the content pack to scan through audit logs of security incident records and identify inefficiencies in your security incident life cycle.

Before you begin

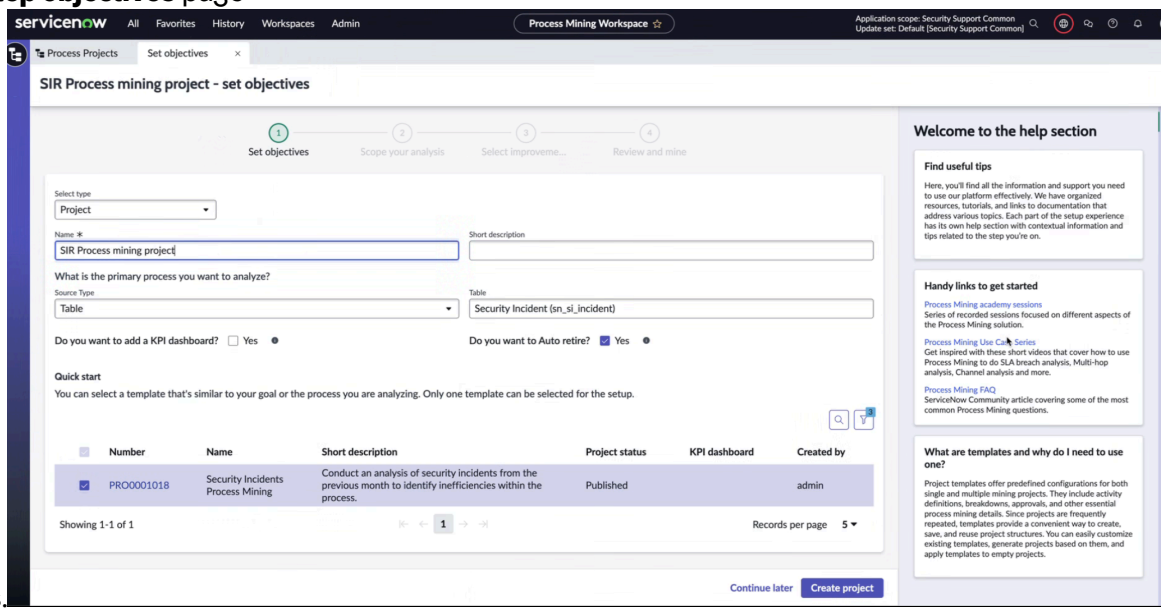
Role required: sn_process_optimization_analyst and sn_si_read

Procedure

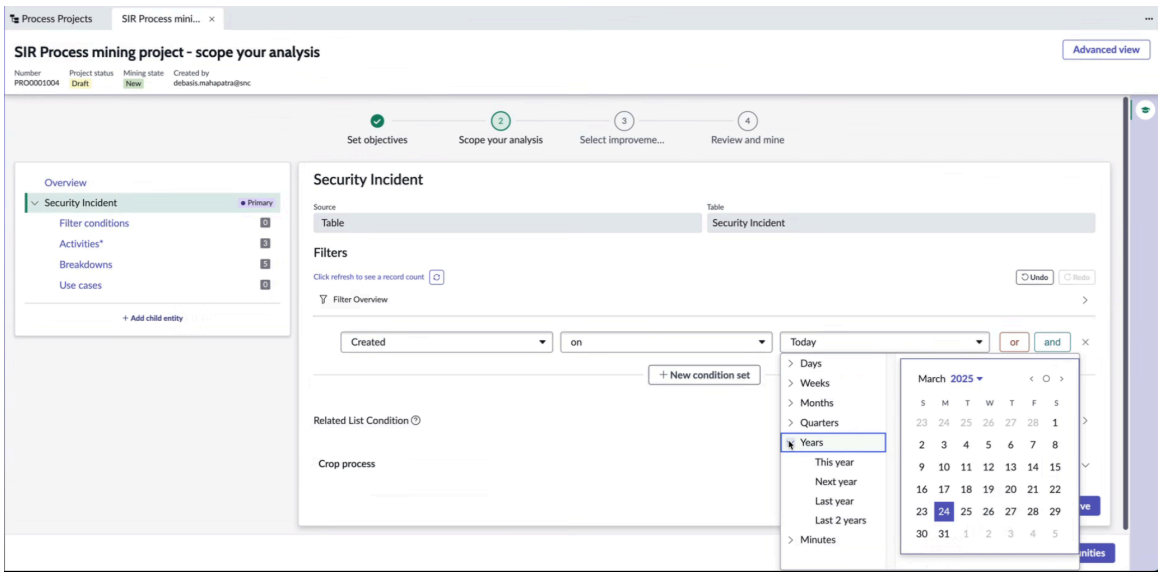
1. Navigate to **All** > **Workspaces** > **Process Mining Workspace**.
2. Select **Create New Project**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Step objectives** page opens.



3. Enter a process mining project name in **Name**.
4. **Optional:** Add a short description about your project in **Short Description**.
5. Select **Source Type** as Table.
6. Select the `Security Incident (sn_si_incident)` in **Table**.
7. Select the default template, and then select **Create project**.
   The project dashboard appears with all the configured settings.
8. Select the edit ( ) icon corresponding to **Scope of the analysis** and configure the filters to set the number of records to mine.



9. Select **Select improvement opportunities** and configure the improvements for your security incidents.
   A list of improvement opportunities displays. For information about configuring improvement opportunities, see Working with improvement opportunities.
10. Select **Review and mine** and then select **Mine project**.
11. Select **Sample mine** or **Full mine**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

12. Select **Confirm & Mine** to start the mining.
    The mining starts and the status of mining is displayed.

Process Mining use cases for security incidents

The following Process Mining use cases provide various analysis methods that you can use to identify inefficiencies during the resolution of your security incidents.

Multi-hop analysis

Security incidents that are reassigned multiple times to different teams might result in a resolution delay. By analyzing the reasons of reassignments for such security incidents, and where the incidents are held up for longer durations, you can improve the overall efficiency.

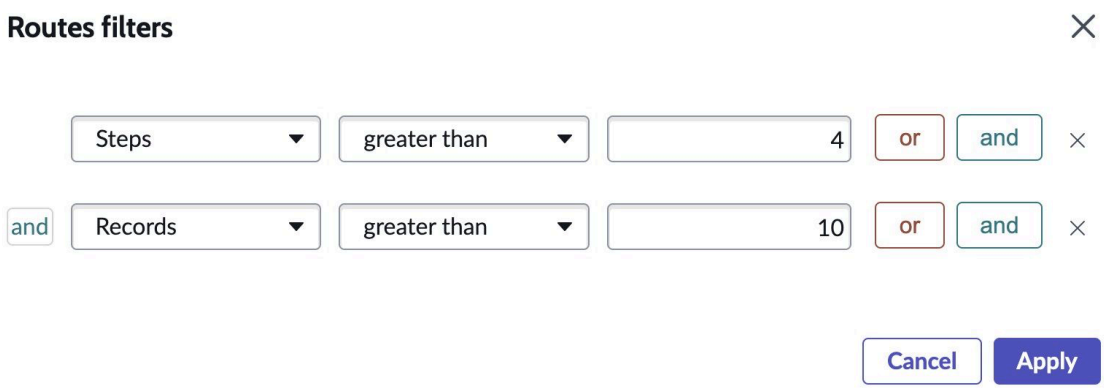
The following are example steps to get the list of security incidents that took the longer routes:

1. Navigate to **Workspaces** > **Process Mining Workspace**.
2. Select **Assignment group**.
3. Open a project, and navigate to **Analyst Workbench**.

   When you open a mined process optimization project, by default the Analyst Workbench opens.

4. Select **Variation Analysis**.
5. Select the filter ( ) icon, and set the filter similar to the following:
   - Steps greater than the average number of steps.
   - Records greater than the minimum number of records that have taken a longer route.

   Note: You can configure the values as per your requirement.



6. Select **Apply**.

   All the records that match the filter criteria appear. Select a record to view the closure route of the record.

7. Select a record, and then select **Show Route**.

   The route traversed by the record appears. You can use this route to identify the step where the incidents were held up for a longer duration than expected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SLA breach analysis

You can use process mining to analyze security incidents that have breached a certain SLA (Service Level Agreement.)

The following are example steps to get the list of security incidents that breached the SLA:

1. Navigate to **Workspaces** > **Process Mining Workspace**.
2. Open a project, and navigate to **Analyst Workbench**.

   When you open a mined process optimization project, by default the Analyst Workbench opens.

3. From the Advanced filters, select **Conditions**.
4. Select the arrow corresponding to **Related List Condition**.
5. Set the conditions similar to the following:
   - Use the **Select** list to select the `Task SLA` table.
   - Set the value of the **Greater than or equal to** field to `1`.
   - Set the value of **Has breached** to **True**.
   - To identify security incidents which breached a specific SLA, set a **SLA definition** filter.



6. Select **Apply**.

   All the records that match the conditions appear. Select a record to view the route of the record for analysis.

Priority analysis

You can use the process mining to review and improve the existing priority assignment process to your security incidents.

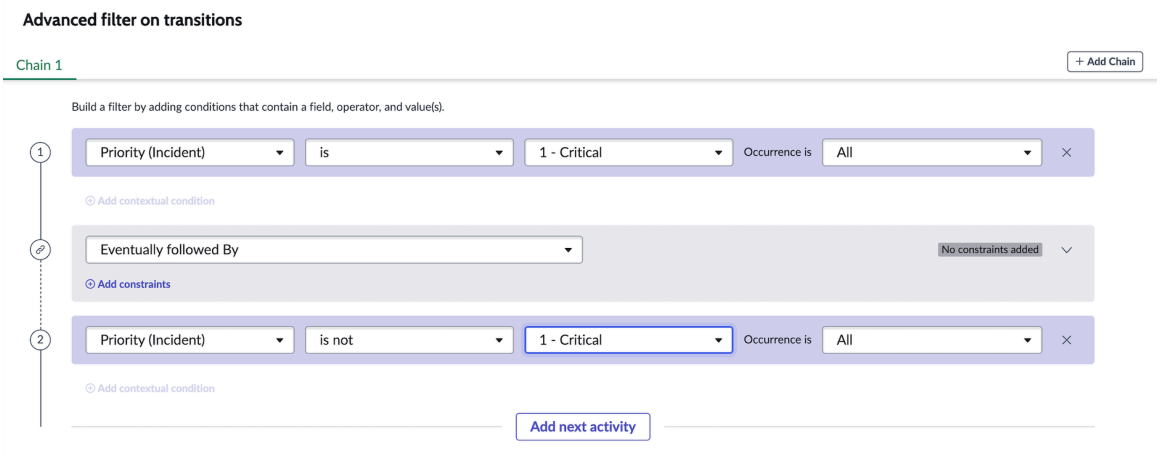
The following are example steps to get the list of security incidents for which are priority was modified:

1. Navigate to **Workspaces** > **Process Mining Workspace**.
2. Open a project, and navigate to **Analyst Workbench**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you open a mined process optimization project, by default the Analyst Workbench opens.

3. Select **Priority**.
4. From the Advanced filters, select **Transitions**.
5. In **Advanced filter on transitions**, configure the following:
   a. Set Priority is 1 - Critical.
   b. Select **Eventually followed By**
   c. Priority is not 1 - Critical.



6. Select **Apply all chains**.

The map shows all the security incidents that were assigned a priority 1 and their priority was later lowered.

Bottleneck analysis

You can use the process mining to review the state transitions of your security incidents. This analysis identifies the transitions that are not usual and the time delay caused because of such.

The following are example steps to perform the bottleneck analysis:

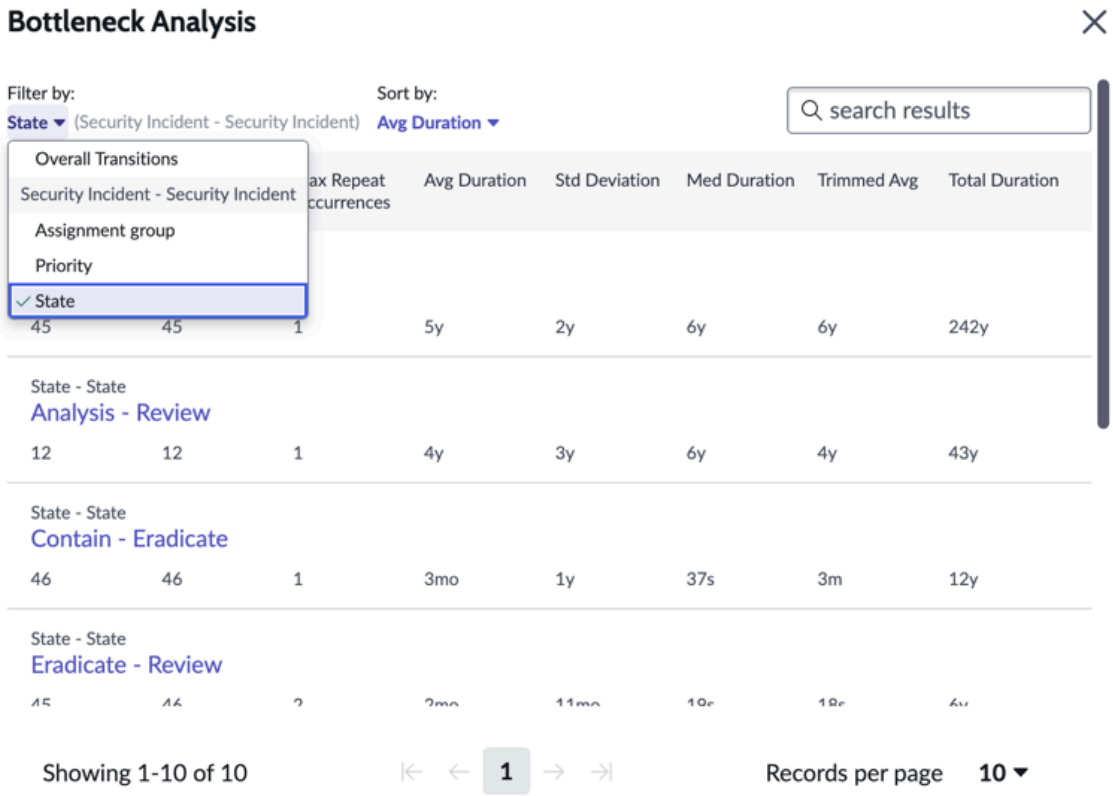
1. Navigate to **Workspaces** > **Process Mining Workspace**.
2. Open a project, and navigate to **Analyst Workbench**.

When you open a mined process optimization project, by default the Analyst Workbench opens.

3. Select **Bottleneck Analysis** from the **Model Options**.

The screen displays the state transitions for the security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Select the **Filter by** to identify bottleneck transitions. Alternatively, use the search bar to search for bottleneck transitions. For example, to identify incidents which were moved to other states from the Closed state, use "Closed " or "Closed -".

Long time to start than resolve

You can use the process mining to review the incidents that take a long time to get to the Draft state, but then were closed in a relatively shorter time.

The following are example steps to identify security incidents that were in the Draft state for more than two days and were closed within 30 minutes after moving to the Analysis state:

1. Navigate to **Workspaces** > **Process Mining Workspace**.
2. Open a project, and navigate to **Analyst Workbench**.

   When you open a mined process optimization project, by default the Analyst Workbench opens.

3. From the Advanced filters, select **Transitions**.
4. In **Advanced filter on transitions**, configure the following:
   a. Set `State (Incident)` is `Draft`.
   b. Select **Eventually followed By**
   c. Select **Add constraints** and set **From** as 2 days.
   d. Select **Add next activity**.
   e. Set `State (Incident)` is In `Analysis`.
   f. Select **Eventually followed By**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

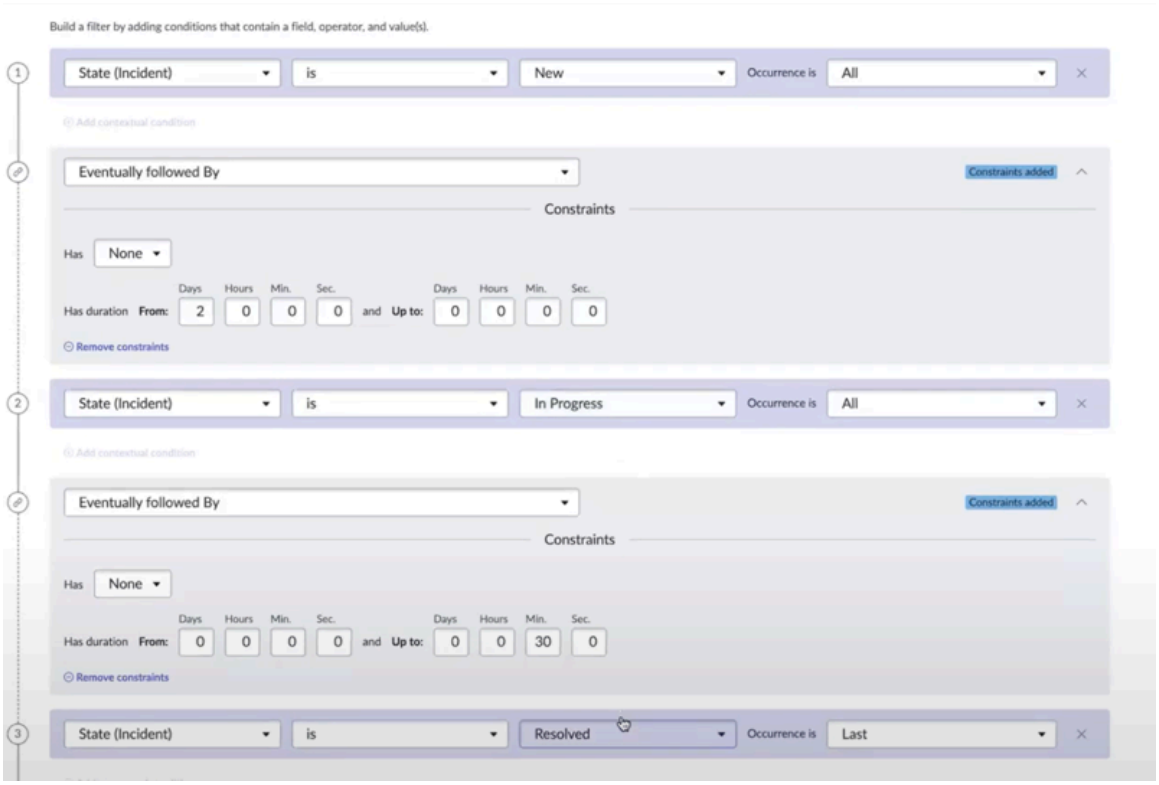
g. Select **Add constraints** and set **Up to** as 30 minutes.

h. Select **Add next activity**.

i. Select **Eventually followed By**

j. Select **Add constraints** and set **Up to** as 30 minutes.

k. Set `State (Incident)` is `Closed`.



5. Select **Apply all chains**.

6. Select **Breakdown Filters** and sort by **Longest Avg Duration**.

Managing security incidents and inbound requests

After a security incident has been created, there are numerous types of information that can be added and viewed as your analysis of the issue progresses toward resolution.

> **Important:** The latest features in Security Incident Response are exclusively available in the Security Incident Response Workspace. Please install or upgrade to the latest Security Incident Response or Security Incident Response Workspace version to access and leverage features such as Shift-Handover, Risk Score Calculator, etc.

This section describes the following:

- Create an inbound request
- Manage observables
- Manage lookups and scans
- Manage on-demand orchestration
- Calculate the severity of a security incident
- Manage post incident activities
- Close security incidents

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create an inbound request

Unlike security incidents, inbound requests are generally of a lower priority. Requests for a lookup, scan, or a new badge are examples of inbound requests.

Before you begin

Roles required: sn_si.basic role or higher

Procedure

1. Navigate to one of the Requests forms.
   For example, **All** > **Security Incident** > **Inbound Requests** > **Assigned to Me**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Security request

Field	Description
Number	[Read only] The automatically generated security request number.
Company	The requester company.
Location	The CI location, if applicable. This field is pre-filled when the CI is selected.
Configuration Item	The configuration item affected by the request.
Priority	The priority of the request.
Opened	[Read only] The date and time that the request was opened.
State	The current state of the security request. Upon security request creation, this field defaults to **Draft**.
Assignment group	The assignment group from which the assigned worker is selected.
Assigned to	The individual assigned to perform the work.
Short description	A brief description of the security request, which is visible to the requester.
Description	The full description of the request, which is visible to the requester.
Work notes	Work notes, which are visible to the requester.

4. When you have completed your entries, click **Submit**.
5. If you must escalate the request to a security incident, click **Convert to Security Incident**.

Manage observables

Observables are artifacts found on a network or operating system that are likely to indicate an intrusion. Typical observables are IP addresses, MD5 hashes of malware files or URLs, or domain names. Threat Intelligence observable table data is available from within a security incident.

Observables information includes value, type, context, and timestamp.

You can create or delete observables manually or automatically through lookup requests.

A new **Finding** column has been added to the **Threat Lookup Results** tab. Possible values are: Malicious and Unknown.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If an IoC lookup request does not find a security incident observable, it is labeled Unknown.

If an IoC lookup request does find a security incident observable, it is labeled Malicious.

During an upgrade, existing items have the **Finding** column set to Malicious.

Note: While Threat Intelligence observables table data is part of a security incident, no other interaction with the Threat Intelligence module is included. For full threat functionality, the Threat Intelligence plugin is available by subscription.

Related topics

Create a security incident observable

Show IoC information for a security incident

You can view IoC information, such as observables and sightings search results associated with a security incident.

Before you begin
Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident for which you want to view IoC-related information.
2. Click the **Show IoC** related link.
3. Click any of the related lists to view or add information for the security incident.

Tab	Description
Observables	View or manually add or edit observables associated with the security incident. For more information, see Manage observables.
Associated Indicators	If Threat Intelligence is activated, you can view any other indicators associated with any of the same threat records.
Sightings Search Results	Contains Sightings Search results.
Sightings Search Details	Contains Sightings Search record details.
Threat Lookups	Stores enrichment data from malware detection systems. This tab only appears when the Threat Intelligence plugin is installed.
Associated Attack Modes/Methods	If Threat Intelligence is activated, you can view any other attack types associated with any of the same threat records.
Security Scan Requests	If Threat Intelligence is activated, you can view scan and lookup requests attached to the security incident.
Resources with Similar IoC	If Threat Intelligence is activated, you can view any other resources with similar indicators.
Users with Similar IoC	If Threat Intelligence is activated, you can view any other users with similar indicators.

4. Click any of the following related links to further update the security incident:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Show Affected Items
- Show Related Items
- Show Enrichment Data
- Show Response Tasks

5. When you have completed your entries, click **Submit**.

Create a security incident observable

You can create and view an observable within a security incident and take appropriate action. Having observables available in the security incident is scalable and reduces response time.

Before you begin

Role required:

- sn_ti_observable.write (write)
- sn_ti_observable.read (read)
- sn_ti_observable.admin (delete)

Procedure

1. Navigate to **Security Incident**.
2. Choose an incident.
3. Click **Security Incident Observables** related list tab.
4. Click **New**.
5. Fill in the fields on the form, as appropriate.

Field	Description
Select classification tag	If you set up and activated security tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the observable. If you did not set up or activate security tags, this drop-down list is not displayed.
Value	The value (for example, IP address or hash) associated with the observable. **Note:** If a threat scan on an IP address or hash, returned malware or some other failure, the IP address or hash value is automatically added to the Observable [sn_ti_observable] table. As such, it can be searched for from the Observables form.
Observable type	Select the observable classification, such as an IP address or file hash. These observable types are defined in the **Observable Types** module.
Incident count	The number of times the observable value has been encountered.
Is composition	This field displays only after the observable record has been saved. If the **Observable Type** is set to anything other that **Observable Composition**, and this new observable is a composition, select this check box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If the **Observable Type** is already set to **Observable Composition**, the check box is selected and read-only. An observable composition is an observable that contains child observables.
Finding	Select one of the following: ○ **Malicious**: Indicates that the observable is harmful to the organization. ○ **Suspicious**: Indicates that the observable might be harmful to the organization. ○ **Clean**: Indicates that the observable is not harmful to the organization. ○ **Unknown**: Indicates that we are yet to determine the observable's finding. ○ Default value: Unknown. For more information, see Threat Lookup Finding Calculators. **Note:** After an upgrade, existing observables are marked Malicious.
Operator	This field appears only when the **Is composition** check box is selected. Depending on your setting in this field, the observables and their children are considered when deciding whether an associated indicator is present. Set this field to **AND** if all the child observables must be present for an associated indicator to be considered present. Set it to **OR** if any of the child observables are present for an associated indicator to be considered present.
Must not be present	This field displays only after the observable record has been saved. If selected, this field signifies that the absence of the observable is the potential issue (for example, a missing registry key).
Location	Using the settings in two properties and a script include definition, you can load Load more IoC data in this field.
Notes	Enter any additional notes about the observable.

6. Right-click in the form header and click **Save**.
You can now click any of the following related lists to view additional information.

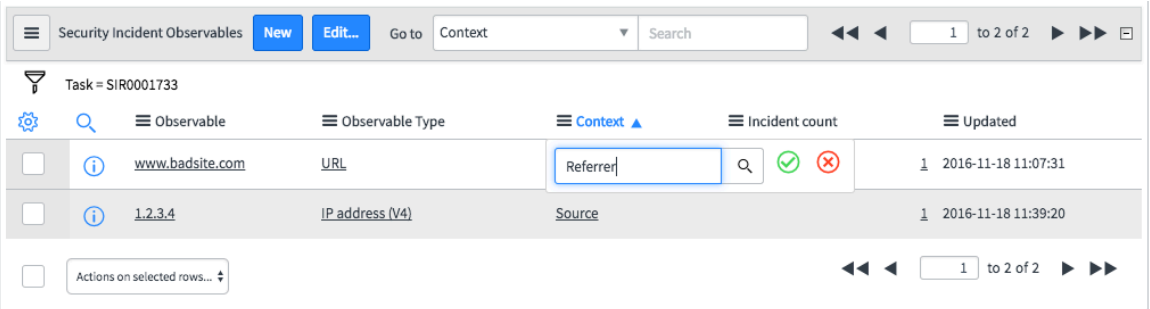
Related List	Description
Related Indicators	Lists indicators that have been identified by the threat source.
Associated Tasks	Lists changes associated with the observable.
Child Observables	Lists related observables that have been identified by the threat source.
Matching Resources for IP	If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related List	Description
Observable Sources	Lists the sources of this observable, along with the confidence level of the source.
Security Annotations	Lists security annotations added to this observable.

7. Returning to the security incident the following information is available.

Note: When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The **Related Configuration Items** and **Related Users** related list tabs are updated accordingly.



Column	Definition
Observable	The value (for example, IP address or hash) associated with the observable.
Observable Type	The specific type of observable.
Context	Selected by the user. Choices are: ○ IP - Source or Destination **Note:** If Threat Intelligence and Palo Alto Networks - Firewall are activated, changing or adding a value to this field causes the Get Log Data Flow Security Operations Palo Alto Networks - Get Log Data workflow to execute. The workflow retrieves enriched threat log data from the firewall and attaches it to the security incident. The information is also parsed and displayed in the Firewall Logs section under the **Enrichment Data** tab. ○ URL - Referrer **Note:** When the user clicks a link in a phishing email, a referrer is the URL of the final jump before the malware URL is accessed.
Incident Count	The number of incidents that this observable appears in. This value is automatically updated when the observable is added to another incident manually or through a workflow.
Updated	Data and time the list was last updated.

Note: If the Threat Intelligence plugin is installed, you can also view the observable in the **Observables** list in the **IoC Repository**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Edit a security incident observable list

Add multiple security incident observables

Manage file observables

Manage file observables provides stringent security measures to store the suspicious files and enables the files type observables for sandbox integration.

Before you begin

Role required: sn_ti_malicious_attachment_access (upload)

Upload the file type observables:

- Automatically: When the security incidents are created for the phishing emails, the attachments in the phishing email are created as file type observables.
- Manually: A security analyst can also upload the suspicious files to create file type observables.

About this task

You can create and view file type observables for a security incident. The suspicious files which are part of the observables are stored in a specific location, which can be accessed by the security analyst to download the file only with a specific role.

Procedure

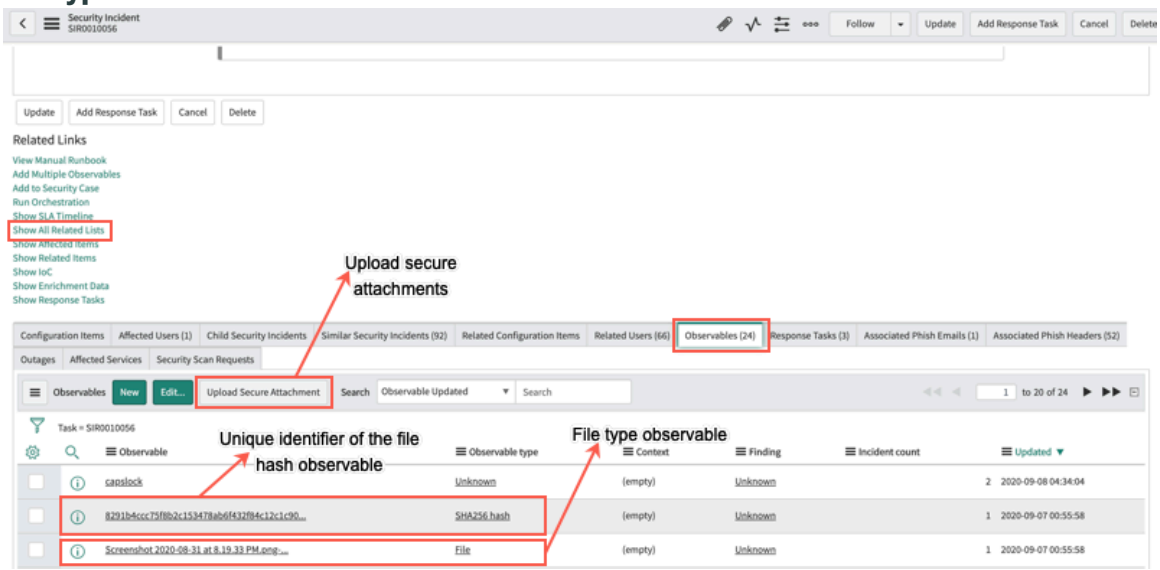
1. Navigate to a security incident.
2. Select **Observables** from the **Show All Related Lists** tab.

   If there are any attachments in the phishing email, then by default those attachments are created as file type observables in the corresponding security incident. Each attachment is created as two observables such as file type and file hash observable.

3. To upload the secure attachments manually:
   - Click **Upload Secure Attachment**.
   - On the Upload Secure Attachments, Click **Choose file** to upload one or more files. Each file is considered as a single observable record.
   - Click **Create File Observables** to create the file type observables such as one is the file type and other one is the file hash which is a unique identifier.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File type observables



Select the file type observable to process for further integrations such as sandbox, threat lookup. In addition, you can also download the attachments from the file type observable.

Note:

The threat lookup (VirusTotal) retrieves the file from the secured attachments for the new file type observables and the below system properties are not applicable for the new file type observables.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

For a quick reference, the file type observable is mapped as a child to the hash observable and hash observable is mapped as a child to file observable.

If the phishing email attachments are exceeding more than the defined size then the observables are not created. You must modify the system properties to support the larger size files.

File size system properties

System property	Description
glide.email.inbound.max_total_attachment_size_bytes	If you are forwarding the phishing email directly, use this system properties value to increase the file size from 18MB to a desired file size.
com.glide.attachment.max_get_size	If you are forwarding the phishing email as an attachment, use this system property value to create the below system properties under global scope to increase the file size from 5MB to the desired size.

You can also create a new file type observable as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Click **New**.

b. Select the **Observable type Category: File**

c. Click **Upload** to attach a file.

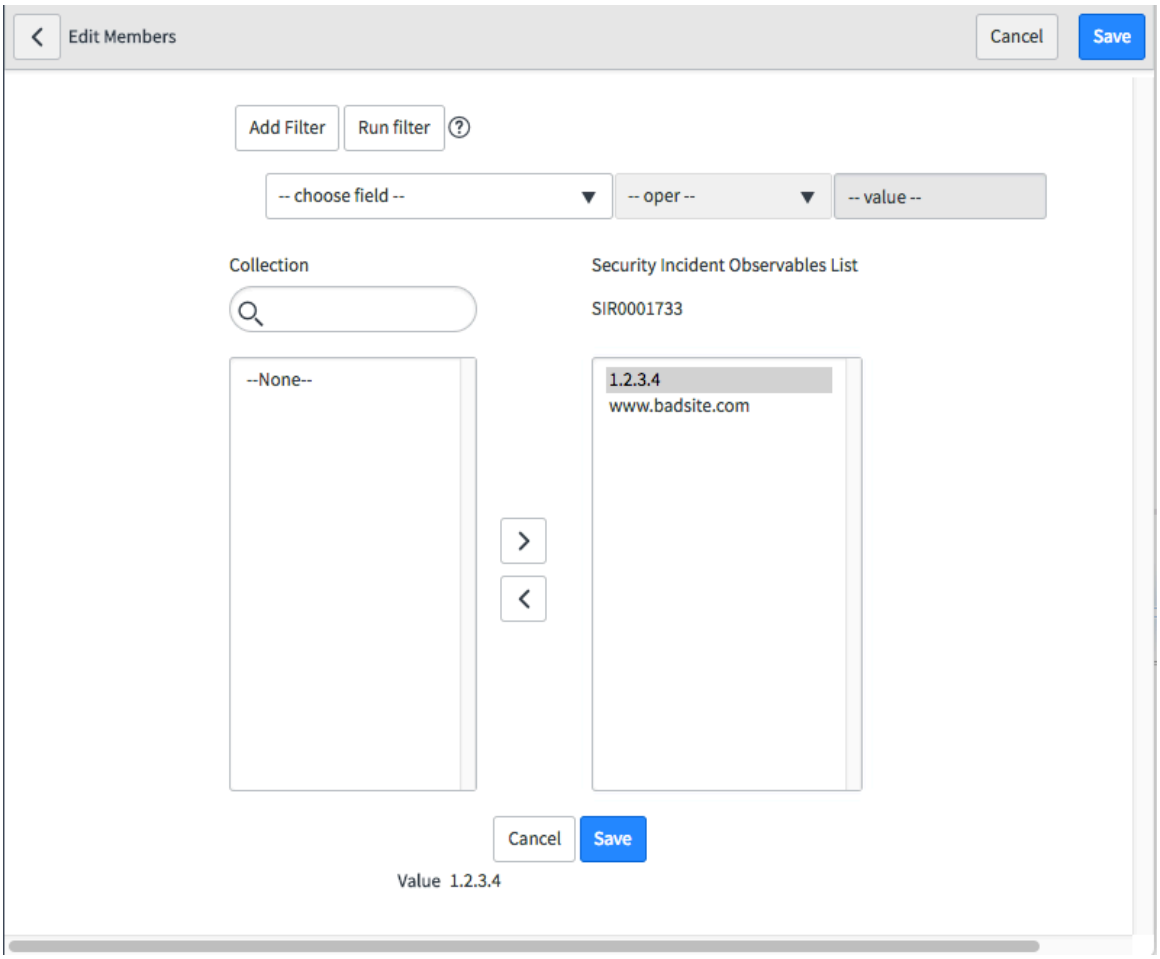
Edit a security incident observable list

You can edit which observables in the list associated with a security incident to display.

Before you begin
Role required: sn_si.basic

Procedure

1. Navigate to **Security Incident**.
2. Choose an incident.
3. Click **Security Incident Observables** related list tab.
4. Click **Edit**.
5. Add or remove observables from the list.
   Create a filter for long lists.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Save**.

> **Note:** When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The **Related Configuration Items** and **Related Users** related list tabs are updated accordingly. Also, if the Threat Intelligence plugin is activated, and you have at least oneSecurity Incident Response integrations integration implementation activated, the Security Operations Integration - Threat Lookup capability executes one or more workflows, and threat security lookups are performed on the observables you added. The results appear in the **Threat Lookup Results** tab.

Related topics

Add multiple security incident observables

Create a security incident observable

Add multiple security incident observables

To save time, you can add multiple security incident observables to the security incident observables list.

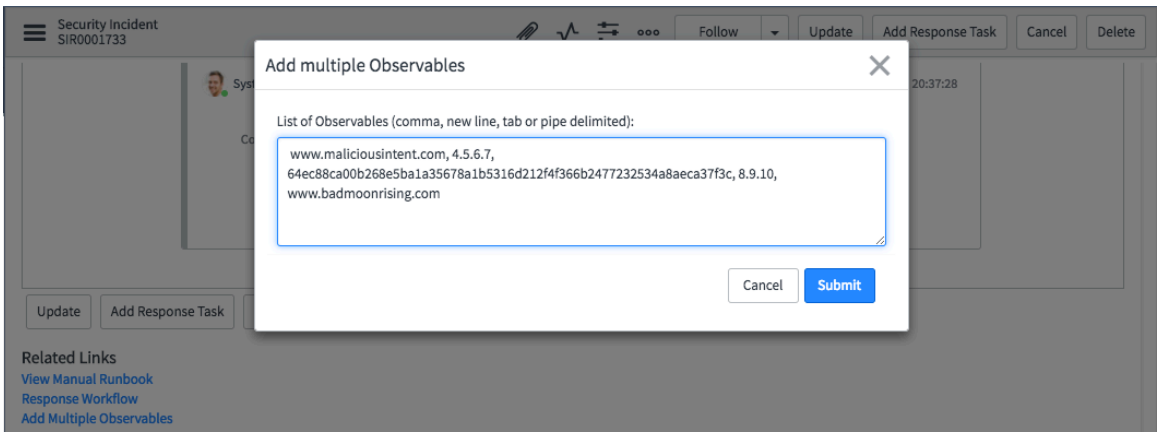
Before you begin

Role required: sn_ti_write

> **Note:** When adding multiple security incident observables, duplicates are ignored during processing.

Procedure

1. Navigate to **Security Incident**.
2. Choose an incident.
3. Click the **Add Multiple Observables** related link.
4. Enter or paste multiple observables.
   Entries can be of any Observable Type. Accepted formats are: comma, new line, tab, or pipe separators.



> **Note:** When you add an observable to the security incident, the system checks for any other configuration items or users associated with it. The **Related Configuration Items** and **Related Users** related list tabs are updated accordingly.

Note: Observable values not auto-detected are assigned to type Unknown.

5. Click **Submit.**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Automatic security incident observable log data enrichment

When certain applications and integrations are set up, including Threat Intelligence and the Palo Alto Networks - Firewall integration, observables information in a security incident can be automatically enriched with threat log data whenever the Source IP for its observables is modified.

When a modification occurs, a business rule initiates a workflow that retrieves data from threat logs on your firewall and enriches the observables information in the security incident.

Before observables can be enriched, the following steps must be performed.

- Threat Intelligence must be activated.
- The Palo Alto Networks Firewall integration must be activated and configured. This can also include Set up SSH credentials to the MID Server.

After that setup has been completed, the act of changing the Source IP of observables associated with a security incident causes a business rule to execute the **Security Operations Palo Alto Networks - Get Log Data** workflow. Workflow activities queue up a search query on the firewall and return a Job ID that is used to retrieve threat logs data from the firewall and attach them as an XML file to the security incident.

Related topics

Get AutoFocus Session Info Enrichment Flow

Security Operations Integration Palo Alto Networks Firewall Launcher workflow

Security Operations Palo Alto Networks - Check and Block Value workflow

Get Log Data Flow

Get WildFire Data Enrichment Flow

Publish observables to a third-party watchlist

You can publish one or more observables or associated indicators to a third-party watchlist. Currently, the only implementation that supports this functionality is CrowdStrike Falcon Host.

Before you begin

Role required: sn_si.analyst

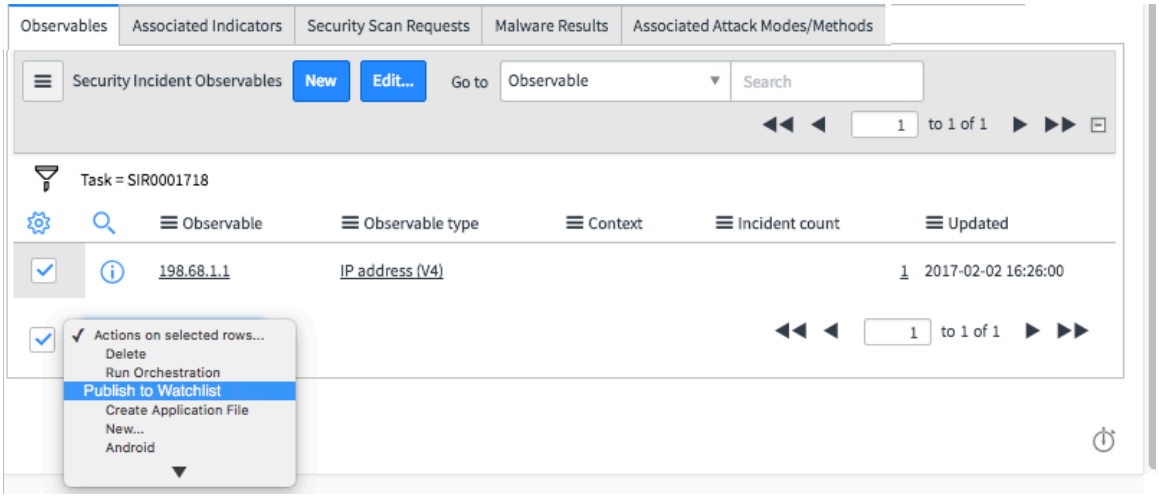
About this task

Note: If no implementations are available, capability actions are not displayed in product menus.

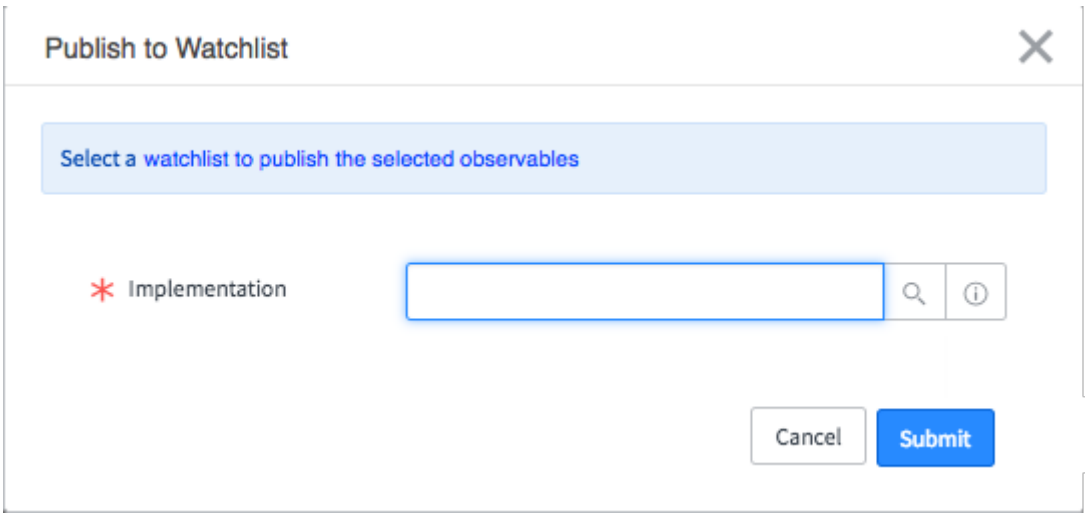
Procedure

1. Navigate to a security incident.
2. Select **Observables** from the **Related List** tab.
3. Click **Publish to Watchlist** in the **Actions on selected rows...** drop-down menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The dialog box appears.



4. Enter or choose the implementation.

> **Note:** A workflow is triggered by the Security Operations Integration- Publish to Watchlist capability when you select the CrowdStrike Falcon Host implementation.

5. Click **Submit**.

Manage lookups and scans

You can perform lookups and vulnerability scans from security incidents and from the security incident catalog to identify potential threats and vulnerabilities.

Submit an IoC Lookup request from a security incident

An IoC lookup automatically runs whenever observables are added to a security incident. Also, if your security incident has attachments, they can be easily found with the press of a button.

Before you begin
For automatic IoC lookups, the Threat Intelligence plugin must be activated.

Role required: sn_si.basic

> **Note:** By default, the **Lookup Type** for **File** is inactive.

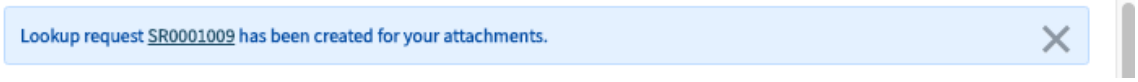
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Create a new security incident or open an existing one if you intend to attach new files to it.
2. Click the paperclip icon in the form header and attach one or more files.
3. When you have completed your entries on the form, right-click the form header and click **Save**. After the record has been saved, a **Lookup attachments** button appears.
4. Click **Lookup attachments**.

   Note: The work notes under **Incident Details** report the progress of the lookup process.

5. You can click the lookup number at the end of the message to view the lookup record. You can click the Lookup reference link to view detailed results.



Submit an IoC Lookup request from the Security Incident Catalog

If the Security Incident Response plugin is activated, you can submit threat lookups for files, hash values, URLs, and IP addresses from the Security Incident Catalog. The requests are submitted and you can view the results in the **My Requests** module.

Before you begin

Role required: none

About this task

Lookups are automatically performed for the default lookup type for each lookup source listed in the lookup record. The results of the lookup request are available in the **My Requests** module.

Procedure

1. Navigate to **All** > **Self-Service** > **Security Incident Catalog**.
2. Click **IoC Lookup**.
3. Click **Lookup files, hash values, URLs or IP addresses**.
4. Enter one or more of the following:

IoC Lookup request

Item to lookup	Description
Files	Click the paperclip icon, then locate and attach the files you want to lookup. **Note:** By default, the **Lookup Type** for **File**is inactive. Files are converted and submitted as a hash value.
URLs	In the **URLs** field, enter the URLs you want to lookup, separated by commas. For example: www.abc.com,www.xyz.net.
IP addresses	In the **IP addresses** field, enter the IP addresses you want to lookup, separated by commas.
Hash values	In the **Hash values** field, enter the hash values you want to lookup, separated by commas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item to lookup	Description
	Note: When the **Lookup Type** for **File** is inactive, this value is the default action for both **File** and **Hash values**.

5. When you have made your selections, click **Submit**.
6. To view the status and/or results of the lookups, navigate to **Self-Service** > **My Requests**.
7. Click the SR number for the request.
   The work notes under **Activity** list the tasks performed during the lookup, including the creation of individual lookups for each file, hash value, URL, or IP address, and the lookup results.

Submit a vulnerability scan request from a security incident

If your security incident has one or more configuration items (servers, computers, and so on), they can be scanned for vulnerabilities from the Security Incident Response form.

Before you begin

The Vulnerability Response plugin must be activated.

Role required: sn_si.write

Procedure

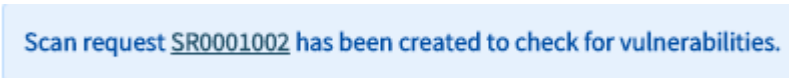
1. Create a security incident and include at least one resource.
   You can also open an existing incident that has configuration items.
2. When you have completed your entries on the form, right-click the form header and click **Save**.
   After the record has been saved, a **Scan for Vulnerabilities** related link appears.

   Note: If the **Scan for Vulnerabilities** related list is not shown, you must navigate to **Vulnerability** > **Scanners**, set up at least one scanner, and set its default to **true**.

3. Click **Scan for Vulnerabilities**.

   Note:

   A message appears at the top of the security incident form, along with a link to the scan record.

4. You can click the scan request number to view the scan record.
   The incident details show the results of the scan in the Security Scan Request record.

Submit a vulnerability scan request from the Security Incident Response catalog

You can submit vulnerability scans for CIs and IP addresses from the Security Incident Response catalog. The requests are submitted and you can view the results in the **My Requests** module.

Before you begin

Role required: none

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Self-Service** > **Security Incident Catalog**.
2. Click **Vulnerability scan**.
3. Click **Scan Configuration Item and IP addresses**.
4. Enter one or more of the following to be scanned.

Vulnerability Scanners

Item to be scanned	Description
Configuration item	In the **Configuration Item to scan** field, select the CI to be scanned.
IP addresses	In the **IP addresses to scan** field, enter the IP addresses, separated by commas.

5. When you have made your selections, click **Submit**.
   If an observable is found, an indicator is created, according to STIXX standards.
6. To view the status and/or results of the scans, navigate to **Self-Service** > **My Requests**.
7. Click the SR number for the request.
   The work notes under **Activities** list the tasks performed during the scan, including the creation of individual scans for each CI or IP address, and the results of the scans.

Manage on-demand orchestration

During Security Incident Response analysis, a security analyst may want to perform a task that is driven by a security incident workflow. For example, run a process dump on a particular CI. This can be accomplished with on-demand orchestration.

Each registered Security Operations application includes several on-demand orchestrations in the base system. You can define custom on-demand orchestrations, as needed.

On-demand orchestration can be invoked from a choice list at the bottom of the following lists and forms in Security Incident Response:

- Security Incident form
- Security Incident list
- Security Incident Observables related list
- Configuration Items related list

Note:

- A property in Security Support Common called **sn_sec_cmn.use_on_demand_tbl_as_allowed** defines which workflows are available for on-demand execution.
- If the property is set to **true**, only workflows specified in the On Demand Orchestration [sn_sec_cmn_on_demand_orchestration] table are available.
- If the property is set to **false** (default), all workflows for applications configured in the SecOps Application Registry are available.
- Depending on the setting of the property, the list of workflows available is tailored to the type of information being analyzed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Perform on-demand orchestration from the Security Incident form

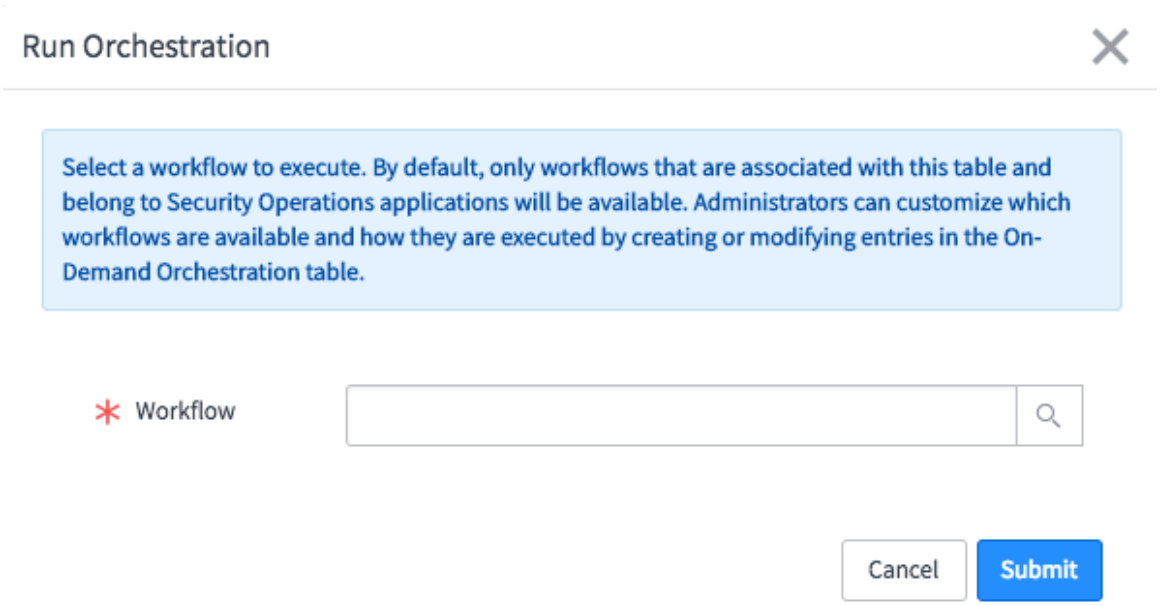
On-demand orchestration can be invoked from a choice list at the bottom of the Security Incident form.

Before you begin

Role required: sn_si.write

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show Open Incidents**.
2. Select the record (security incident, observable, or CI) for which you want to run a workflow.
3. Click the **Run Orchestration** related link.
   The **Run Orchestration** dialog box opens. The appearance of the dialog box depends on the setting of the sn_sec_cmn.use_on_demand_tbl_as_whitelist property in Security Support Common.



4. Click the lookup icon and select the workflow you want to run.
   The selected workflow runs. For details, see Security Incident Response Orchestration flows and actions.

Perform on-demand orchestration from the Security Incident list

On-demand orchestration can be invoked from the Security Incident list, as well as from related lists in Security Incident Response.

Before you begin

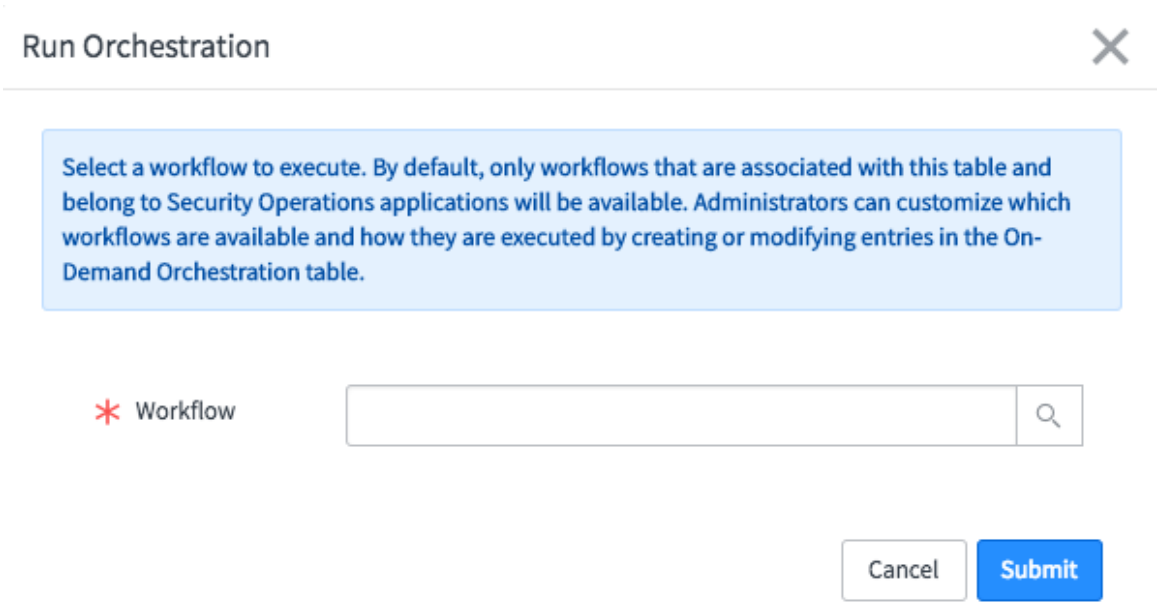
Role required: sn_si.write

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show Open Incidents**.
2. Select the check box next to the security incident for which you want to run a workflow.
3. Click the **Actions on selected rows** choice list at the bottom of the screen, and click **Run Orchestration**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Run Orchestration** dialog box opens. The appearance of the dialog box depends on the setting of the sn_sec_cmn.use_on_demand_tbl_as_whitelist property in Security Support Common.



4. Click the lookup icon and select the workflow you want to run.
   The selected workflow runs. For details, see Security Incident Response Orchestration flows and actions.

Define new on-demand orchestrations

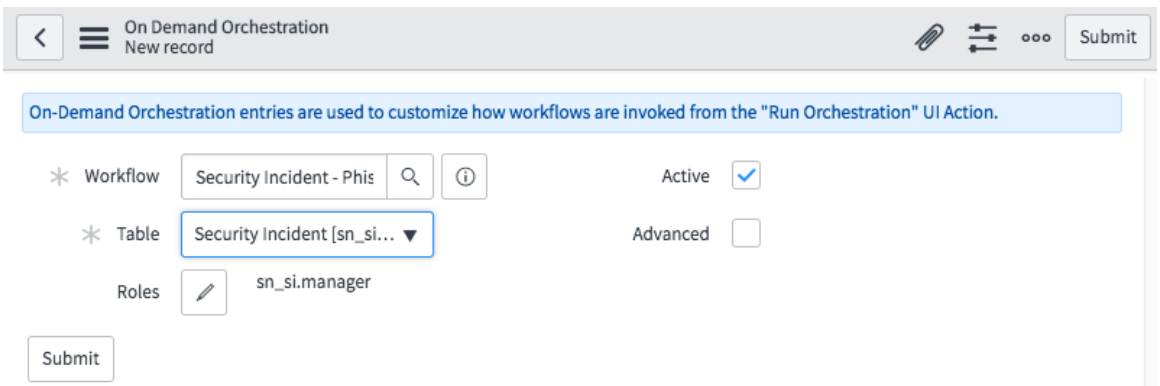
In the base system, you can select on-demand orchestrations that execute predefined workflows. You can define new on-demand orchestrations to customize how workflows are invoked from the **Run Orchestration** choice lists.

Before you begin

Role required: sn_si.write

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **On-Demand Orchestration**
2. Click **New**.



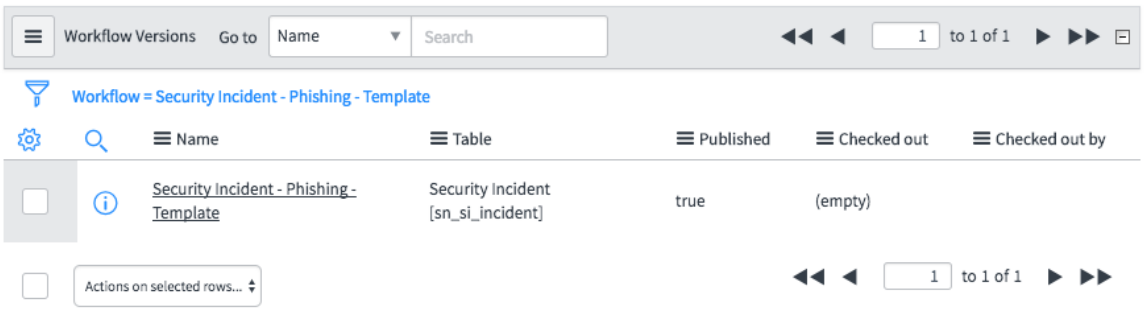
3. Fill in the fields, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

On Demand Orchestration

Field	Description
Workflow	Select the workflow to be included in the **Run Orchestration** choice list.
Table	Select the table on which the selected workflow is executed. If the table does not match the table configured for the selected workflow, you must select the **Advanced** check box and modify the **Execution script** to pass the correct record to the workflow on execution.
Roles	As needed, select additional roles to restrict who can see this workflow in the **Run Orchestration** choice list.
Active	Select this check box to activate this on-demand orchestration record.
Advanced	Select this check box to modify the execution script so that it passes the correct record to the selected table for this workflow.
Execution script	Modify the execution script so that it passes the correct record to the selected table for this workflow. This field appears only if the **Advanced** check box is selected.

4. Right-click in the record header, and select **Save**.
The **Workflow Versions** related list appears.



5. If you need to make additional modifications to the workflow, you need to check it out.

Related topics

Work with workflow versions

Register new Security Operations applications for on-demand orchestration

In the base system, Security Operations applications are automatically registered when they are activated. Registration allows the workflows associated with the applications to be available for on-demand orchestration requests. If needed, you can define new applications and associate workflows with them for on-demand orchestration.

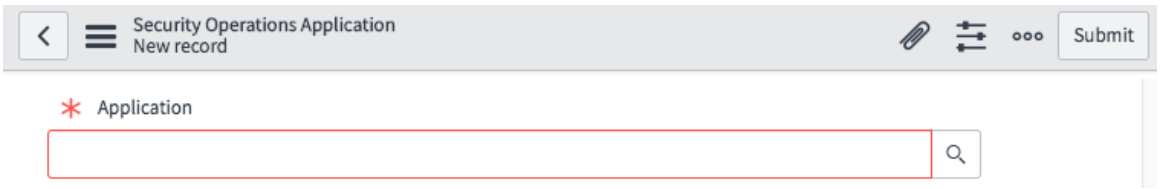
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

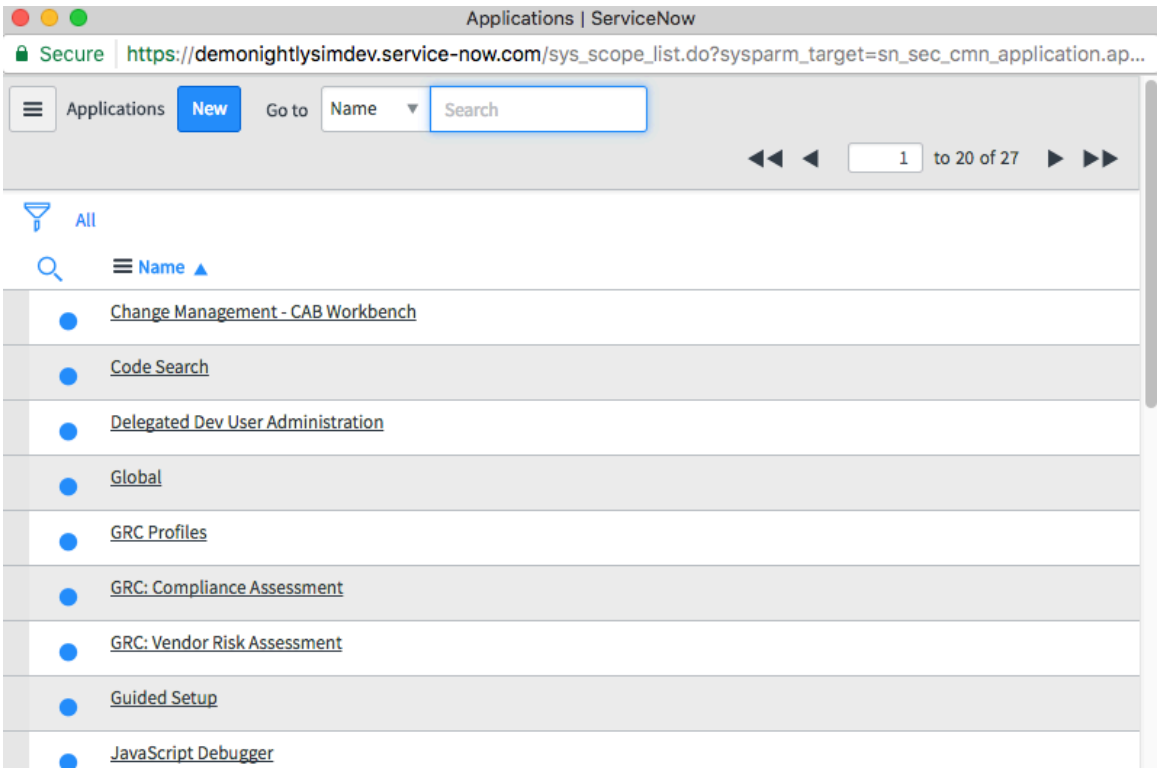
Role required: sn_si.write

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **SecOps Application Registry**, and click **Register Application**.
   The Security Operations Application screen appears.

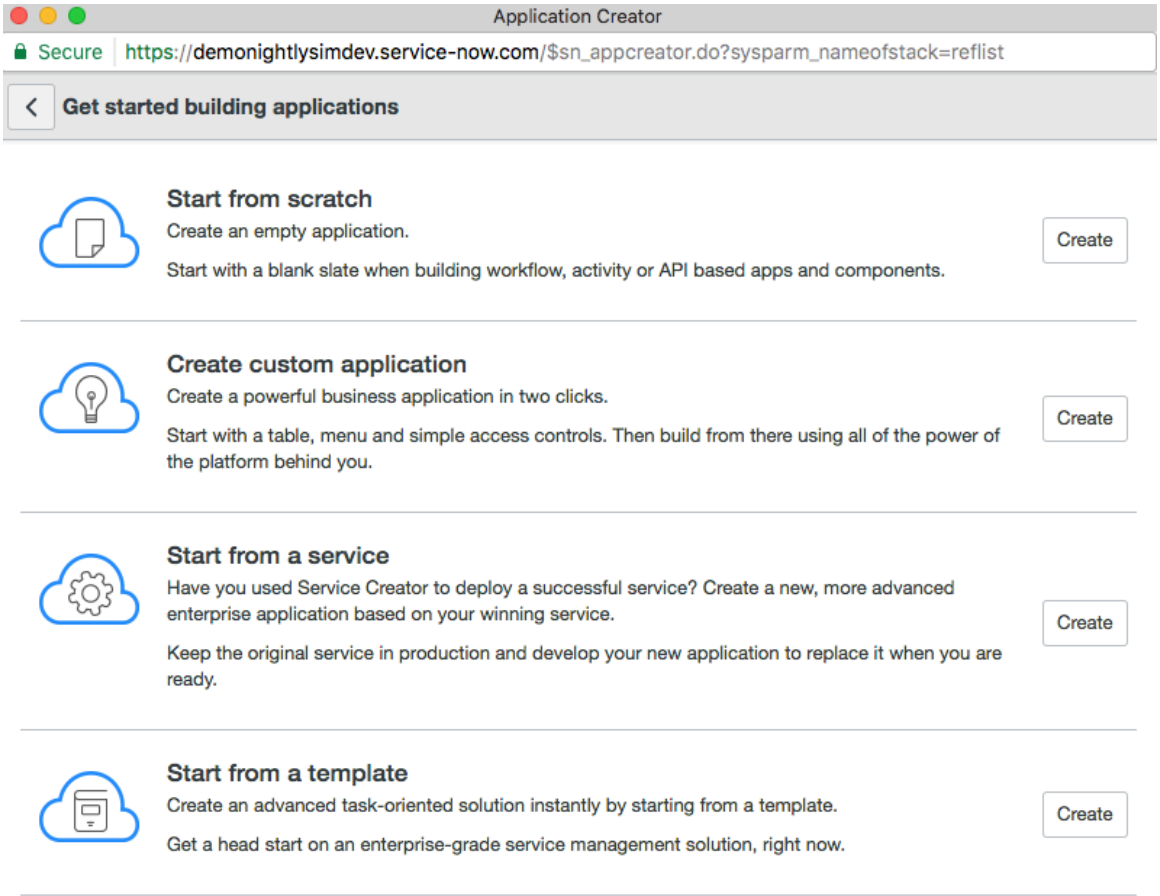


2. In the **Application** field, click the lookups (magnifying glass) icon.
   The Applications screen appears.



3. Click **New**.
   The Application Creator screen appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: The options that display depend on the applications you have activated. For detailed information on creating new applications, see Building applications.

4. After the application has been generated, you can create scripts for setting up on-demand orchestration.

Note: Setting up on-demand orchestration for new applications requires advanced technical knowledge of scripting and creating triggers for the scripts (business rules, UI action, workflows, and so on). For more information, contact ServiceNow Professional Services.

Add information to a security incident

After a security incident is created, you can add more details to aid in analysis, such as access roles and different kinds of notes.

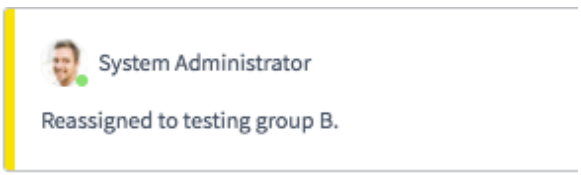
Before you begin

Role required: sn_si.basic

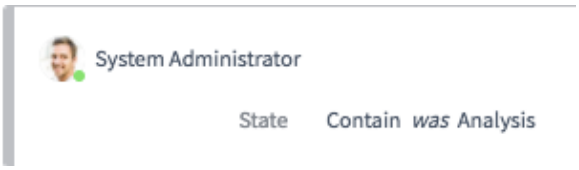
Procedure

1. If it is not already open, open the security incident you want to update.
2. Click the **Incident Details** tab.
3. Fill in the fields, as needed.

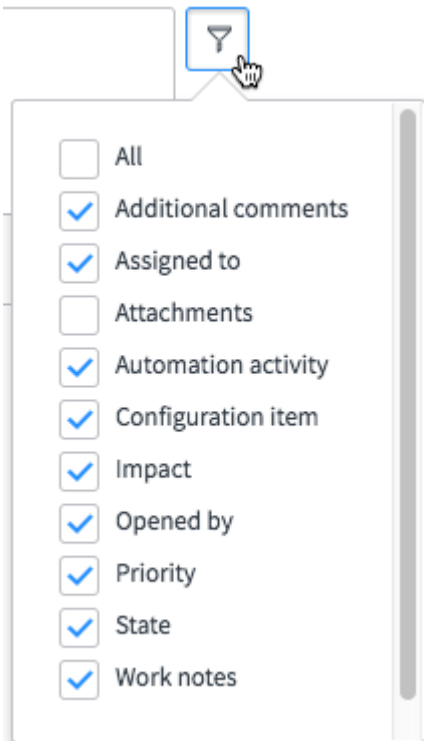
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Read access	Gives a user with the **special access** role read access to the security incident. The user is able to read and write work notes. **Note:** ○ If a user is added to both **Read access** and **Privileged access** lists, then only the **Privileged access** permissions persist. ○ User with sn_si.admin role only can modify both read access and privileged access.
Watch list	Click the lock icon to add users who are notified when changes to the security incident occur. After the field is unlocked, options are available for adding or removing multiple users or entering user email addresses. When you have completed your entries, click the lock icon to lock the field.
Privileged access	Gives a user with the **special access** role read and write access to all fields of the security incident except **Assigned to**. Users with special access roles have their own module containing all security incidents assigned to them. No other modules are available to them. No one else can see the **Visible to Me** module. **Note:** Only an assigned user or someone with a security role (for example, sn_si_analyst or sn_si.admin) can change the **Assigned to** field. If a user is added to both **Read access** and **Privileged access** lists, then only the **Privileged access** permissions persist.
Work notes list	Click the lock icon () to add users who are notified when new work notes are added. After the field is unlocked, options are available for adding or removing multiple users or entering user email addresses. When you have completed your entries, click the lock icon to lock the field.
Description	Enter a full description of the security incident, along with any information that can help to find the cause or resolve the issue.
Secure notes	Only user roles with sn_si.admin and sn_si.analyst can view or edit the secure notes.
Work notes	Type work notes that are not visible to the customer. Work notes appear in the **Activity** area.
Activity	Displays information manually entered in Work notes, and all dynamically updated task activity (actions, comments, work notes, and so on) on related records for this security incident. Work notes appear with a yellow color band. 

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Automatically generated notes appear with a gray color band. 

4. You can limit the types of information displayed in the **Activity** field by clicking the filter ( ) icon.



Note: The **Automation activity** check box allows you to include any enrichment performed by this security incident, including workflow activities, risk score updates, and so forth.

5. Click any of the following tabs to further update the security incident:
   - Related Records
   - Post Incident Review
   - Closure Information
6. When you have completed your entries, click **Submit**.

Add related problems, changes, and incidents to a security incident

You can add related records, such as problems, changes, and incidents to existing security incidents.

Before you begin
Role required: sn_si.basic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. If it is not already open, open the security incident you want to update.
2. Click the **Related Records** tab.
3. Fill in the fields, as needed.

Field	Description
Problem	Select a Problem (PRB) record that resolves the underlying issue that caused this security incident to be created. The PRBs for this incident are typically created by right-clicking in the security incident form header and selecting **Create Problem**.
Parent	Select a task record related to the underlying issue that caused this security incident to be created.
Parent security incident	Select a security incident record related to the underlying issue that caused this security incident to be created. See Parent and child security incident relationships.
Incident	Select an Incident (INC) record that resolves the underlying issue that caused this security incident to be created. The incident is typically created by right-clicking in the security incident form header and selecting **Create Incident**.
Change request	Select a Change Request (CHG) record that resolves the underlying issue that caused this security incident to be created. The change request is typically created by right-clicking in the security incident form header and selecting **Create Change**.

4. Click any of the following tabs to further update the security incident:
   - Incident Details
   - Post Incident Review
   - Closure Information
5. When you have completed your entries, click **Submit**.

Invoke a process dump for an enriched process in Windows

A security analyst can run a process dump on a specific process, dump it into a file, and post it to a shared site on an internal network. An analyst can then view a deny listed process, highlighted in red in a security incident, and perform additional analysis.

Before you begin

The following are required:

- A client running Windows Vista or higher, or a server running Windows Server 2008 or higher.
- The ProcDump command-line utility installed, with a system environment variable that points to the procdump executable file path. The name of the variable must be PROCDUMP. This name is used in a powershell script.

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to the security incident with the enriched process on which you want to invoke a procdump by clicking **All** > **Security Incident** > **Show Open Incidents**, and open a security incident.
2. Click the **Enrichment Data** tab.
3. Click the **Retrieve Running Processes** enrichment record.
4. Select the check boxes for the running processes you want to perform a procdump for, click the Actions on selected rows drop-down list at the bottom of the list, and click **Run Procdump**. An **Initiated prodump workflow for selected process** message appears at the top of the list, and the **Security Incident Response - Run procdump** workflow executes.

View information in a security incident

You can perform several other actions on an existing security incident using the related links.

Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident you want to update.
2. Within **Related Links**, you can perform the following tasks,

Option	Description
View Manual Runbook	View a list of runbooks available for this secu rity incident.
Response Workflow	View any workflow associated with this inci dent.
Add Multiple Observables	Adds a list of observables in comma, new line, tab, or pipe delimited formats.
Add to Security Case	Adds the security incident to one or more se curity cases. You can also create a new securi ty case and add this security incident to it.
Get QRadar IP Summaries	If a QRadar integration is available, and con tains valid CIs, source, and destination IP ad dresses, it triggers the QRadar workflows and displays the results in work notes.
Run Orchestration	Choose and run a Security Operations work flow.
	You can view an SLA timeline from a Task SLA record or from an SLA definition.
Show All Related Lists	Displays all standard related lists and any lists added manually. **Note:** Manually added items are avail able only in this view.
Show Affected Items	Displays the lists of CIs, users, and services directly affected by this incident

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Show Related Items	Displays the lists of related incidents, CIs, users, and groups affected by this incident.
Show IoC	Displays the lists of observables, indicators, malware, modes and methods, and security scan requests associated with this incident.
Show Enrichment Data	Displays the lists of enrichment data, process es, services, statistics, lookups, firewall logs, and compromised user information associat ed with this incident.
Show Response Tasks	Displays the lists of tasks, SLAs, risk score au dits, outages, and Exchange searches associ ated with this incident.
View Details in External System	If this security incident was generated from an external application, directly or by events, and a link to the originating data was provid ed, the **View Details in External System** ac tion opens the URL. You can view and search through the logs that generated this incident.
Scan for Vulnerabilities	If Vulnerability Response is activated, and you have selected at least one affected CI for the security incident, you can submit a scan request to determine what vulnerabilities ex ist on the CI.

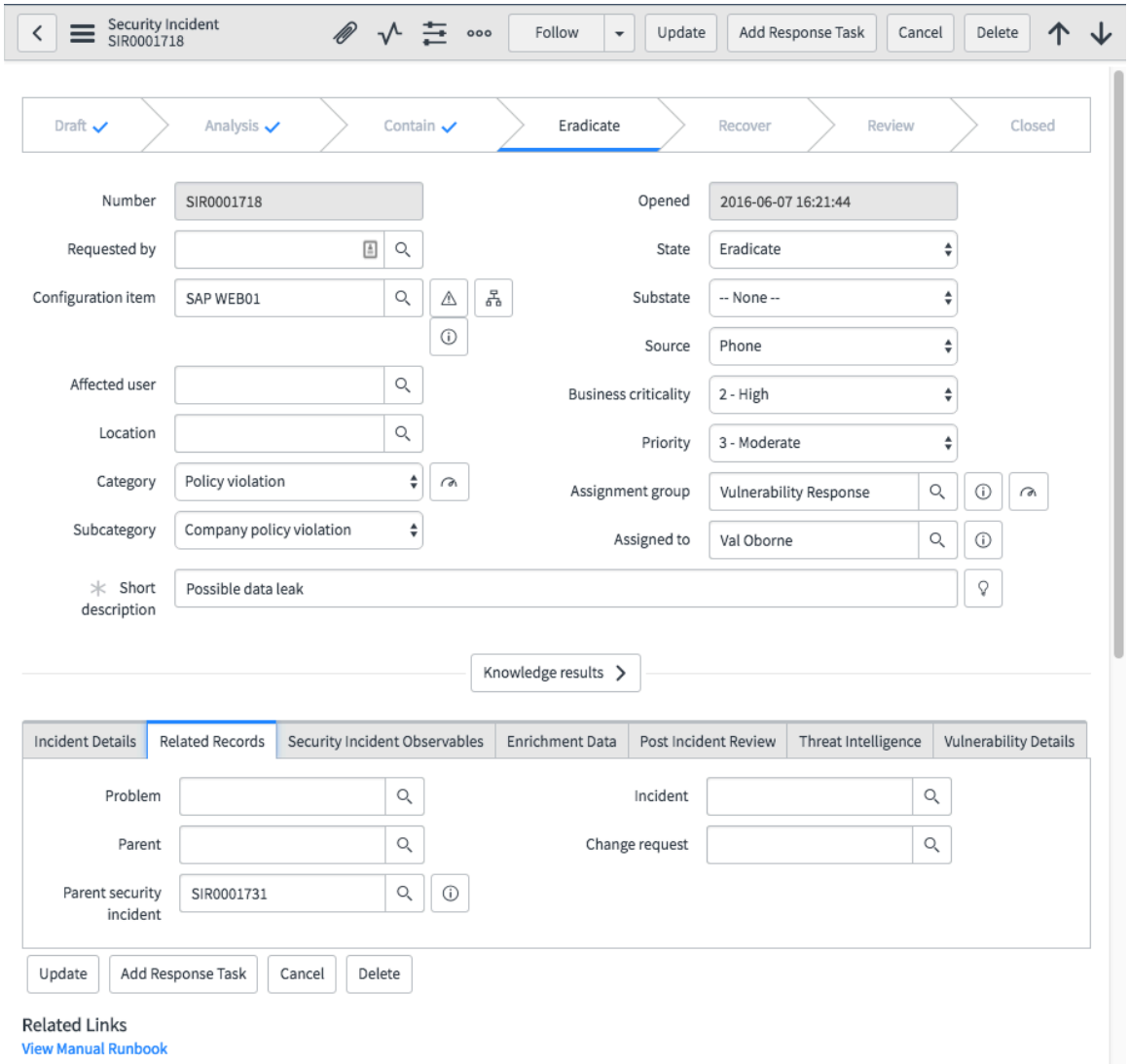
Parent and child security incident relationships

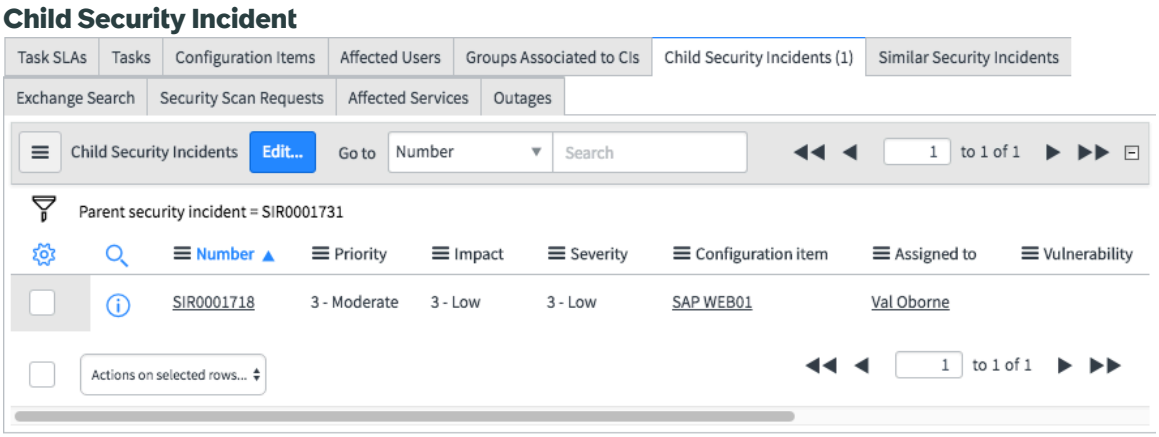
You can associate and track the impact of any given issue using parent and child security incident relationships in Security Incident Response.

Using the **Related Records** tab, you can add a **Parent security incident** issue to any Security Incident Response form. This feature automatically makes the incident a child that appears in the **Related Lists - Child Security Incidents** tab of the parent issue.

Note: You cannot make an existing parent security incident its own child by using the same number for both incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

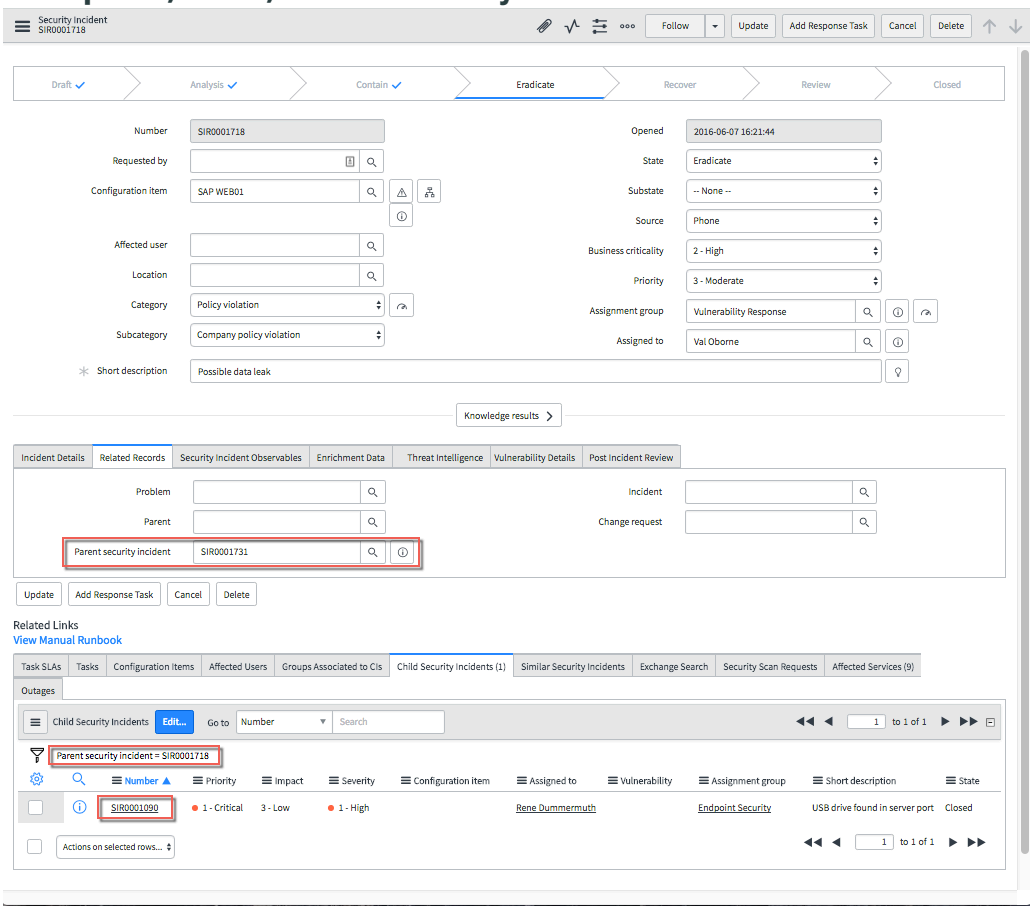




You can add one or more **Child Security Incidents** to any security incident record, as well, using the **Edit** button in the **Child Security Incidents** tab. In the following example, all three records are connected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Grandparent, Parent, and Child security incidents



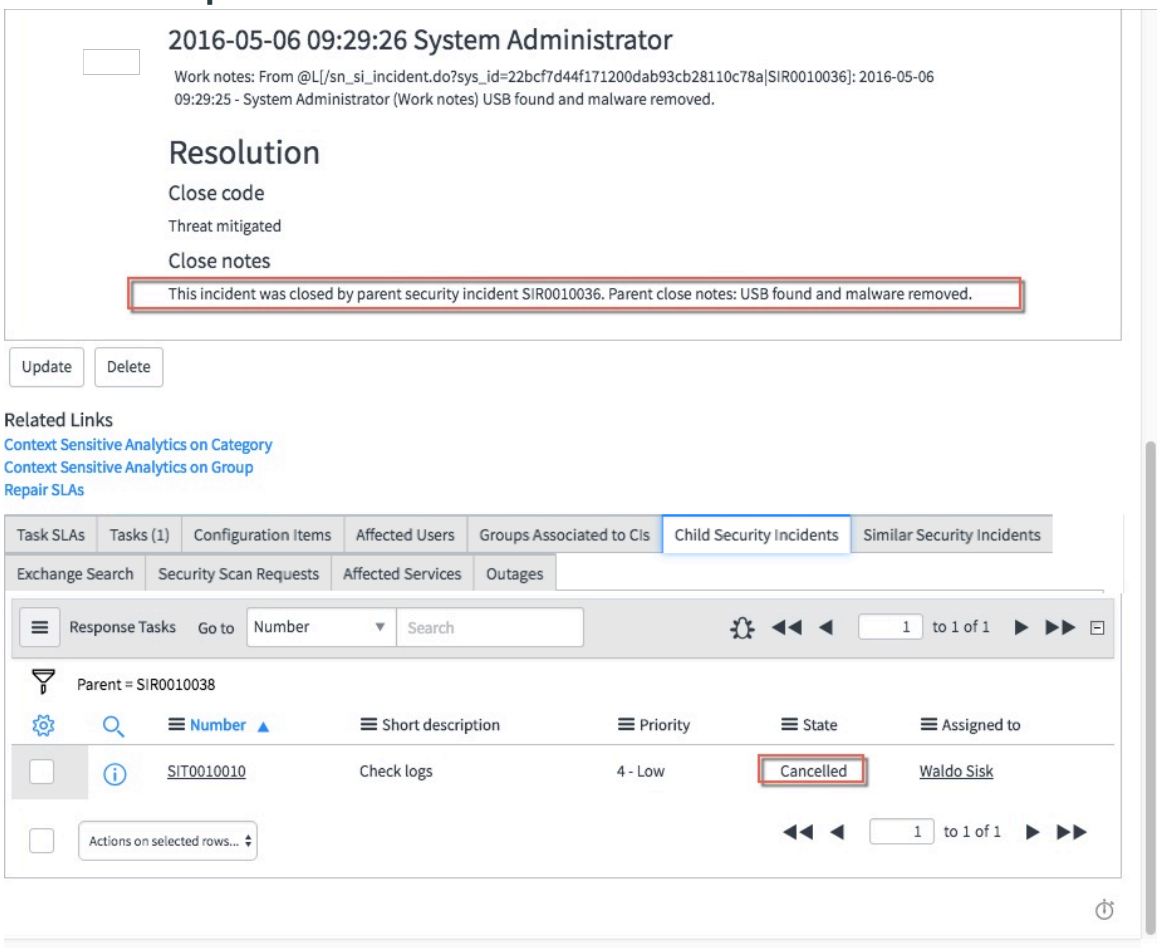
Note:

- All work notes recorded in the parent are propagated to any active children in **Activities** under the **Incident Details** tab.
- The **Parent** field is used to associate the security incident with a parent record, such as a major incident, problem, or change request, that is outside the Security Incident module. For grouping multiple security incidents to a main security incident, the **Parent security incident** field is used.

When a parent is closed or canceled, any active children are also closed or canceled. Any active **Response Tasks** on the child incidents are canceled. If there are no other open **Tasks**, the child incident is closed. When closed, the **Post Incident Interview** records the closure and the information found on the **Closure Information** tab is propagated from the parent to the children.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Close Child Response task



View affected items for a security incident

You can view affected items, such as CIs, affected users, and affected services associated with a security incident.

Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident for which you want to view affected items.
2. Click the **Show Affected Items** related link.
3. Click any of the related lists to view or add information for the security incident.

Tab	Description
Configuration Items	Affected configuration items (CI). After affected CIs are identified, you can manually add affected resources from this related list.
Affected Users	After affected users are identified, you can manually add affected users from this related list.
Affected Services	View or add business services associated with the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tab	Description
	Note: If an affected CI is added after the security incident is opened, it is a good idea to right-click in the form header and select **Refresh Impacted Services**.

Note: If the Security Operations Integration - Get Running Processes integration capability is active, and you add a CI to a security incident, the Get Running Processes workflow runs and retrieves a list of running processes on the CI.

If the Security Operations Integration - Isolate Host integration capability is active, you can select one or more CIs and restrict their system connections to other devices. To do this, select the check boxes for the CIs and click **Isolate Host** from the **Actions on selected rows** choice list.

4. Click any of the following related links to further update the security incident:
   - Show Related Items
   - Show IoC
   - Show Enrichment Data
   - Show Response Tasks
5. When you have completed your entries, click **Submit**.

View related items for a security incident

You can view related items, such as similar and child security incidents, related users, vulnerability groups, and vulnerable items associated with a security incident.

Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident for which you want to view related items.
2. Click the **Show Related Items** related link.
3. Click any of the related lists to view or add information for the security incident.

Tab	Description
Child Security Incidents	Select a task record related to the issue that caused this security incident to be created.
Similar Security Incidents	View any other security incidents associated with any of the same observable records.
Related Configuration Items	Displays a list of security incidents containing configuration items with the same observable as this security incident. This list can be filtered using the **CI exclusions** filter group. When an observable is added to a security incident this list is automatically updated. By default, observables with a context type of Destination are excluded.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tab	Description
Related Users	Displays a list of security incidents containing users with the same observables as this security incident. This list can be filtered using the **User exclusion** filter group. When an observable is added to a security incident this list is automatically updated. By default, observables with a context type of Destination are excluded.
Related Filter Group	After configuration items are identified, any matching CI or Filter group are automatically added.
Vulnerability Groups	If Vulnerability Response is activated, you can view vulnerability groups associated with this security incident.
Vulnerable Items	If Vulnerability Response is activated, you can view vulnerability items associated with this security incident.
Risks	If any of the core Risk Management plugins (Policy and Compliance Management, Audit, Management, or Risk Management) are activated, you can view or add risks associated with the security incident. You can add this related list from the form header context menu under **Configure** > **Related Lists**.
Configuration item events	If Event Management is activated, you can view events.
Configuration item alerts	If Event Management is activated, you can view alerts.
Customer Service Cases	If Customer Service is activated, you can view Customer Service case information.

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show IoC
   - Show Enrichment Data
   - Show Response Tasks
5. When you have completed your entries, click **Submit**.

View enrichment data for a security incident

You can view enrichment data, such as running processes, running services, and network statistics associated with a security incident.

Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident for which you want to view enrichment data.
2. Click the **Show Enrichment Data** related link.
3. Click any of the related lists to view or add information for the security incident.

> **Note:** Raw data details are stored in an attachment to the enrichment data record. If they exceed the field limit, displayed details are truncated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tab	Description
Running Processes	Stores the records created by the Security Incident Response **Get Running Processes** workflow.
Running Services	Stores the records created by the Security Incident Response **Get Running Services** workflow.
Network Statistics	Stores the records created by the Security Incident Response **Get Network Statistics** workflow.
Domain Lookups	If the WhoisXML API Integration plugin is activated, stores the records created by a Whois lookup.
Firewall Logs	Stores enrichment data from firewall logs, such as the Palo Alto Network firewall logs.
Compromised User Info	Stores accounts identified as being compromised through a Have I Been Pwned? lookup.

Note: The **Security Enrichment Data** tab shows raw enrichment data from Security Incident Response workflows, such as retrieving network statistics or running processes. This tab can be viewed by clicking the **Show All Related Lists** related link.

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show Related Items
   - Show IoC
   - Show Response Tasks
5. When you have completed your entries, click **Submit**.

View response task information for a security incident

You can view response task information, such as task SLAs, risk score audits. and outages associated with a security incident.

Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident for which you want to view response tasks.
2. Click the **Show Response Tasks** related link.
3. Click any of the related lists to view or add information for the security incident.

Tab	Description
Tasks	Displays tasks already defined for the security incident. You can manually create a response task or and Create a task from this related list.
Response Tasks	Displays actions to be performed in response to the security incident.
Task SLAs	View or add active task SLAs that were defined for the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tab	Description
Risk Score Audits	An audit record for each instance of a risk score being changed.
Outages	View or manually add new outage records associated with the security incident.
Email Search	A list of records that holds search criteria to run queries on an email server, such as a Microsoft® Exchange Server (based on the implementation installed), and stores the results received. **Note:** if the Security Operations Integration- Email Search and Delete capability is not active, the **Email Search** related link is not displayed.

4. Click any of the following related links to further update the security incident:
   - Show Affected Items
   - Show Related Items
   - Show IoC
   - Show Enrichment Data
5. When you have completed your entries, click **Submit**.

View related events and alerts in security incidents

As a security incident is being worked on, you can view the details of the events. For alerts, you can view and acknowledge these alerts, and create incidents or security incidents from them as needed.

Before you begin

You must have the Security Incident Response Event Management support plugin activated.

Role required: si.sn_agent

Procedure

1. Navigate to any security incident list (for example, **All** > **Security Incident** > **Incidents** > **Unassigned Incidents**).
2. If the resources affected by the security incident you are viewing have received alerts or events within the previous 24 hours, one or both of the following related lists appear.
   - Security Incident CI Alerts
   - Security Incident CI Events
3. Click the related list you want to view.

Related list	Description
Security Incident CI Alerts	You can view details for alerts received within the previous 24 hours. You have the option of clicking **Acknowledge** to indicate that you are aware of the alert and it is being handled. Use **Close** to indicate that the alert is not important.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related list	Description
Security Incident CI Events	You can view details for event received within the previous 24 hours.

View security incident to customer service case mapping

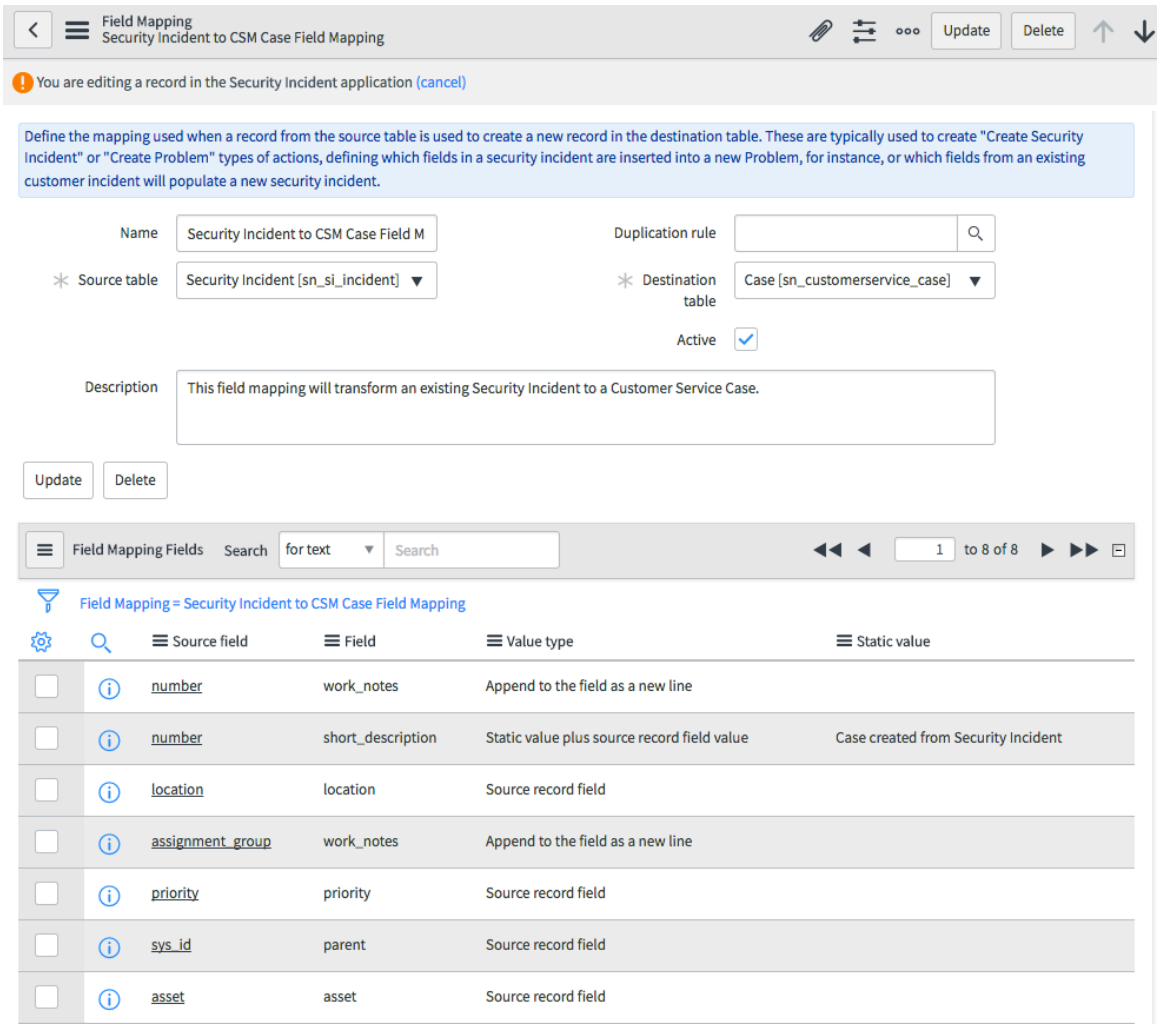
Security Incident Response ships with a default field mapping that maps a security incident to a Customer Service case. You can view the security incident to CS case default map.

Before you begin

Role required: sec_cmn.read

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Field Mapping**.
2. Click **Security Incident to CSM Case Field Mapping** to view the default map.



3. You can edit the mapping, as needed.
4. When you have completed your changes, click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

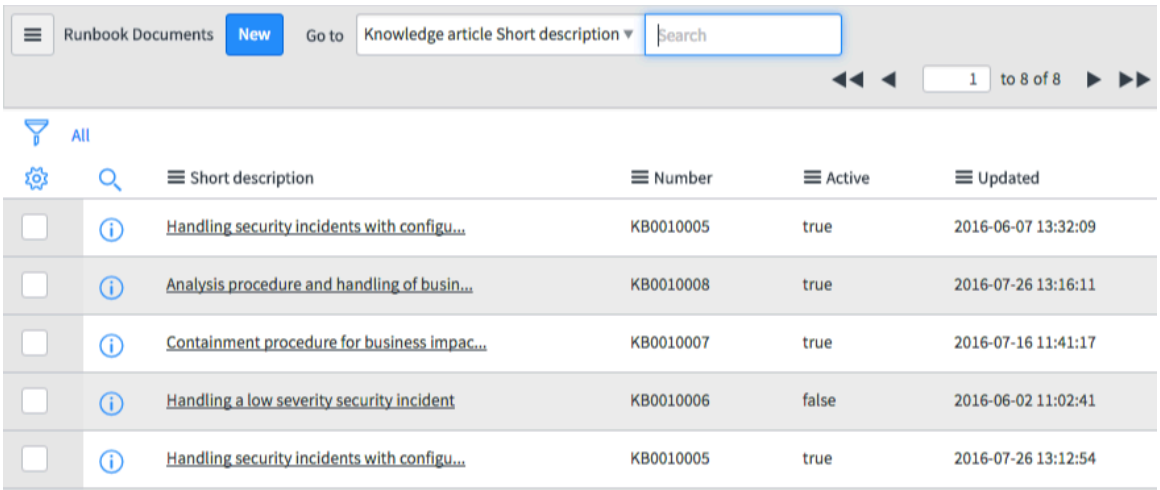
View a Security Incident Response runbook

Runbooks give you access to procedures related to tasks you are working on.

Before you begin
Role required: sn.si.knowledge_admin

Procedure

1. Navigate to **All** > **Security Incident** > **Manual Runbook** > **View Runbook Documents**.
2. Select a runbook from the list.



3. To create a runbook, click **New**.
   For more information, see Create a runbook.

Identify all configuration items affected by a security incident

If you know which resource (server, desktop or other configuration item) is behind a security incident and want to identify related resources and business services that can be affected, you can use the Business Service Management (BSM) map.

Before you begin
Role required: admin or sn_si.admin

About this task
The BSM map displays the upstream and downstream dependencies for a selected root CI.

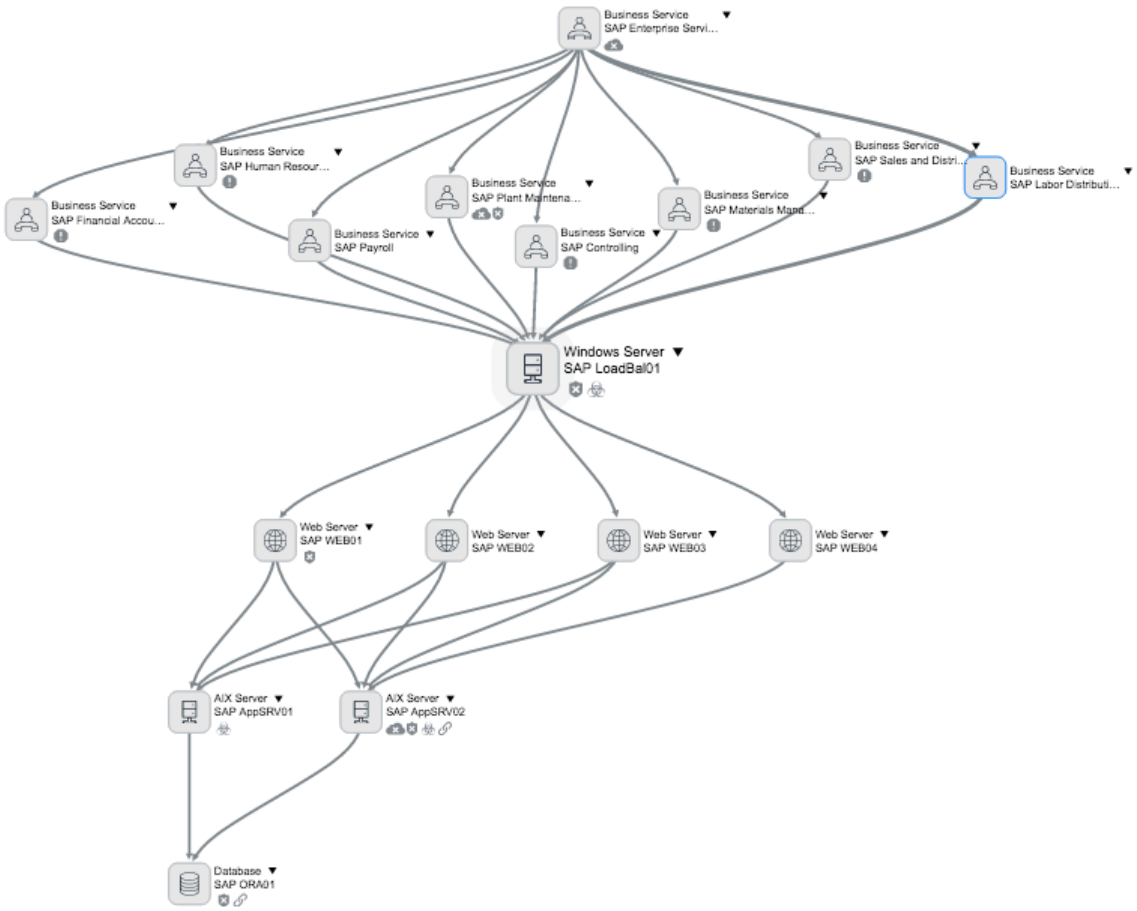
There are two methods you can use to view the BSM map for a CI:

- If you want to view CIs from the context of a task, view from the security incident form.
- If you do not want to view CIs from a task viewpoint, view from the navigation bar.

Procedure

1. From the Security Incident form, populate the **Configuration item** field, and click the BSM map icon ( ).
   The BSM map screen displays the map for the last incident you accessed in Incident Management or the last security incident you accessed in Security Incident Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Click the icons next to a configuration item to view different kinds of details about the resource (server, desktop, or other CI).

   For example, click (⚠) to view alerts associated with the CI.

   Note: To view a list of all the available icons, click **Filters** above the BSM map and expand **Filter Task Types**.

3. To arrange the map in different configurations, select any of the formats listed above the map (**Vertical**, **Horizontal**, **Radial**), or click **Filters** to filter the map for easier viewing.

4. If you opened the BSM map from the security incident form, you can add a dependent CI to the security incident by right-clicking the CI and selecting **Add Affected CIs**.
   You can also add multiple CIs at a time. Drag a box around the CIs you want to add, right-click the box, and select **Add Affected CIs**.
   The CIs are added to the Affected CIs related list of the security incident.

Calculate the severity of a security incident

You can calculate the severity of a security incident using predefined calculators.

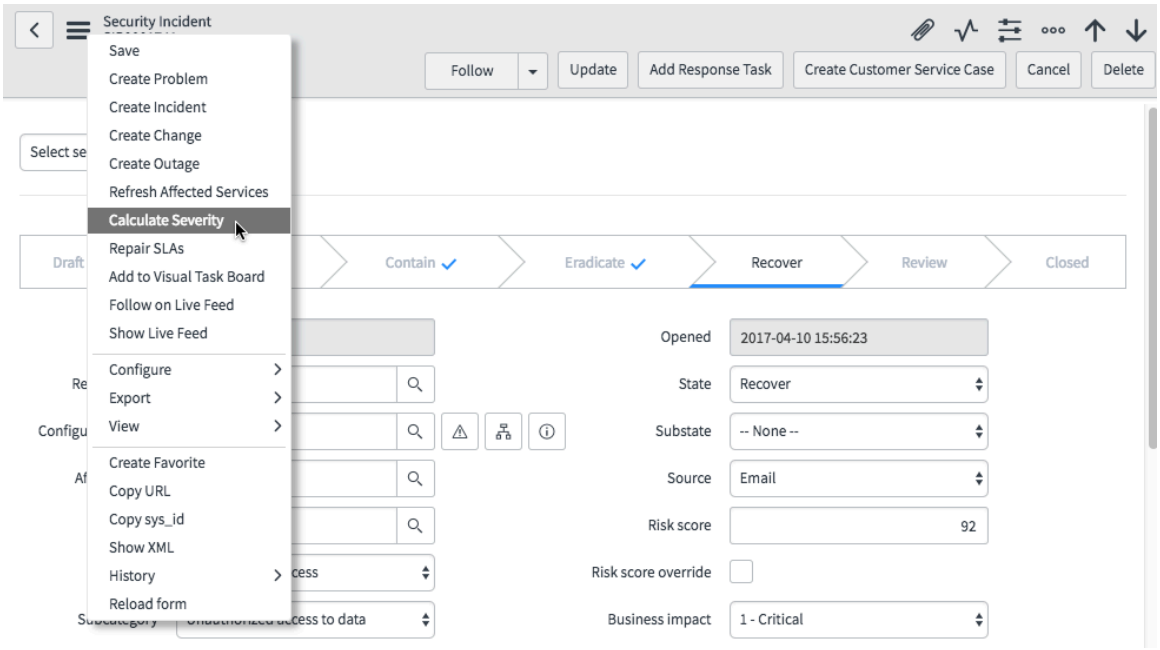
Before you begin

Role required: sn_si.basic

Procedure

1. If it is not already open, open the security incident you want to calculate the severity for.
2. Click the form header context menu and select **Calculate Severity**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The severity is calculated based on the predefined rules for base calculators. For more information, see Understanding security incident calculators.

Search for and delete phishing emails

Deleting phishing emails can help reduce exposure to a specific attack across an organization. You can manage phishing emails on your email server by searching, granting approvals, and deleting them.

Before you begin

Roles required: sn_sec_cmn.cap_email_read

You can determine how many users were targeted by a phishing attack by querying an email record associated with a security incident.

Supported software:

- Microsoft® Exchange Server 2010

Limitation: When searching the body of emails, you can search a maximum of 1,500 mailboxes.

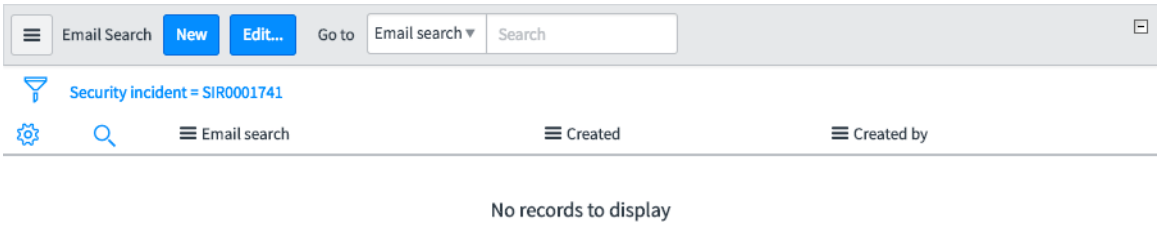
About this task

This feature is used by the Security Operations Integration - Email Search and Delete flow to run a query against your email server. Depending on the search criteria you select, the search identifies all emails within a phishing attack, and returns the total number of emails affected or details from the emails affected.

Procedure

1. Navigate to **All** > **Security Incident** > **Show Open Incidents**.
2. Choose a security incident.
3. If the **Email Search** related list is not visible, click the **Show All Related Links** related link.
4. Click the **Email Search** related list.

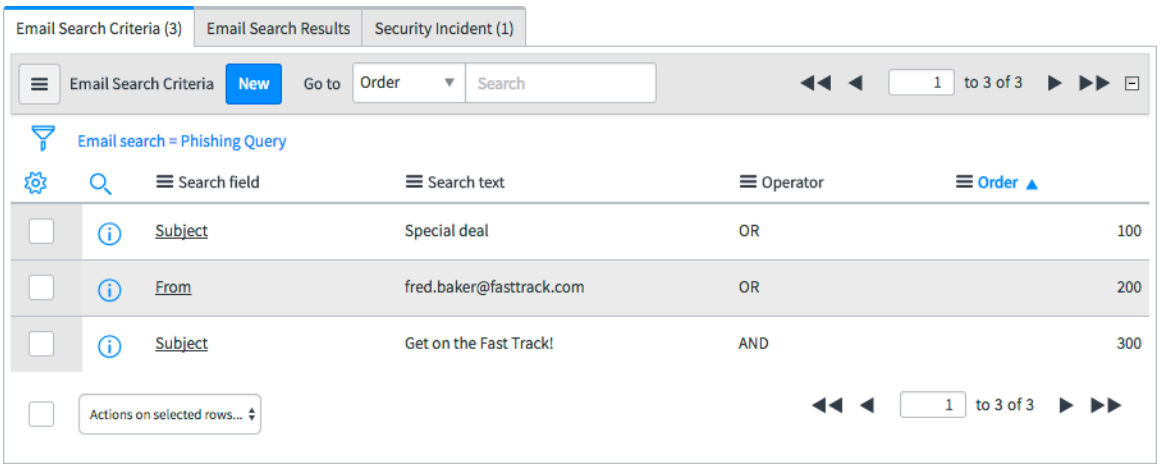
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **New**.
6. Fill in the fields, as appropriate.

Field	Description
Name	Name of the search query
Query from criteria	A preview of the query run on the email server. Generated from all the associated active search criteria records.
Description	Describe what the search query is looking for.

7. Right-click in the form header and select **Save**.



8. Click the **Email Search Criteria** tab and click **New**.
9. Fill in or edit the fields, as appropriate.

Field	Description
Email search	Displays the name of the email search. You can change it if needed.
Search field	Field to search in the email server. The search field has the following choices: **Subject** This criteria searches for emails that contain the Subject line text specified in the **Search text**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	field. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, email read status, recipient, and message ID, are returned. **From** This criteria searches for emails that contain the sender's full email address (for example, jane.doe@abc.com) specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, email read status, recipient, and message ID, are returned. **Note:** You cannot use the **From** and **Recipient** fields in the same query. **Recipient** This criteria searches for emails that contain the recipient's full email address (for example, john.doe@abc.com) specified in the **Search text** field. It also searches for emails in the To, Cc, and Bcc fields. For emails that meet this search criteria, the total number of phishing emails and the details of each email, including the email date received, email read status, recipient, and message ID, are returned. **Note:** You cannot use the **From** and **Recipient** fields in the same query. **Body** This criteria searches for emails that contain the body text specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails is returned.

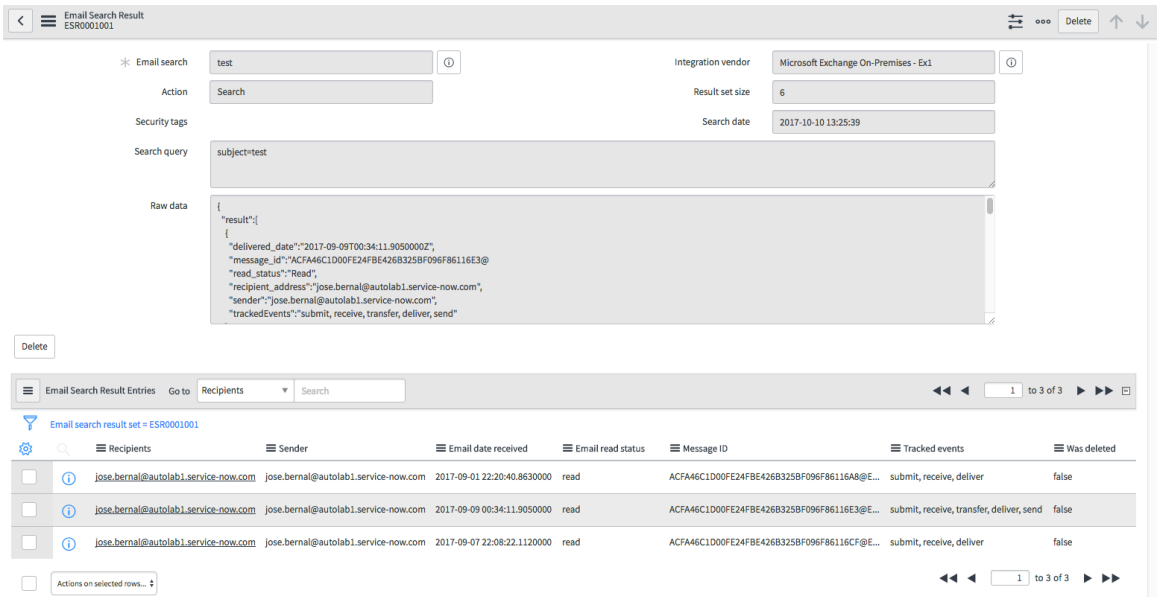
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: When searching the body of emails, you can search a maximum of 1,500 mailboxes. **Cc:** This criteria searches for emails that contain the Cc full email address (Ex: jane.doe@abc.com) specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails is returned. **Bcc:** This criteria searches for emails that contain the Bcc full email address (Ex: jane.doe@abc.com) specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails is returned. **Attachment** This criteria searches for emails that contain either the attachment file name or attachment contents specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails is returned. **Note:** Only plain text attachments are supported for searching the attachment contents. **Retention Policy** This criteria searches for emails that contain retention policy numbers specified in the **Search text** field. For emails that meet this search criteria, the total number of phishing emails is returned.
Active	Select this check box to activate this email search query.
Operator	Possible values are AND and OR. You can define how search criteria are combined to run in the email server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

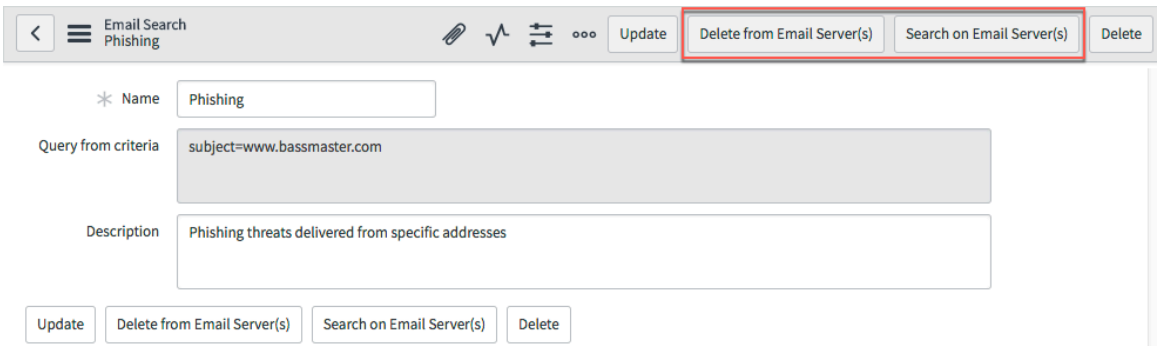
Field	Description
Order	The order in which the search query is built from the search criteria.
Search Text	The text to search for. Single quotation marks, double quotation marks, and colons are not supported.

10. Click **Submit**.
11. Repeat as needed to define additional search criteria.
12. You can view the results of the search by clicking the **Email Search Results** tab.



Each line of the Email Search Result Entries form represents a separate email.

13. After you have created a search criteria record, two buttons appear in the Email Search form: **Delete from Email Server(s)** and **Search on Email Server(s)**.



14. To search for emails in the selected server that meet the search criteria you defined, click **Search on Email Server(s)**.

Create a security incident knowledge article

As you work with security incidents and response tasks, knowledge articles automatically display to provide pertinent information about the task you are performing. Your organization can create and maintain articles in the security incident knowledge base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.knowledge_admin

About this task
Knowledge articles share security information, document the types of cyber threats that your organization faces, and provide answers and responses to these threats.
If needed, you can organize knowledge articles into runbooks, which create associations between the articles and specific tasks. For example, you can configure a runbook with conditions that cause a knowledge base article about phishing to be displayed when you are creating a security incident for a phishing attack. For more information, see Create a Security Incident Response runbook.

Knowledge articles in runbooks can also be associated with specific tasks in a playbook. For more information, see Associate a knowledge article with a playbook task.

The benefits of knowledge articles include the following.

- Employees have one source of information that is easy to search.
- Information can be kept up-to-date, as knowledge articles have a defined life cycle: create, review and update, publish, and retire.
- When you manually create a security request, incident, or response task, a list of relevant articles is presented as you type the short description.

Note: It is important to assign a knowledge manager to each security incident knowledge base.

Procedure
1. Navigate to **All** > **Security Incident** > **Catalog & Knowledge** > **Knowledge**.
2. Click the Create an Article icon ( ).
3. Fill in the fields on the form, as appropriate.

Knowledge form

Field	Description
Number	The automatically generated KB number.
Knowledge base	The knowledge base selected for this article.
Category	The category for this article.
Published	When this knowledge article was published. This value is set when the article is created, and updated when the article is published.
Valid to	When this knowledge article expires. This article will not appear in search results after this date or if a date is not selected.
Image	An image that appears beside the article when searching from the legacy knowledge portal.
Workflow	[Read-Only] The publication state of the article, such as Draft or Published. When inserting a new article from an existing article, the state of the new article is reset to **Draft**.
Source	The task this knowledge article was created in response to, if any. This field is set automatically when you create the knowledge article from a task record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Attachment link	Check box for downloading an attached file automatically when a user accesses the article, instead of opening the article view. Add an attachment to the article to use this option.
Display attachments	Check box for displaying attachments to users viewing this knowledge article. Attachments appear below the article text. Add one or more attachments to the article to use this option.
Short description	The title of the article. This title appears when browsing and searching knowledge, and at the top of the article.
Text	Content for the article. Use the WYSIWYG HTML editor to create content. A preview of the content appears when browsing and searching knowledge.

Note: If you are creating a knowledge article to be associated with a playbook task, set the **Knowledge base** field to **Security Incident Response Runbook**.

4. Click **Submit** to create the article.

What to do next

Any additional steps required to publish the article, such as approvals, depend on the publishing workflow for the knowledge base.

Related topics

Create a Security Incident Response runbook

Escalate a security incident

If an escalation path exists for a security incident, the Escalate button is available in the security incident header.

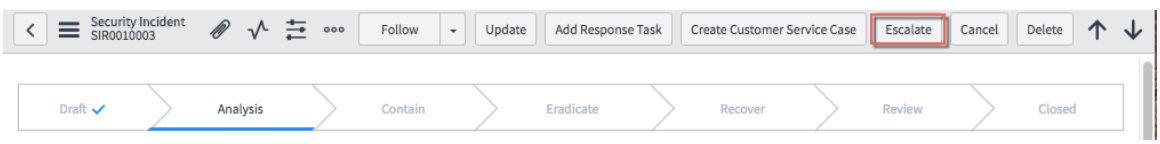
Before you begin

Role required: sn_si.admin

You must have an escalation group created to see this button. See Create a Security Operations user-defined escalation group for more information.

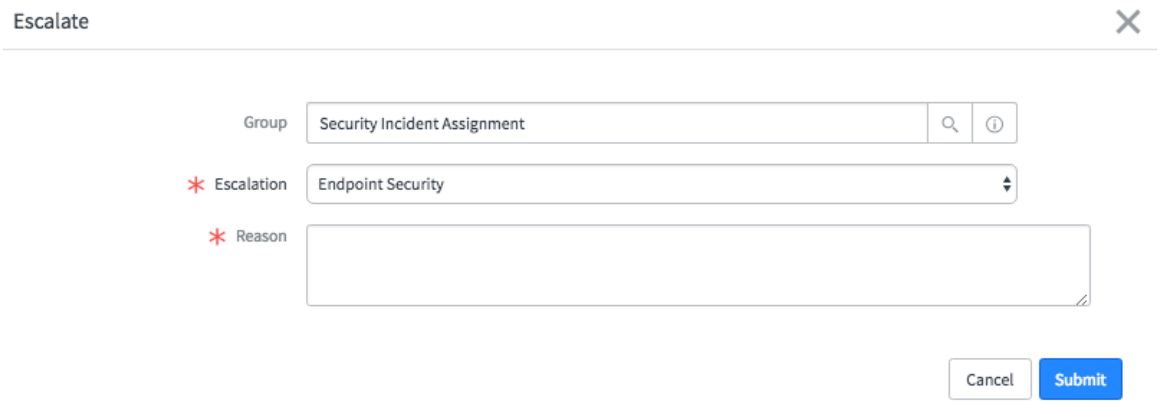
Procedure

1. Navigate to **All** > **Security Incident** > **Show Open Incidents**.
2. Open the incident you want to escalate.
3. Click on the **Escalate** button.



4. Choose an escalation group.
5. Enter a reason for the escalation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Click **Submit.**
   Updates **Assignment Group** and **Assigned to** on the security incident.

Manage post incident activities

Based on the requirements of your business, a review of the origins and handling of security incidents is often needed.

The Post Incident Review functionality in ServiceNow provides many tools for automating, tracking, auditing, and simplifying this process.

This section describes the following:

- Assign post incident review roles
- Configure an assessment trigger condition
- Perform a questionnaire-based post incident review
- Create PIR assignment rules
- Post incident review report

Assign post incident review roles

You can target questions to specific pre-defined groups by assigning roles to Post Incident Review (PIR) categories.

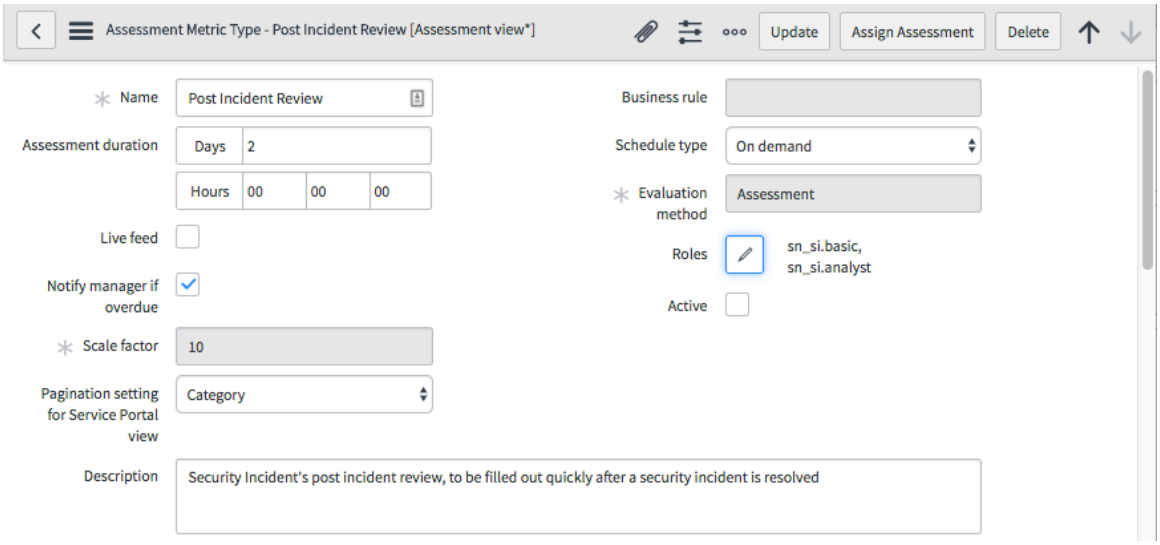
Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Assessments** > **Metric Definition** > **Types**.
2. Under the **Types** column, search for a **Post Incident Review** record.
3. Open the record.
4. Assign one or more roles for this category of questions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Update**.
6. Navigate to **User Administration** > **Users**.
7. Choose a user
8. Add one or more metric type roles to the user record.

> **Note:** The roles must correspond to roles assigned in the Post Incident Review category.

Post incident review report

The Post Incident Review (PIR) reports feature enables you to set up and download the post incident review reports using the Post Incident Review tab.

The security admin can create and configure the report templates and map those templates to the security incident using the report configuration. A security analyst can then view or download the report after the security incident is resolved and the status is updated to Review state.

A PDF report is generated and attached to the security incident when the incident is moved to the Closed state after successful configuration.

> **Note:** The reports feature is applicable and supported from Orlando Patch9.

To customize your post incident review reports, you must do the following configuration.

1. **Report Templates**: Customize and configure the following report template features to add additional information on the report:
   a. Timeline
   b. Branding
   c. Template Scripts
2. **Report Configuration**

This section describes the configuration procedure:

Report Templates

Use the Report Templates section to create primary and additional report templates that are applied to the security incidents to generate the Post Incident Review report. You can format

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and configure the report based on your requirements. The templates also help you to include the assessment details in the template.

The following are a few optional steps that can be performed while building the template:

1. Configuring the branding information.
2. Setting up the page size and page margin.
3. Adding any security incident-related fields (both custom and standard).
4. Using the following predefined custom tokens:
   a. *$sessionUser*: Returns the logged in username
   b. *$date*: Returns the current date
   c. *$if_not_null_start & $if_not_null_end*: If these tags are used against any fields, then the tags are displayed only if the value exists. For example:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Including the related list data using the template scripts. For more information, see the section below on **Template Scripts**.
6. Including the timeline information using the Timeline Filters. For more information, see the section below on **Timeline**.
7. Managing and formatting the template content such as attachments, tables, and images.

Note: The enhanced report template toolbar features are available only from the Paris release version.

Report templates key points:

1. The images attached to the report template are displayed on the Post Incident Review report only when they're included in the sys_attachment table.

   Note: Images selected from the db_image table won't be displayed on the post incident review report.

2. Videos aren't supported in the post incident review report.
3. The URLs in the PDF are non-clickable. To enable the URLs non-clickable (.) is denoted as (dot).
4. The report isn't generated if the size of the report template exceeds 50MB.
5. The font family selected for the report template content won't be applied to the PDF if it isn't supported by the PDF generator.

   Note: If the corresponding font is not there, the PDF generator identifies the closest alternative font and then generates the PDF.

6. If you provide higher page margin values, generate post incident review report is failed. For example, Top and Bottom margin > 450 and Left and Right margin > 450.
7. If a large text is included in the report template without spaces, then the text may be truncated. Preview the text and modify it accordingly.

The security admin can preview the report using the **Preview Report** button available on the Report Template page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

Select a Security incident to preview a report with this template option and select **Preview Report**.

Branding

You can add the branding template name, header and footer image, header and footer text, generate page numbers, and include the branding record in the report template after it's created.

The following is a sample branding report format:

Report template branding key points:

1. The maximum size allowed for the header and footer image is 5MB. If the size exceeds more than the specified limit, then an error message, 'Image format cannot be recognized' is displayed in the security incident.
2. The footer text length is limited to 100 characters.
   a. If the footer image text and report content are overlapped while previewing, you must change the branding record.
   b. If the footer text contains a URL link, then it may overlap on to the footer image. Preview and correct it as required.

Timeline

Timeline configuration enables you to create and modify the timeline filters as required. You can filter the activity types that should be included in the report, configure if the child tasks should be included or excluded in the report, and configure if the images should be included or excluded in the report.

If you want to use and populate any timeline configuration, you must add the tag as mentioned below: *`${timeline:timeline name}`*. Two sample timeline configurations as an example are provided in the set up that are used in the Phishing Report template and Default Report template. You can modify and reuse the configurations.

Template Scripts

Use the template scripts to include the related lists data, date and time stamp, and any other data that aren't directly dot-walkable. The following is an example:

Construct a template script to display the related list on report template:

1. To prepare the related list data, call PostIncidentReportUtils.fetchRelatedListDataForReport method.
2. To represent the step1 data in the table format and style, call the ReportTemplateUtil.constructTablefunction method.

If you want to use and populate any template script, then you must add the tag template script tag as *`${template_script:script name}`*.

Following are a few sample template scripts provided to configure and modify your post incident reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample template scripts

Script name	Description
formatted_current_date	Returns the current local date and time in the DDMMYYYY 00.00 AM or PM format. For example, 21 Jan 2021 3:51 PM PST.
si_affected_users	Returns the affected users from the related list in a tabular form.
si_assessments	Returns the post incident assessment results in a tabular form.
si_associated_phish_emails	Returns the associated phishing emails from the related list in a tabular form.
si_associated_phish_headers	Returns the associated phishing headers from the related list in a tabular form.
si_business_criticality	Returns color coded business criticality value.
si_malicious_observables	Returns the malicious observables from the related list in a tabular form.
si_observables	Returns the observables from the related list in a tabular form.
si_priority	Returns color coded priority value.
si_response_tasks	Returns the response tasks from the related list in a tabular form.
si_time_to_identify	Returns the duration spent in Draft and Analysis state.
si_time_to_resolve	Returns the time to resolve the incident.

Report template scripts key points:

1. If a related list is added with more than five columns, the table data is truncated during the PDF generation. Each column minimum width is set to 124px.
2. If a template script is unable to load the content in the report template due to technical issues, an error message is displayed on the report, 'Error while evaluating the template script' and the security admin must evaluate the correctness of the script to resolve the issue.
3. si_assessments: By default, all the assessment categories are added to the report. The security admin can filter the data by modifying the template script as required. Add the `categories: sys_id1,# sys_id2;` parameter to filter the data.
4. Time to resolve and time to identify scripts: Use the definition records that are part of the metric-related list. If the definition records are unavailable for the security incident, then create or add those definition records to populate the values for the two fields.

Note:

By default, the Security Admin doesn't have access to view the version records of any table. You must add an admin role to access the version records and revert to the previous version.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Report Configuration

Use the Report Configuration section to set up the conditions and apply the report templates to the Security Incidents. You can add one primary report and one or more additional report templates to the same condition.

The following is an example condition that is provided to apply the Phishing Report template to the Phishing category incidents and the other one to apply the Default Report template to all the security incidents. The Default Report template would be applied to the security incidents if the conditions aren't met.

Procedure to turn off the new implementation

1. Deactivate the following business rules:
   a. Generate PIR PDF
   b. Create Knowledge On Closure New
2. Activate the following business rules:
   a. Generate PIR when in Review and Close
   b. Create Knowledge On Closure
   c. [Regen PIR on closure/cancel/delete]
3. Activate the UI rule, *`Hide PIR field when empty`*.
4. Go to the form layout in the security incident form. Under **Post Incident Review** section:
   a. Remove PIR report picker from the PIR section
   b. Add the Post Incident Report field to the PIR section

Configure Post Incident Review (PIR) report properties for child security incidents

You have an option to configure the following two PIR report properties for child security incidents:

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Note: Users with the administrator [admin] role can view the properties. Users with the Security administrator [sn_si.admin] role can modify them.

Configure PIR report properties for child security incidents

Property	Usage
sn_si.generate_pir_report_for_child_si	Option to enable the generation of Post Incident Review (PIR) reports for child security incidents. • **Type**: true | false • **Default value**: false • **Location**: Navigate to All > System Properties > All Properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure PIR report properties for child security incidents (continued)

Property	Usage
sn_si.include_child_si_timeline_in_pir	Option to include the timeline of the child security incidents in the parent Security Incident's PIR report. • **Type**: true | false • **Default value**: false • **Location**: Navigate to All > System Properties > All Properties.

Manage Post Incident Review Report

Manage post incident review report includes the information that was configured and applied by the Security Admin, and the security analysts can modify the timeline filters at run-time and download it.

Before you begin

Role required:sn.si_analyst

About this task

The Security Analyst can select either of the available primary or additional report templates, and configure the timeline filters, preview, and download the report. The Security Analyst can also directly download the report with the timeline configuration which was last applied.

The Security Analyst can access the reports using the Post Incident Review tab.

Procedure

1. Navigate to the security incident in the Review State.
2. Click **Post Incident Review** tab.
3. If the security incident is in the **Review** state:
   Report Template:
   - By default, the primary report template that was configured on the set up page will be applied to the security incident and will be available to download.
   - The analyst can choose other reports from the drop down list to configure and download the report.
4. **Configure/Preview:**

   A security analyst can preview and modify the report template configuration. In the current configuration, the security analyst can only modify the timeline filters.

   In case the configuration is modified for the primary report before the security incident is closed, the post incident review report which is attached to the security incident will be updated as per the modifications done by the security analyst. After closure, the analyst will be able to modify the configuration and download the report on the go. However, the attached report would follow the last configuration before closure.

   To Configure/Preview the report, perform the following steps:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the desired report template from the **Report Template** drop down list on the **Post Incident Review** tab.

b. Click **Configure/Preview** tab.

c. **Update** or configure the timeline filters as required.

d. Use the **Show Images** checkbox to either include or exclude the images from the timeline. If unchecked, then only the names of the images are included in the timeline section.

e. Use the **Show Child Tasks** check box to list all the child tasks associated with the security incident.

5. **Save** the configuration and click **Preview** tab to preview and download the report.
6. Click **Download** to directly download the report.

Configure an assessment trigger condition

Define rule conditions and generate required and optional assessments for specific security incidents.

Before you begin

Role required: sn_si.admin

Note: To use the Post Incident Review Assessment Trigger Conditions feature, you must upgrade to Security Incident Response 11.0. Before upgrading, you must revert any customizations done to the Post Incident Review Metric type and trigger conditions. In addition, you may also have to revert the customizations done to the business rules specific to the post incident review.

- Require assessments to be complete
- Store assignee

Procedure

1. Navigate to **All** > **Security Incident** > **Administration** > **Post Incident Review - Assessments Setup**.
2. In the **Assessment Trigger Conditions Configure** section, click **Configure**.

   Note: On the Assessment Configurations form, and within the Assessments Configurations section, the **Generate assessments** check box is selected by default.

   - When you select the check box, an optional assessment is created for every security incident.
   - When you deselect the check box, the assessments are not generated. The assessment rules are not displayed and you cannot configure conditions for the security incidents.

3. On the Assessment Configurations form, in the Conditions section, specify the required information.

   a. In the **Name** field, specify the rule name.

   b. In the **Fulfilment** field, specify the fulfilment type.

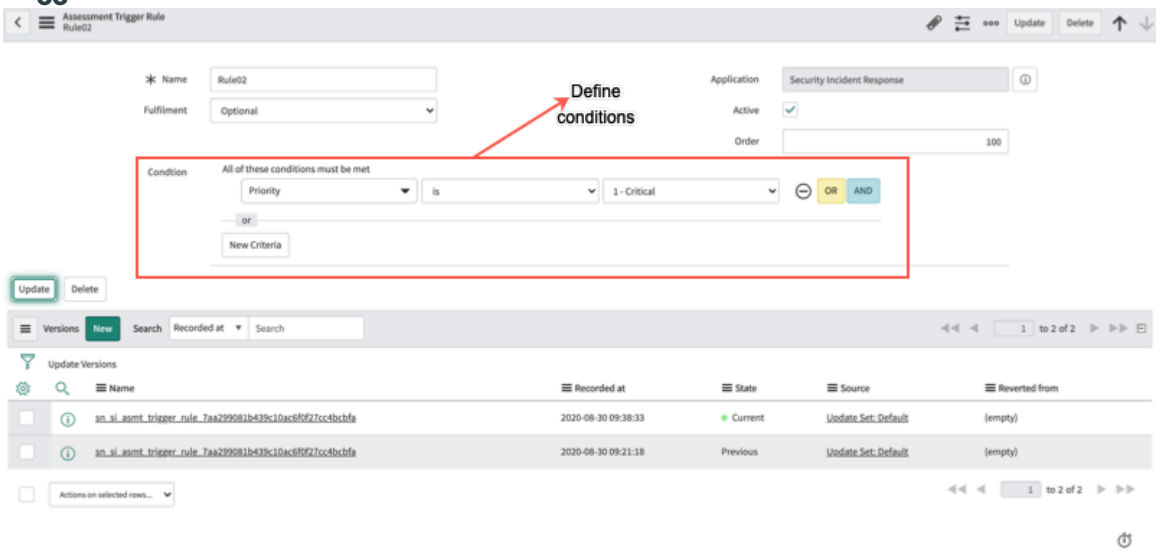
   c. To configure a condition, click the rule record and define conditions in the **Condition** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- If you create a rule without defining a condition in the **Condition** field, then the condition is evaluated as true and the rule is applicable for all security incidents.
- You can define a specific rule to make the assessments either mandatory or optional, and the assessments are not generated for the remaining security incidents, which don't match the defined rules.

Trigger conditions



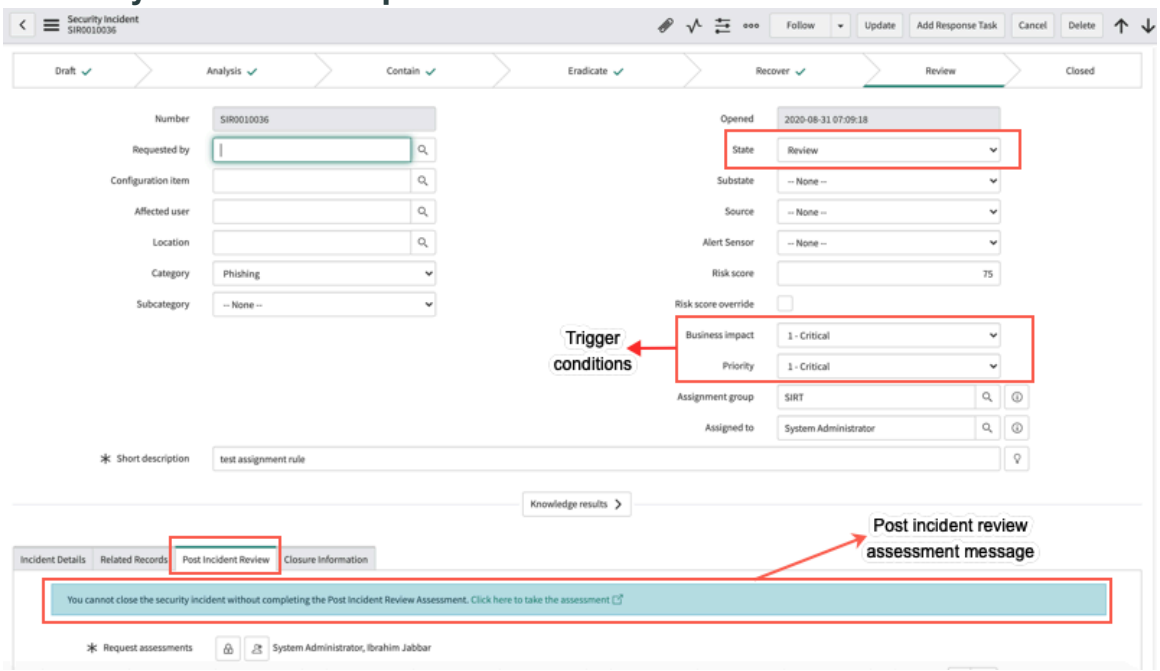
Assessment trigger conditions examples

The following examples provide different scenarios on how mandatory and optional assessment trigger conditions are generated.

- On the Assessment Trigger Condition form, generate mandatory assessments when the **Priority** and **Business Impact** for a security incident is set to **Critical** on the **Assessment Trigger Rule** page. In such scenario, the security analysts cannot close the incident until the mandatory assessments are completed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mandatory assessment example



- As you can see, in this example, If a security incident is in a **Review** state, security analysts cannot close the security incident without completing the **Post Incident Review Assessment**. An assessment link is available to take the assessment to the security analysts who are assigned (or who had requested for the assessment) to the incident.
- On the Assessment Trigger Condition form, generate optional assessments when the **Priority** and **Business Impact** for a security incident is set to **High**. In this example, if the security analysts do not complete the assessments and close the security incident, the assessments are automatically canceled.
- In case, if the mandatory or optional assessments does not match the security incident, assessments are not generated for such security incidents. A security analyst can close the security incident without completing the Post Incident Review assessment.

Perform a questionnaire-based post incident review

You may decide that a post incident review of the security incident is warranted. A post incident review describes what happened, helps to determine why the incident occurred, and identifies how it can be avoided or handled in the future.

Before you begin

Role required: sn_si.admin, sn_si.manager, sn_si.analyst

Note: Any user can participate in a post incident review questionnaire, regardless of role. Roles can be assigned to a review.

About this task

The ServiceNow Security Incident Response application can automate the collection of post incident review information from everyone involved with a security incident by using questionnaires. If you decide to use a questionnaire as part of a post incident review, a list of questions, relevant to the security incident, is sent to the user-defined list of participants. As each user completes the questionnaire, the post incident report is automatically generated. The report compiles all the information related to the security incident, as well as all responses to the post incident review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

While an initial list of questions is provided with the base system, they are customizable. You can create categories and add new questions to them, or you can change individual questions within existing categories. You can ask questions based on roles. You can define when certain questions are asked. There can be questions you ask only for your UNIX servers, for example, or only when there is criminal activity. You can define questions that are asked depending on the answer to another question or on the value in a field on the form. There can even be questions that are filled in entirely by querying the database.

After the security incident is resolved and moved to **Review** state, assessments are generated for all assigned users and users who are directly added from the **Request assessments** list.

The questionnaire can be a helpful tool for gathering information about the handling of the security incident from various sources.

During the review, you can add more users to the list or remove existing users from the list, unless they have already started filling out the questionnaire. If you add new users to the list, they receive the questions when the record is saved. The security incident cannot be closed until all questionnaires have been completed. As questionnaires are completed by each user, the post incident report is automatically generated (and regenerated) and displayed on the **Post Incident Review** tab.

To start a post incident review:

Procedure

1. Create a security incident, or open an existing one by navigating to **Security Incident** > **Incidents** > **Assigned to Me (or Assigned to Team or Unassigned Incidents)**.
2. Click the **Post Incident Review** tab.
3. The **Request assessments** field defaults to the individual in the **Assigned to** field.
   Click the lock icon to add other users to the review list. After the field is unlocked, options are available for adding or removing multiple users, roles, or entering user email addresses.
4. When you have completed your entries, click the lock icon to lock the field.

   Note: You can also define conditions which, when met in a security incident, can cause specific users to be automatically added to the **Request assessments** field for that security incident. For example, when a security incident **Category** is changed to **Phishing**, specific individuals who have expertise in phishing threats can be added to the post incident review list. For more information, see Create PIR assignment rules.

5. Click **Update**.
   When the incident goes into the **Review** state (or immediately, if it is already in the **Review** state), each of the users in the review list receives an initial email notification. Reminders are sent as the due date nears. When each user accesses the questionnaire from the email link or by going to **Post Incident Review** > **My Pending Reviews**, the questions shown are drawn from all categories that fit this security incident. If new users are added to the review list before the due date is reached, they are sent notifications when the security incident is saved.

   As users complete their questionnaires, the post incident report compiles the data and displays the report in the **Post Incident Review** tab. The questionnaire data is displayed in the **Findings** tab.

Create post incident review questionnaire categories

You can use the questionnaire categories that come with the base system or create your own categories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn.si_admin

About this task
To create a new category of questions:

Procedure
1. Navigate to **All** > **Security Incident** > **Post Incident Review**.
2. Click **Review Questions**.
   A list of categories is displayed, along with their order and filters that define under what conditions the questions are asked (for example, only when the security incident category is *`Criminal activity`*). Each category is a section in the post incident review questionnaire and the questions in each category are included only when the security incident matches the Condition filter. For example, for a category of questions applying only to Linux servers, you would set up a filter that selected security incidents where the affected resource type was Linux Server. In that category, you would then create all questions needed when a security incident was on a Linux Server. You use one of the categories supplied in the base system or create a new category. This procedure assumes that you want to create a new category before defining questions.
3. Click **New** in the list of categories.
4. Fill in the fields on the form, as appropriate.

Security incident

Field	Description
Name	Name for the category that appears on the security incident questionnaire.
Type	Post Incident Review is the default.
Create Stakeholders	Unused by Security Incident Response.
Table	This field is auto-assigned once the form is submitted.
Filter	Enter the condition that determines when questions in this category are used. If a security incident record matches this filter, the questions is included in a post incident review for that security incident. Filters can use any data on the record, or on other records linked to this record. For example, the department of the requesting user's manager.
Application	Scope application for the incident.
Weight	Numeric value that represents the importance of this metric relative to other metrics in the same category. By default, the weight is 10.
Total Metrics	Number of metrics used by the category.
Description	Description of the questionnaire.

5. Click **Submit** to save the category.

Compose post incident review questions
You can use the questions that come with the base system or create your own questions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.admin

About this task
The methods for gathering post incident review information can be in the form of questions or as data automatically collected using scripts.

Questions can depend on the answers to other questions. For example, you might ask if all necessary logs were available. If the answer is No, you ask a follow-up question to ascertain which of the needed logs were not enabled.

Scripted data collection, also called script metrics, gather data related to the security incident via scripts you write. This action can go well beyond the data in the security incident record itself. For example, a script metric could gather the recent outage time for a server affected by this security incident.

Finally, you can mix the two types. Questions can have default values taken from a script, or simply from a field in the security incident record. When you use a `Default Answer from...` type of question, you can choose if you want the user to always answer the question – with the default value providing them an initial value – or if you want the user to only be asked the question if the script or field comes up empty.

To create a new question:

Procedure
1. Navigate to **All** > **Security Incident** > **Post Incident Review**.
2. Click the category for which you want to create a new question.
3. Click the **Assessment Metrics** tab.
4. Click **New**.
   You can also click an existing question to modify it.
5. Fill in the fields on the form, as appropriate.

Metric form

Field	Description
Name	Name of the metric (question or script). If the metric is a scripted data collection, this name appears on the post incident report.
Category	The category that the metric belongs to. The system automatically populates this category if you create a new metric from the Metric Category form. **Note:** You cannot change the category if the **Depends on** field is set or if another metric depends on this metric
Method	Indicates the type of metric, as follows: ○ *`Assessment`*: A question that has no default value. There are several data types that can be defined in the **Data Type** field on the **Field Type** tab, such as check boxes, choice lists, text input. ○ *`Script`*: Scripted metric. Obtain values by writing a custom script. The *`Script`* method is compatible with the **Duration**, **Number**, and **Percentage** data types.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ *Default answer from field*: A question where the default response comes from a selected field in the security incident. Selecting this option adds two fields to the **General** tab: ▪ *Default answer*: Select the field in the security incident that contains the default answer for the question. For example, for the question: "Who initially reported this incident?", the **Requested by** field would be a likely choice. ▪ *Ask question*: Specifies when to ask the question: always or only if the **Default answer** field is empty. Using the example above, the question would be asked if the **Requested by** field is empty. ○ *Default answer from script*: A question where the default answer comes from a script. The answer may be a number, string, or percentage. The **General** tab adds a field: *Ask question*: as the Specifies when to ask the question: always or only if the script does not provide a default answer. The script is defined on the **Field Type** tab. **Note:** If you select a **Data type** that is incompatible with the selected **Method**, the system automatically changes the **Method** to a compatible value.
Weight	[Required] Numeric value that represents the importance of this metric relative to other metrics in the same category. By default, the weight is 10. This field is visible and required unless the **Data type** is **Date**, **Date/Time**, or **String**. These data types are not included in results calculations.
Order	[Required] Numeric value that determines the order of the metric question on assessment questionnaires, relative to other metric questions in the same category. The metric with the smallest order value appears as the first question in the category section. By default, the order is 100. **Note:** It does not matter which order value you use for metrics with the Script method, as they do not appear on questionnaires.
Active	Check box that determines whether this metric is used. If the check box is not selected, it is as if the metric record does not exist.
Mandatory	Check box that makes the metric question mandatory (selected) or optional (cleared) on assessment questionnaires. Users cannot submit questionnaires until they provide valid responses to all mandatory questions, which are denoted by a red field status indicator. This field is visible only if the **Depends on** field is empty, and the data type is not **Checkbox**.

6. Click the **General** tab and fill in the fields, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

General tab

Field	Description
Question	Text to use as the question on security incident review questionnaires. Enter a clear, straightforward question that is easy to answer, such as **How did we contain the incident**
Description	Information about the metric and what it evaluates. If the *Method* is **Assessment**, include details that help users understand how to answer the question. This text appears as a hint when a user points to the question text on the questionnaire.
Depends on and Displayed when	Select a question in the **Depends on** field that the current question depends on. For example, the question, "What additional logs were needed?" depends on the question "Were all needed logs available?" Next, use the **Displayed when** field to identify when you want the dependent question to appear in questionnaires. For example, if you want the dependent question to be asked only when the user answers **No** to the "Were all needed logs available?" question, select **No** in the **Displayed when** field. **Note:** The system prevents the creation of recursive dependencies between metrics. For example, if Metric A depends on Metric B, Metric B cannot depend on Metric A.

7. Click the **Field Type** tab and fill in the fields, as appropriate.

Field Type tab

Field	Description
Data type	The data type of the expected response the list of types available depends on for the selected method. If the method is **Assessment**, the data type determines how users answer the corresponding question on questionnaires. If the method is **Script**, the data type determines how the system calculates assessment results. **Note:** If another metric depends on this metric, you cannot change the data type.
Randomize answers	Check box that determines whether to present the answer options for this metric question in a random order each time a user opens an assessment questionnaire that contains the question. Answer preference can be influenced by the order in which answer options appear. This can result in biased results. Randomizing answer options can help prevent this bias. This field is visible only if you select **Likert scale** or **Choice** in the **Data type** field.
Dependent plugin	[Required if the *Method* is **Script**.] Plugin that contains the tables queried in the script. The system executes the metric script only if the plugin is active. The default

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	available values are **Asset Management**, **CMDB**, **Core**, **Cost Management**, **Procurement**, and **Software Asset Management**. This field is visible only if the *Method* is **Script**. **Note:** ○ If the Core default value is used, the script is always run. ○ If you are an administrator, you can add more choices of plugins to the field.
Scale definition	Setting that determines whether lesser or greater numerical values equate to a good score in assessment result calculations. Select **Low** if lesser numerical values are better, such as for a metric that measures the number of defects for a vendor. Select **High** if greater numerical values are better, such as for a metric that measures user satisfaction on a scale of one to five. The default value is **High**. This field is visible and required unless the *Data type* is **Date**, **Date/Time**, or **String**. The results for these data types are not included in results calculations.
Min	Lowest numerical value to be used as an answer option on assessments or as a scaled value in a scripted metric. This field is visible and required only if certain data types are selected. If the data type is **Choice** or **Likert Scale**, this field is read-only and is set automatically based on the smallest metric definition *Value*.
Max	Highest numerical value to be used as an answer option or scaled value. This field is visible and required only if certain data types are selected. If the data type is **Choice** or **Likert Scale**, this field is read-only and is set automatically based on the largest metric definition *Value*.
Script	Script that obtains the desired system information. The script has one input variable, set with the ID of the security incident (primary), and three possible output variables set by the script, string_result, scaled_result, and actual_result. When the data type is String, only the string_result is required. This field is visible and required when the *Method* is **Script**, or the default value comes from a script.
Template	A predefined set of common answers to use for the question. For example, a frequency template would likely start with a value of "Never," and go up to the top value of "Always." This field is visible and required only if the *Data type* is **Template**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If another metric depends on this metric, you cannot change the template.

8. **Optional:** When you have completed your entries, click **Update**.

Create PIR assignment rules

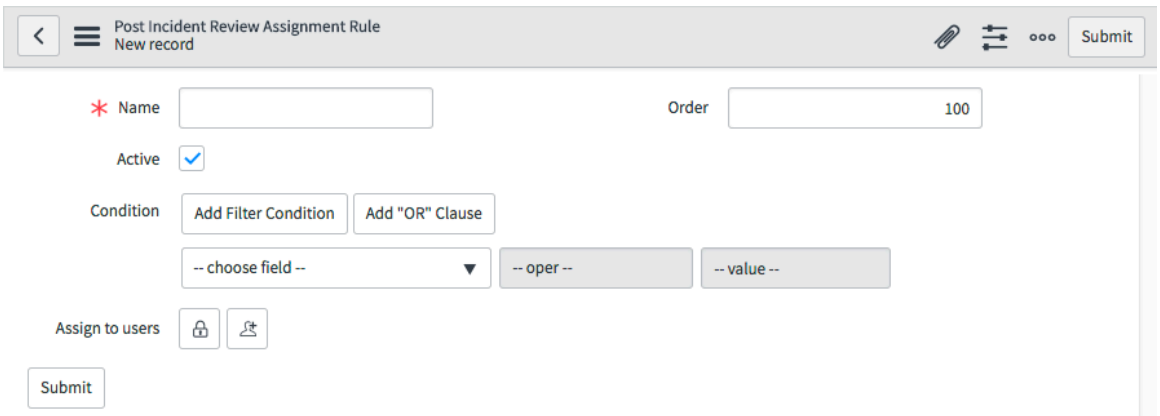
In addition to manually adding users post incident review assessment list for a security incident, you can define assignment rules for automatically adding users to the list.

Before you begin

Role required: sn_si.admin, sn_si.manager, sn_si.analyst

Procedure

1. Navigate to **All** > **Security Incident** > **Administration** > **Post Incident Review - Assessments Setup**.
2. Drill down to the **User Assignment Rules** section.
3. Click **Configure**.
4. Click **New**.



5. Fill in the fields, as needed.

Field	Description
Name	The name of this assignment rule.
Active	Select this check box to make the rule active.
Order	Enter a numerical value to specify where in the list of assignment rules this rule should appear. Lower numbers appear at the top of the list. **Note:** Only the first matching assignment rule is executed, and only the users defined in that rule are added to the assessment list.
Condition	Use the condition builder to define the conditions that must be met in the security incident for this rule to be executed. For more information, see the example below.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

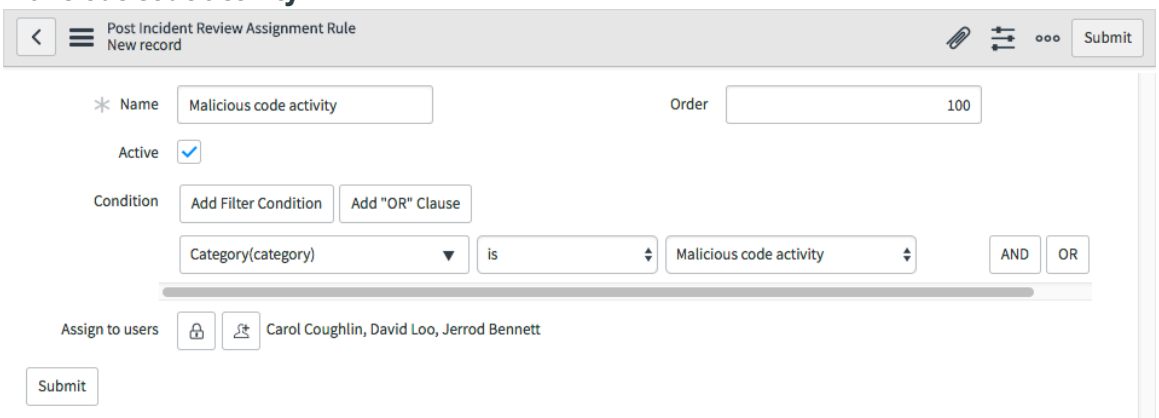
Field	Description
Assign to users	Click the lock icon to add users to the review list. After the field is unlocked, options are available for adding or removing multiple users, roles, or entering user email addresses.

6. Click **Submit**.

Example: Malicious code activity

In the post incident review assignment rule shown here, when a security incident with the **Category** field set to **Malicious code activity** transitions to the **Review** state, the three users identified (who happen to be experts in dealing with malicious code activity) are added to the list of users who will receive the post incident review questionnaire for this security incident.

Malicious code activity



Close security incidents

When a security incident has transitioned to the Review state, it's possible to close it and enter an appropriate closure code. Closure codes can be searched on later for ease of location.

Before you begin

Role required: sn_si.write

About this task

Procedure

1. If the security incident you want to close isn't already open, navigate to **Security Incident** > **Incidents** > **Show All Incidents**, and locate the security incident you want to close.

   Note: If there are any post incident review assessments that haven't been completed for this security incident, the security incident can't be closed. Return to **Security Incident** > **Post Incident Review** > **All Incomplete Reviews**, locate the reviews that are incomplete, and either ask the reviewers to complete their reviews or cancel the remaining assessments.

2. Select the **Closure Information** tab and fill in the fields, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident

Field	Description
Create knowledge article	The option to create a draft knowledge base article that contains the contents of the post incident review.
Close code	The close code that best describes the reason you're closing this security incident. ○ Investigation completed ○ Threat mitigated ○ Patched vulnerability ○ Invalid vulnerability ○ Not resolved ○ False positive
Closed by	Displays the user who closed the security incident after the record is updated.
Closed	Displays the date and time of closure after the record is updated.
Close notes	Additional notes that describe the outcome of closing this security incident.

3. Select **Update**.
4. The assigned user can manually change the **State** to **Closed**.

Note: To prevent users from modifying attachments on a closed security incident, enable the `sn_si.lock_attachments_on_closure` system property.

When a parent incident is closed, all response tasks belonging to the child incident are canceled. If there are no other types of tasks, the child incident is also closed.

Add closure information to a security incident

When a security incident is in the Review or Closed state, you can enter closure information.

Before you begin

Role required: sn_si.basic

Procedure

1. If it isn't already open, open the security incident you want to update.
2. Select the **Related Records** tab.
3. Fill in the fields, as needed.

Field	Description
Create knowledge article	The option to generate a knowledge article using the contents of the post incident report.
Close code	The close code that best describes the reason for closing the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Closed by	[Read only] Displays the user who closed the security incident.
Closed	[Read only] Displays the date and time the security incident was closed.
Close notes	How the security incident has been closed, including lessons learned, resolution, and so on.

4. Select any of the following tabs to further update the security incident:
   - Incident Details
   - Post Incident Review
5. Select **Submit**.

Restrict access to security incidents

Manage the access of the security incidents that contains sensitive information. You can enforce security incident restrictions to determine who can access a certain incident and limit the access only to specific users or groups.

Before you begin

Role required: sn_si.admin

About this task

Security incident restrictions enable you to hide critical security incidents from being accessed by other users in a particular organization. These restrictions enable you to provide a more granular way to control the security incidents a user can access. You can enforce a security incident restriction by enabling the **Enforce restriction** check box, and then selecting the users or groups who are allowed to access the particular security incident.

After you enforce the restriction on specific security incidents and limit the access to certain users or groups, then all the other remaining users in your organization won't be able to access these security incidents even if they search for a particular restricted security incident.

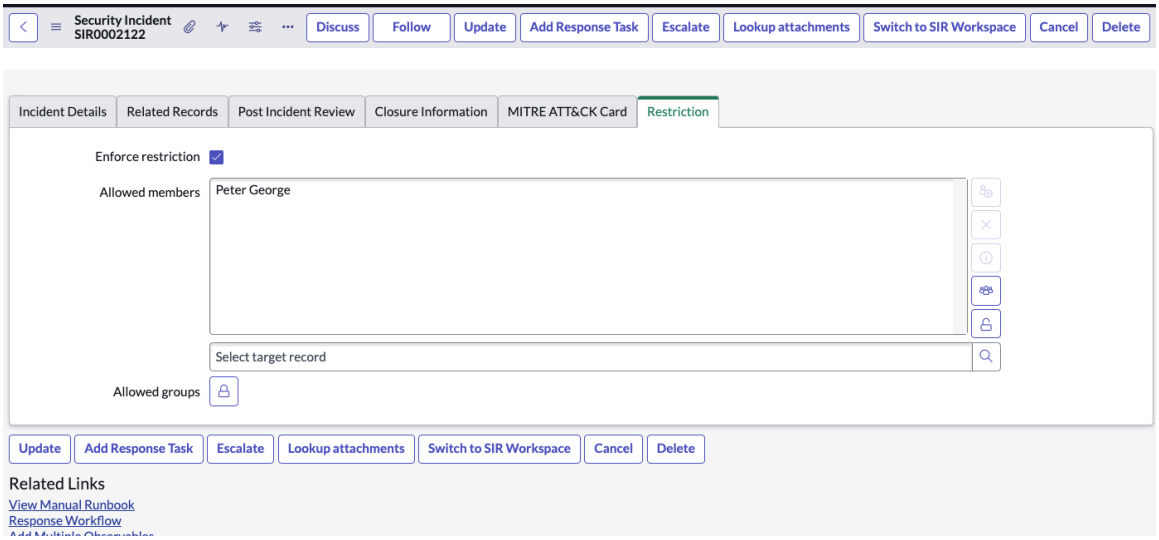
Procedure

1. Open a security incident that you want to restrict.
2. If you are using classic UI, perform the following:

   a. Click the **Restriction** tab.

   b. Select the **Enforce restriction** check box to enable the restriction of the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. In the Allowed members field, click the icon to select the users who can access the security incident.

d. Select the icon to add yourself as the allowed user.

e. Select the icon to add or remove users.

f. In the Allowed groups field, click the icon to select the groups who can access the security incident.

g. Select the icon to add or remove groups.

> **Note:** After the **Enforce restriction** check box is enabled for the security incident, only the sn_si.admin and allowed members or groups will have access to the security incident.

h. Click **Update**.

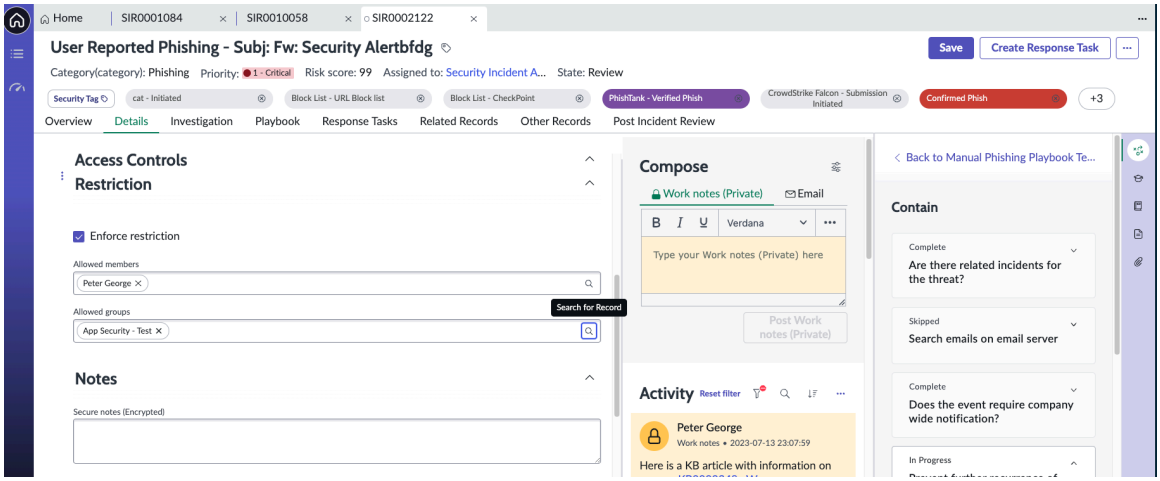
3. If you are using SIR Workspace, perform the following:

a. From the security incident, click the **Details** tab.

b. Scroll down and click the **Restriction** section.

c. Select the **Enforce restriction** check box to enable the restriction of the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



d. In the Allowed members field, select the users who can access the security incident using the Search option.

e. In the Allowed groups field, select the groups who can access the security incident using the Search option.

> **Note:** After the **Enforce restriction** check box is enabled for the security incident, only the sn_si.admin and allowed members or groups will have access to the security incident.

f. Click **Save**.

Manage security threats using the Security Analyst Workspace

Security Incident Response includes a new user interface called the Security Analyst Workspace that features powerful tools for assisting in analysis, including the playbook, peek view, and tabs for working on multiple security incidents.

Purpose-built for security analysts, the powerful tools in the Security Analyst Workspace allow you to analyze the ever-growing volume of data associated with security incidents. And automated actions significantly reduce the security incident investigation time, which can be the difference between stopping an attack and suffering a breach.

Before using the Security Analyst Workspace

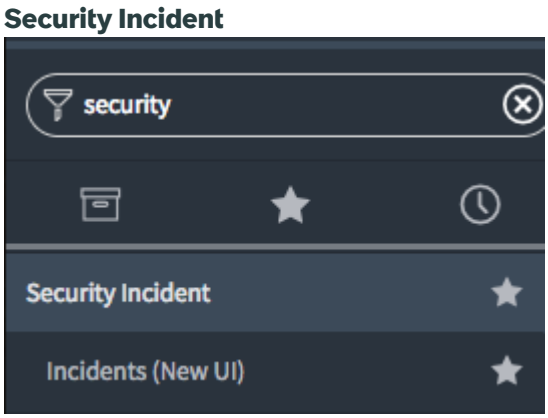
Before you can begin using the Security Analyst Workspace, you must ensure that your instance has at least London Patch 3 installed, you have the correct roles defined, and have downloaded the Security Incident Response UI application from the ServiceNow Store.

> **Note:** If your instance is running a version earlier than London Patch 3, you must request the Security Incident Response UI plugin through the HI Customer Service system.

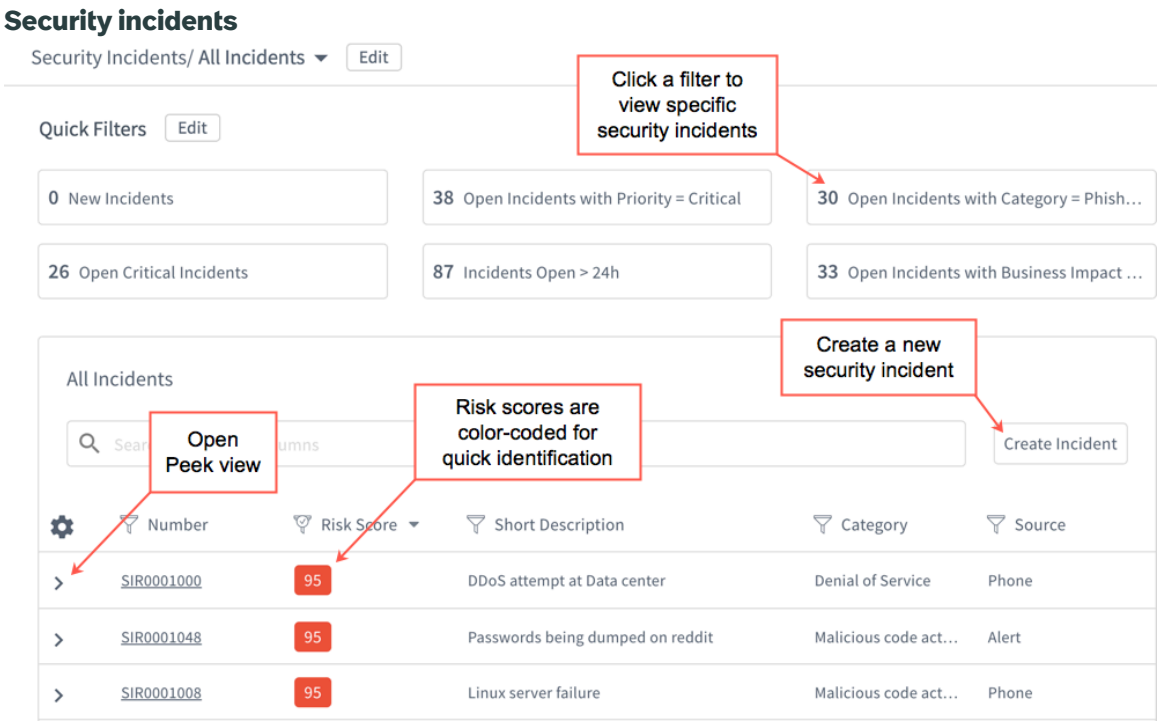
Access the Security Analyst Workspace

To access this new workspace, navigate to **Security Incident** > **Incidents (New UI)**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

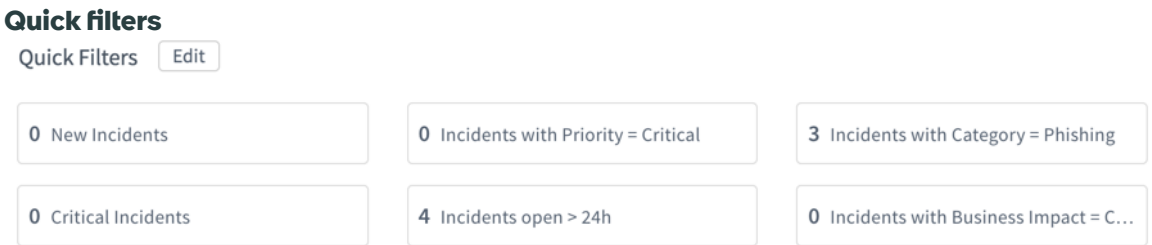


The workspace opens in a separate browser tab.



Locate the security incidents you want to analyze with Quick Filters

The Security Analyst Workspace provides several tools for filtering the list of security incidents so you can quickly find the security incidents you want to analyze. The Quick Filters let you select a subset of the security incidents based on criteria in the filter.



Simply click the quick filter you want to use.

Note: You can click an **Edit** button to identify which quick filters you want displayed on the list screen. A minimum of one filter must be selected, up to a maximum of six.

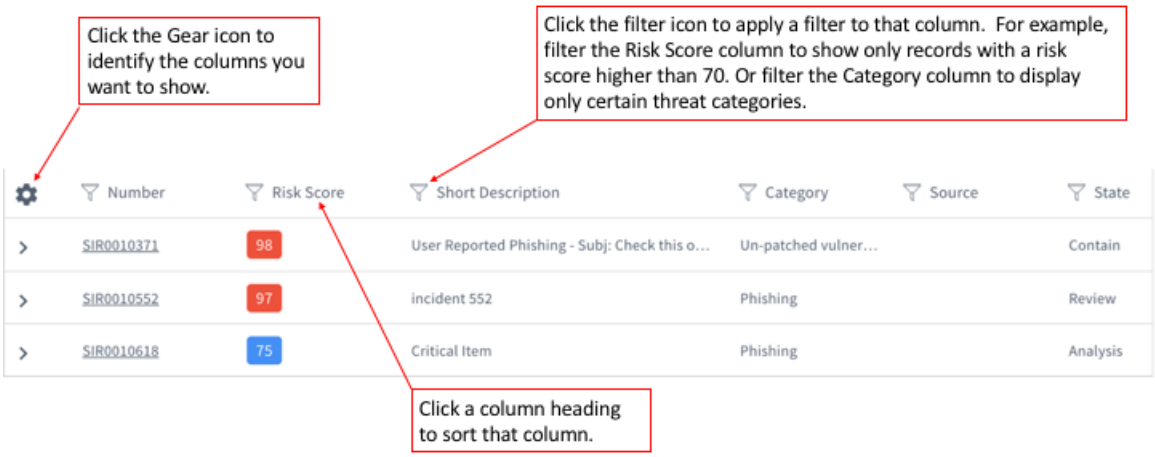
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can define additional quick filters, as well as primary filters for the Security Analyst Workspace, using the classic environment. For more information, see Set up primary and secondary filters for Security Analyst Workspace.

Personalize the security incident list

As with all lists in your instance, the Security Analyst Workspace provides tools for personalizing the list and sorting the information displayed to meet your analysis needs.

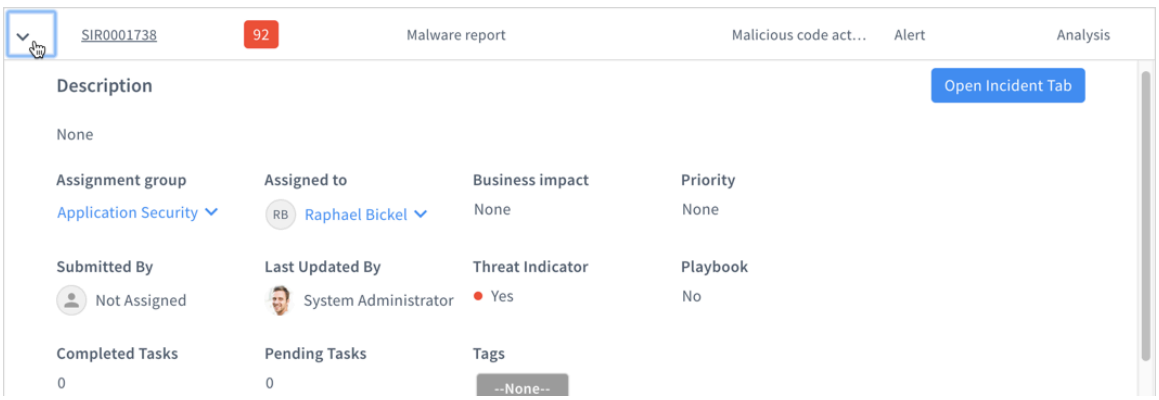
Personalize the security incident list



Save time with Peek view

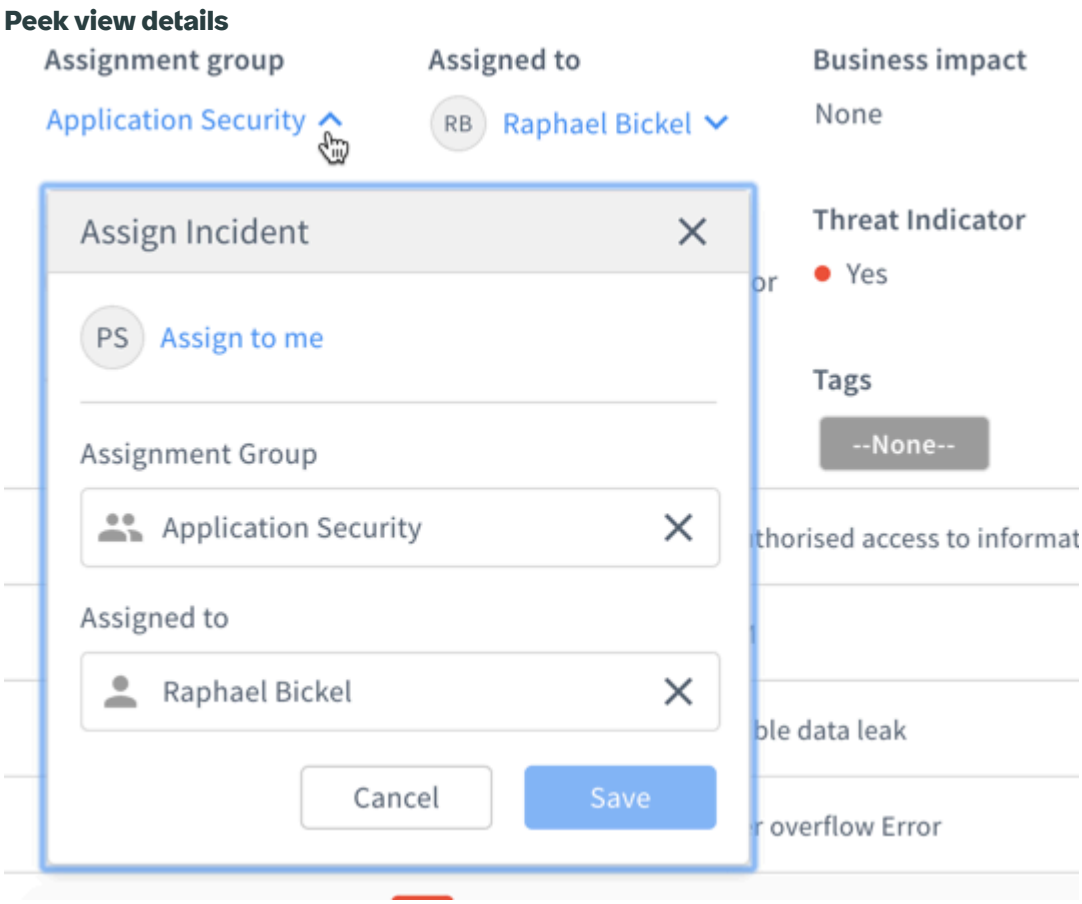
Before opening a security incident record, you can save time using the Peek view. This feature allows you to quickly locate vital security artifacts without having to reload the entire page. Simply click the **>** icon to the left of a security incident number to take a peek.

Peek view



The peek view provides a snapshot of vital information in a single view. This view can save valuable time when you are working with multiple incidents. You can click the down arrows on certain fields to make on-the-fly updates, such as assigning an assignment group or a specific analyst.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Perform quick actions on a security incident

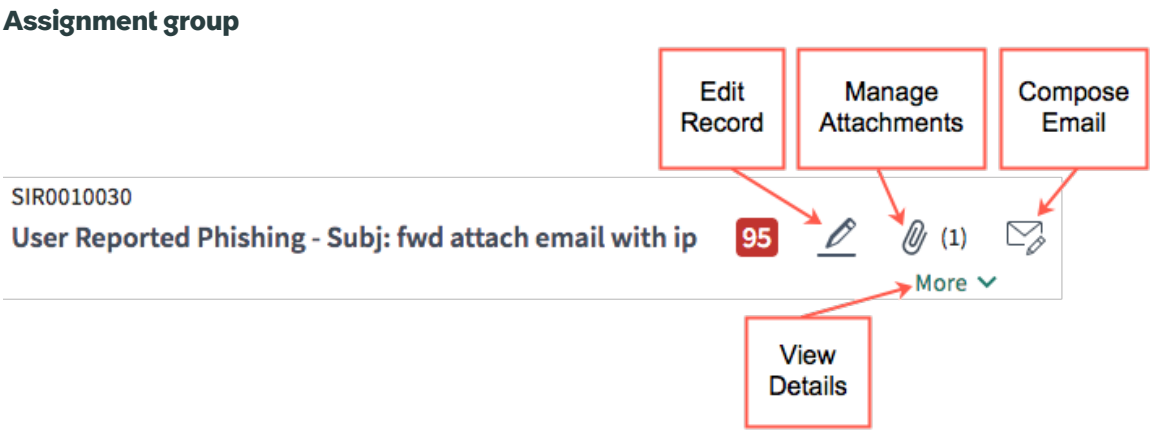
After you have selected and opened a specific security incident, you can perform time-saving actions on the record.

- If you security incident is open, click the **Edit Record** icon to make quick changes to any of its fields. If the record is closed, you can change only its tag.
- Click **Manage Attachments** to attach files to the security incident. You can also download or remove attached files and edit the encryption applied to the attachments.
- Click **Compose Email** to send a quick email to a colleague. Emails can be free-form, or you can send canned emails selected from a list of templates. Emails sent and replies received are captured in the Incident Timeline.

  Note: You can create custom templates that contain reusable content for emails and email notifications. Variables can be used for inserting information specific to the security incident or alert, such as the subject line, priority, or threat category. Use the Security Incident [sn_si_incident] table for emails and email notifications related to Security Incident Response. For more information, see Email templates

- Click **More** to view a quick snapshot of the security incident, such as the description, business impact, and priority. You can also click the down-arrow in the **Assignment group** and **Assigned to** fields to make on-the-fly changes to those fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Work with multiple security incidents

The tabbed interface allows you to keep several security incidents open simultaneously so you can switch between them with a single click. This can save time and allow you to see the big picture when threats from multiple sources are identified.



View analysis information in the security incident tabs

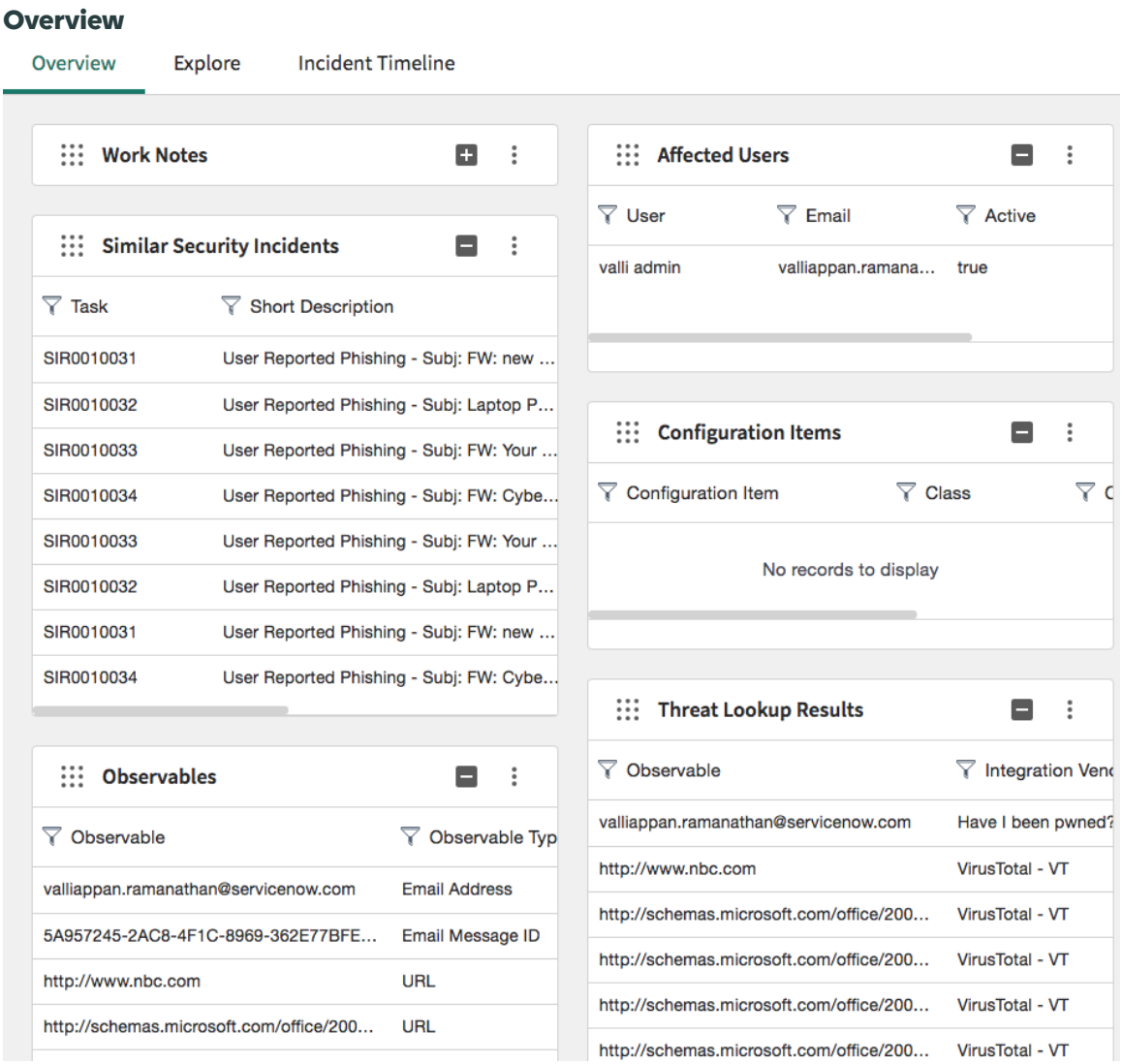
When you open a security incident record, three tabs are shown:

- Overview
- Explore
- Incident Timeline

Overview tab

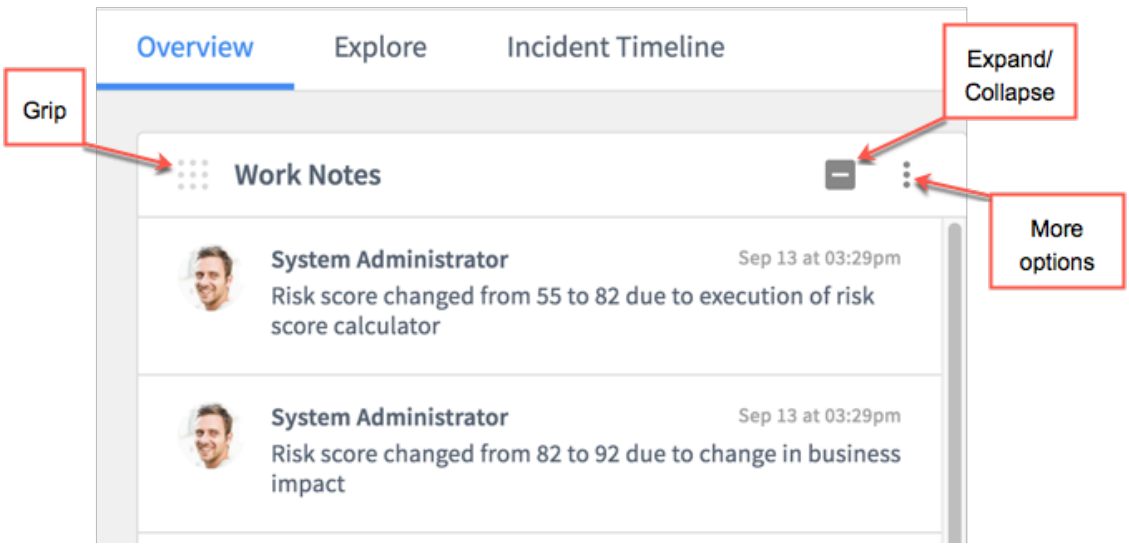
Use the **Overview** tab to view information in a security incident in a single location. No need to open another application or console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The tiles that are displayed on the **Overview** tab are customizable. You can collapse and expand them as needed, and you can move them around by dragging the **Grip** icon. Click the **More options** icon to delete a tile or change its heading text.

Overview tab

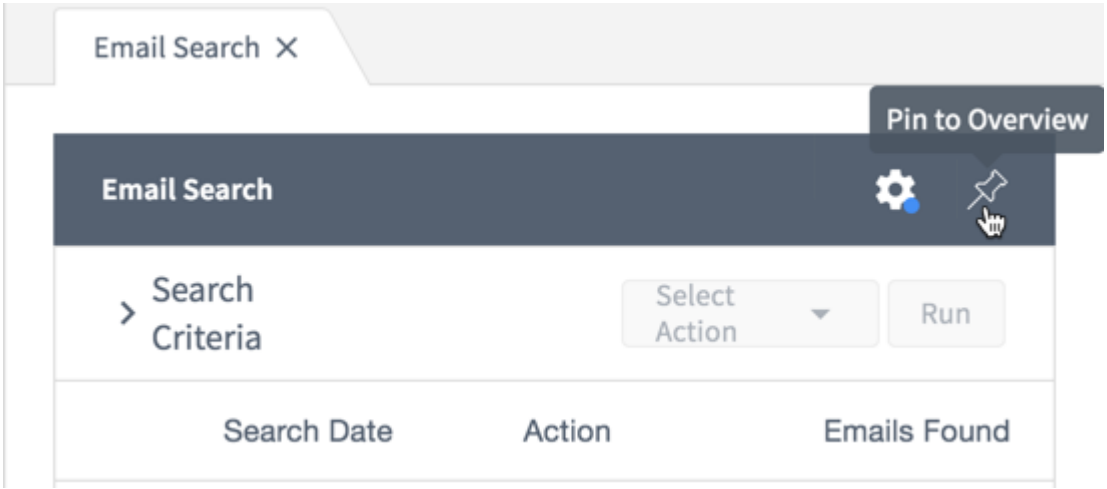


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Explore tab

Configure the tiles displayed on the **Overview** tab using the **Explore** tab. Simply select the tiles you want to view from the left-hand pane, and click the **Pin** icon. Pinned tiles automatically appear in the **Overview** tab.

Expore tab



The left-hand pane of the **Explore** tab includes a wide variety of information that you can display on the **Overview** tab. For example, expand **Observables** to display these related lists.

- Observables
- Threat Lookup Results
- Security Scan Results
- Domain Lookups
- Observable Enrichment

Additional related lists are available under **Users**, **Configuration Items**, and **Incidents**.

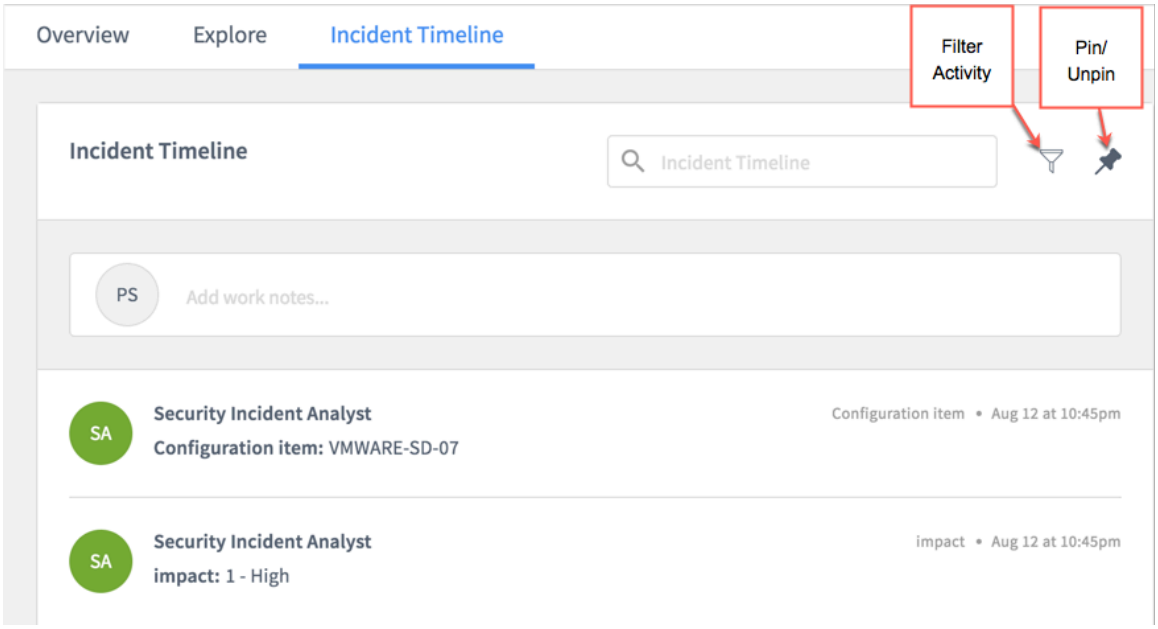
Incident Timeline tab

Use the **Incident Timeline** tab during your investigation for tracking purposes. Every time an action is performed on a security incident, the system records it in the Incident Timeline.

- You can also manually add worknotes to the timeline by typing them in the **Add work notes** box and clicking **Post**.
- You can search for a specific timeline activity using the Search box.
- The **Filter Activity** icon allows you to display only the types of timeline activity you want to see (for example, only incidents created by a specific analyst).
- You can add or remove the Incident Timeline from the **Overview** tab using the **Pin/Unpin** icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident Timeline tab



Handle security incidents using the Playbook

Resolve certain types of security threats in a step-by-step manner using the built-in Security Analyst Playbooks. For example, an analyst can use the playbook to resolve phishing attacks and threats caused by malicious code activities. For more information, see Resolve security threats with the playbook.

Resolve security threats with the playbook

Use the Playbook to resolve certain types of security threats in a step-by-step manner. For example, you can resolve phishing attacks and threats caused by malicious code activity using playbooks.

Before you begin

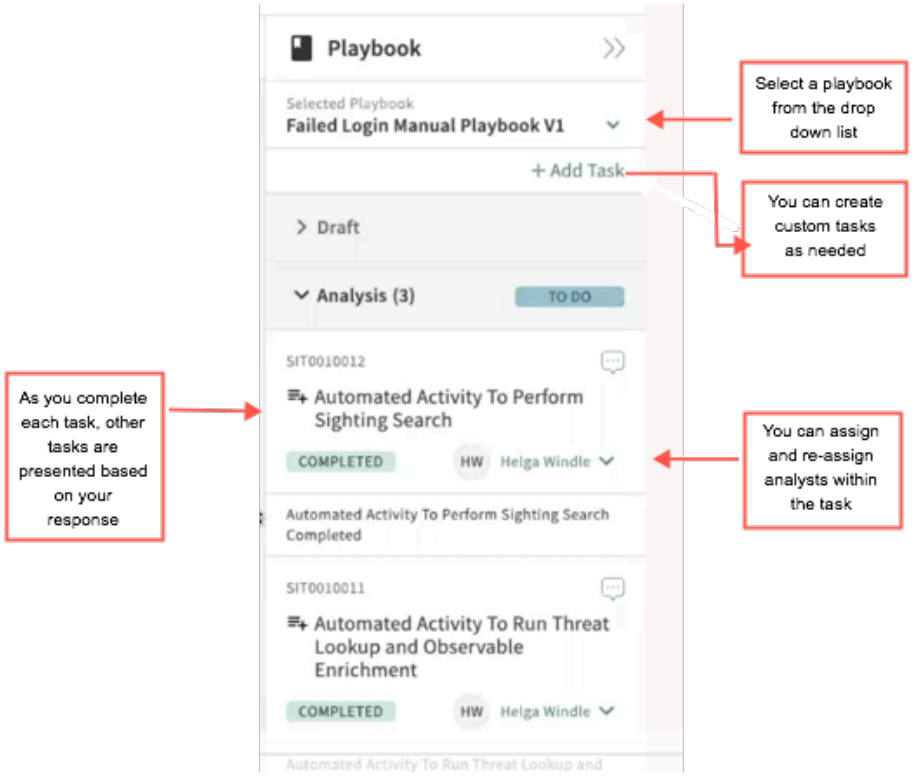
Role required: sn_si.admin or admin

About this task

Each group of tasks (Analysis, Contain, and so forth) leads you through a series of questions and other activities for resolving the threat.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

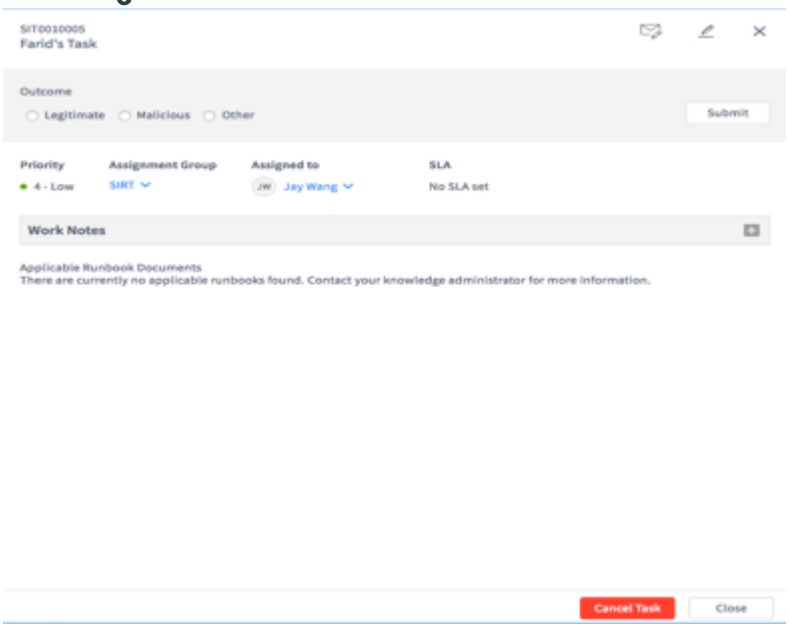
Playbook



As you work through each task, enter work notes to help analyze similar attacks in the future. After a threat is identified, you can also use information in the playbook to quarantine the threat, isolate similarly affected assets, and remove malware.

Knowledge articles, included in each task, provide tips and other information to help you perform the needed steps.

Knowledge articles



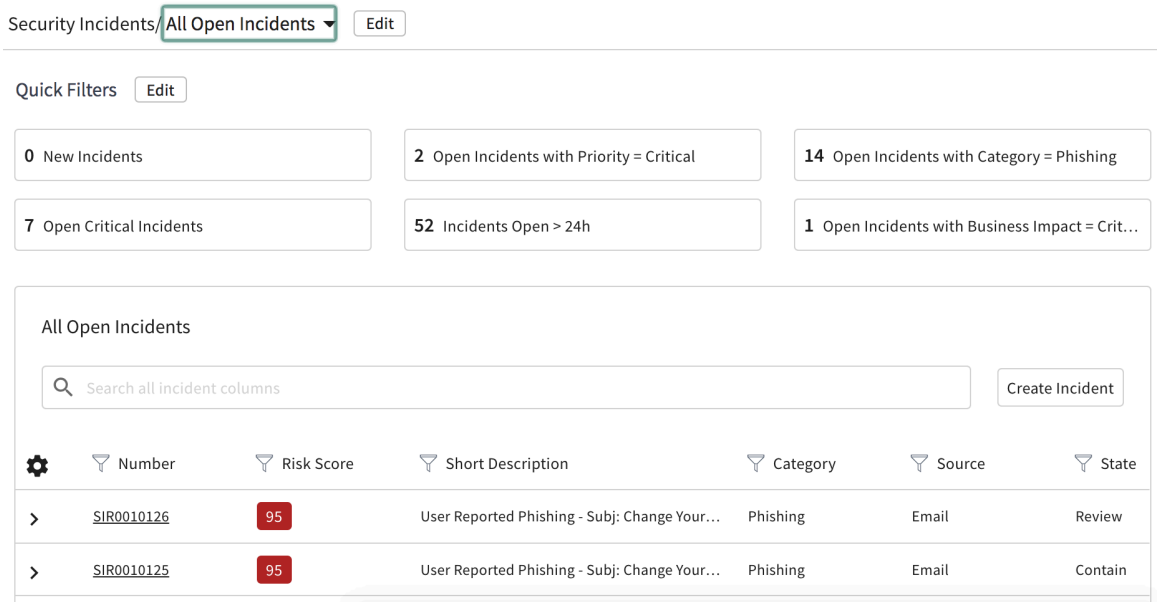
The base system includes knowledge articles for each of the playbook tasks. You can, however, write your own knowledge articles and associate them to playbook tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For an example of how to use the playbook to analyze and resolve a specific threat, see Resolving user-reported phishing attacks with the playbook.

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents (New UI)**.
   The Security Incidents screen shows security incidents that have been assigned to you.



2. You can click the **Assigned to me** choice list to select a different filter, such as all open incidents or all unassigned incidents.
   Alternatively, you can click one of the Quick Filters to view security incidents of a particular type, such as only Critical incidents.
3. Click the security incident you want to analyze.

   Consider prioritizing security incidents with high risk scores.

4. If the playbook pane on the right-hand edge of the screen is closed, click the playbook icon ( ) to open it.
   If no playbook is assigned to the security incident, you can select a playbook from the Selected Playbook choice list as shown below:



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can also assign a different playbook to the security incident. To include a playbook in the Selected Playbook choice list or to change the playbook for a security incident, see Enable playbooks for analyst selection for details.

The playbook specific to the type of security threat opens. It is divided into categories of similar tasks. For example, you use the tasks in the **Analysis** group to determine the validity and scope of the threat. The **Contain** group includes tasks for isolating the threat to a specific user or asset. The tasks in the **Eradicate** group guide you through the process of removing the malware or reimaging the host.

5. Click the first group (**Analysis**), and then click the first task in the playbook.
6. Follow the prompts in the task.
   - Some tasks ask a question, such as "Is Email Part of Campaign?" Perform the necessary analysis to answer the question, and select **Yes** or **No**.
   - If you have defined knowledge articles and associated them with playbook tasks, the articles appear when you start work on a task.
   - Some tasks are transitional. They simply instruct you to perform an action, such as adding observables to a security incident. After you complete the action, click **Mark as Completed**.

   As you complete tasks, subsequent tasks are presented to you based on the choices you make. Grayed out groups (such as **Recover**, **Review**, and so forth) may be activated by your choices.
7. Continue working on each task presented to you until you have completed all tasks to resolve the threat and close the security incident.

Related topics

Add a custom task to the playbook

Resolving user-reported phishing attacks with the playbook

The Phishing playbook guides you through the tasks necessary for analyzing and resolving a phishing attack reported by one of your company's employees.

How security incidents are created from user-reported phishing attacks

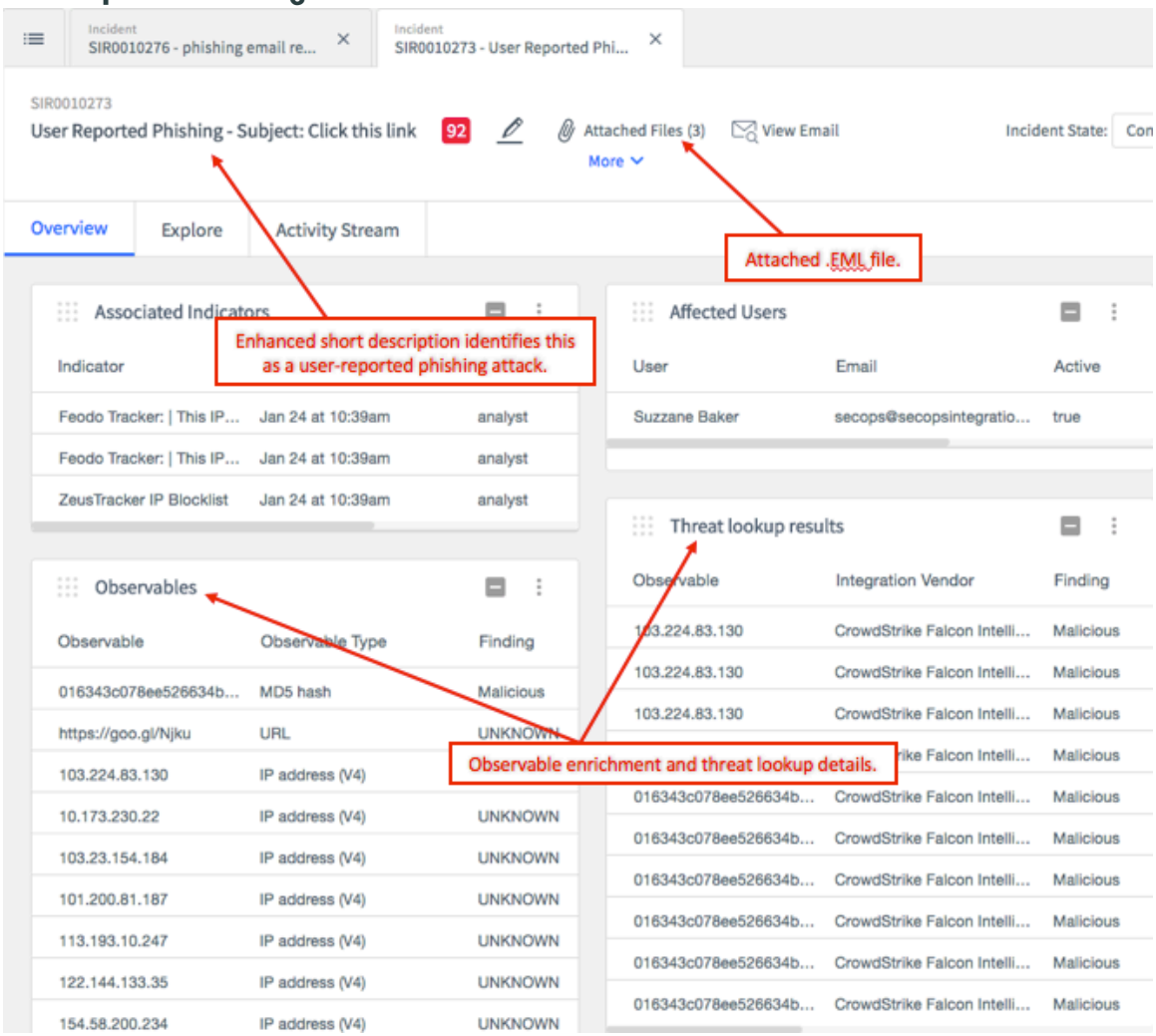
During Security Incident Response setup, your system administrator creates a series of email matching rules that can identify emails that contain signs of a phishing attack. When employees receive a suspicious email that contains the common signs of a phishing attack (as defined by your security policies), they can send it as an .EML attachment to the phishing email address defined by your organization.

When the email is received at the phishing email address, the .EML attachment is parsed and its information is compared to the email matching rules. If a match is found, a security incident containing the following information is created:

- The short description includes User Reported Phishing, followed by the actual subject from the originating email.
- The .EML file is attached to the security incident.
- If the .EML contained any observables, they are parsed, and enrichment and threat lookups are automatically performed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

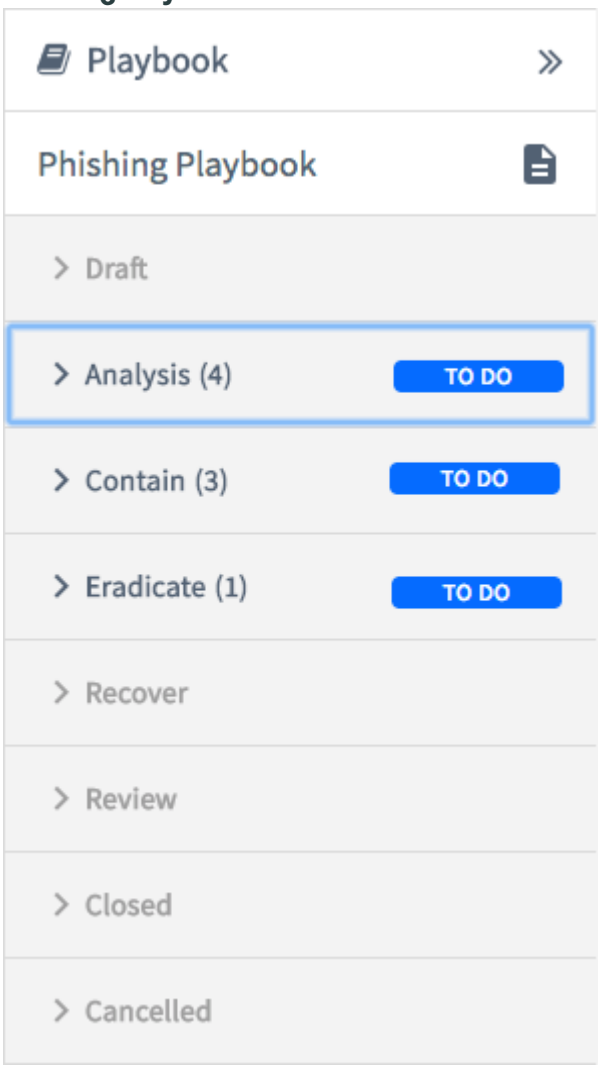
User Reported Phishing



When a Phishing category security incident is opened, the Phishing Playbook is automatically available. Simply click the playbook icon ( ) to open the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Phishing Playbook



The Phishing playbook contains tasks to help you analyze, contain, and eradicate a phishing threat. The tasks are organized into states (for example, **Analysis**, **Contain**, and so forth). When all tasks for a state have been completed, the playbook guides you to the next state.

Analyzing security incident details

When the security incident is in the Analysis state, you are given tasks to perform basic investigation of the incident, including:

- Determining the validity of the incident.
- Studying the impact of the potential threat.
- Coordinating an effective response to the incident.

As you work through the tasks:

- Familiarize yourself with the knowledge articles.
- Open the email attachment and examine it for signs of common phishing elements.
- Review threat lookup results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Containing the security incident

When the security incident is in the **Contain** state, you are given tasks to review the details of the email. To ensure that threats cannot enter your organization, update your network defenses, in the form of Intrusion Defense System (IDS) and Intrusion Prevention System (IPS) signatures and rules.

As you work through the tasks:

- Take actions to limit threat impacts, such as isolating the impacted devices.
- Examine the observables attached to the email.
- Determine whether any email contents are associated with a known threat, including:
  - URL
  - Email sender
  - Phishing URL
  - IP address of the sender's SMTP server

Eradicating the malware

After you deploy updated signatures and rules to your antivirus solution, use the tasks in the **Eradicate** state to determine if malware is present and handle it accordingly.

As you are work through the tasks:

- Scan the endpoints of affected devices for the presence of malware.
- Remove any malware found.
- As a last resort, wipe and reimage the host devices.

Reviewing the security incident

If you have determined that a phishing attack was a false alarm when performing the Analysis tasks, the security incident moves to the **Review** state and you need to notify your users so they know it is safe to open the email attachment.

Closing the security incident

When all tasks in the playbook have been completed, the security incident is moved to the **Closed** state. You must enter closing comments before the incident can be closed.

Cancelling a security incident

When a security incident is in the **Review** state, and you have successfully informed your users that the email is not a threat, the **Cancelled** state becomes active and you can cancel the security incident.

Note: The Recover task is not used in the Phishing playbook.

Associate a knowledge article with a playbook task

As you analyze security threats using the Security Incident Response playbook, you can view knowledge articles for each task if defined by your organization. If knowledge articles are not present, you can create them and associate them with playbook tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

As you use the playbook in Security Incident Response, take note of the text associated with each task. For example, the first task in the Phishing category is **Was Alert Employee-Submitted?** This is the short description of the task and you need this text (exactly as it appears in the playbook) to associate a knowledge article with the task.

Role required: sn_sir.knowledge_admin, and either sn_si.admin or admin

Procedure

1. Navigate to **All** > **Security Incident** > **Catalog & Knowledge** > **Knowledge**.
2. Create and publish a knowledge article for a specific playbook task.
3. Navigate to **Security Incident** > **Manual Runbook** > **Create New Runbook**.
4. Create a runbook, filling in the following information:

Field	Description
Knowledge article	Select the published knowledge article you want to associate with the playbook task.
Table	Select Security Incident Response Task [sn_si_task].
Condition	Set the condition builder to: ○ **Option:** Select **Short description**. ○ **Operator:**Select **is**. ○ **Input value:** Enter the short description for the task, exactly as it appears in the playbook.

5. Click **Submit**.
   The next time you run the playbook and select this task, the associated knowledge article is displayed.

Related topics

Create a security incident knowledge article

Create a Security Incident Response runbook

Add a custom task to the playbook

The Security Analyst Workspace base system includes a series of tasks for each threat category. You can create custom tasks that meet the unique needs of your system or customers.

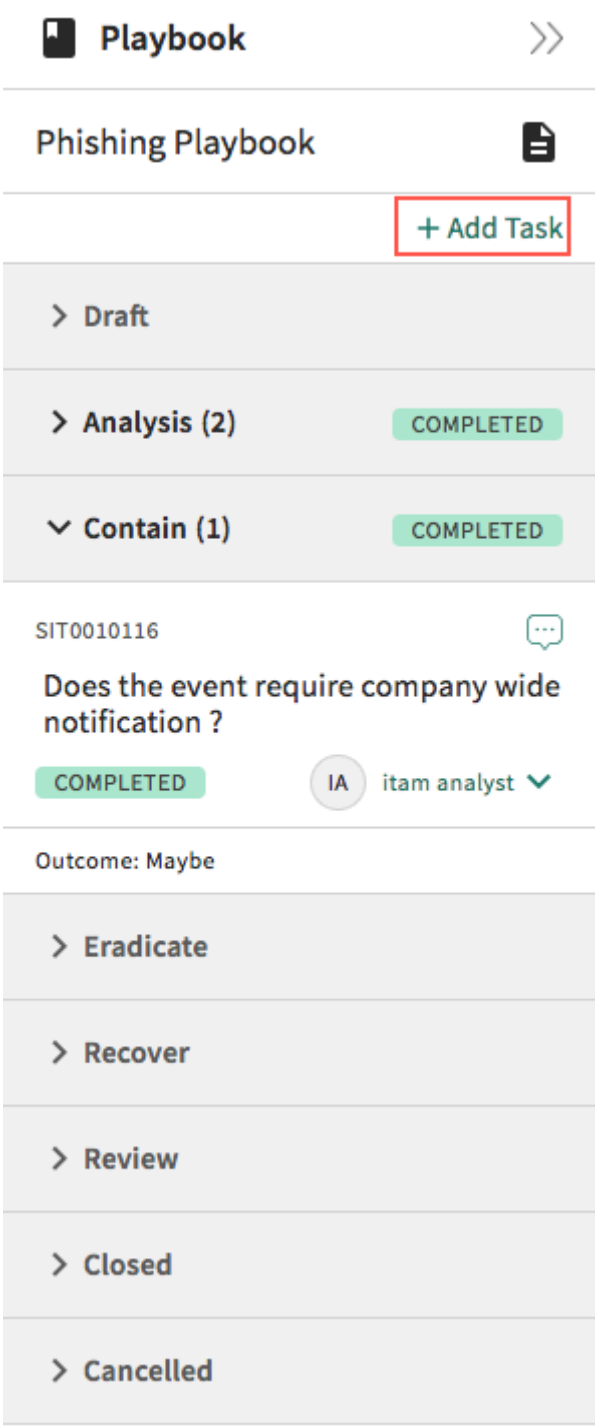
Before you begin

Role required: sn_si.basic or security_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

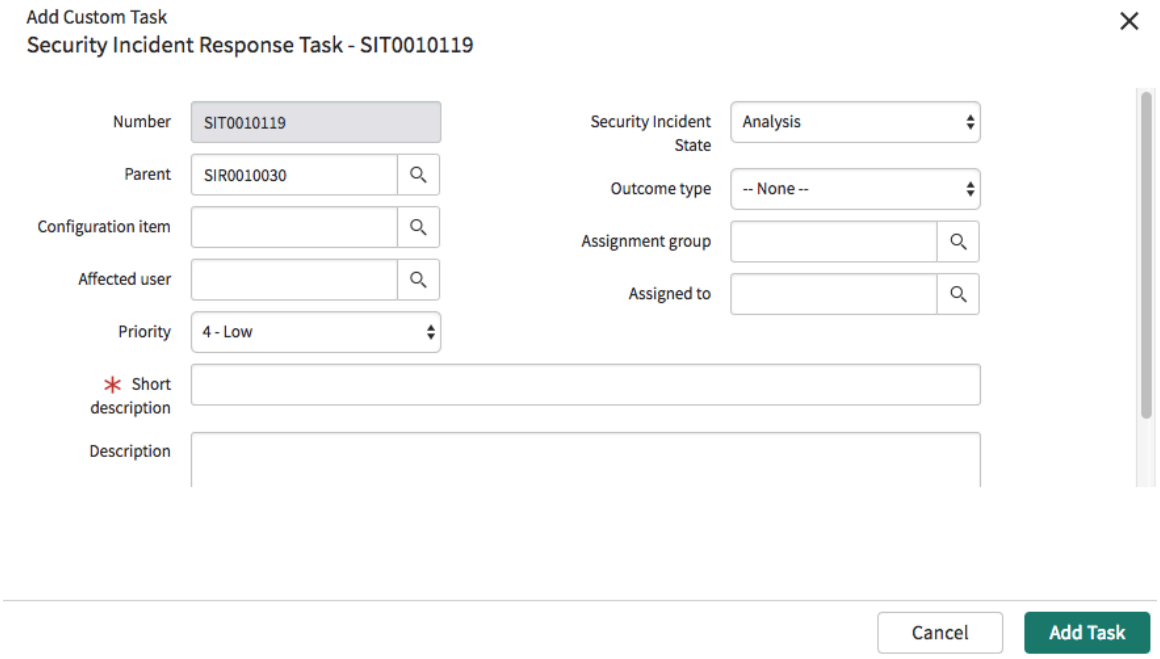
Procedure

1. With the playbook open, click **Add Task**.



The Add Custom Task screen opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Fill in the fields, as needed.

Field	Description
Number	[Read only] The automatically-generated security incident task number.
Parent	The number of the related security incident.
Configuration item	The configuration item affected by the security issue, if any.
Affected user	The user affected by the security issue, if any.
Priority	Select the priority used to determine when this task should be performed.
Security Incident State	The current state of the security response task. You can select a future state, if needed.
Outcome type	If you have the sn_si.basic role, select **Yes/No** as the outcome type. If you have the security_admin role, you can create a custom outcome type with multiple custom output values. For example, you can define a task with dependant values based on the threat category. For more information, see Choice lists
Assignment group	The assignment group from which the assigned worker will be selected.
Assigned to	The individual assigned to perform the task.
Short description	A description of the Security Incident playbook task.
Description	Enter a description for the selected task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. When you have completed your entries, click **Add Task**.
   The task is inserted in the playbook following the current task.

Sightings searches on user-reported phishing and malware attacks

Perform sightings searches on emails or observables to determine how often certain types of attacks, such as phishing attacks or communications with a malicious IP or URL occur in your network. Each occurrence is considered a sighting. Sightings searches for observables must be configured for your log stores or security information and event management (SIEM).

Watch this three-minute video to learn how to use the sighting search feature to locate phished users, and track phishing and malware observables within the log store on your network.

The following terms are used to describe user-reported phishing attacks:

- Phished user: A user who has received a phishing email.
- Victim user: A user who has interacted with the phishing URL, typically by clicking a link in the phishing email. This action potentially exposes credentials to the attacker.

As you start analyzing a phishing incident, you can Perform an email sightings search or Perform an observable sightings search to identify other users in your organization who are impacted by the same phishing attack. Search your log stores to identify phished and victim users. After you have identified the list of affected users, create child security incidents to perform comprehensive incident response procedures using the tools available in Security Incident Response.

Note: You can also use the following approach to perform a sightings search:

- Navigate to **Security Incidents** > **Show All Incidents** and click on a security incident.
- Click **Show IoC** under Related Links. A list of observables is displayed.
- Select an observable from the list and from the **Actions** list, select either of the following options:
  - Run Web Traffic Sightings Search
  - Run Email Traffic Sightings Search
- Specify the time frame and click **Search** to perform a sightings search.

Saved sighting search configurations

Configure sighting searches and create saved configurations for SIEMs or other log stores for instances of observables to determine the presence of malicious observables in your environment.

Note: Saved Searches and Inplace queries are supported for Splunk Integration only.

Related topics

Create sightings search configuration records

Perform an email sightings search for user-reported phishing attacks

Search for users who have received phishing emails based on observables such as email subject, sender name, or message ID. You can then contain and eradicate these phishing emails from your organization.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Search the Splunk email traffic logs to gather the list of recipients of a suspicious email. The search can be performed using the email sender, email message ID, or the email subject associated in a security incident as the criteria.

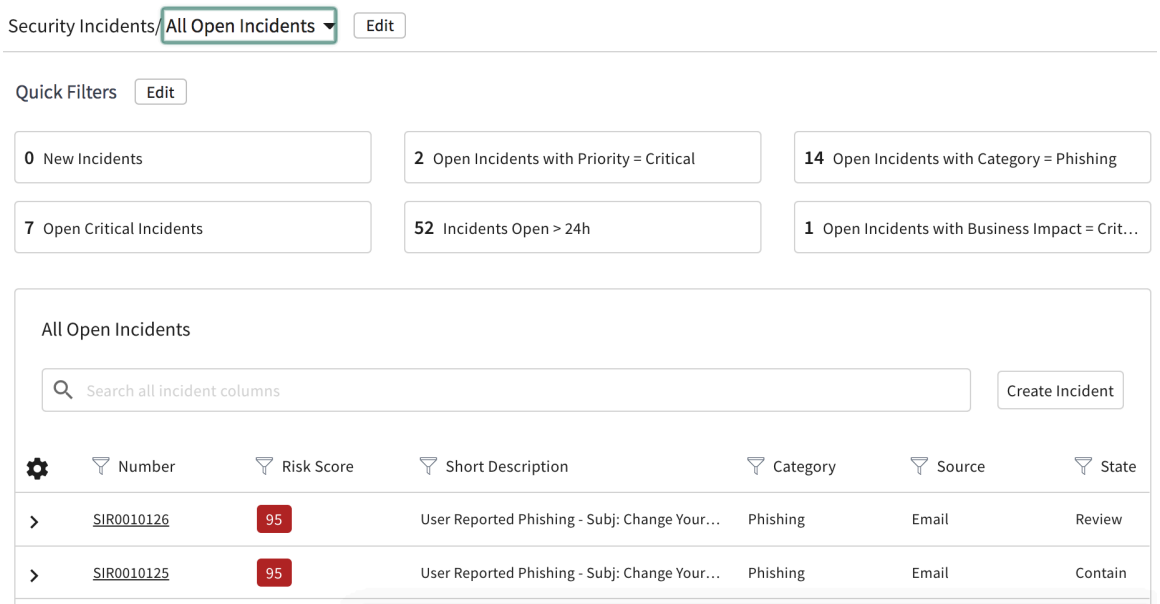
Note:

- This implementation of sightings search for email-based observables has been tested only with the Splunk Enterprise log store.
- The Splunk log events must be Common Information Model (CIM) compliant for the sightings search query to return accurate results.

Procedure

1. To see the security incidents assigned to your team, navigate to **Security Incident** > **Incidents (New UI)**.
2. From the **Security Incidents** list, select one of the filters, such as all **open incidents**, **all incidents assigned to you**, or **all incidents**.

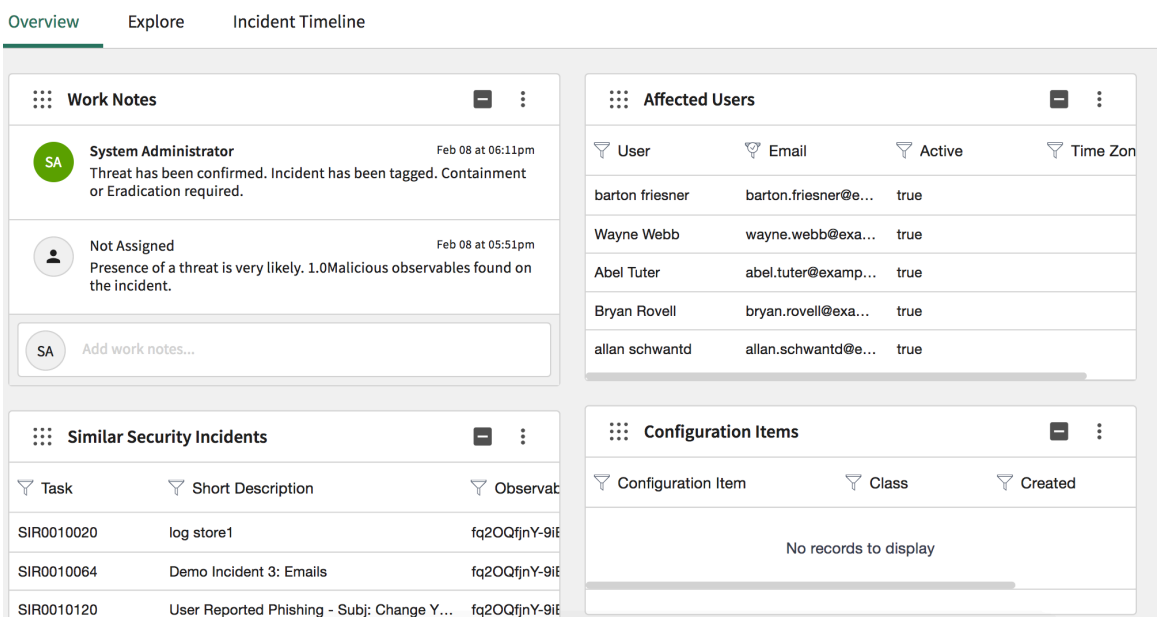
   To view security incidents of a particular type, such as critical incidents or phishing emails, click one of the **Quick Filters**.



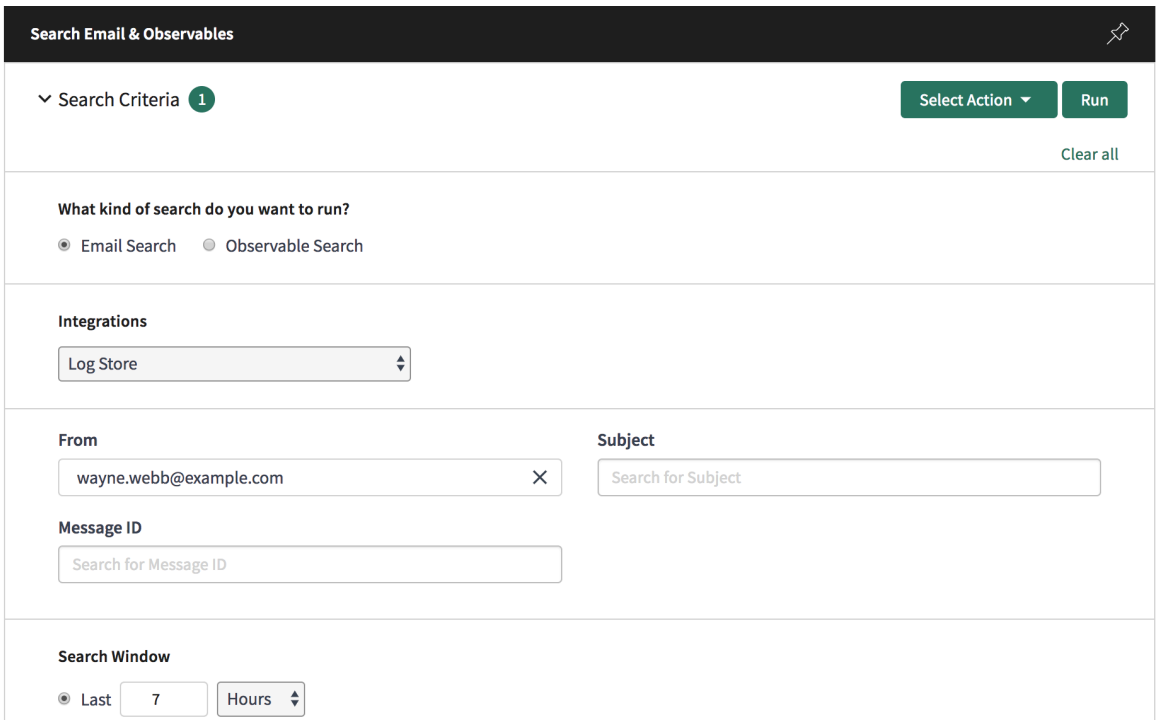
3. Click the security incident that you want to analyze.

   The Overview tab provides an overview of the security incident including a list of observables, affected users, and similar security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click the **Explore** tab.
5. Under **Incident Data**, navigate to **Investigation** > **Search Email & Observables**.



6. Expand the Search Criteria section.
7. Select **Email Search** as the type of search that you want to run, and specify the rest of the search criteria.

Search criteria form

Field	Description
Integrations	Integrations type. Select **Log Store** from the list.

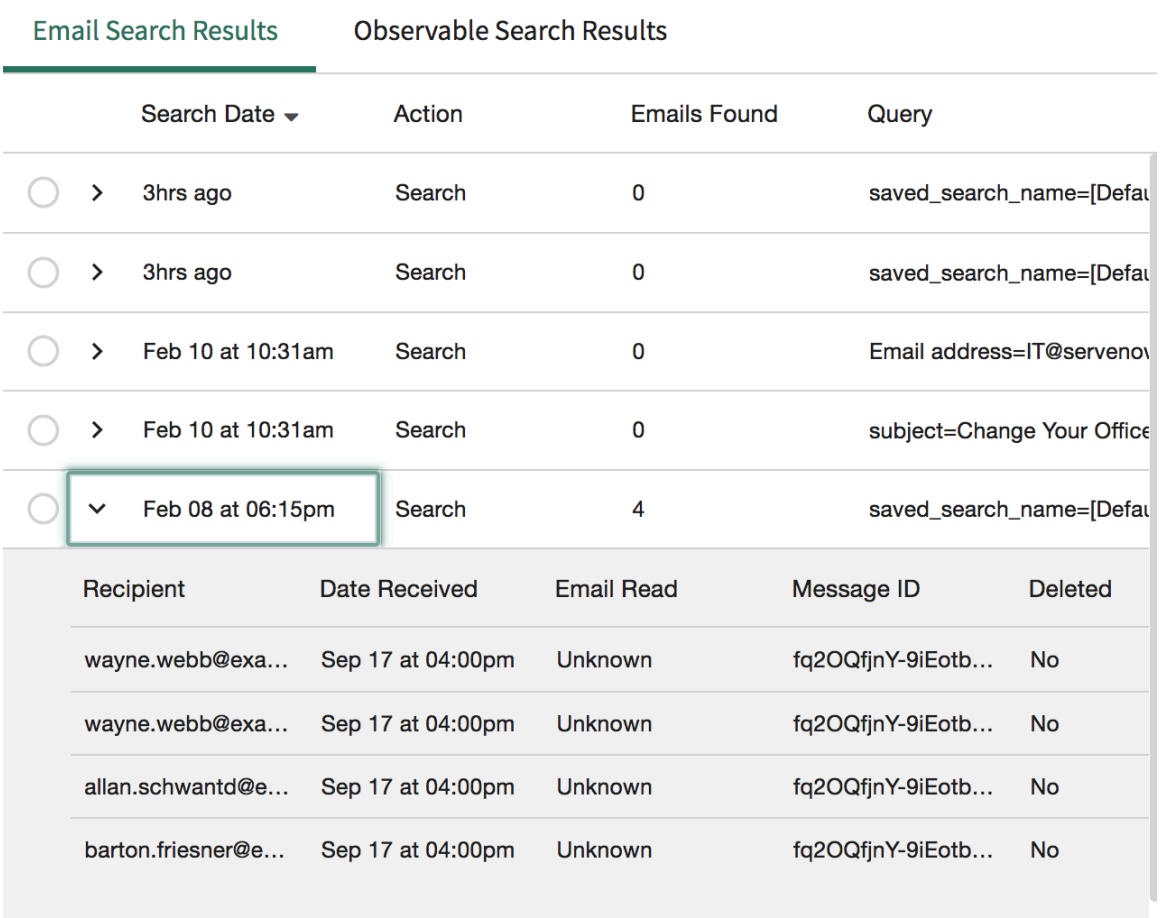
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This feature is supported only with the Splunk log store.
From	Full email address of the sender (for example, jane.doe@example.com).
Message ID	Email message ID from the log store.
Subject	Subject for the phishing email.
Search Window	Time window for the search (for example, the last 24 hours).

8. From the **Select Action** list, select **Search** and then click **Run**.

   The Splunk log store is searched using the criteria that you enter, and the users targeted by the phishing attack are shown on the **Email Search Results** tab. The total number of phishing emails and the details of each email, including the email date received, recipient, and message ID, are displayed.

9. To view the list of users who received the phishing email, click the **>** symbol in the Search Date column.



10. To view a list of users who received the email, navigate to **Users** > **Affected Users**.

    The Phished User column identifies the email recipients.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Affected Users page shows only the user records that are present on the ServiceNow instance.

11. To further investigate the users who are targets of the phishing attack, follow these steps:
    a. Select the check boxes next to the user names.
    b. From the list, select **Create Child Security Incident**, and click **Run**.
    A message is displayed to show that a child security incident has been created. To view the child security incidents associated with a parent incident, click the **Explore** tab and navigate to **Incidents** > **Child Security Incidents**.

Result
The list of phished users is displayed.

Perform an observable sightings search for user-reported phishing and malware attacks

Perform sightings searches on observables to find out how many users have visited a malicious or suspicious website within a specific period.

Before you begin
Role required: sn_si.analyst

About this task
You can perform a network traffic search on observables such as the URL, destination host, or the destination IP address associated with a security incident.

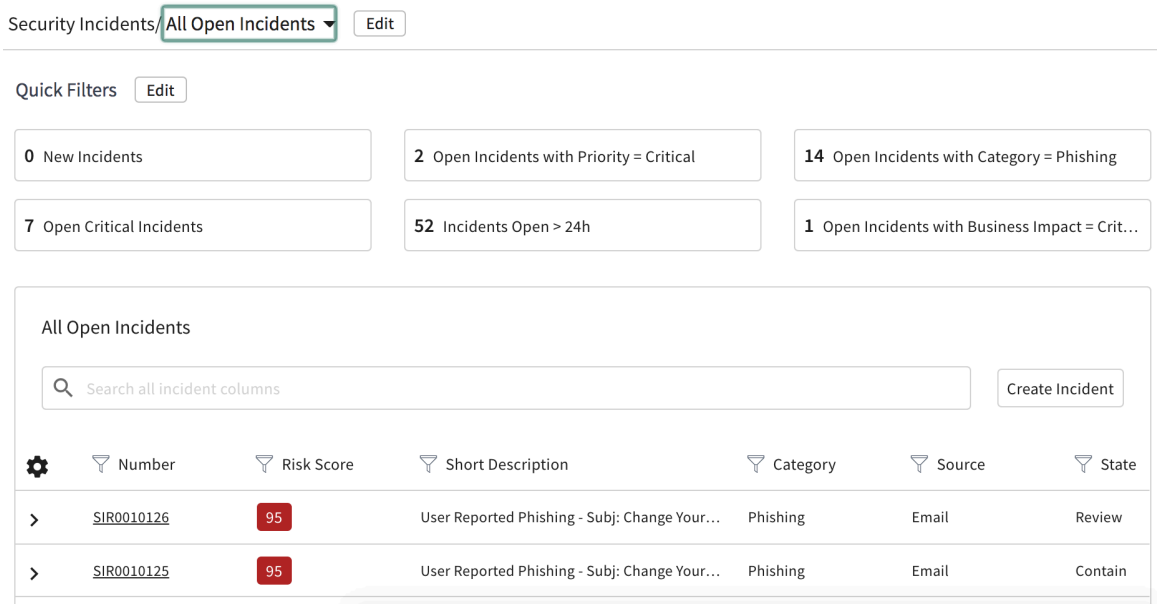
Note:

- This implementation of sightings search for observables has been tested only with the Splunk Enterprise log store.
- The Splunk log events must be Common Information Model (CIM) compliant for the sightings search query to return accurate results.

Procedure
1. To see the security incidents that are assigned to your team, navigate to **Security Incident** > **Incidents (New UI)**.
2. From the **Security Incidents** list, select a different filter, such as all **Incidents Assigned to Me**, **All Open Incidents**, or **All Incidents**.

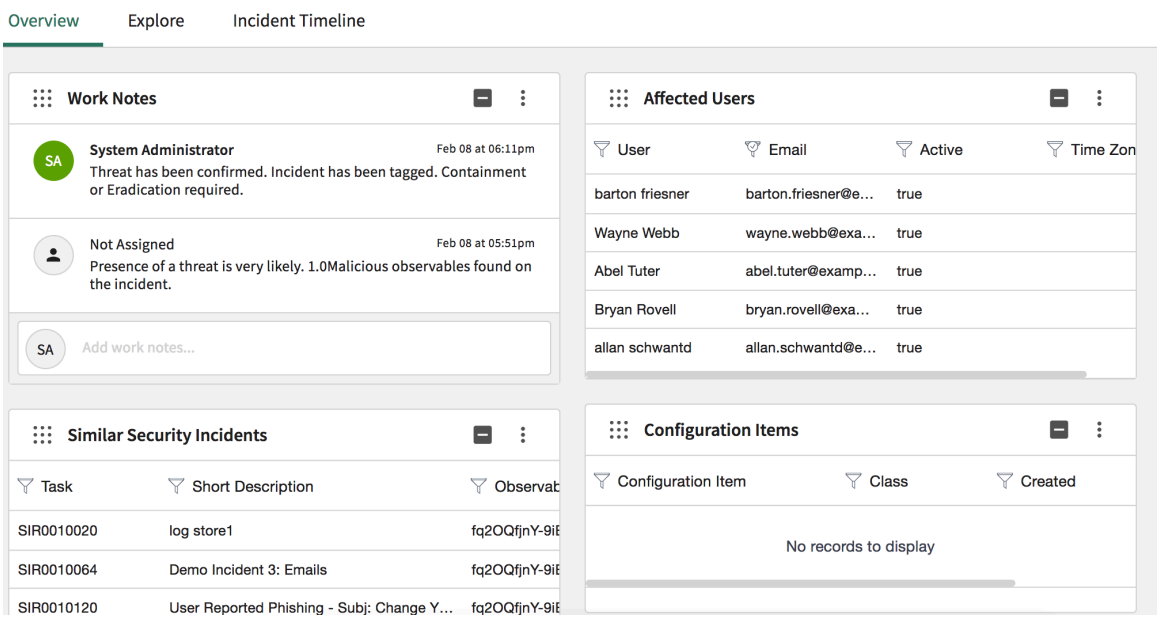
   To view security incidents of a particular type, such as critical incidents or phishing emails, click one of the **Quick Filters**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click the security incident that you want to analyze.

   You can see an overview of the security incident including a list of observables, affected users, and similar security incidents.

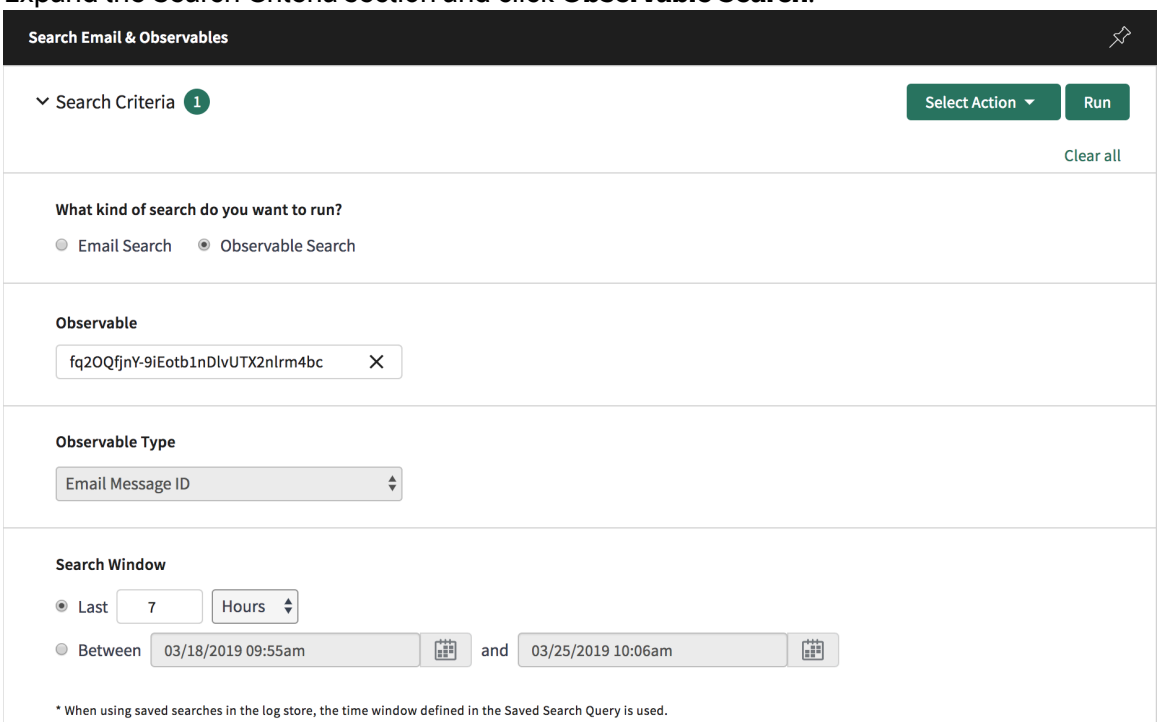


   In the Observables section, notice that the Observable column shows the email address, subject, and URL. Notice also that the Finding column shows that the URL was automatically scanned when the phishing email was submitted and determined to be a known malicious URL. The Incident Count column shows the other incidents that share the same observable. These artifacts indicate that you are likely ready to move on to containment procedures for this phishing attack, including determining how many users in the organization have been affected.

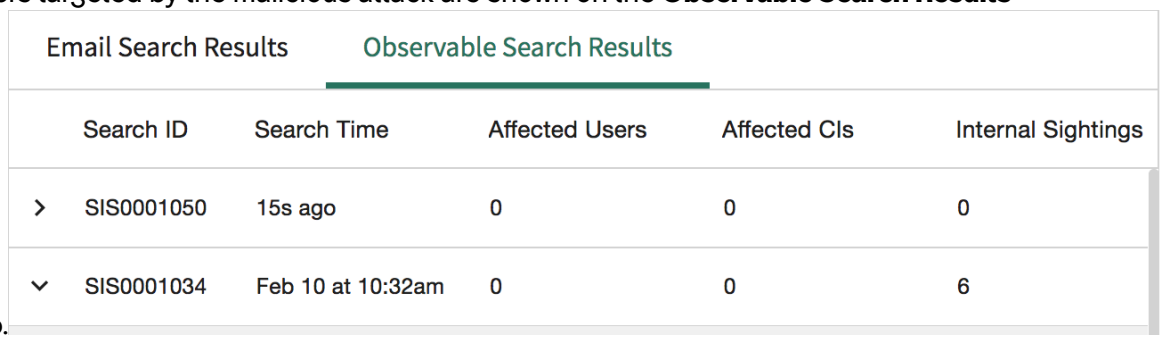
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Navigate to **Explore** > **Investigation** > **Search Email & Observables**.
5. Expand the Search Criteria section and click **Observable Search**.



6. Enter the observable that you are searching for, and a time window for the search (for example, Last 24 Hours).
7. From the **Select Action** list, select **Search**.
   The Splunk log store is searched using the criteria that you entered and the key users targeted by the malicious attack are shown on the **Observable Search Results** tab.



8. To view the users who received the email, navigate to **Users** > **Affected Users**.

   The Phished User column identifies the recipients of the phishing email and the User Interaction column identifies users who clicked a phishing URL or interacted with a suspicious

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

email address. The User Interaction column is set to true or false, depending on whether the user clicked the malicious link or IP.

Note: The Affected Users page shows only the user records that are present on the ServiceNow instance.

9. To further investigate the users who clicked the phishing email and potentially compromised their credentials:

   a. In both the Phished User and User Interaction columns, select the check boxes next to the user names that show **true**.

   b. Click **Create Child Security Incident** and then click **Run**.
   A message is displayed to show that a child security incident has been created. To view the child security incidents associated with a parent incident, click the **Explore** tab and navigate to **Incidents** > **Child Security Incidents**.

Result
The list of phished users is displayed.

Create sightings search configuration records

Create multiple sightings search configuration records and use them while querying multiple log stores or varying the search parameters.

Before you begin
Role required: sn_si.admin

- The CIM add-on must be installed on the Splunk instance.
- Saved Searches and Inplace queries are supported for Splunk Integration only.

About this task
You can also create sightings search configuration records to invoke saved searches on the Splunk enterprise log store.

Note: The search configuration queries rely on Splunk log data to be Splunk Common Information Model (CIM) compliant.

With saved search configurations, you can:

- Create custom searches that combine multiple event records.
- Design-efficient and effective searches.
- Use parametrized inputs in the Splunk saved search.

The base system includes the sample configurations as shown in this image:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Saved search configurations

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

The saved search and Inplace configuration queries are example queries and can be substituted with appropriate parameters for your environment. Create additional saved search configurations as required. When you define a saved search configuration, the name and the parameters in the search query must match the saved configuration defined on your Splunk instance. If the name and parameters are not the same, you may not see accurate results when you perform a sightings search.

Note: On your Splunk instance, navigate to the Searches, Reports, and Alerts page and locate your saved search query. Click the **Permissions** link to navigate to the Permissions page. Select the **All Apps** radio button and enable the **Read Permission** option for **Everyone**. This will change the Sharing column value from Private to App for your saved search query. If this is not set, saved search query may not return any results.

To verify if the saved search configuration matches the configuration defined on your Splunk instance:

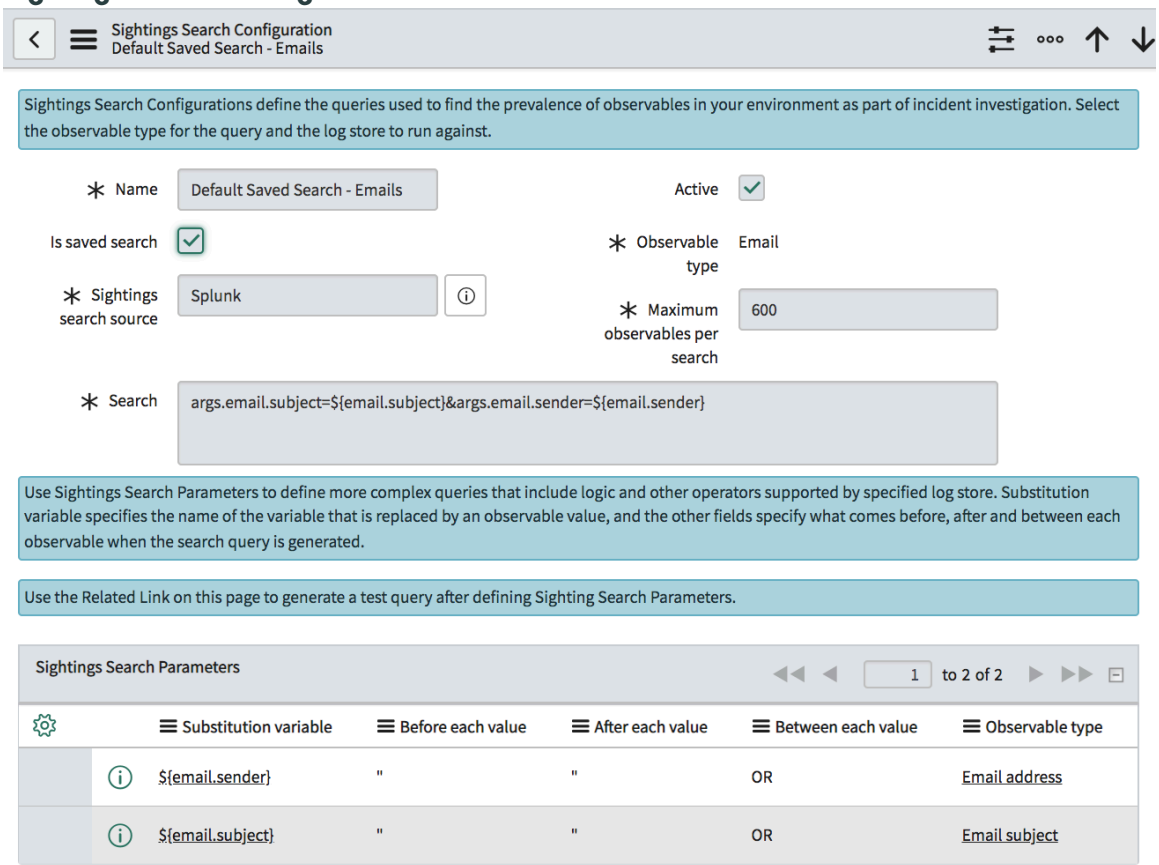
1. Navigate to **Settings** > **Searches, Reports, and Alerts**.
2. Change **App Context** to **All**.

   A list of search reports is displayed.
3. Confirm that the saved search query is present in the list.

For example, the Sightings Search Configuration form contains the email address and email sender as search parameters:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sightings Search Configuration form



In your Splunk instance, define the saved search with the same name, Default Saved Search - Emails, and the same search parameters for the email address and email subject. If the name and search parameters are not the same, sightings search does not generate accurate result.

Procedure

1. Navigate to **Security Operations** > **Integrations** > **Sightings Search Configuration** and create a new record (see table for field descriptions).

Sightings Search Configuration form

Field	Description
Name	Name of the configuration.
Is saved search	Saved search configuration is created if you select this option.
Sightings search source	The source for the sightings search. Select the Splunk log store as the source.
Active	Option for the saved search status. Only active search configurations can be used to perform a sightings search.
Observable type	Observable type can be any observable type such as IP, hash value, URL, domain name, and so on.
Maximum observables per search	Maximum number of observables to be returned from the search.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Search	The default search string is `$(observable)`, but you can define your own search query by specifying parameters that are supported by the Splunk log store.

2. Click **Submit**.

Result
You have created a sightings search configuration record.

What to do next
After defining the search query, click **Generate Sightings Search Test Query**, and specify a list of observable values to generate a test query based on this saved search configuration.

Playbook Resources

Security Incident Response provides a rich set of playbook resources that include a comprehensive library of playbooks, subflows, and actions. You can create or configure playbooks quickly and easily without writing complicated code. You can use these playbooks to resolve security threats in a step-by-step manner.

Playbook resources include the following:

Security Incident Response playbooks	Security Incident Response playbook actions
The playbooks provided with the base system are designed to accelerate the security incident investigation process by automating complex and mundane tasks. Playbooks are highly configurable and are built using ServiceNow's Flow Designer technology. To configure, copy the playbook provided with the base system and modify it using the simple drag-and-drop graphical interface. See Security Incident Response playbooks.	Complex actions that are critical for building playbooks are available as **Action Libraries**. These Action Libraries enable security administrators to create playbooks without writing any complicated code. See Security Incident Response playbook actions.

Activate a Security Incident Response flow

Security administrators and flow designers can use the Security Incident Response flows to automate the process of resolving security incidents in the organization.

Before you begin
Role required: sn_si.admin, action_designer, and flow_designer

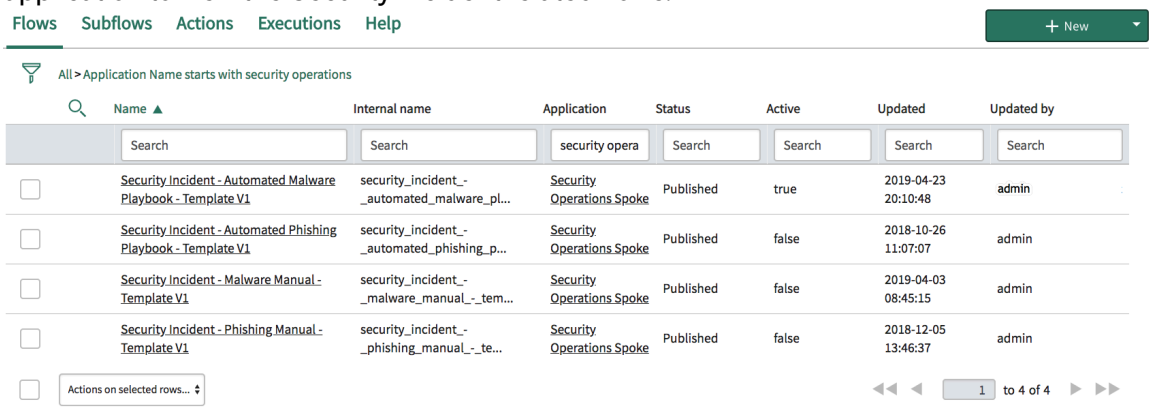
About this task
The flows provided with the base system are in an inactive state. Activate these flows before you use them.

Procedure

1. Download and install the Security Operations Spoke application.
   This Spoke application provides security operations actions that you can use while defining Security Incident Response flows.

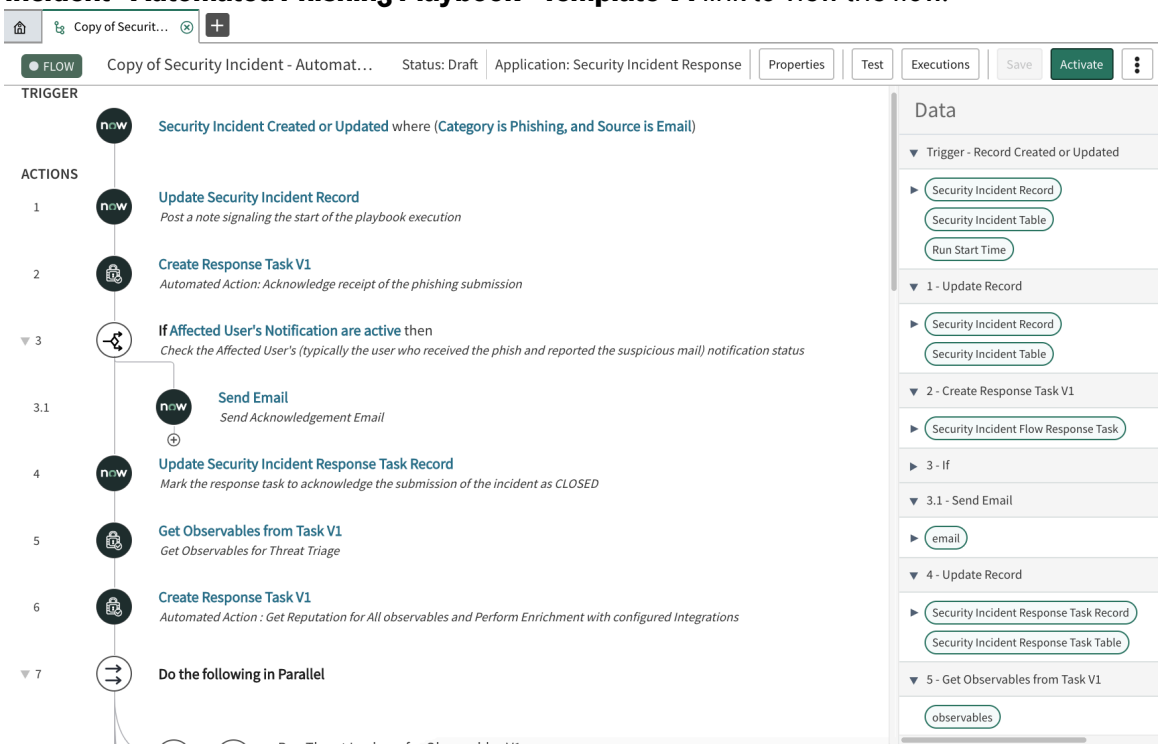
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Navigate to **Flow Designer** > **Designer** and search for the Security Operations Spoke application to view the Security Incident related flows.



Notice that the flows have a published status and are inactive.

3. For example, if you want to activate the Automated Malware Playbook flow, click the **Security Incident - Automated Phishing Playbook - Template V1** link to view the flow.



Note: You cannot edit the flows provided with the base system as they are read-only flows. You can use these flows as they are or make a copy and modify them as required.

4. Click **Activate** to activate the flow.

Result

The Automated Phishing Playbook flow is active and ready to use.

Security Incident Response playbooks

You can invoke the security incident playbook flow automatically or manually.

A Playbook is visible only if at least one playbook is associated with a security incident. The playbook component works only for the Process Automation Designer (PAD) built processes and not for the flow designer-built flows. For the existing flow designer enabled flows, it will continue to work, and the activities will be continuing to be rendered as response tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response supports two types of Playbooks:

- Process-based Playbooks
- Flow-based Playbooks

In addition to the listed playbooks, there are also subflows in Security Operations Spoke that can be called from the flows playbook. Ransomware is one of that subflows.

Activate these flows before you use them. For more information, see Activate a Security Incident Response flow.

Process-based Playbooks

The playbook component works only for playbooks built in Workflow Studio and not for flows. However, existing flow-based playbooks will continue to work and the activities will be continuing to be rendered as response tasks.

Security Incident Response provides the following playbooks with the base system.

Playbook for Manual Phishing

The Manual Phishing Playbook provides step-by-step guidance for your analysts on how they can manually resolve specific types of security threats in your phishing activities.

Overview

The Manual Phishing Playbook template is designed to perform the phishing response tasks manually and includes a sequence of actions that includes trigger conditions. You can use the PAD templates to perform the steps in the phishing response playbook and resolve these incidents efficiently.

This playbook can be used if a security incident is created or updated. You need to activate the Manual Phishing Playbook on the Process Automation Designer (PAD) and then perform all the tasks, such as analysis, contain, eradicate, and review.

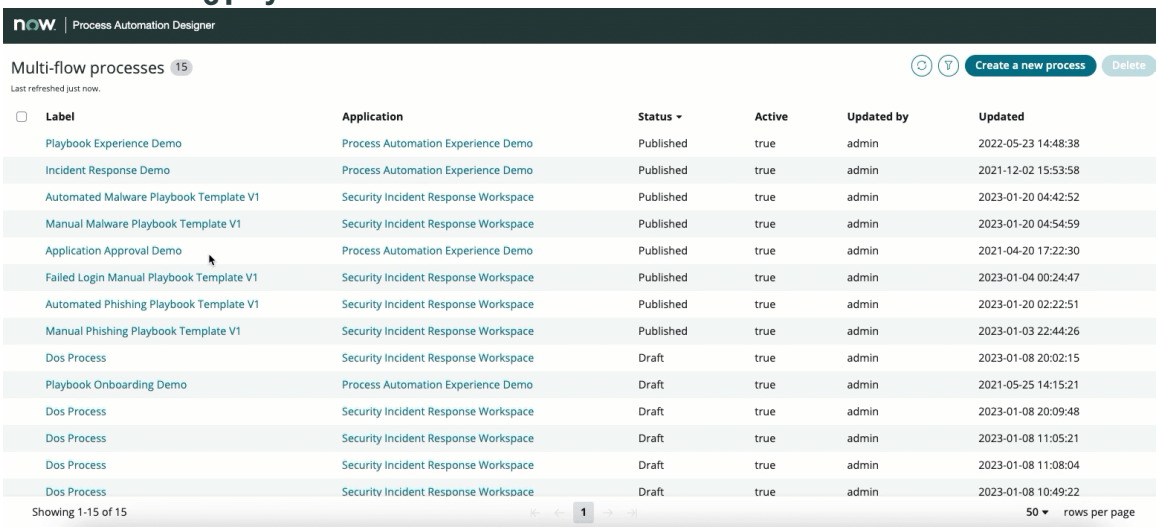
The following are the stages of the process definition and correspond to the security incident state:

- Analysis
- Contain
- Eradicate
- Review

Each stage has activities within it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Manual Phishing playbook



Once you mark a task complete in a stage, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the tasks in a stage, you can move to the next stage. The status is reflected in the left-hand panel as you keep completing tasks and stages. An Activity Log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the stages. You can choose to edit any field or click Finish to complete the process of creating the entitlement.

Create playbooks for Manual Phishing in Workflow Studio

Use these steps to create playbooks for Manual Phishing in Workflow Studio.

Before you begin

Role required: sn_si.admin or sn_si.manager

Procedure

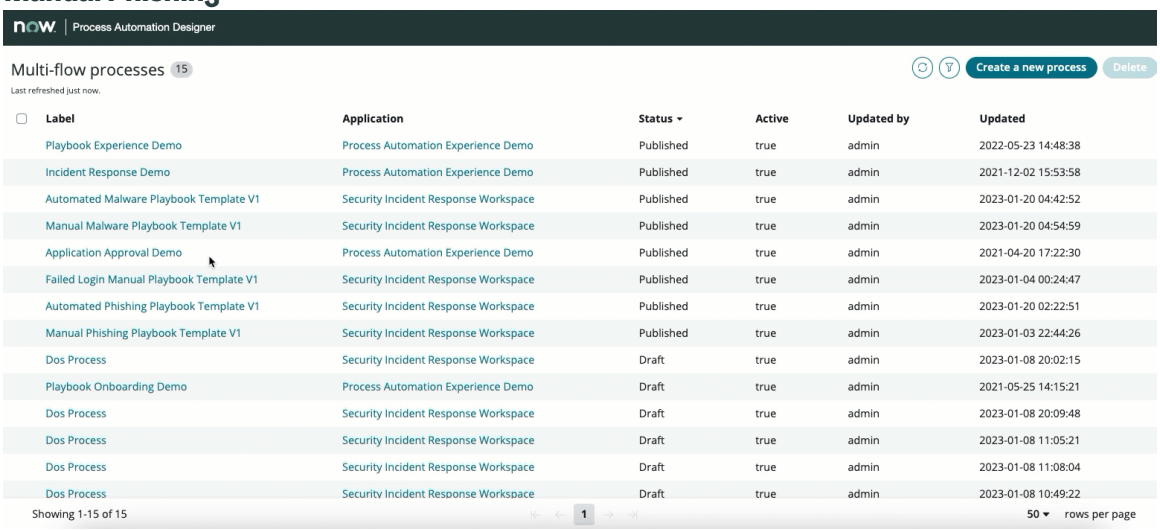
1. Click **All** > **Process Automation Designer** > > **New** and select **Playbook**.

   For example, Manual Phishing Playbook Template V1.

2. Enter a name for the playbook, the description, and the application for which the playbook is being created.
3. Click **Select a trigger**.
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your playbook must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your playbook must run by selecting a table and filling in the conditions.
   For example, the trigger condition is when a security incident of category Phishing is created.

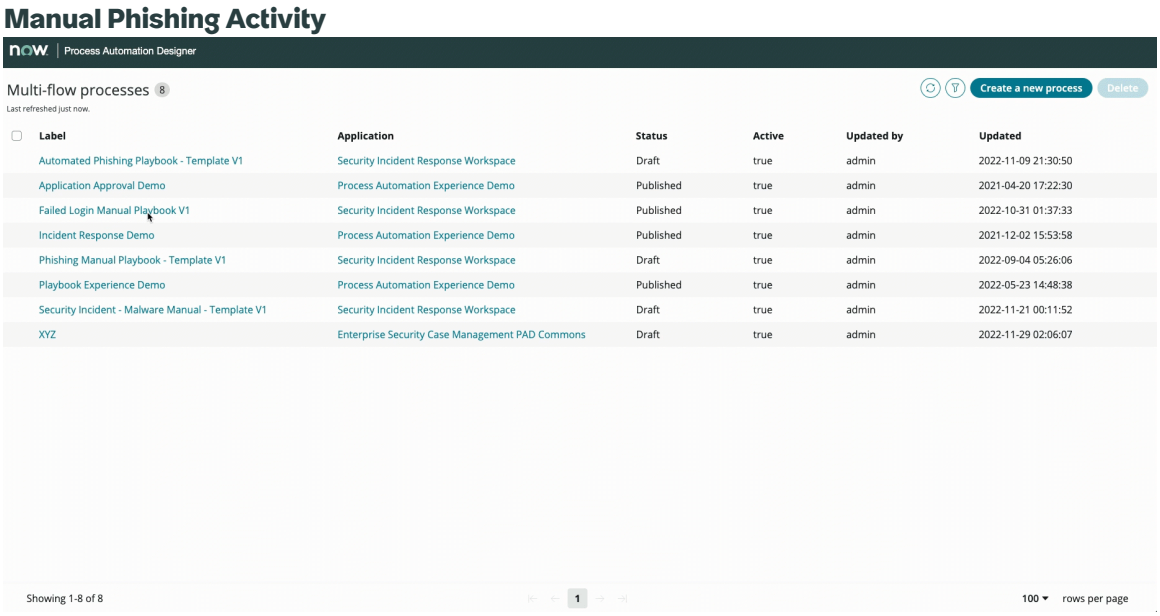
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Manual Phishing



7. Click **Go to Designer**.
8. To start designing your automated process, click **Add a new stage**.
   The stage properties pane opens on the right side of the UI.
9. In the stage properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the stage would run.
10. Click **Save and close**.
11. To add another stage, click **Add another stage**.
    Similarly, you can create as many stages as you want. In this example, you can create a stage for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** stage starts immediately and has no run condition. **Contain** stage start after the previous stage is completed and has a run condition that is based on the outcome of an activity in the previous stage.
    After adding the stages, you need to add process activities for each stage.
12. Click **Add another activity** under a particular stage (For example, Analysis stage).
    The Add activity pop-up opens.
    a. In the Add activity pop-up, select the required activity definition.
13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to stages. Similarly, you can create other process activities under each stage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



14. In the Activity properties pane, add a run condition and indicate when to start the activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Add parallel activities

If the **When to Start** field is set to **With Previous**, then parallel activities can be initiated.

For moving from one stage to the next stage

If no run condition is defined, the stages and activities are executed sequentially.

You can use the run condition to skip activities or stages. In this example, **Contain stage begins when the outcome of 'Does the email have threat indicators?' is Yes**.

To move from one stage to another stage, you can use the platform provided **activity definition – Update Record**. This will update the state field of security incident, and resume the playbook execution to the next stage.

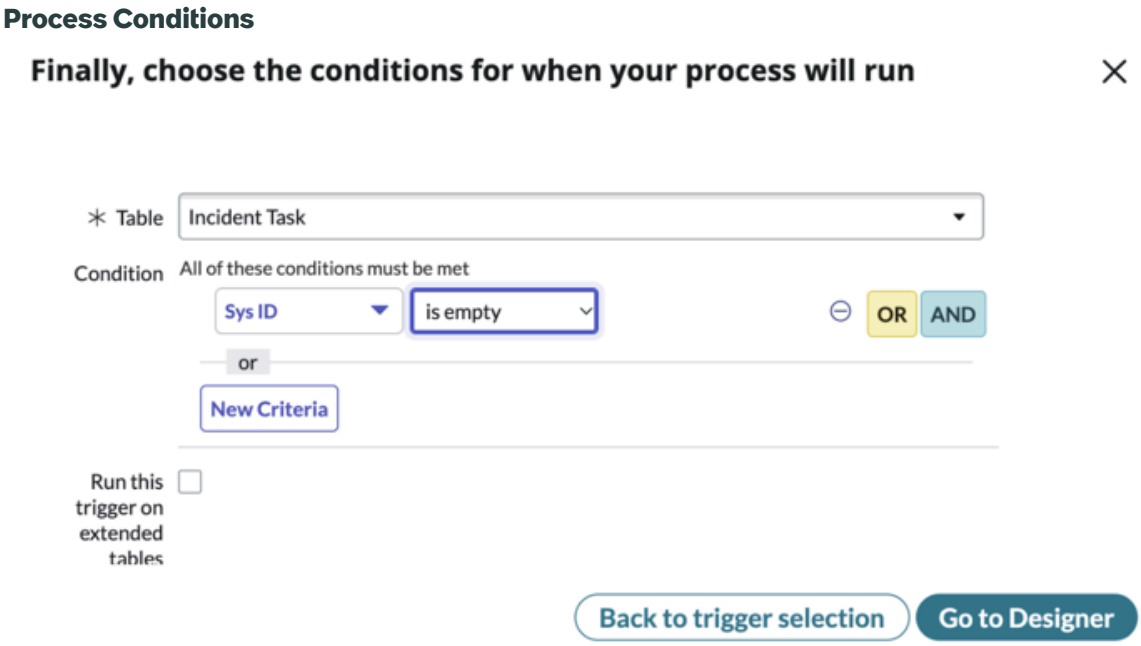
However, the challenge with this activity definition is that, if say that the playbook is in the Analysis stage, and if the user had manually updated the state to say review, the Update Record activity will again change the state to Contain to continue the playbook execution. This will override the manual change done.

To overcome this, in the base system an activity definition called **Update Task State** is provided. This activity won't override the security incident state, if the current state of the state of the security is ahead of the stage in the playbook.

Create a Process definition with dummy trigger condition

A process definition always requires a trigger condition. But, if you aren't sure when the process should be triggered, you can still create a process definition with a dummy trigger condition. Set the trigger condition as **sys_id is empty**. This condition will never be met.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Using the Manual Phishing playbook

Use these steps to learn how you can use the Manual Phishing playbook in the SIR Analyst Workspace and its capabilities.

Before you begin

Role required: sn_si.admin or sn_si.manager or sn_si.analyst

Procedure

1. In the SIR workspace, open a security incident.
2. Click the **Playbook** tab.

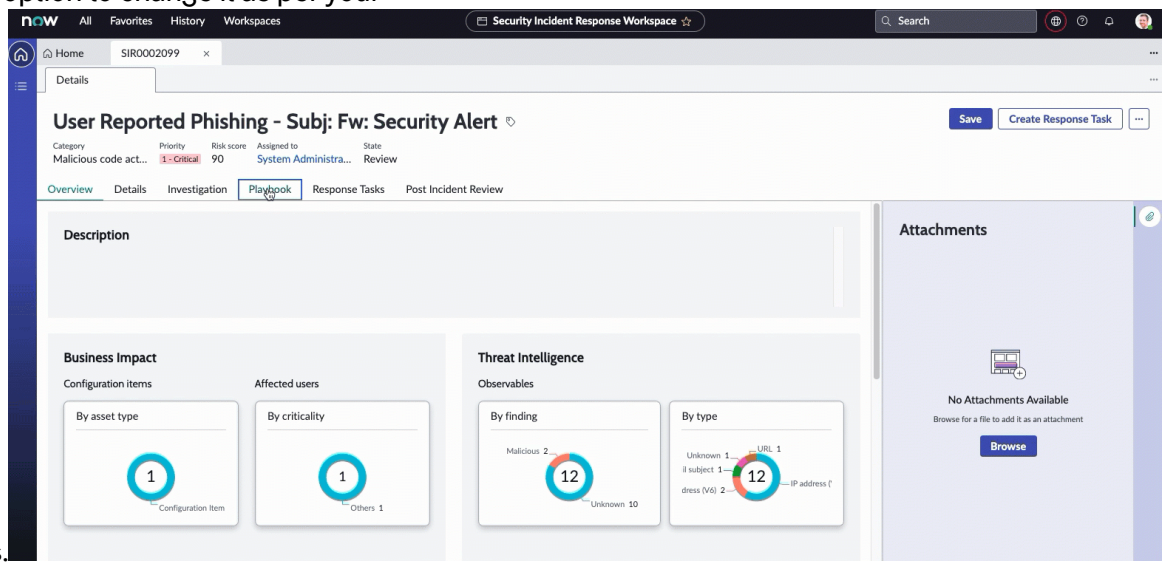
   You can view the playbooks that have been enabled for the security incident. You can also see details like the category of the security incident, risk score.

   Note: If you don't see any playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Click the **Manual Phishing Playbook**.
4. Click each stage to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have the option to change it as per your requirements.



6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to change them as per your requirements. If there's any remaining activity or user action that you need to perform, it's displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Workspace Playbook summary

The following describes the process summary.

- Understand legacy flow-based playbook.
- List down possible activities, stages after analyzing the flow. Look for the steps where true Orchestration can be created.
- Take each activity and check if base system provided activity definition can fulfill the use case or not.
- List down activity use cases, which need new activity definitions to be implemented. Classify them - Interactive, non-interactive or automated. To create an activity definition:
  - Create a subflow or an action for the use case.
  - Decide whether the associated data must be captured in flow data table or a custom table.
  - If using flow data table, create flow data definition in **sys_flow_data_definition**. While creating a flow data record in the subflow, select the flow data definition created.
  - Create an **activity definition**.
  - Map the automation plan.
  - Fill in the **Activity Experience** properties.
  - Create an Action under Playbook Actions. There should be an existing activity action to assign it to the activity definition.
  - To override the default card experience based on the experience type selected, add playbook override by using Activity UI concept.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Some activities can be made to handle both automatic and interactive using wait for user input flag in the subflow. This input can be passed while configuring the activity in the process definition.
- After you have all the activity definition required for your process, start building the process definition using Workflow Studio.

Playbook for Automated Phishing

The Automated Phishing playbook provides step-by-step guidance for your analysts on how they could resolve specific types of security threats in your Automated Phishing activities.

Overview

The Automated Phishing playbook template is designed to automate the phishing response tasks and contains a sequence of actions that includes trigger conditions. You can use the playbook templates in Workflow Studio to automate the steps in the phishing response playbook and resolve these incidents efficiently. This playbook template contains a sequence of reusable actions designed to respond to phishing attacks. Each flow has a trigger (condition), a sequence of actions, and subflows that you can annotate.

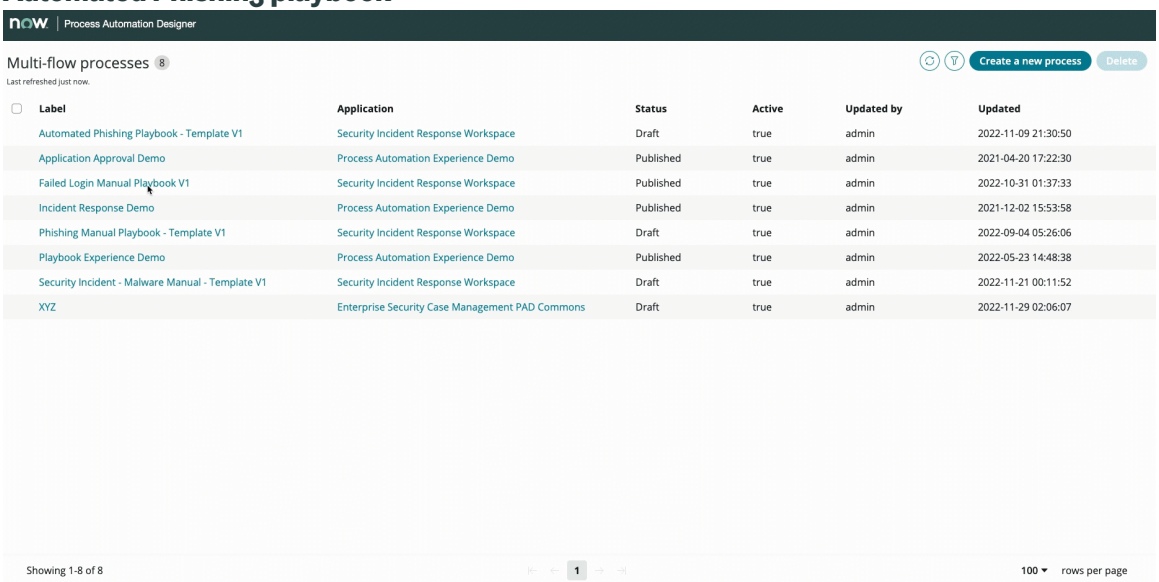
In this playbook, there won't be any user interaction when a security incident's category is set to phishing. This playbook can be used if a security incident is created or updated. You need to activate the Automated Phishing Playbook in Workflow Studio, and this playbook automatically performs all the tasks, such as analysis, contain, eradicate, and review.

The following are the stages of the process definition and corresponds to the security incident state:

- Analysis
- Contain
- Eradicate
- Review

Each stage has activities within it.

Automated Phishing playbook



Once you mark a task complete in a stage, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

tasks in a stage, you can move to the next stage. The status is reflected in the left-hand panel as you keep completing tasks and stages. An Activity log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the stages. You can choose to edit any field or click Finish to complete the process of creating the entitlement.

Create processes for Automated Phishing in PAD

Use these steps to create processes for Automated Phishing in the Process Automation Designer (PAD).

Before you begin

Role required: sn_si.admin or sn_si.manager

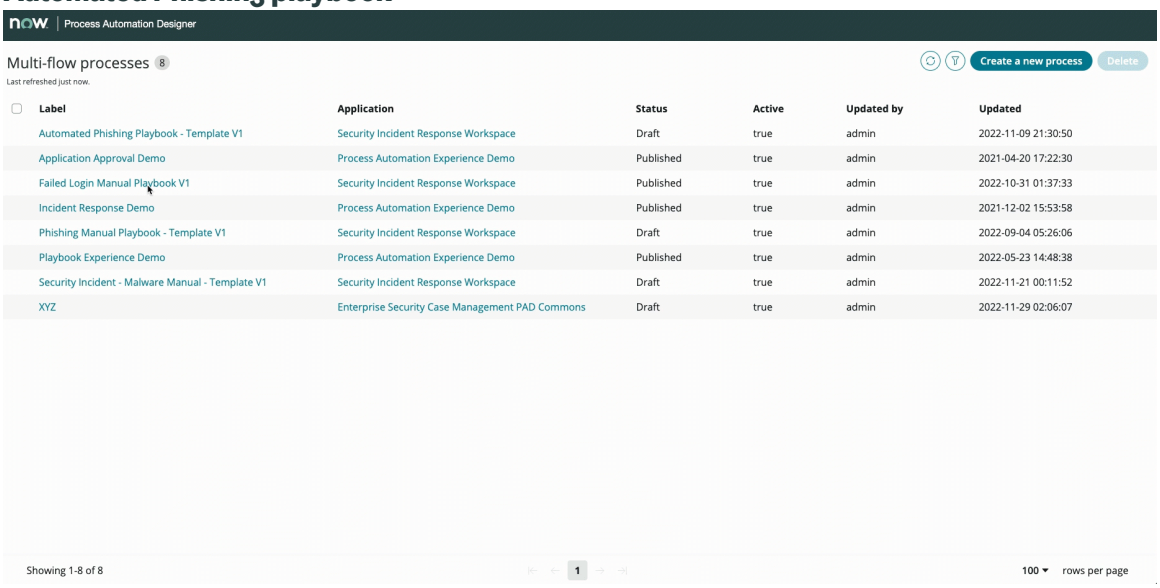
Procedure

1. Click **ALL** > **Process Automation Designer** > > **Create a new process**.

   For example, Automated Phishing Playbook Template V1.

2. Enter a name for the process, the description, and the application for which the process is being created.
3. Click **Select a trigger**.
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your process must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your process must run by selecting a table and filling in the conditions.
   For example, the trigger condition is when a security incident of category Phishing is created.

Automated Phishing playbook

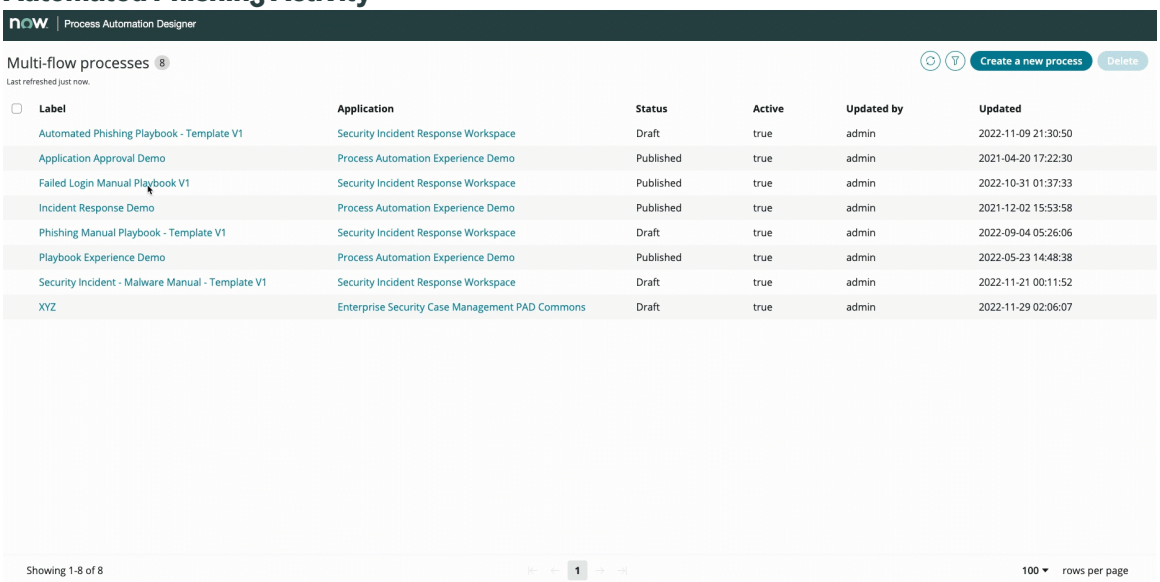


7. Click **Go to Designer**.
   The Process Automation Designer page opens.
8. To start designing your automated process, click **Add a new stage**.
   The stage properties pane opens on the right side of the UI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. In the stage properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the stage would run.
10. Click **Save and close**.
11. To add another stage, click **Add another stage**.
    Similarly, you can create as many stages as you want. In this example, you can create a stage for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** stage starts immediately and has no run condition. **Contain** stage start after the previous stage is completed and has a run condition that is based on the outcome of an activity in the previous stage.
    After adding the stages, you need to add process activities for each stage.
12. Click **Add another process activity** under a particular stage (For example, Analysis stage).
    The Add activity pop-up opens.
    a. In the Add activity pop-up, select the required activity definition.
13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to stages. Similarly, you can create other process activities under each stage.

Automated Phishing Activity



14. In the Activity properties pane, add a run condition and indicate when to start the process activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Using the Automated Phishing playbook

Use these steps to learn how you can use the Automated Phishing playbook in the SIR Analyst Workspace and its capabilities.

Before you begin

Role required: sn_si.admin or sn_si.manager or sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

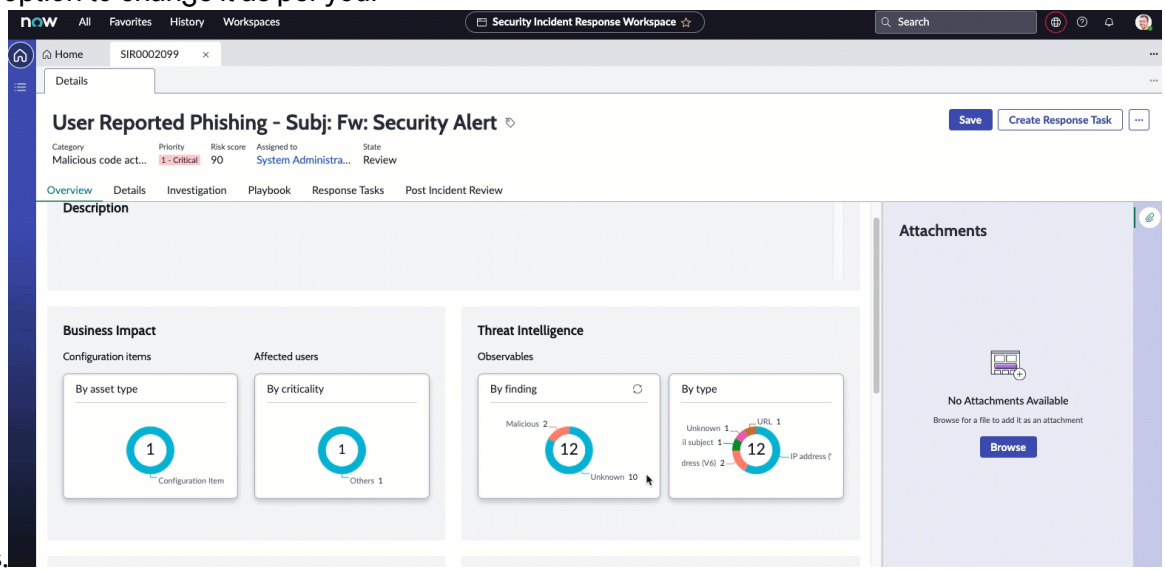
Procedure

1. In the SIR workspace, open a security incident.
2. Click the **Playbook** tab.

   You can view the playbooks that have been enabled for the security incident. You can also see details like the category of the security incident, risk score.

   Note: If you don't see any playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Click the **Automated Phishing Playbook**.
   For automated phishing, the tasks are automatically performed for the security incident.
4. Click each stage to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.
   You have the option to change it as per your requirements.



6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to change them as per your requirements. If there's any remaining activity or user action that you need to perform, it's displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Playbook for Manual Malware

The Manual Malware playbook provides step-by-step guidance on how analysts can manually resolve malware alerts more efficiently.

The Manual Malware playbook template is designed to manually perform the steps involved in handling malware alerts from the endpoint or the network. You can use the playbook templates in Workflow Studio to perform the steps in the Manual Malware playbook and resolve these alerts efficiently. This playbook includes trigger conditions, a sequence of actions, and subflows that you can annotate. This playbook contains a sequence of reusable actions designed to respond to malware attacks. Each flow has a trigger (condition), a sequence of actions, and subflows for annotation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

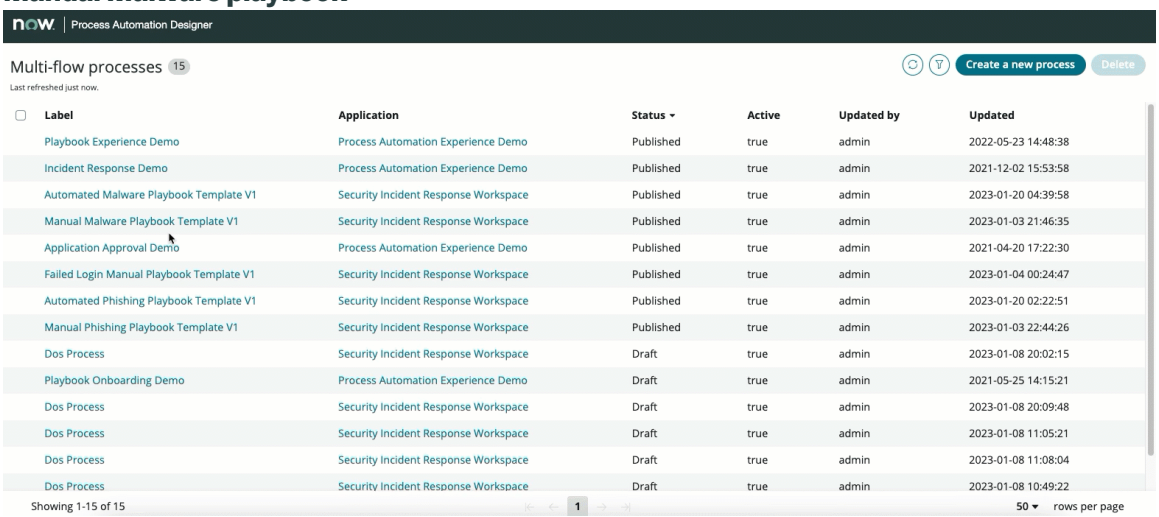
This playbook can be used if malware is created or updated. You need to activate the Manual Malware Playbook in Workflow Studio and create all the tasks, such as analysis, contain, eradicate, and review.

The following are the stages of the process definition and correspond to the malware alert state:

- Analysis
- Contain
- Eradicate
- Review

Each stage has activities within it.

Manual Malware playbook



After you mark a task complete in a stage, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the tasks in a stage, you can move to the next stage. The status is reflected in the left-hand panel as you keep completing tasks and stages. An Activity log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the stages. You can choose to edit any field or click Finish to complete the process of creating the entitlement.

Create processes for Manual Malware in PAD

Use these steps to create processes for Manual Malware in the Process Automation Designer (PAD).

Before you begin

Role required: sn_si.admin or sn_si.manager

Procedure

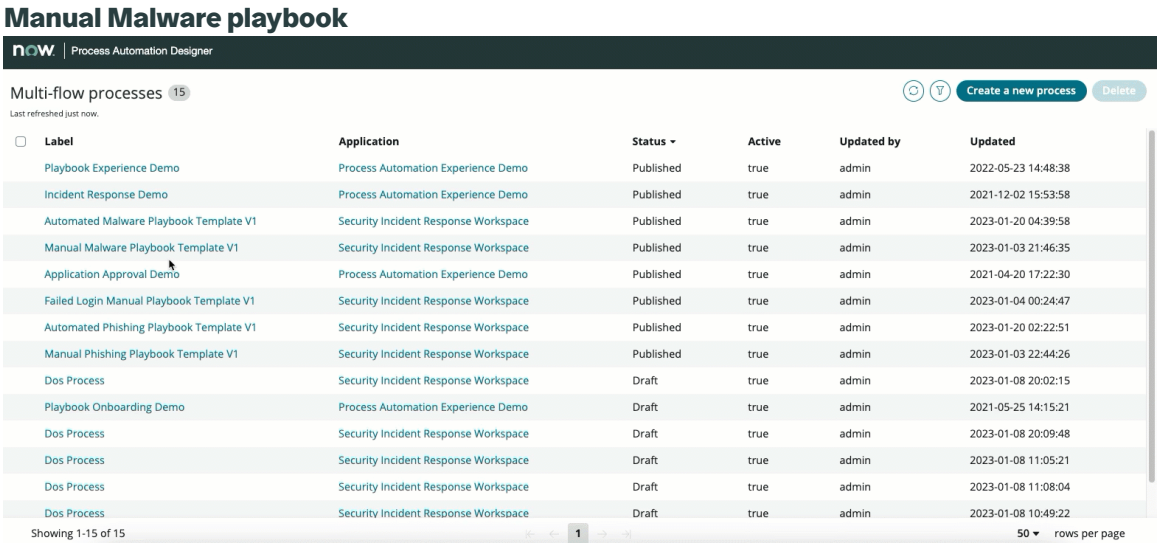
1. Click **ALL** > **Process Automation Designer** > > **Create a new process**.

   For example, Manual Malware Playbook Template V1.

2. Enter a name for the process, the description, and the application for which the process is being created.
3. Click **Select a trigger**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

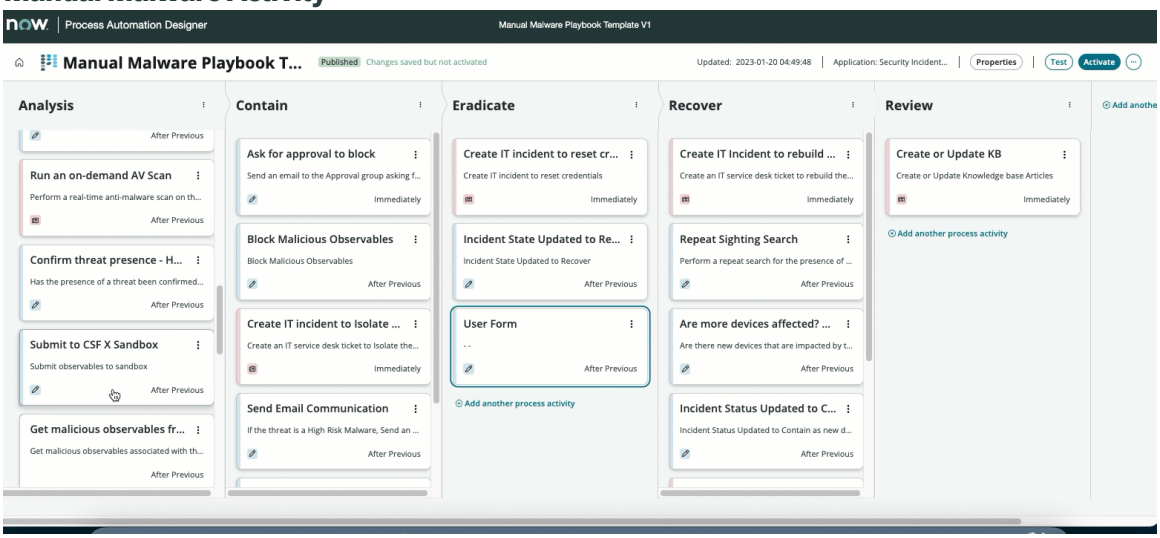
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your process must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your process must run by selecting a table and filling in the conditions.
   For example, the trigger condition is when a security incident of category Phishing is created.



7. Click **Go to Designer**.
   The Process Automation Designer page opens.
8. To start designing your automated process, click **Add a new stage**.
   The stage properties pane opens on the right side of the UI.
9. In the stage properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the stage would run.
10. Click **Save and close**.
11. To add another stage, click **Add another stage**.
    Similarly, you can create as many stages as you want. In this example, you can create a stage for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** stage starts immediately and has no run condition. **Contain** stage start after the previous stage is completed and has a run condition that is based on the outcome of an activity in the previous stage.
    After adding the stages, you need to add process activities for each stage.
12. Click **Add another process activity** under a particular stage (For example, Analysis stage).
    The Add activity pop-up opens.
    a. In the Add activity pop-up, select the required activity definition.
13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to stages. Similarly, you can create other process activities under each stage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Manual Malware Activity



14. In the Activity properties pane, add a run condition and indicate when to start the process activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Using the Manual Malware playbook

Use these steps to learn how you can use the Manual Malware playbook in the SIR Analyst Workspace and its capabilities.

Before you begin

Role required: sn_si.admin or sn_si.manager or sn_si.analyst

Procedure

1. In the SIR workspace, open a security incident.
2. Click the **Playbook** tab.

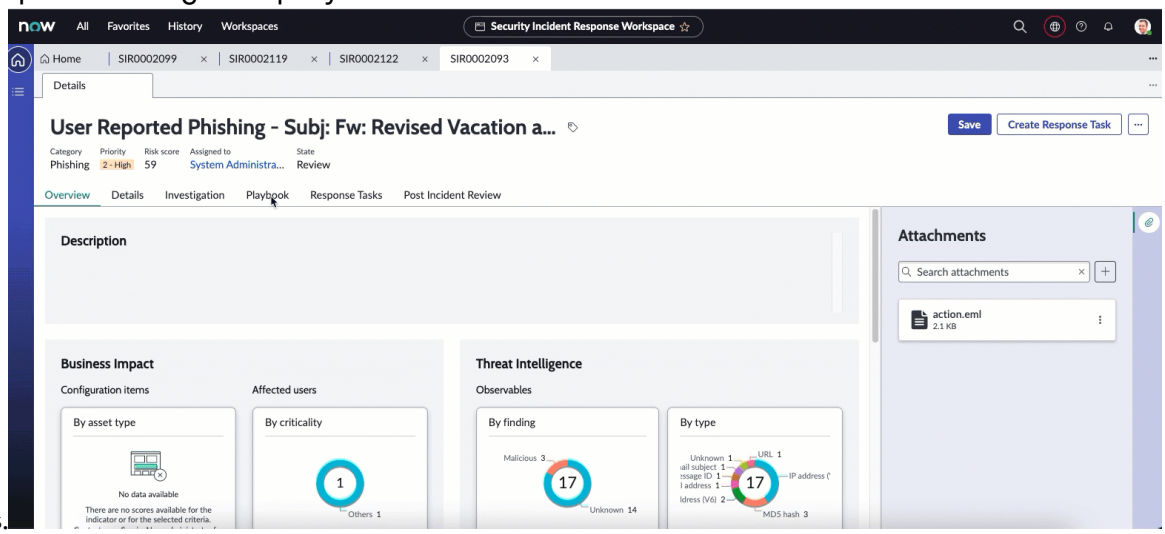
   You can view the playbooks that have been enabled for the security incident. You can also see details like the category of the security incident, risk score.

   Note: If you don't see any playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Click the **Manual Malware Playbook**.
   For manual malware, the tasks are automatically performed for the security incident.
4. Click each stage to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have the option to change it as per your requirements.



6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to change them as per your requirements. If there's any remaining activity or user action that you need to perform, it's displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Playbook for Automated Malware

The Automated Malware playbook provides a sequence of automated steps that helps analysts resolve malware alerts more efficiently.

The Automated Malware playbook template is designed to automate the steps involved in handling malware alerts from the endpoint or the network. You can use the playbook templates in Workflow Studio to automate the steps in the Automated Malware playbook and resolve these alerts efficiently. This playbook includes trigger conditions, a sequence of actions, and subflows that you can annotate. This playbook contains a sequence of reusable actions designed to respond to malware attacks. Each flow has a trigger (condition), a sequence of actions, and subflows for annotation.

This playbook can be used if a security incident is created or updated. You need to activate the Automated Malware playbook in Workflow Studio, and this playbook automatically performs all the tasks, such as analysis, contain, eradicate, and review.

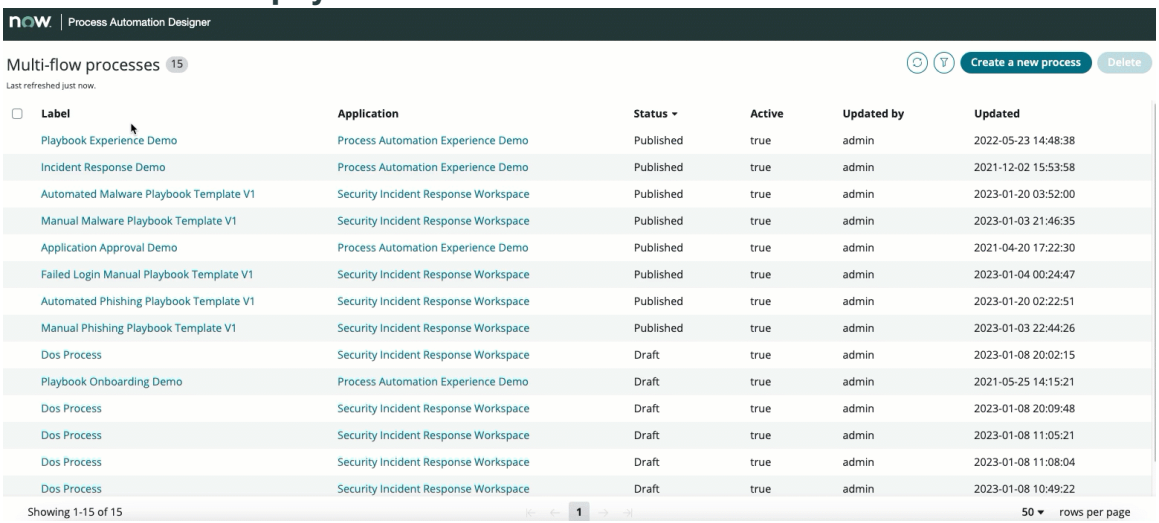
The following are the stages of the process definition and corresponds to the security incident state:

- Analysis
- Contain
- Eradicate
- Review

Each stage has activities within it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Automated Malware playbook



Once you mark a task complete in a stage, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the tasks in a stage, you can move to the next stage. The status is reflected in the left-hand panel as you keep completing tasks and stages. An Activity log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the stages. You can choose to edit any field or click Finish to complete the process of creating the entitlement.

Create processes Automated Malware in PAD

Use these steps to create processes for Automated Malware in the Process Automation Designer (PAD).

Before you begin

Role required: sn_si.admin or sn_si.manager

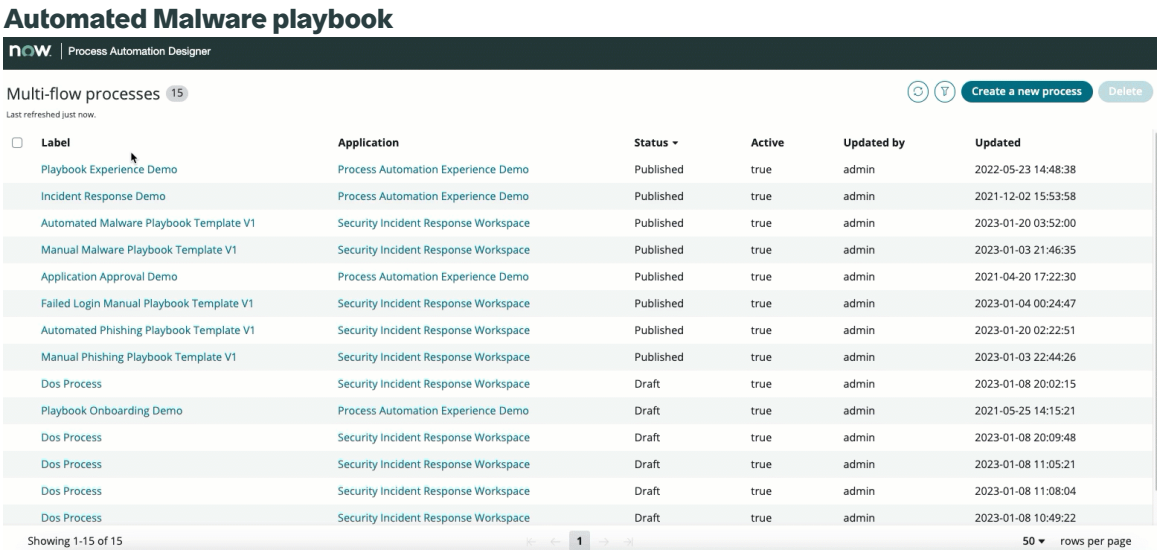
Procedure

1. Click **ALL** > **Process Automation Designer** > > **Create a new process**.

   For example, Automated Malware Playbook Template V1.

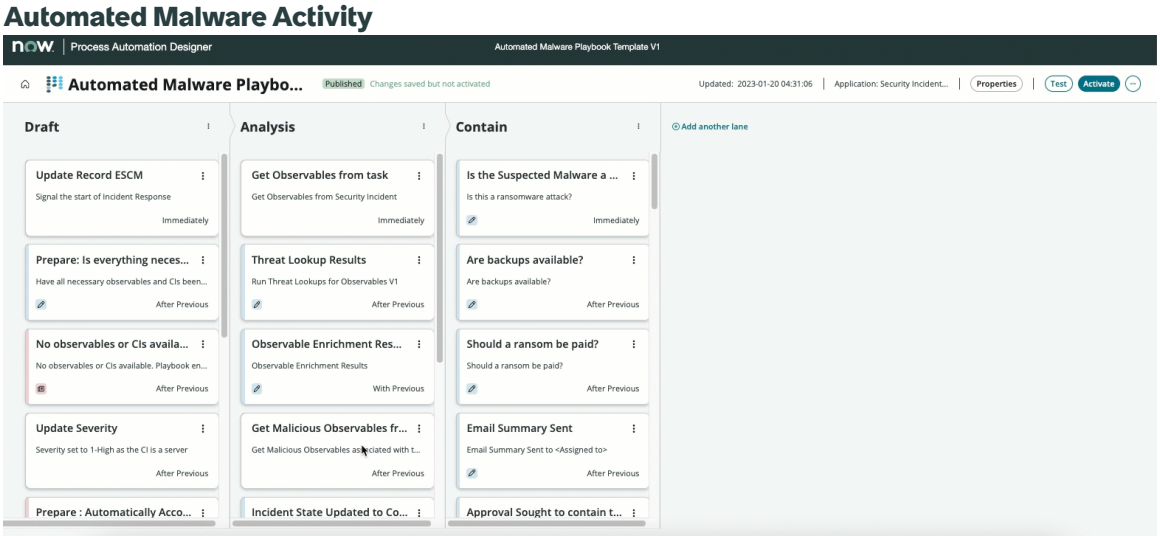
2. Enter a name for the process, the description, and the application for which the process is being created.
3. Click **Select a trigger**.
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your process must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your process must run by selecting a table and filling in the conditions.
   For example, the trigger condition is when a security incident of category Phishing is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Click **Go to Designer**.
   The Process Automation Designer page opens.
8. To start designing your automated process, click **Add a new stage**.
   The stage properties pane opens on the right side of the UI.
9. In the stage properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the stage would run.
10. Click **Save and close**.
11. To add another stage, click **Add another stage**.
    Similarly, you can create as many stages as you want. In this example, you can create a stage for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** stage starts immediately and has no run condition. **Contain** stage start after the previous stage is completed and has a run condition that is based on the outcome of an activity in the previous stage.
    After adding the stages, you need to add process activities for each stage.
12. Click **Add another process activity** under a particular stage (For example, Analysis stage).
    The Add activity pop-up opens.
    a. In the Add activity pop-up, select the required activity definition.
13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to stages. Similarly, you can create other process activities under each stage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



14. In the Activity properties pane, add a run condition and indicate when to start the process activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Using the Automated Malware playbook

Use these steps to learn how you can use the Automated Malware playbook in the SIR Analyst Workspace and its capabilities.

Before you begin

Role required: sn_si.admin or sn_si.manager or sn_si.analyst

Procedure

1. In the SIR workspace, open a security incident.
2. Click the **Playbook** tab.

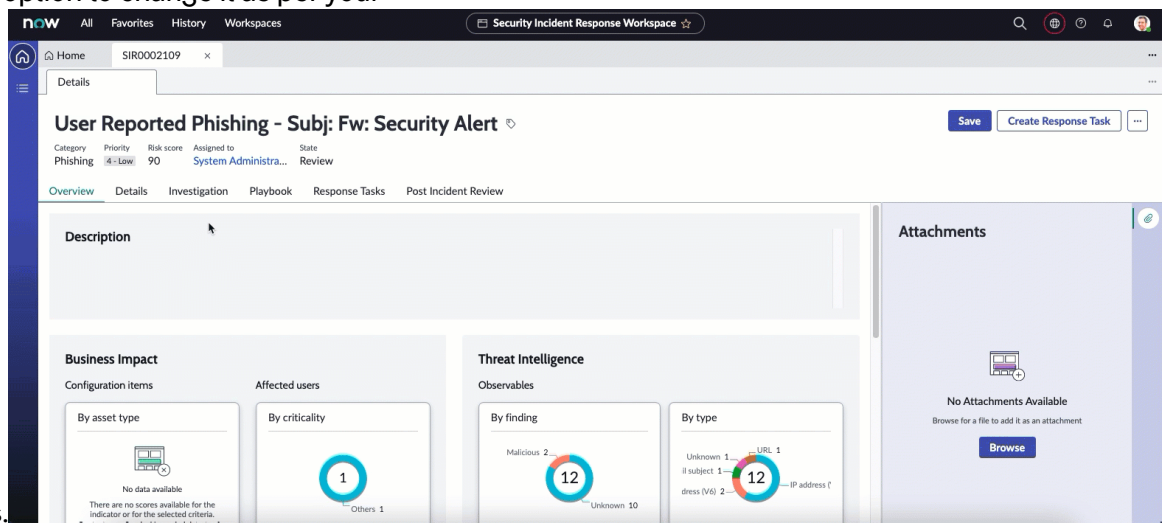
   You can view the playbooks that have been enabled for the security incident. You can also see details like the category of the security incident, risk score.

   Note: If you don't see any playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Click the **Automated Malware Playbook**.
   For automated malware, the tasks are automatically performed for the security incident.
4. Click each stage to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have the option to change it as per your requirements.



6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to modify them as per your requirements. If there's any remaining activity or user action that you need to perform, it is displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Playbook for Failed Login Manual

The Failed Login Manual playbook provides guidance and helps optimize the investigation of failed login security incidents.

When a user makes certain unsuccessful login attempts (as per the SIM configuration), a security incident is created. These unsuccessful login attempts may either be false positives or attempts made by attackers to obtain access to user email accounts.

You can use the playbook templates in Workflow Studio to perform the steps in the Failed Login playbook and resolve failed login security incidents efficiently. This playbook includes trigger conditions, a sequence of actions, and subflows that you can annotate. This playbook contains a sequence of reusable actions designed to respond to failed login security incidents. Each flow has a trigger (condition), a sequence of actions, and subflows for annotation.

This playbook can be used if a failed login security incident is created or updated. You need to activate the Failed Login Manual Playbook in Workflow Studio and create all the tasks, such as analysis, contain, eradicate, and review.

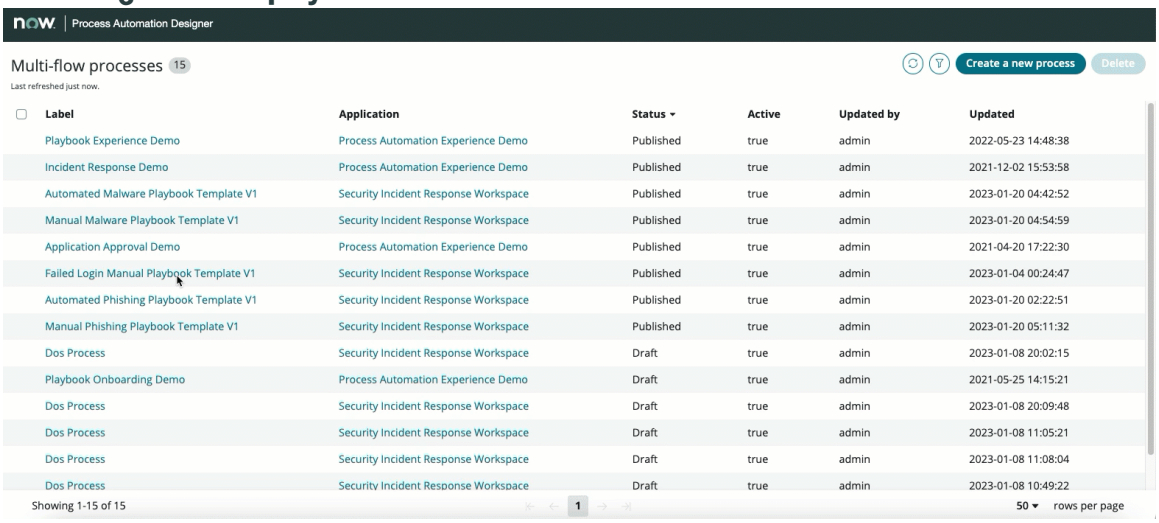
The following are the stages of the process definition and corresponds to the security incident state:

- Analysis
- Contain
- Eradicate
- Review

Each stage has activities within it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Failed Login Manual playbook



Once you mark a task complete in a stage, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the tasks in a stage, you can move to the next stage. The status is reflected in the left-hand panel as you keep completing tasks and stages. An Activity log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the stages. You can choose to edit any field or click Finish to complete the process of creating the entitlement.

Create processes for Failed Login Manual in PAD

Use these steps to create processes for Failed Login Manual in the Process Automation Designer (PAD).

Before you begin

Role required: sn_si.admin or sn_si.manager

Procedure

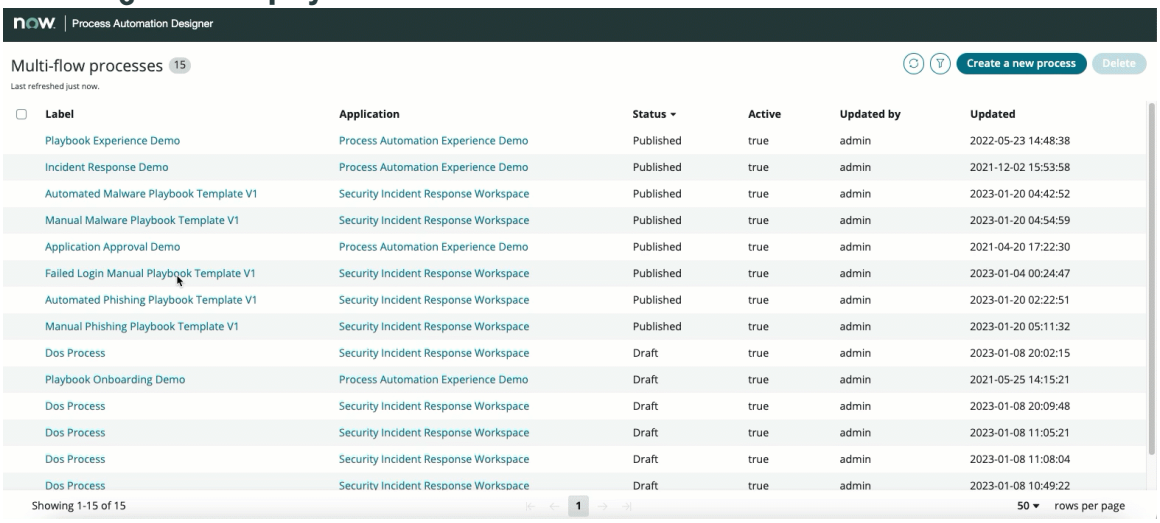
1. Click **ALL** > **Process Automation Designer** > > **Create a new process**.

   For example, Failed Login Manual Playbook Template V1.

2. Enter a name for the process, the description, and the application for which the process is being created.
3. Click **Select a trigger**.
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your process must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your process must run by selecting a table and filling in the conditions.
   For example, the trigger condition is when a security incident of category Phishing is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

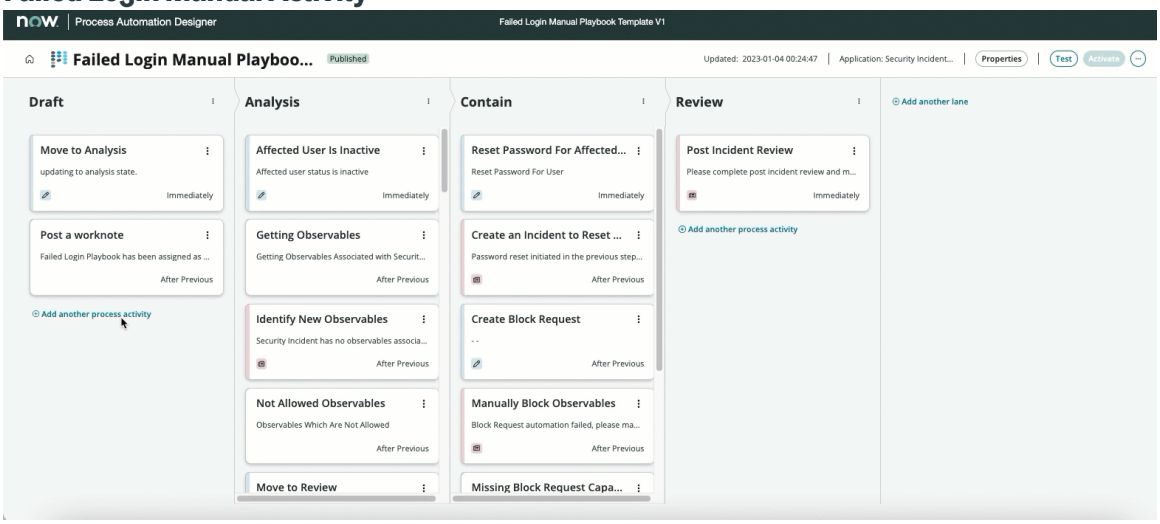
Failed Login Manual playbook



7. Click **Go to Designer**.
   The Process Automation Designer page opens.
8. To start designing your automated process, click **Add a new stage**.
   The stage properties pane opens on the right side of the UI.
9. In the stage properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the stage would run.
10. Click **Save and close**.
11. To add another stage, click **Add another stage**.
    Similarly, you can create as many stages as you want. In this example, you can create a stage for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** stage starts immediately and has no run condition. **Contain** stage start after the previous stage is completed and has a run condition that is based on the outcome of an activity in the previous stage.
    After adding the stages, you need to add process activities for each stage.
12. Click **Add another process activity** under a particular stage (For example, Analysis stage).
    The Add activity pop-up opens.
    a. In the Add activity pop-up, select the required activity definition.
13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to stages. Similarly, you can create other process activities under each stage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Failed Login Manual Activity



14. In the Activity properties pane, add a run condition and indicate when to start the process activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Using the Failed Login Manual playbook

Use these steps to learn how you can use the Failed Login Manual playbook in the SIR Analyst Workspace and its capabilities.

Before you begin

Role required: sn_si.admin or sn_si.manager or sn_si.analyst

Procedure

1. In the SIR workspace, open a security incident.
2. Click the **Playbook** tab.

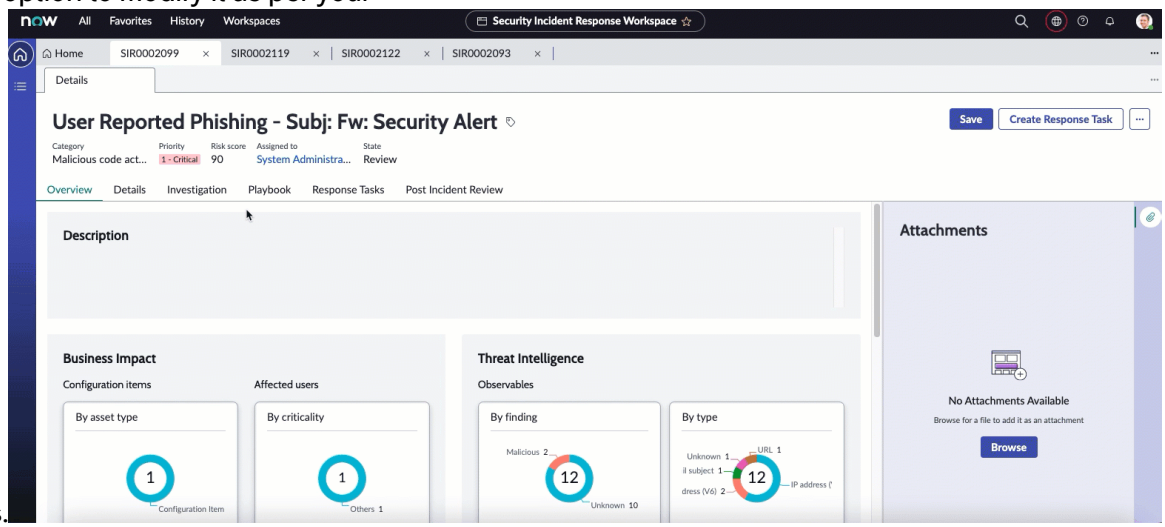
   You can view the playbooks that have been enabled for the security incident. You can also see details like the category of the security incident, risk score.

   Note: If you don't see any playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Click the **Failed Login Manual Playbook**.
   For Failed Login Manual, the tasks are automatically performed for the security incident.
4. Click each stage to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have the option to modify it as per your requirements.



6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to change them as per your requirements. If there's any remaining activity or user action that you need to perform, it is displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Flow-based Playbooks

Using the Flow Designer, security administrators and flow design authors can more easily transition from manual or undocumented playbooks to automated and repeatable playbooks. The drag-and-drop feature provides flexibility in moving objects, condition checks, parallel branching, decision tables, and more.

Security Incident Response provides the following playbooks with the base system.

In addition to the listed playbooks, there are also subflows in Security Operations Spoke that can be called from the flows playbook. Ransomware is one of that subflows.

Activate these flows before you use them. For more information, see Activate a Security Incident Response flow.

Playbook for Automated Phishing

The Automated Phishing playbook helps you resolve certain types of security threats in a step-by-step manner. With the flow designer templates, you can automate the steps in the phishing response playbook and resolve incidents quickly and efficiently.

You can use templates authored with flow designer to automate the tasks in the Phishing Response Playbook to analyze and resolve phishing attacks in your organization.

The phishing response playbook includes the following flows and subflows:

- Security Incident - Automated Phishing Response Template: This template is designed to automate the phishing response tasks and contains a sequence of actions including a trigger.
- Security Incident - Phishing Manual Template: This template is the existing manual phishing response workflow. Set the category to Phishing to activate the flow.

These templates contain a sequence of reusable actions designed to respond to phishing attacks. Each flow has a trigger (condition), a sequence of actions and subflows that you can annotate for readability. To access these flows, you must install the Security Operations spoke.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Activate these templates before you can use them. See Activate a Security Incident Response flow for details.

- Run Threat Lookups for Observables: Performs threat lookups of selected observables.
- Enrich Observables: Allows you to enrich observables with additional information from various sources.
- Assess Phishing Email Impact: Allows you to assess the impact of the phishing email. When you receive an email at the phishing email address, this subflow parses the .EML attachment and compares the information to the email matching rules.
- Eradicate Phishing Emails: Allows you to delete or eradicate phishing emails to help reduce exposure to a specific attack.
- Run Sighting Search on Observables: Determines the prevalence of a threat over time or test remediation or eradication efforts.
- Create Block Requests: Blocks communication with observables associated with the incident.

These subflows represent a set of reusable operations that you can use in multiple playbooks. You can use these subflows to define custom templates (flows) according to your requirements.

To create custom templates (flows), follow the instructions in Flows.

Run the automated phishing response playbook flow

Using the flow designer, you can define and automate tasks in the playbook to analyze and resolve phishing attacks against your organization.

Before you begin

- Role required: sn_si.admin, flow_designer, and action_designer
- Install and configure the following integrations with the right credentials:
  - Block Request (Security Operations Palo Alto Networks NGFW Integration)
  - Observable Enrichment
  - Sighting search
  - Threat Lookup
  - Microsoft Office Exchange

About this task

When employees receive a suspicious email that contains the common signs of a phishing attack (as defined by your security policies), they can send it as an .EML attachment to the phishing email address defined by your organization. Using the tasks defined in the automated phishing playbook flow, you can triage, analyze, contain, and eradicate a phishing threat. These tasks can be invoked as part of different incident states (for example, Analysis, Contain, and so forth). When a phishing security incident is created, the automated phishing flow can be automatically triggered. Using flow designer, you can view the details of the various incident response actions as they are invoked.

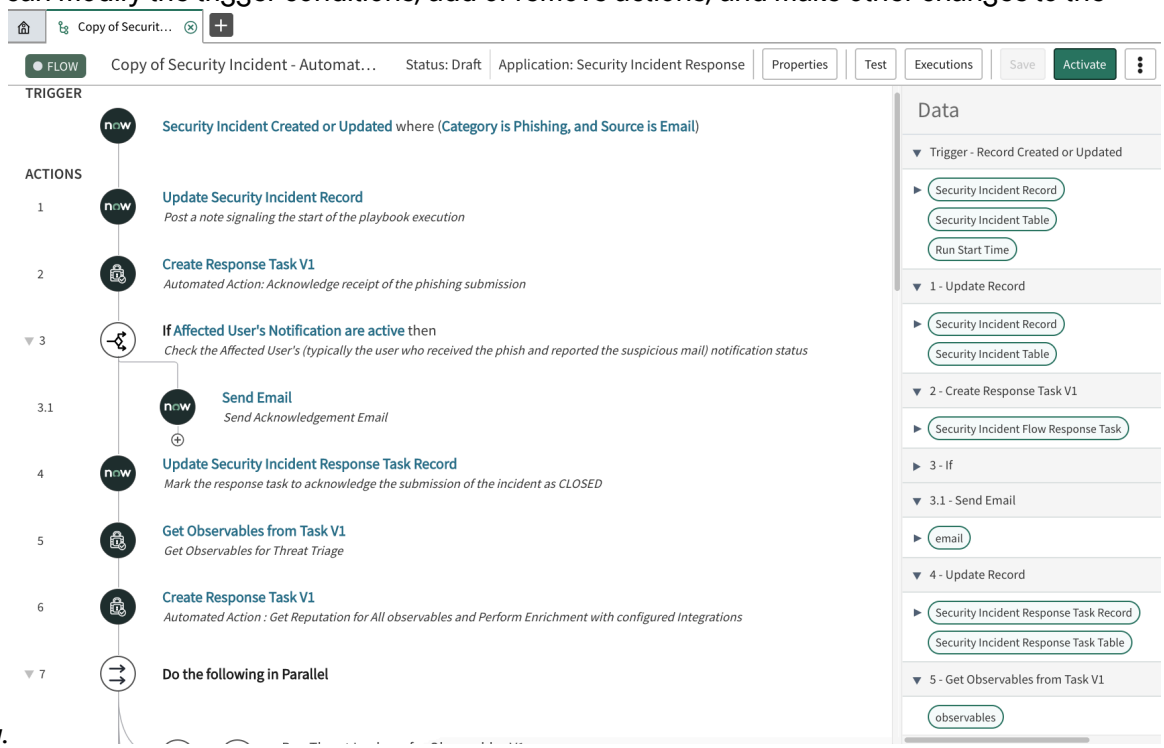
Note: The Security Incident - Automated Phishing Response Template V1 playbook flow is Read Only. You can make a copy of the flow and make changes as required.

The following steps describe how to make a copy of the phishing playbook template and walks you through some of the tasks in the flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

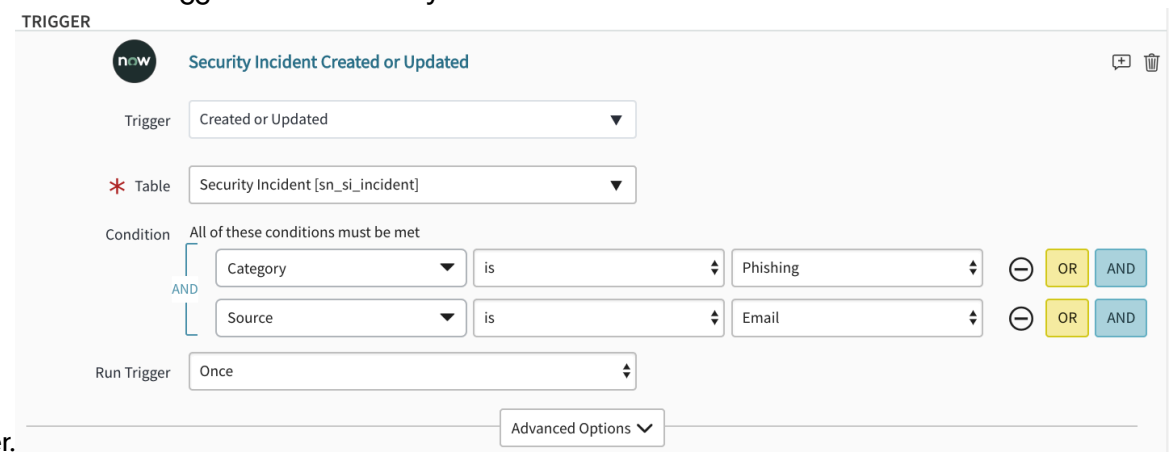
Procedure

1. Navigate to **All** > **Flow Designer** > **Designer** to view the flows available with the Security Operations Spoke.
2. Click the **Security Incident - Automated Phishing Response Template VI** link.
3. In the Flow page, click the more icon , make a copy of the flow and open it for your use. You can modify the trigger conditions, add or remove actions, and make other changes to the flow.



This image shows the trigger conditions, and the steps that the flow executes. The right-hand panel shows the data flow. Click an icon to expand the step and view the details.

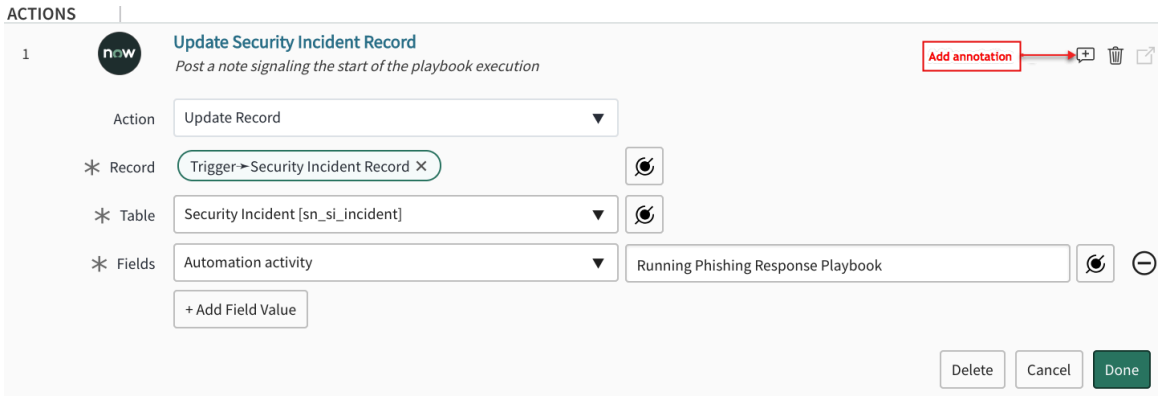
4. Click the **Trigger** icon.
   In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and how often you want the flow to execute the trigger.



When the conditions defined in the flow (Category is Phishing and Source is Email) are met in the incident record, the tasks in the automated phishing flow start executing sequentially. You can modify the trigger, add annotations, add or delete conditions, and so on.

5. Click the **Update Security Incident Record** link.

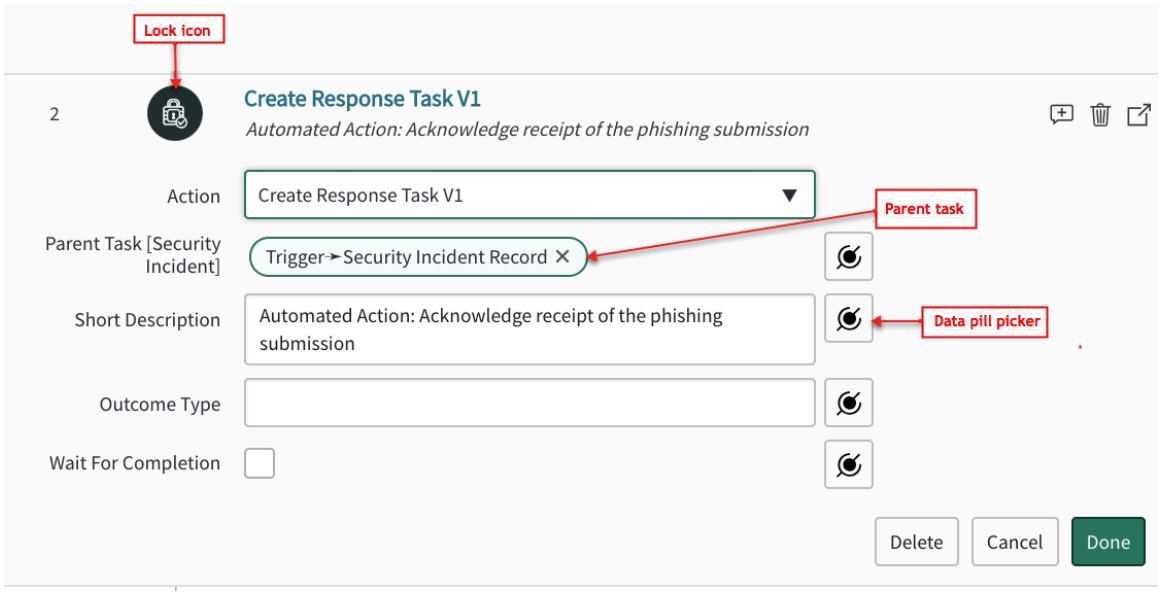
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Update Security Incident Record is the first step in the flow. Click the annotation icon to add a note to the security analyst indicating that a phishing incident has occurred, and the automated phishing playbook flow has begun executing.

6. Proceed with the step 2 in the flow, and click the **Create Response Task** link.

   In this step, the flow creates an automated response task to acknowledge receipt to the submitter of the incident or the affected user.

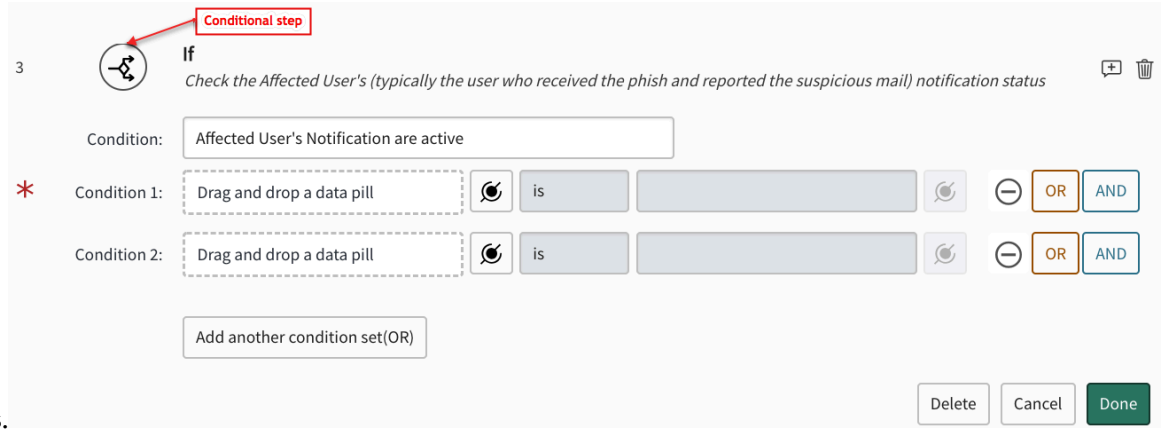


Notice the **Parent Task [Security Incident]** field references the parent record associated with this step. You can pick any reference record by using the data pill picker icon or drag the relevant reference item from the right-hand panel. Notice the lock icon . The lock icon indicates that step does not require any user intervention.

7. In step 3, the flow collects additional details of the affected user (typically the user who submitted the incident) to ensure that it can send a notification successfully.

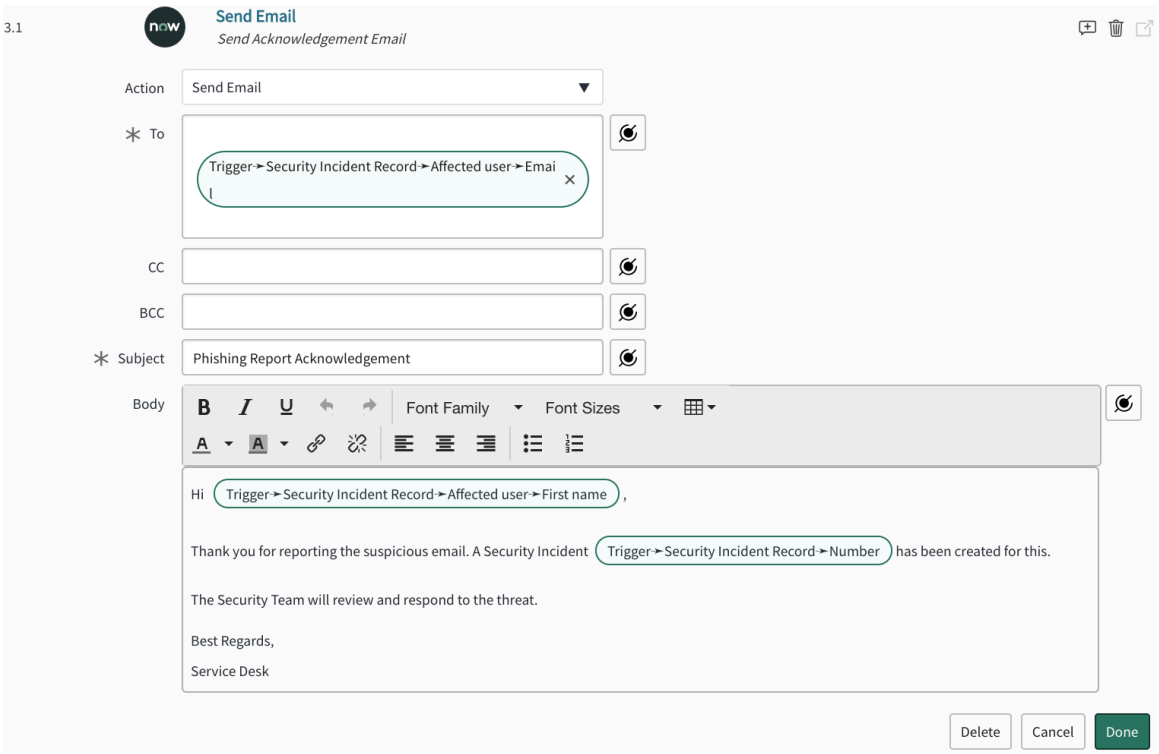
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can specify conditions to check if the affected user's status is active and the user is able to receive



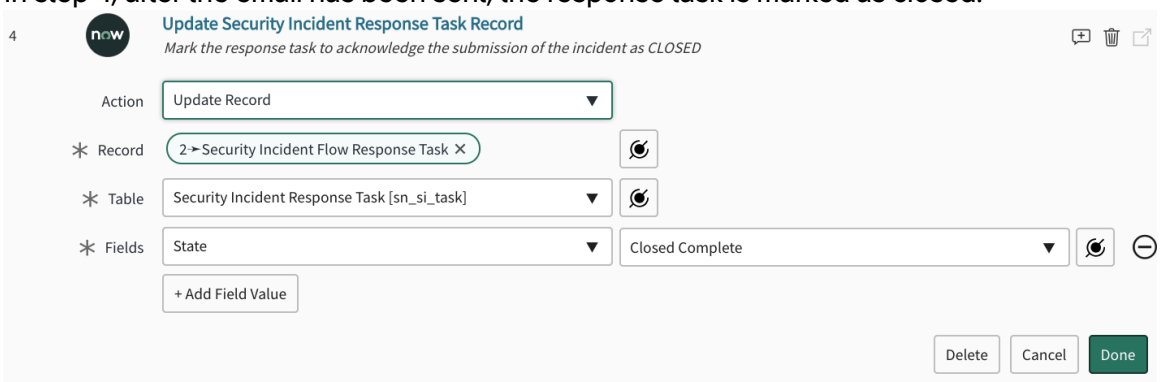
notifications.

Notice the conditional step icon in step 3. The flow executes the next step (3.1) only if the specified conditions are met.



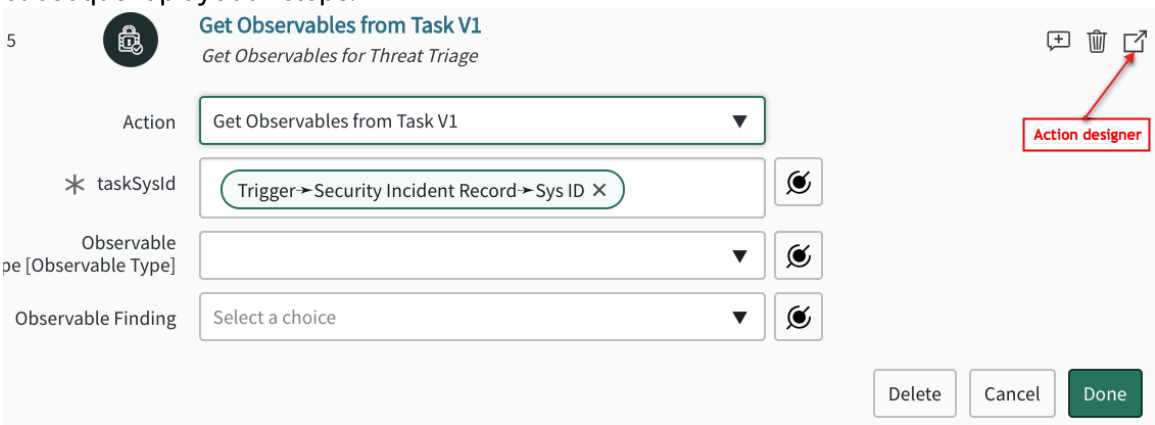
When the conditions defined in step 3 have been met successfully, the email is sent.

8. In step 4, after the email has been sent, the response task is marked as closed.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

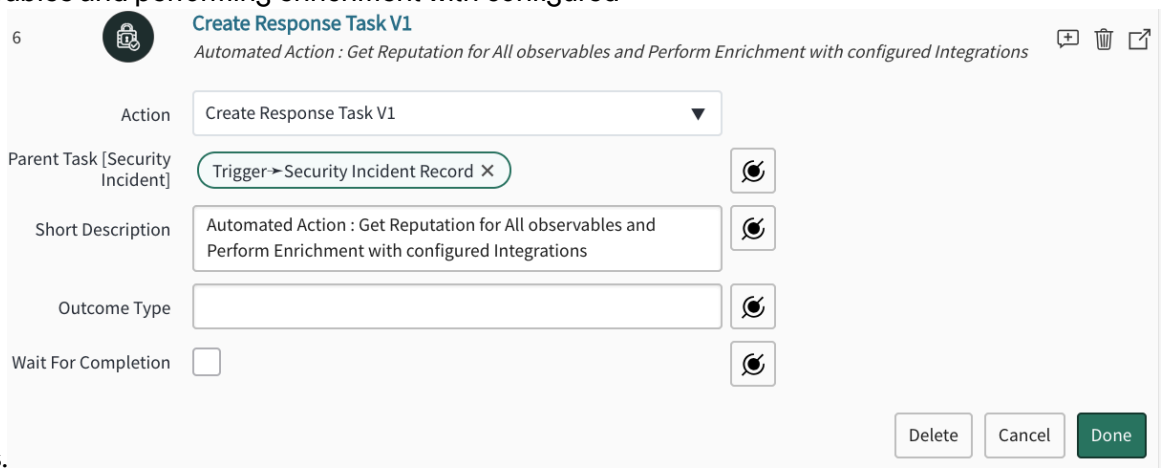
9. In step 5, all the observables involved in the incident (such as email subject, email address from which the phishing email was sent, phishing URL) or observables belonging a selected category (hash, file, or domain) are collected to perform additional automated actions in the subsequent playbook steps.



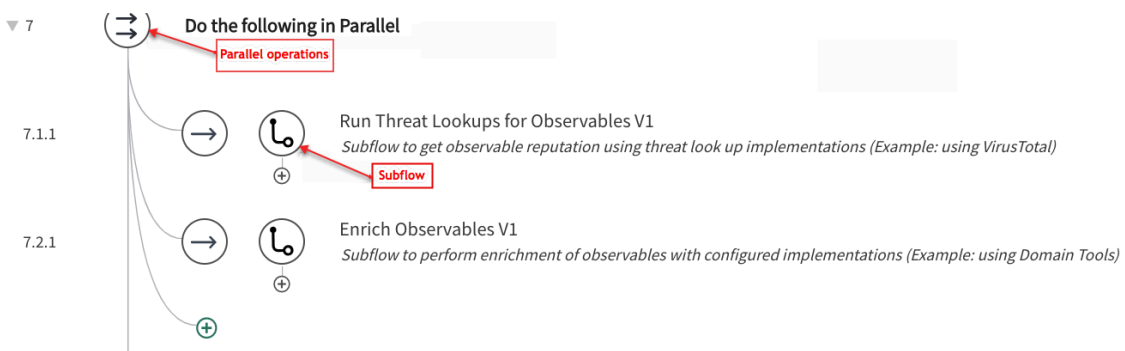
Click the action designer icon to see a detailed view of the action.

To view the Action Designer page, expand a step in the flow and click the action designer icon.

10. In step 6, an automated response task is created.
This task captures the beginning of process of getting the reputation of all observables and performing enrichment with configured integrations.

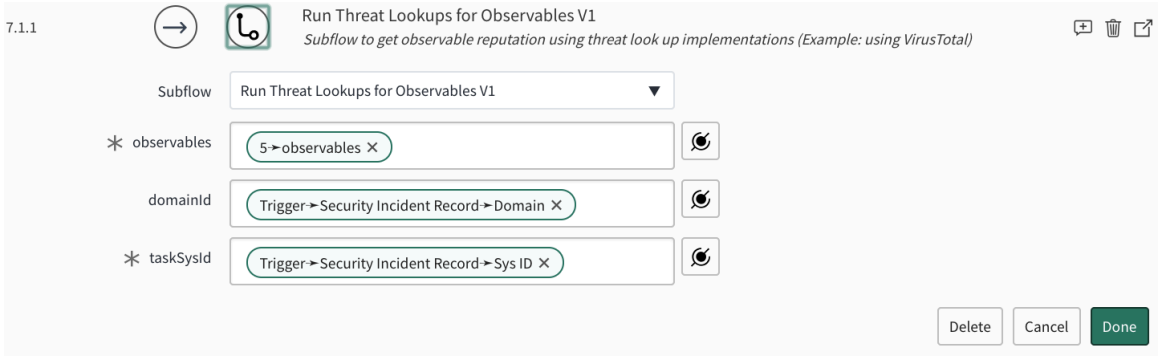


11. In step 7, two subflows are called:
    - Run Threat Lookups for Observables: This subflow is used to get the reputation of all observables using threat look up implementations.
    - Enrich Observables: This subflow is used perform enrichment of observables with configured implementations.



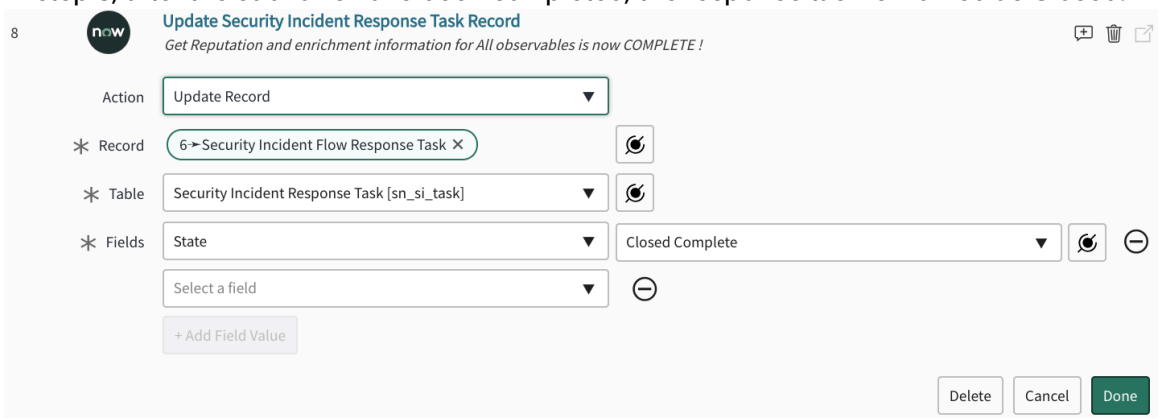
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Notice the icons for this task. The parallel operations icon indicates that both the tasks will be performed in parallel and the subflow icon indicates that the task being performed is a subflow as shown below:

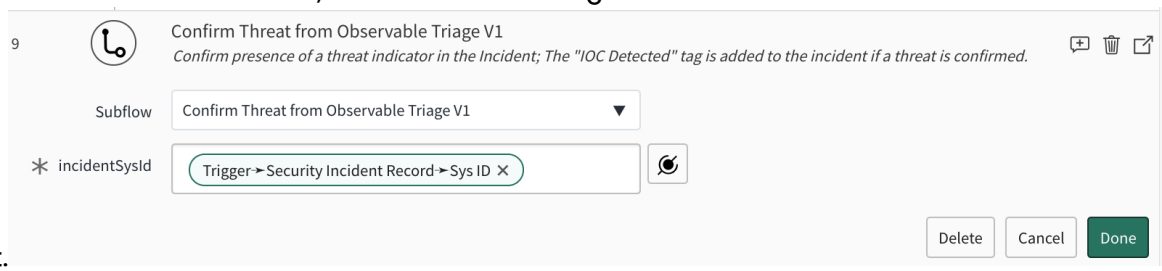


Notice the number 5 in the observables field. This indicates that the threat lookup will be run on observables retrieved in step 5. This subflow in turn calls existing workflows and actions as shown in the Subflow Designer.

12. In step 8, after the subflows have been completed, the response task is marked as Closed.

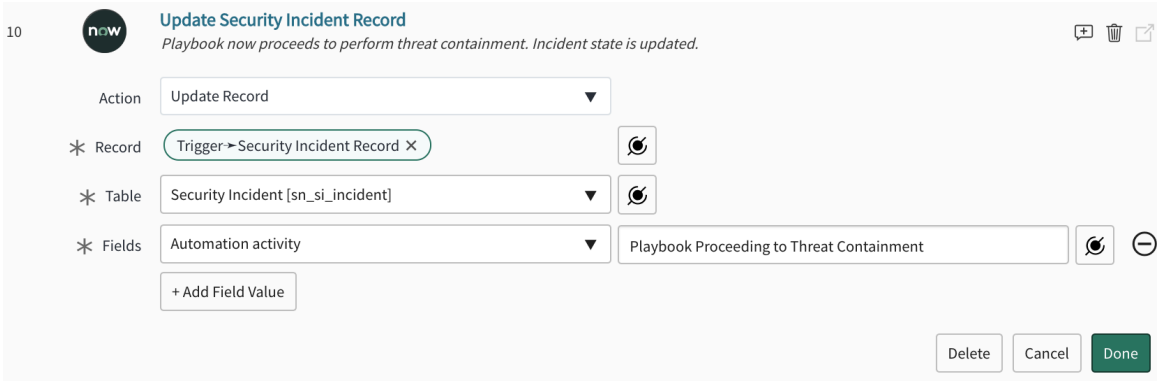


13. In step 9, the Confirm Threat from Observable Triage subflow is called. This subflow is used to confirm the presence of a threat indicator in the incident. If the threat is confirmed, an 'IOC Detected' flag is added to the incident.

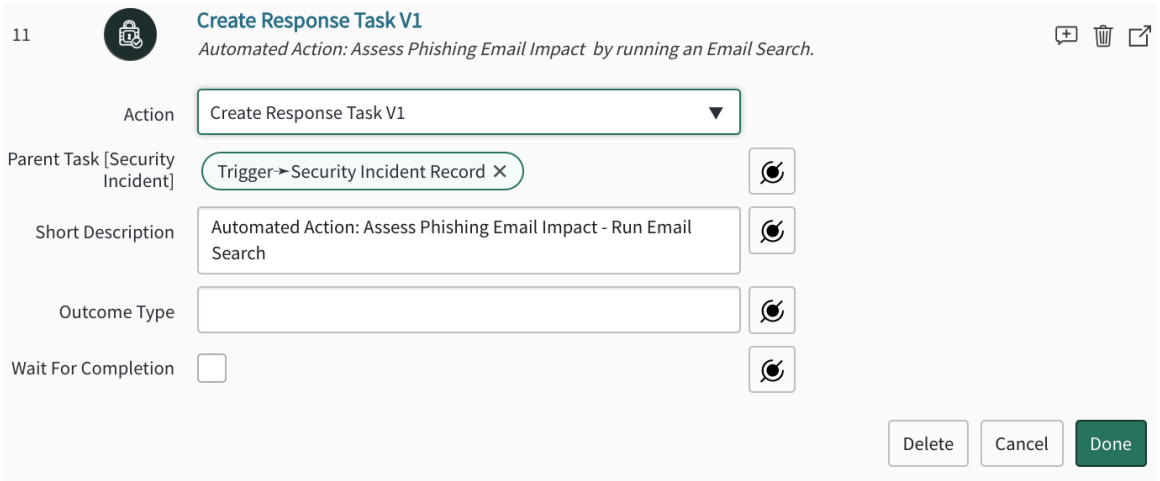


14. When the threat is confirmed, in step 10, you update the security incident and add a note indicating that threat containment tasks will be launched.

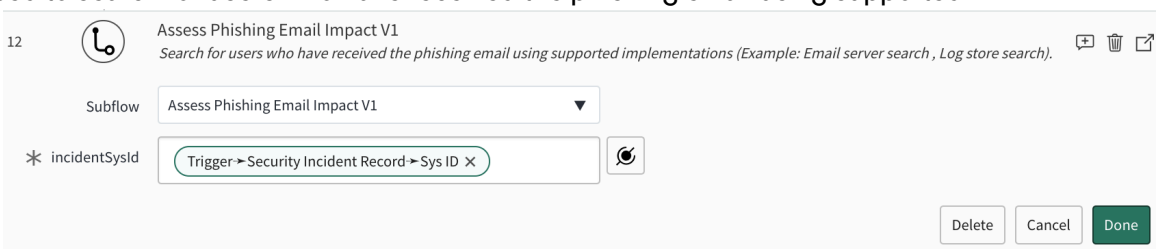
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



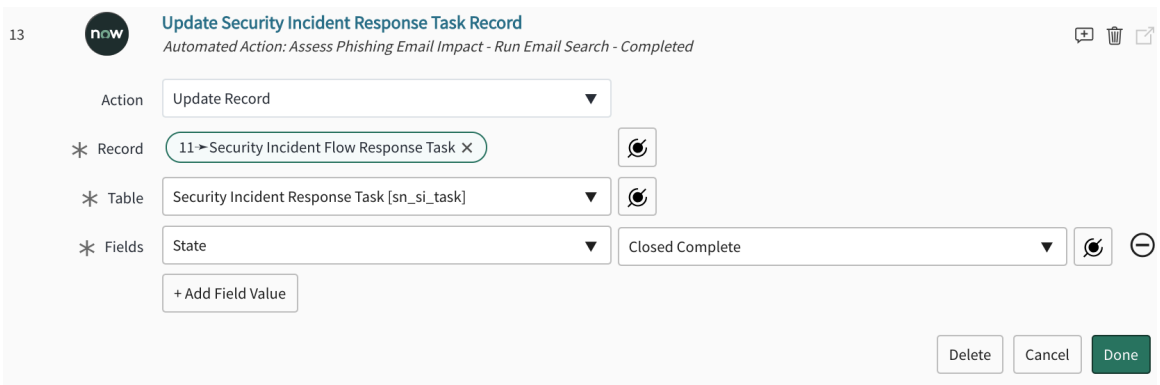
15. Step 11 is an automated response task that captures the start and completion of the task used to assess the impact of the phishing emails.



16. In step 12, the Assess Phishing Email Impact subflow is called. This subflow is used to search for users who have received the phishing email using supported implementations.

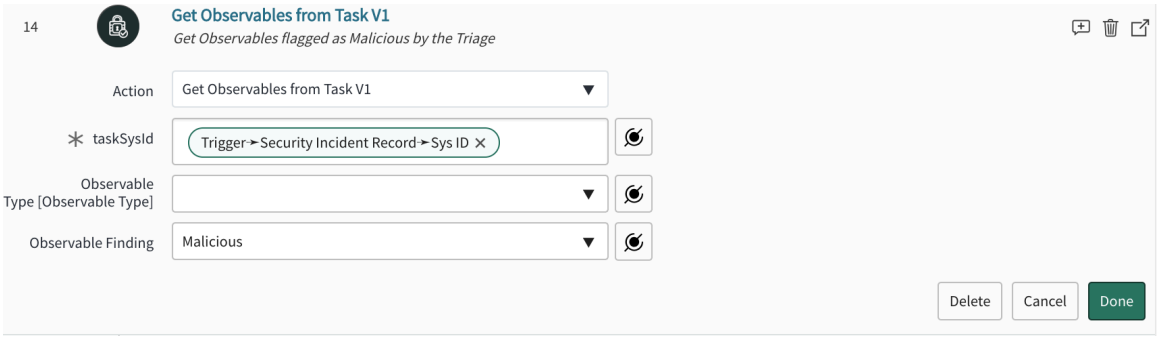


17. In step 13, the task is marked as closed to indicate that the Assess Phishing Email Impact subflow has been executed.

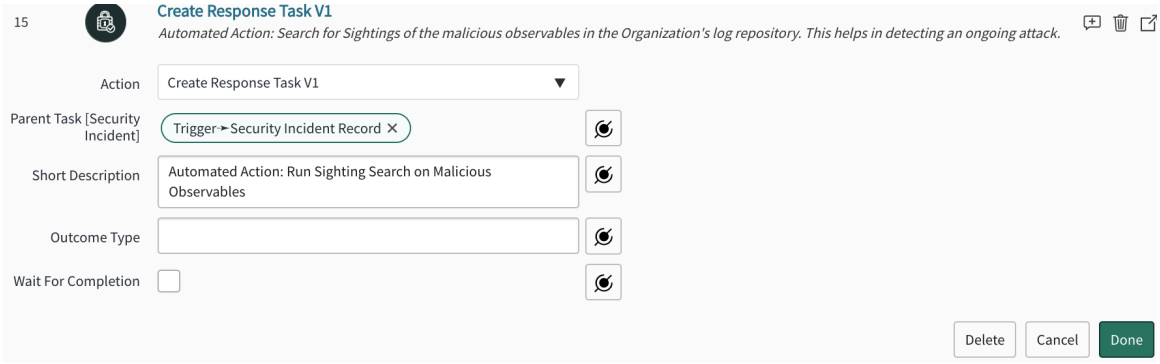


18. Step 14 is used to retrieve all observables that have been marked as malicious.

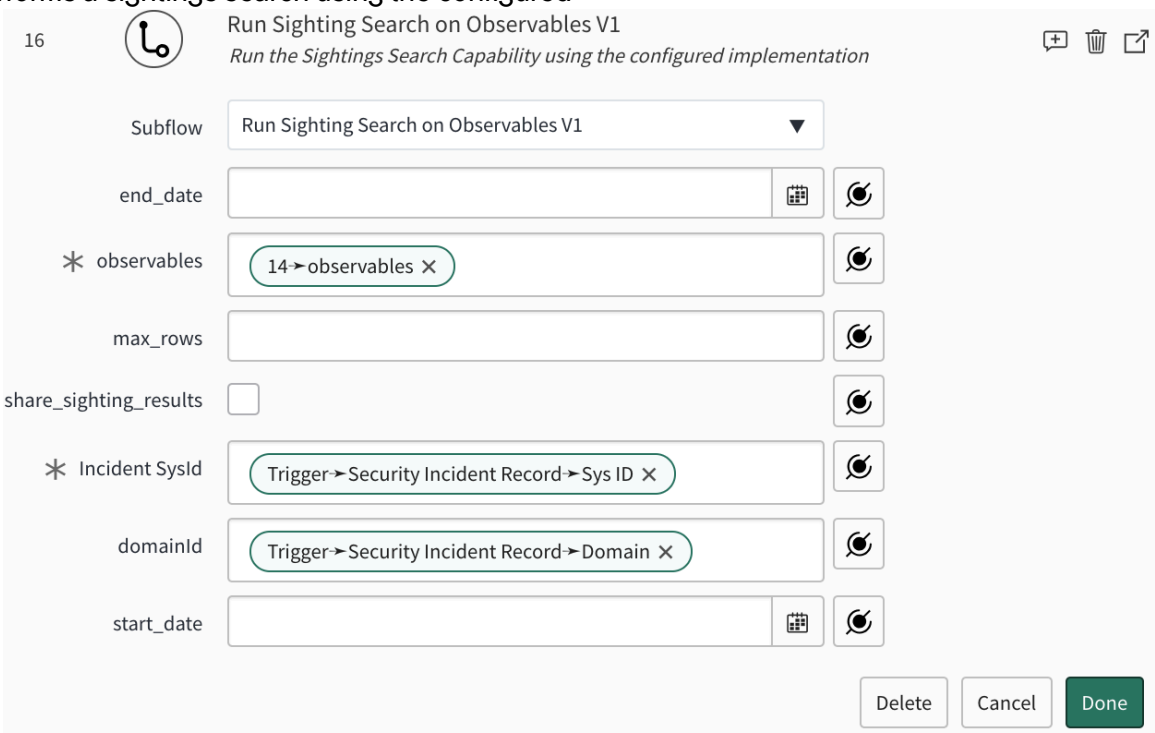
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



19. Step 15 is an automated response task that captures the start and completion of the sighting search of observables task.



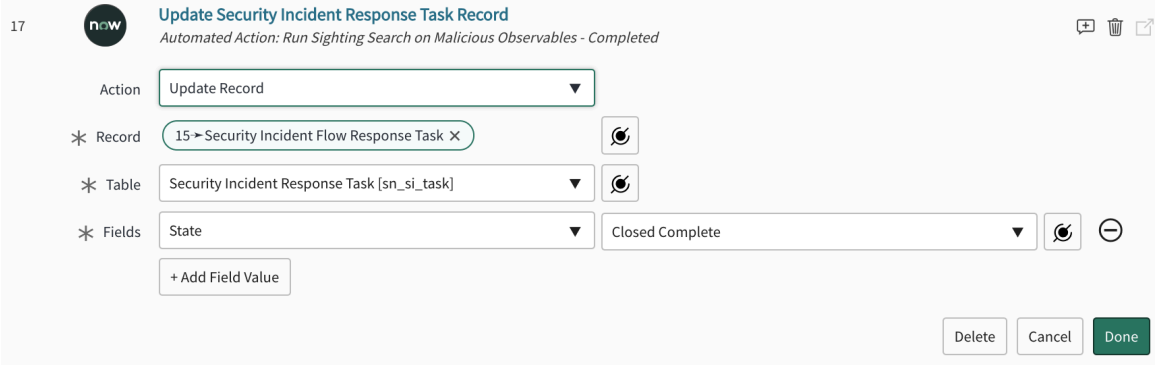
20. In step 16, the Run Sightings Search on Observables subflow is called. This subflow performs a sightings search using the configured



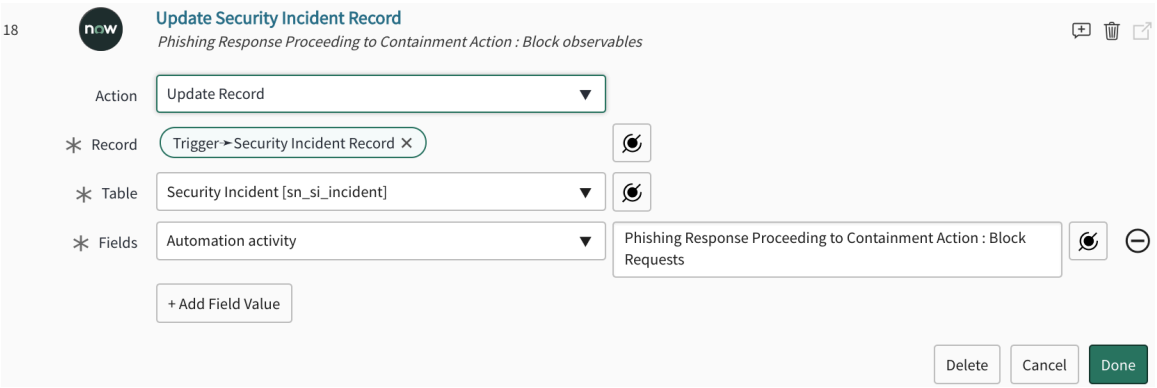
implementation.

21. In step 17, the task is marked as closed to indicate that the Run Sightings Search on Observables subflow has been completed.

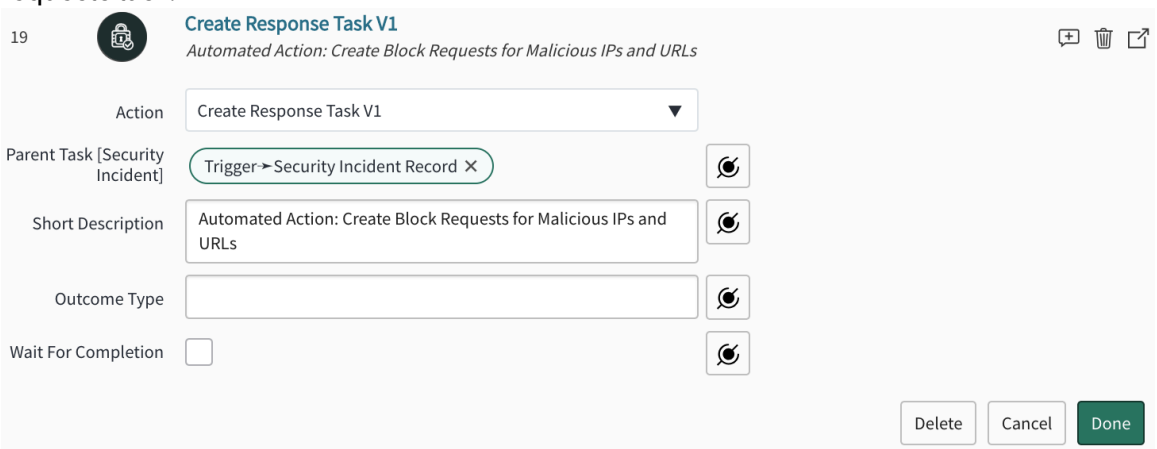
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



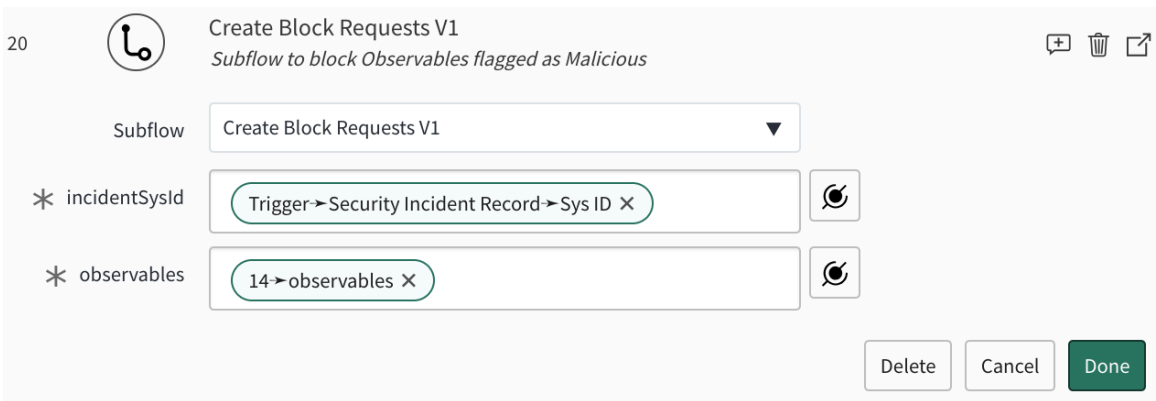
22. After you have identified the malicious observables, in step 18, you update the security incident record to indicate that the containment actions will now commence.



23. Step 19 is an automated response task that captures the start and completion of the block requests task.

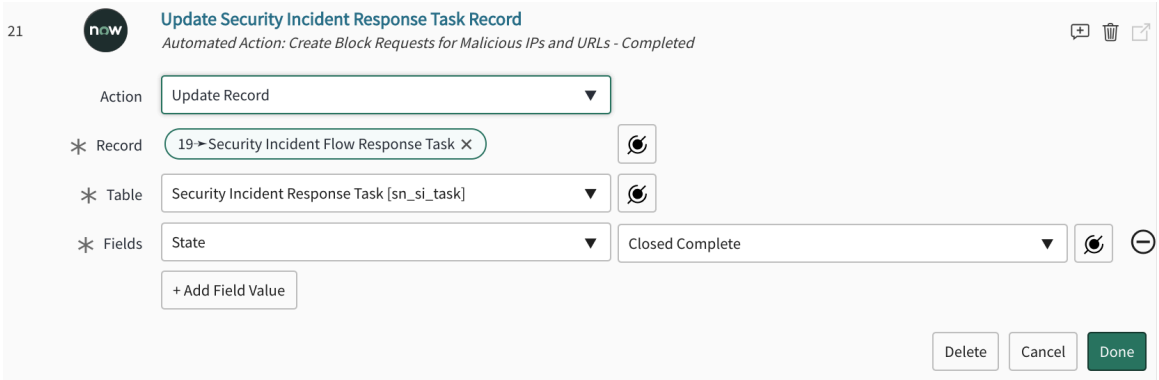


24. In step 20, the Create Block Requests subflow is called. This subflow is used to block malicious observables.

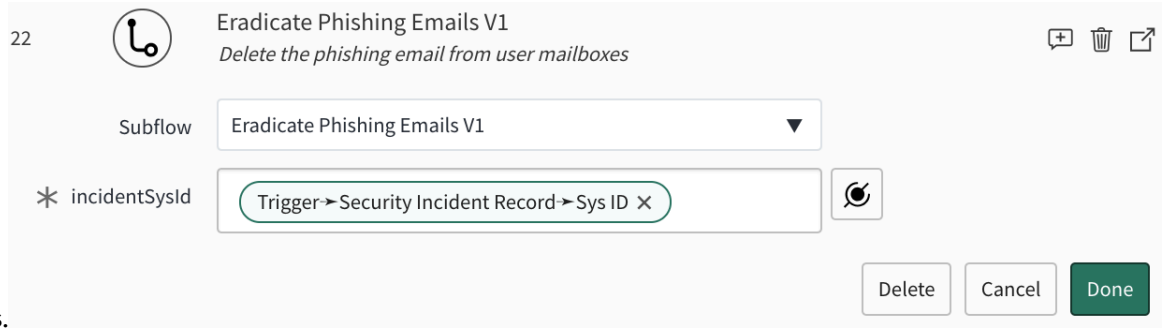


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

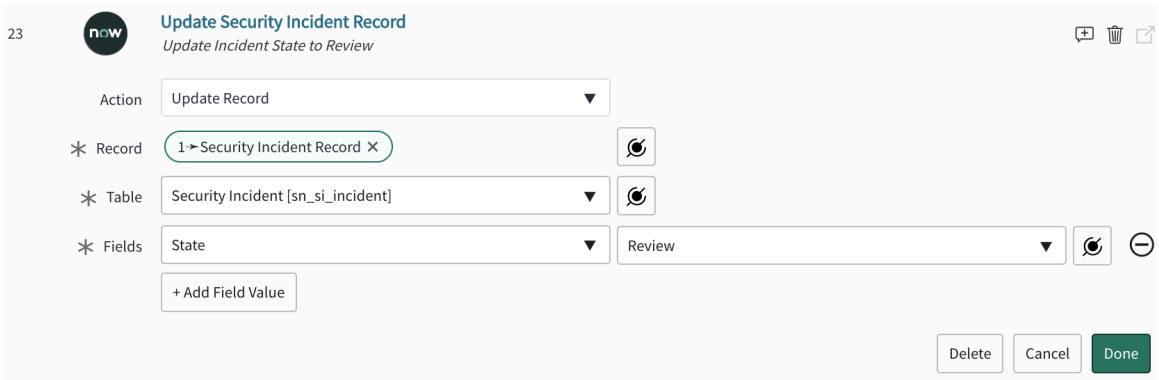
25. In step 21, the task is marked as closed to indicate that the Create Block Requests subflow has been completed.



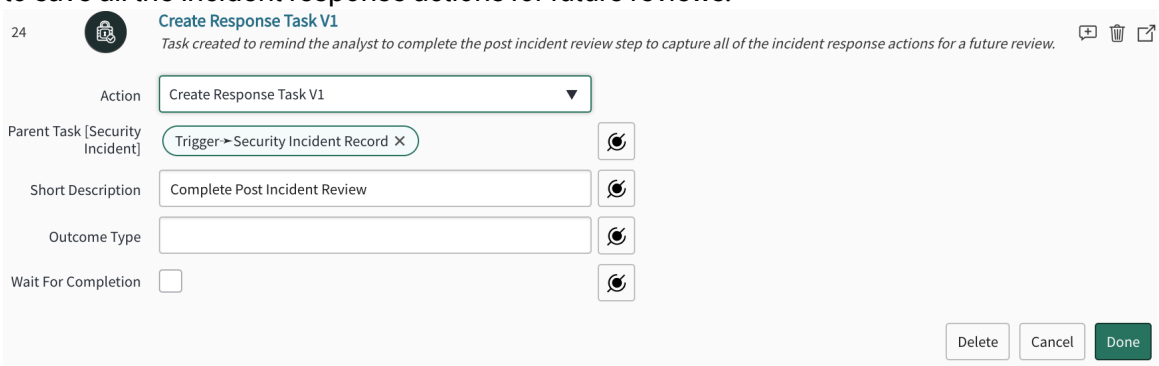
26. In step 22, the Eradicate Phishing Emails subflow is called. This subflow is used to delete phishing emails from user mailboxes.



27. After the phishing emails have been deleted, in step 23, you update the security incident record to indicate that the incident status needs to be reviewed.



28. In the last step, the flow creates an automated response task. This task is used to send a reminder to the security analyst to save all the incident response actions for future reviews.

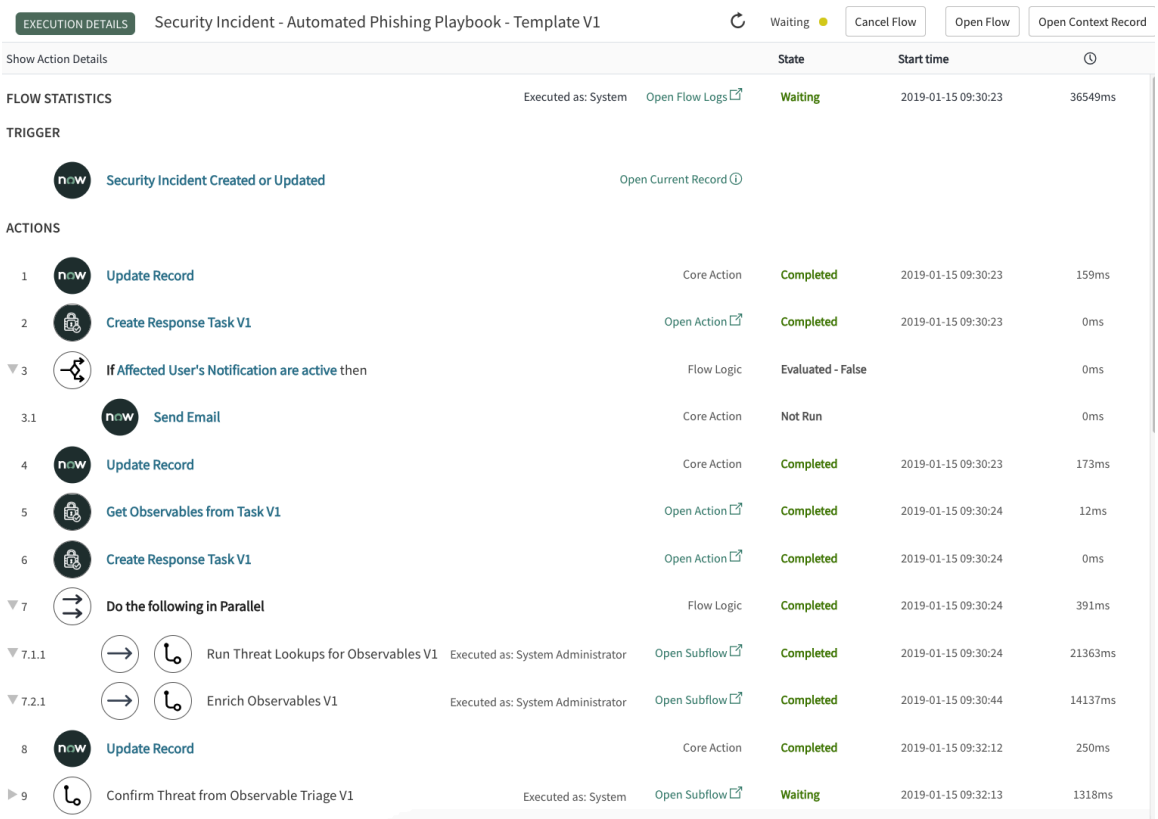


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

You can click **Test** to simulate the actions in the flow before you publish it. After testing the flow, click **Activate** to activate the flow and execute it.

Click **Executions** to view the execution details of the flow.



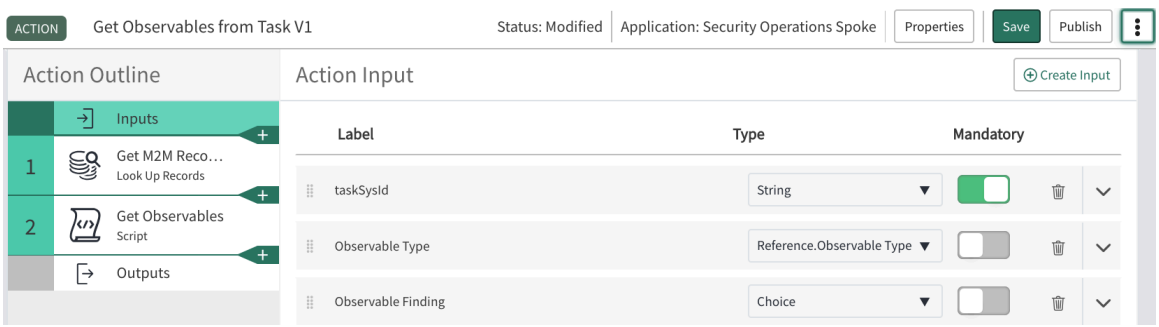
View automated phishing response playbook flow action designer

You can drill down to the Action Designer to view detailed information about the actions being performed for a specific step in the automated phishing response playbook flow.

This page describes the Action Designer page for the Get Observables from Task step. Click a task in the Action Outline panel to view the details.

Action Input

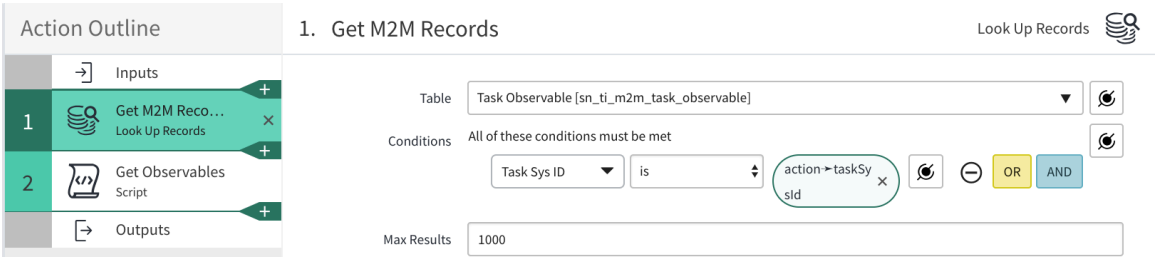
This section shows details on how the action was created including the incident id, the type of observable (hash or IP) and observable finding (malicious emails only).



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

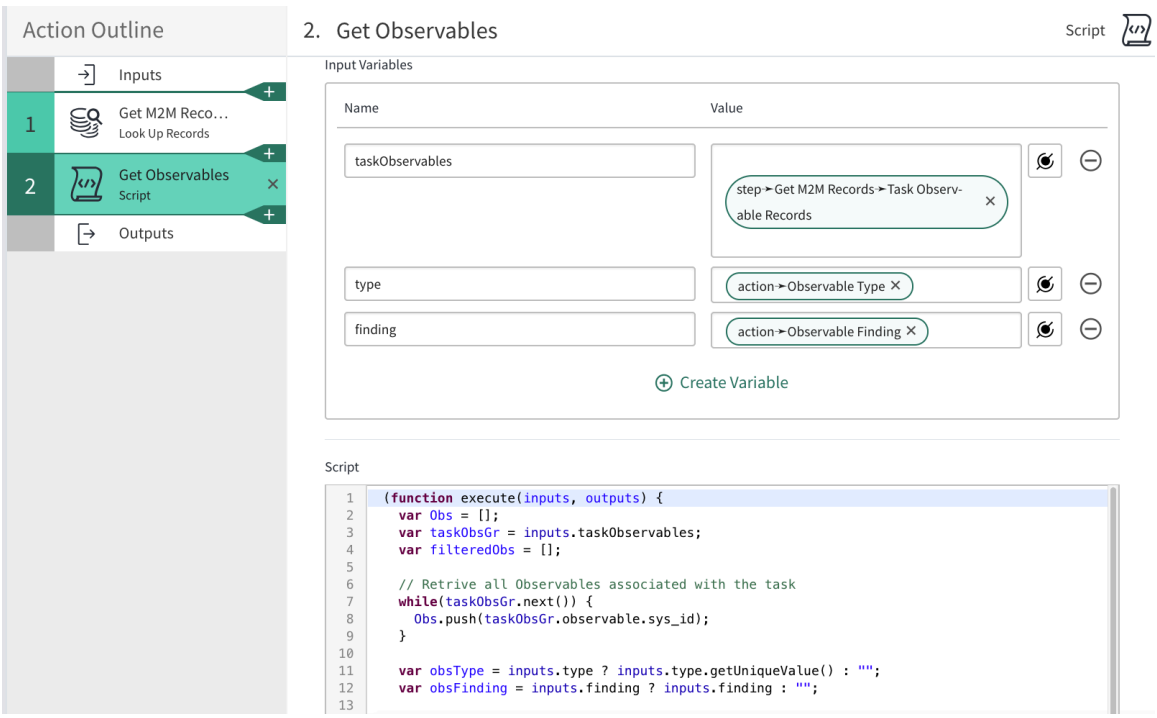
Get M2M Records

This section shows the conditions that have been defined to search for observables in a specified table.



Get Observables

This section shows the script used to retrieve observables based on the specified filter conditions. Finally, the observables meeting this criteria and the count is displayed.



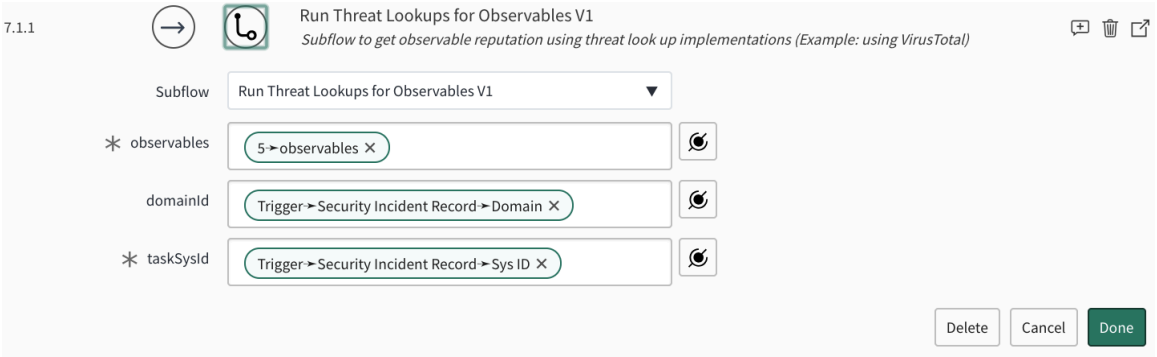
Note: All actions defined in this flow are reusable and can be modified according to your requirements.

View the automated phishing response playbook subflow designer

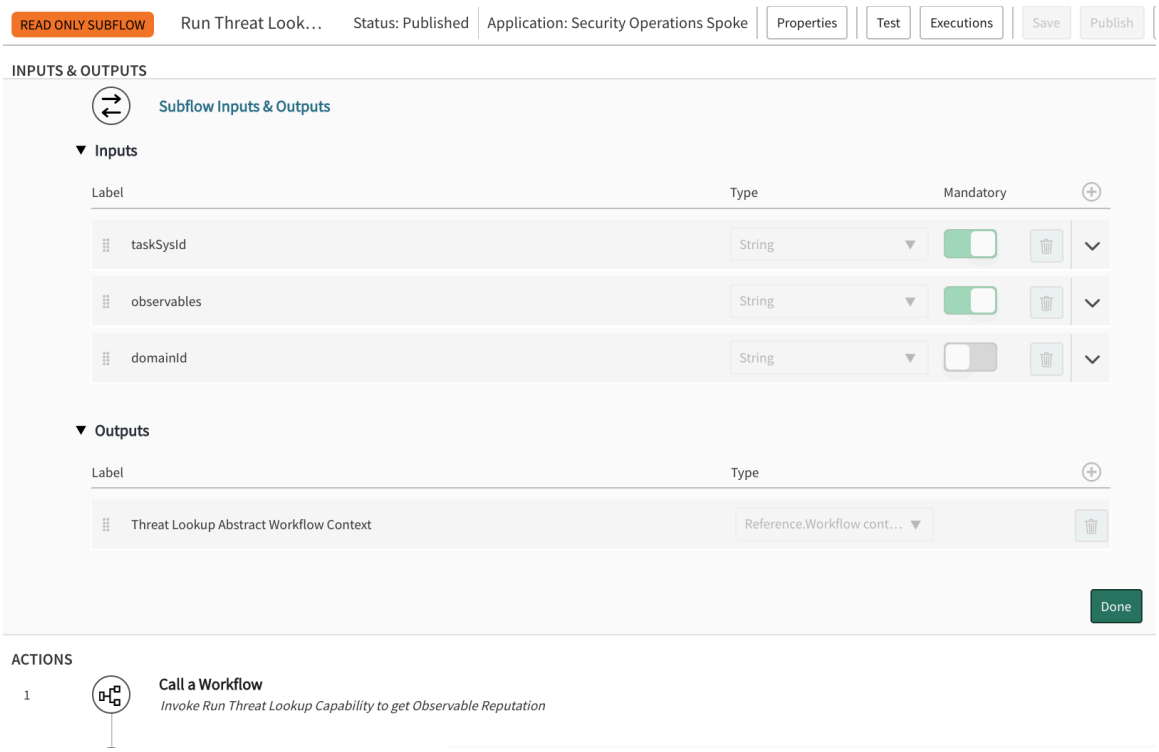
You can drill down to the Subflow Designer to view detailed information about the subflow being executed as part of the automated phishing response playbook flow.

You can launch the Subflow Designer to view additional details of a subflow. The Subflow Designer page for the Run Threat Lookups for Observables subflow is shown here. Click the icon in the image below to view the Subflow Designer.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



In the Subflow Designer page, you can see the inputs and outputs for this subflow, and the underlying workflow actions that are being executed.



Note: This subflow is read only and cannot be edited. You can add or delete subflows to the step but you cannot modify the subflow.

Playbook for Automated Malware

The Automated Malware playbook provides a sequence of automated steps that helps you resolve malware alerts quickly and efficiently.

Use the malware playbook flow to automate the steps involved in handling malware alerts from the endpoint or the network. The flow template includes trigger conditions, a sequence of actions and subflows that are annotated for readability.

These templates contain a sequence of reusable actions designed to respond to phishing attacks. Each flow has a trigger (condition), a sequence of actions and subflows that are annotated for readability. To access these flows, you must install the Security Operations spoke and Security Operations Palo Alto Networks - WildFire app from the ServiceNow Store.

Note: You must activate these templates before you can use them.

The following flows and subflows are included:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Incident - Automated Malware Playbook Template: This template is designed to automate the responses to malware alerts and contains a sequence of actions including a trigger.
- Security Incident - Malware Manual Template: This template is the existing manual malware response workflow that is activated when the category is set to Malicious Code Activity.

Subflows

- Confirm Threat from Observable: Verifies if the observables is malicious and needs to be addressed.
- Set Incident Severity: Sets a severity status for the incident.
- Ransomware Playbook: Determines whether it is a ransomware attack.

These subflows represent a set of reusable operations that can be used in multiple playbooks. You can use these subflows to define custom templates (flows) according to your requirements.

To create custom templates (flows), follow the instructions in Flows.

Run the automated malware playbook flow

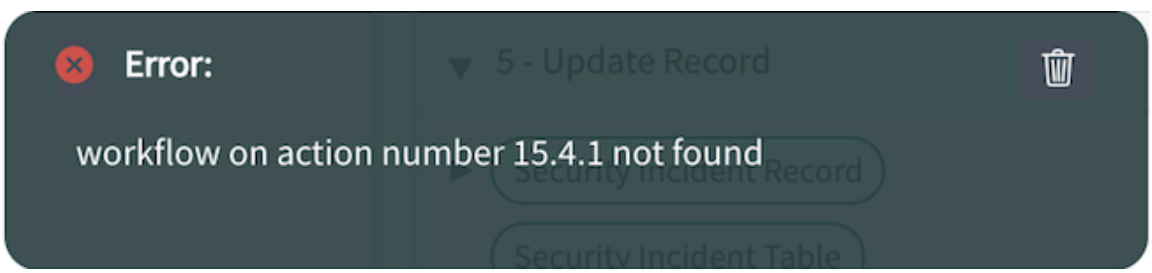
Use this flow to automate tasks in the playbook to analyze and resolve malware attacks against your organization.

Before you begin

- Role required: sn_si.admin, flow_designer, and action_designer
- Install and configure the following integrations with the correct credentials:
  - Palo Alto Networks WildFire for Security Operations
  - Sighting Search (Splunk)
  - Block Requests
  - Threat Lookup
  - Enrich Observables

  Verify that these integrations are working properly before you activate the Security Incident - Automated Malware Playbook Template.

- Security Operations Palo Alto Networks Wildfire App: To access the automated malware playbook flow, you must install the Security Operations Spoke and Security Operations Palo Alto Networks - WildFire app from the ServiceNow Store. If the Security Operations Palo Alto Networks Wildfire App is not installed, you will see an error "workflow on action number 15.4.1 not found" as shown below:



  If you do not want to install this App, delete steps **15.2, 15.3, and 15.4** from the automated malware playbook flow.

- Ensure that the following conditions have been met:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The security incident has been assigned to a security analyst who belongs to the appropriate approval group.
- The security analyst handling the incident must have a valid email address.
- The necessary configuration items and observables have been added to the security incident.

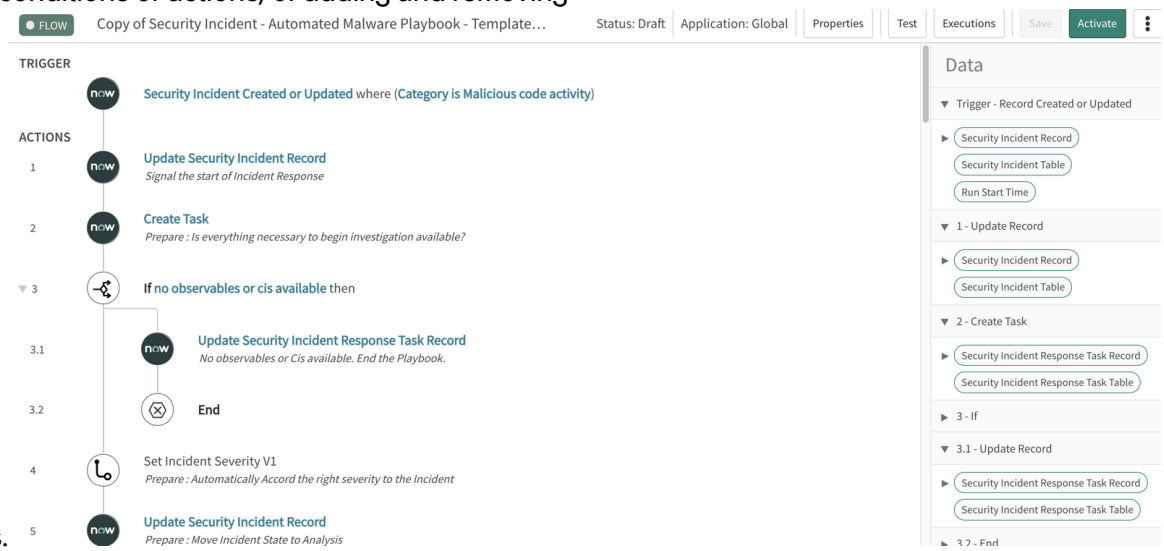
- For **step 21 (Ask for Approval)**, change the Group from **Security Incident Assignment** to your preferred group.
- Step 21 of the flow is a mandatory task approval step where an approval request is sent to the administrator. To approve the request, the administrator must navigate to the Task Approvals page and set the State field to **Approved**. If the task is not approved, the flow designer cannot proceed further and the process ends.

About this task

When a malicious code activity is detected in the network, a security incident is created and the automated malware playbook flow is launched. You can use the tasks defined in the automated malware playbook flow to triage, analyze, contain, and eradicate the threat.

Procedure

1. Navigate to **All** > **Flow Designer** > **Designer** to view the flows available with the Security Operations spoke.
2. Click the **Security Incident - Automated Malware Playbook Template VI** link.
3. In the Flow page, click the more icon , make a copy of the flow and open it for your use. You can now make changes to your flow, such as modifying trigger conditions or actions, or adding and removing actions.

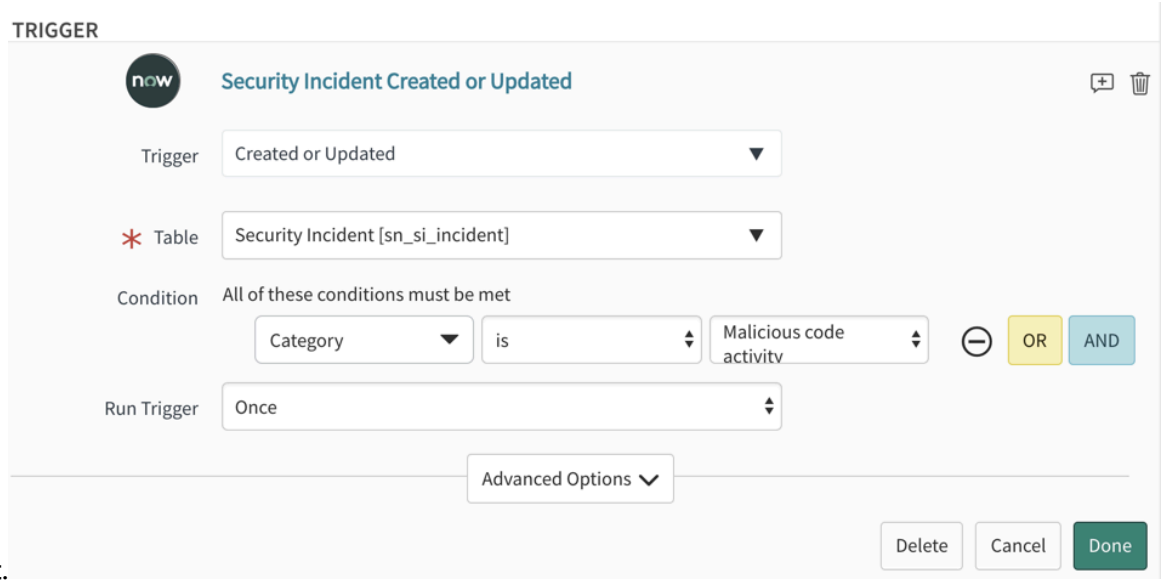


   This shows the trigger and the steps that will be executed with the flow. The-right hand panel shows the data flow. Click on an icon to expand the step and view the details.

4. Click the **Trigger** icon.

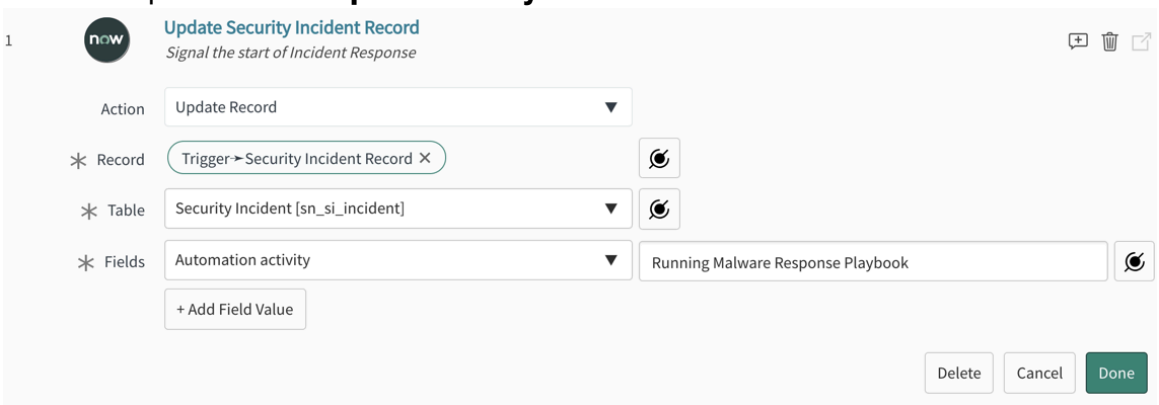
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the first step, you define or set the trigger for the flow. Specify the conditions for the trigger and task to be performed when the conditions are met.



When the condition defined in the flow (Category is Malicious Code activity) is met in the incident record, the tasks in the automated phishing flow start executing sequentially. You can modify the trigger, add annotations, add or delete conditions, and so on.

5. The first step in the flow is **Update Security Incident Record**.

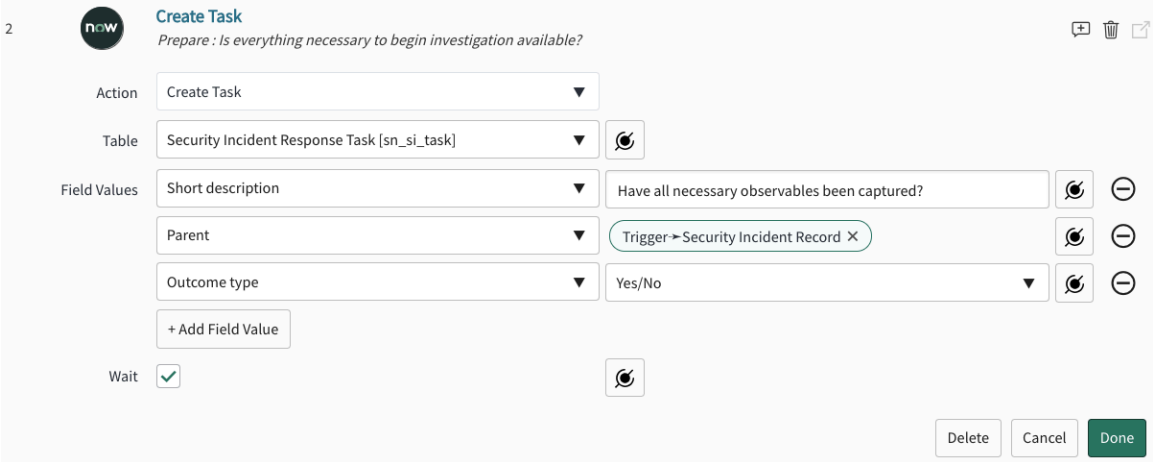


Click the link and click the annotation icon to add a note to the security analyst indicating that there has been some malicious code activity, and the automated malware response playbook flow has begun executing.

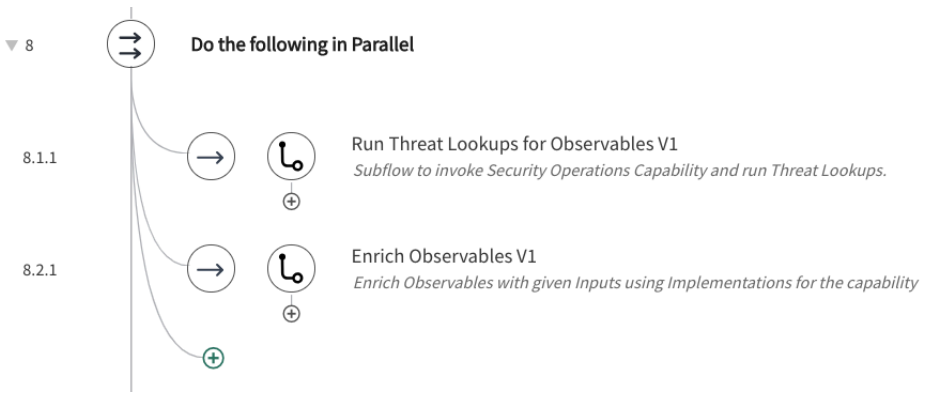
6. Proceed with the step 2 in the flow and click the **Create Task** link.

In this step, an automated response task is created to check if all the necessary observables have been captured and if the investigation can begin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

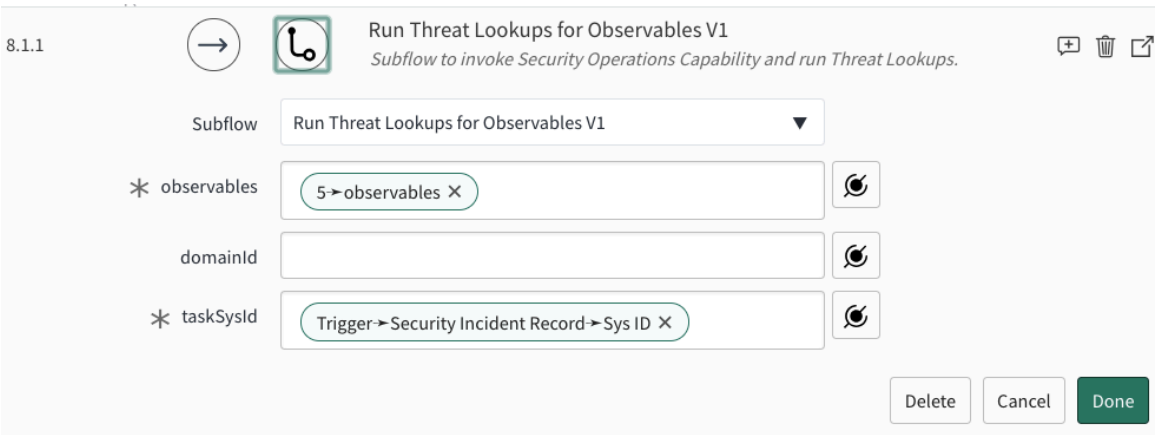


7. If the Outcome type is **No**, this indicates that no observables and CIs are available to initiate the investigation.
   Update the security incident record to indicate that the playbook cannot proceed further.
8. If the Outcome type is **Yes**, the Set Incident Severity subflow automatically assigns the correct severity to the security incident.
9. In the next step, the security incident record is updated.
10. In the next step, all observables involved in the incident or a selected category are collected to perform additional automated actions in the subsequent playbook steps.
11. In the next step, an automated response task is created.
    This task captures the beginning of process of getting the reputation of all observables and performing enrichment with configured integrations.
12. In step 8, two subflows are called:
    - Run Threat Lookups for Observables: This subflow is used to get the reputation of all observables using threat look up implementations.
    - Enrich Observables: This subflow is used perform enrichment of observables with configured implementations.



Notice the icons for this task. The parallel operations icon indicates that both the tasks will be performed in parallel and the subflow icon indicates that the task being performed is a subflow as shown below:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Notice the number 5 in the observables field. This indicates that the threat lookup will be run on observables retrieved in step 5. This subflow in turn calls existing workflows and actions.

13. In the next step, the Run the Look Up Records action is executed.
    This action is used to look up workflow context records where the parent workflows can be one of the following.
    - Threat Lookup Abstract Workflow Context
    - Observable Enrichment Abstract Workflow Context
14. In the next step, the reputation and enrichment results are reviewed for every 8 records.
15. Continue reviewing the next steps:
    a. Update Security Incident Record: Updates the security incident record to indicate that the reputation lookup and enrichment activities have been completed.
    b. Get Observables from Task: Retrieves all the malicious observables associated with the security incident.
    c. Create Task: Checks and confirms if the automated triage runs have been successful.
16. If there are observables that have been flagged as malicious:
    a. Update Security Incident Record: Post a worknote indicating that a threat has been detected.
    b. Create Input Query from Observables: If more than ten observables have been flagged as malicious, the Sighting Search on Observables subflow (on Splunk or Carbon Black) is executed.
17. If the observables are not flagged as malicious, the flow continues with the following steps:
    a. Update Security Incident Record: Post a worknote indicating that no threat has been detected
    b. Get Observables from Task: Identifies all SHA256 Hash Ids from the incident.
    c. Look Up Observable Records: Looks up records that meet this criteria.
18. Continue reviewing the next steps:
    a. For each malicious observable, the **Security Operations Palo Alto Networks - Get Wildfire Data Enrichment** workflow is executed.
    b. Reviews the investigation results to see if they are satisfactory.
    A response task is created to check if the suspected malware is a ransomware attack. If yes, the Ransomware Playbook subflow is executed.

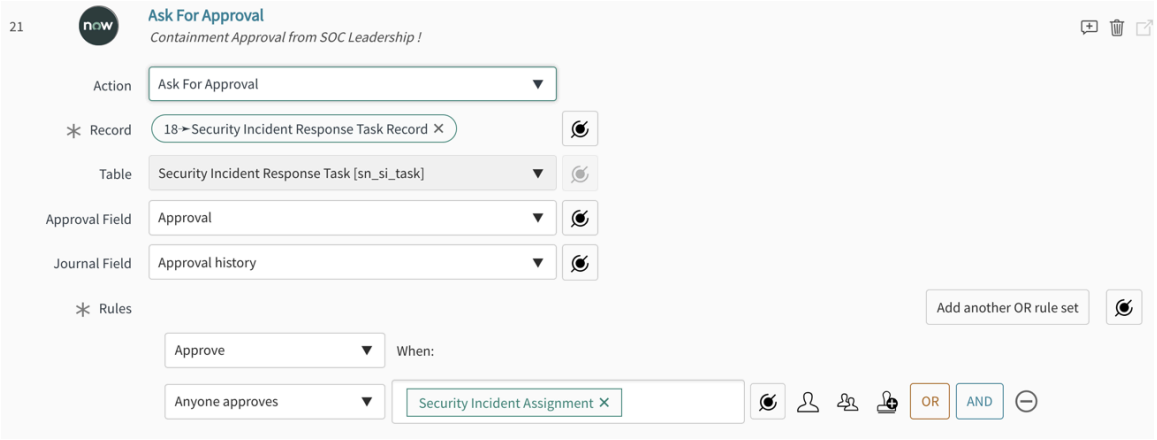
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. In the next step, an email is sent with a summary of the analysis and request for approval to initiate containment procedures.

d. A task is created to capture details of the approval requested.

e. The next step is to update the security incident record.
Post a worknote informing the security analyst that the approval request has been made.

f. Requests approval to contain the malware attacks from your SOC manager.



Note: When an approval request will be generated by the flow, the Work note will be updated with the following message:

`An Approval request has been made for <task id> proceeding with containment.` To approve this task, as a SOC manager, follow these steps manually:

- Navigate to the Task Approvals page.
- You will see the list of approvals. Click the <task id> that is to be approved.
- Change State to **Approve** and Save the updated <task id>.

g. In the next step, the security incident record is updated to track the approval status.

h. Next, a task is created to initiate containment procedures.

i. The Run the Create Block Requests for Malicious Observables subflow is executed and an incident record is created with a request to rebuild the infected device and its assets.

j. Next, a task is created to run sightings search to confirm if the environment is secure.
The sightings search is repeated till no sightings found.

k. Next, a task is created to indicate that the security incident record is ready for review.

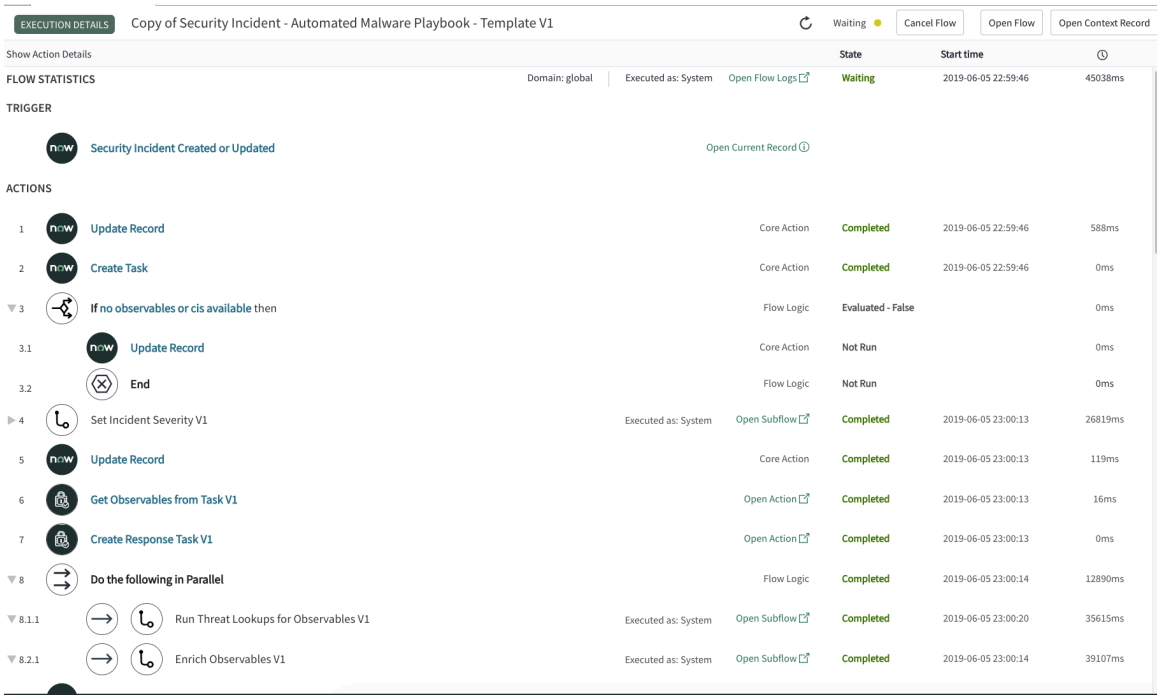
l. Finally, the record is updated and moved to the Review stage.

What to do next

You can click **Test** to simulate the actions in the flow before it is published. After testing the flow, click **Activate** to activate the flow so that it can be executed.

Click **Executions** to view the execution details of the flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Playbook for Failed Login Manual

When a user makes certain unsuccessful login attempts (according to the SIM configuration), a security incident is created.

These unsuccessful login attempts may either be false positives or attempts made by attackers to obtain access to user email accounts. In such scenarios, the Failed Login Manual playbook can provide guidance and help optimize the investigation of failed login security incidents.

Prerequisites

Role required:

- sn_si.admin
- flow_designer

Spoke: Install Security Operations Spoke (sn_sec_spoke)

Key capabilities

The Failed login playbook covers the following capabilities to investigate security incidents:

1. Checks if the affected user is an active/inactive user
2. Filters allowed list observables
3. Enriches the observables
4. Performs automated threat lookup.
5. Sends automated email to the user to confirm the failed login attempt.
6. Assigns tasks to analyst to investigate user access
7. Identifies malicious observables and block IPs and URLs.
8. Resets user password.
9. Updates security incident status
10. Assigns tasks to a security analyst to handle post-incident review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Capabilities required

- Threat Lookup (Virus Total, Hybrid Analysis)
- Observable Enrichment (Whois, ReverseWhois)
- Sighting Search (Splunk, QRadar)
- Observable Blocking (CheckPoint, Palo Alto)

For more information, see the ServiceNow store.

Security analyst experience

To understand how to resolve security threats in a step-by-step manner, see Resolve security threats with the playbook.

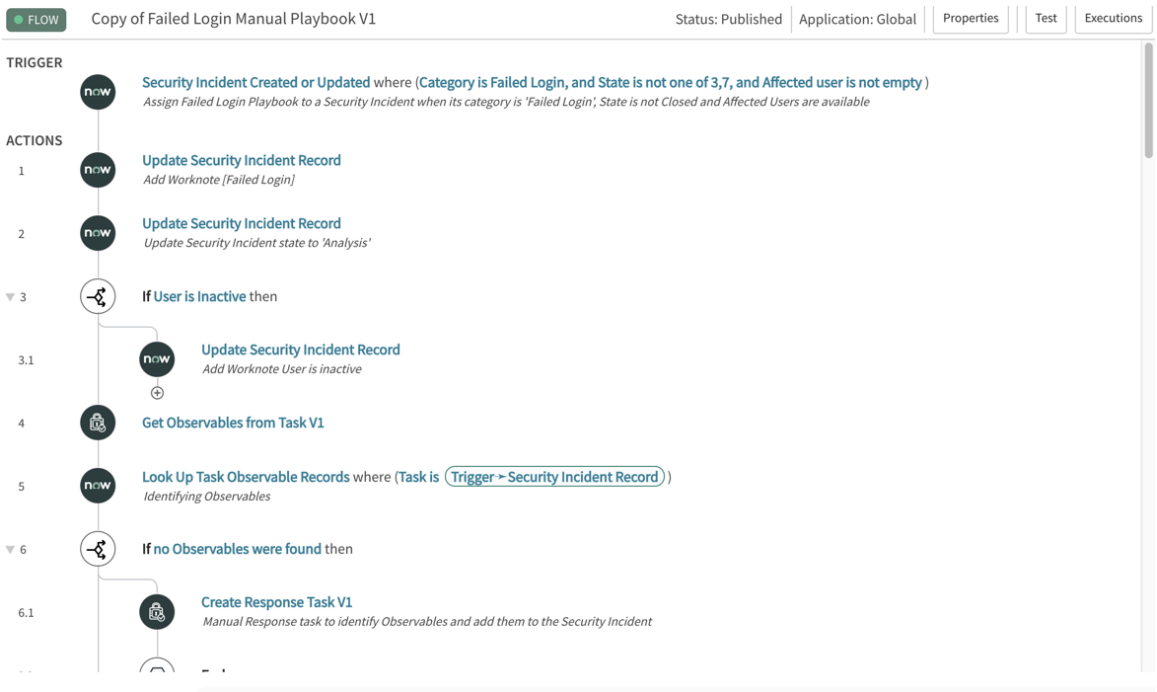
Using Failed Login playbook with Flow Designer capabilities

Getting Started

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **Flow Designer** > **Designer** and click on the **Failed Login** playbook.
3. Make a copy of the following flows to copy the Failed Login Playbook and make the necessary modifications. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).
   - Failed Login Manual Playbook V1
   - Failed Login - Parse User's reply and Update Response Task V1
4. Make the necessary modifications according to your requirement. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).
5. Activate the playbooks.
   - Activate the main flow to use the playbook available with the base system.
   - Activate the copied flows after making any modifications according to your requirements.

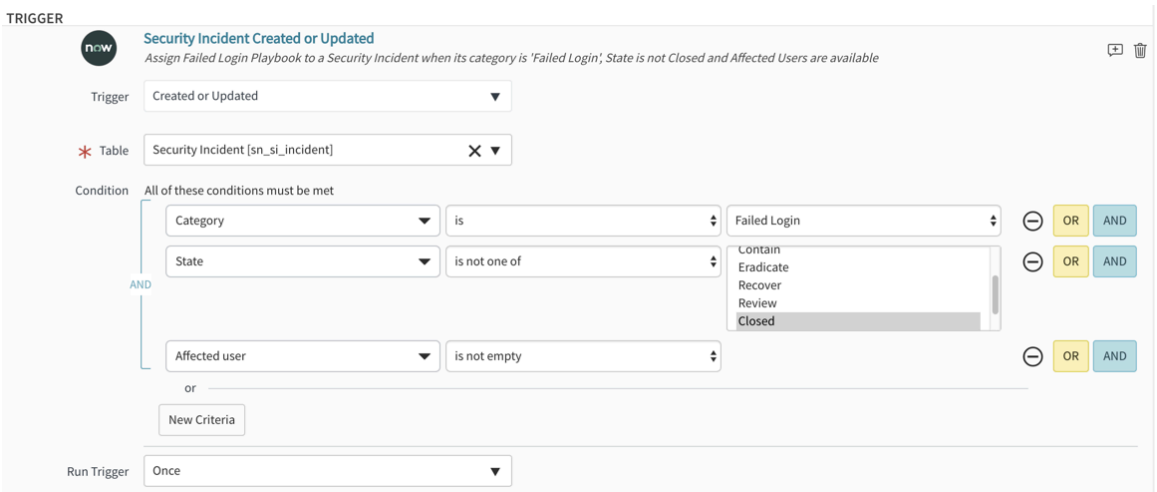
The following image shows a copy of the Failed Login Manual playbook. Review the steps below to get an understanding of the various actions in the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



This playbook is triggered and associated with the security incident when the following conditions are met:

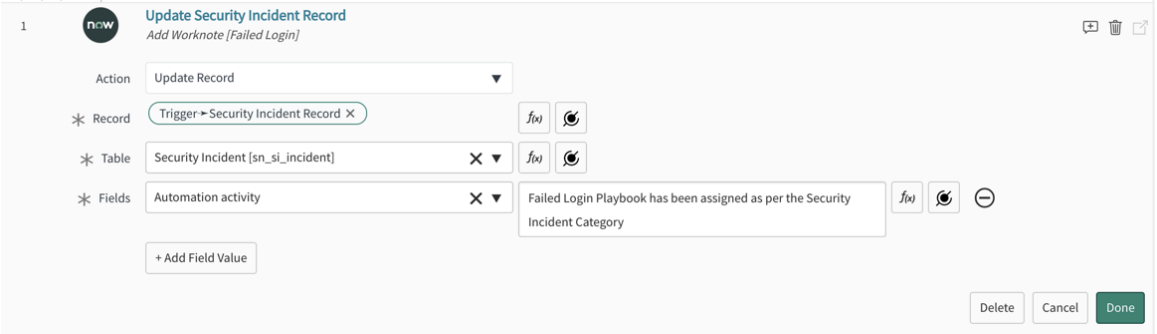
- Category is Failed Login
- Has one or more affected users
- Security incident isn't closed or canceled



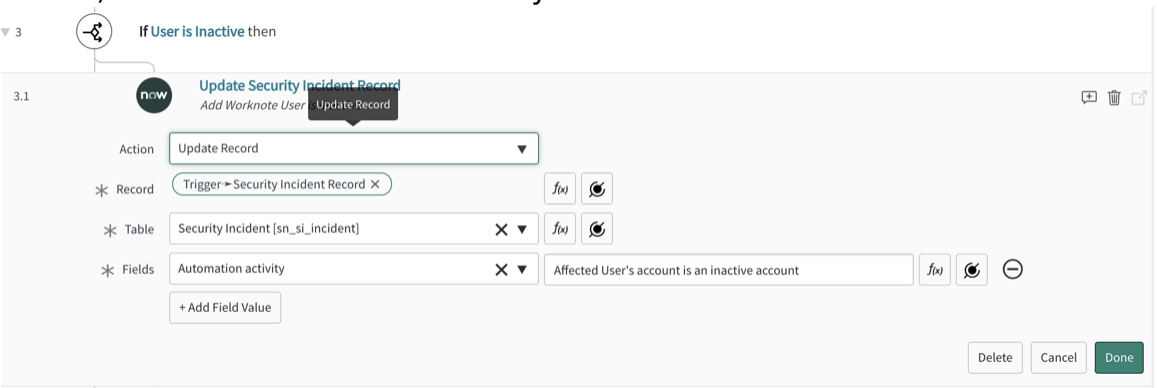
The following steps walks you through the actions, tasks, and subflows that are available in the Failed Login Manual playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. When the playbook starts executing, in Step 1, the playbook is automatically updated with a worknote showing the security incident with the failed login category has been assigned.



2. In Step 2, the playbook is updated and moved to the Analysis state.
3. In Step 3, the playbook checks if the Affected User is an active or inactive user. If the user is inactive, a worknote is added to the security incident that the user account is inactive.



Note: In step 3 of the flow, the flow checks inactive users in the *sn_si_incident* table available in ServiceNow. This step is provided as a guideline and must be modified for your specific environment. If you want to use this functionality, we recommend that you have an Active Directory integration set up in your environment. You can check with your Active Directory integration to find the user status and depending on the response, you can design the next steps for your playbook.

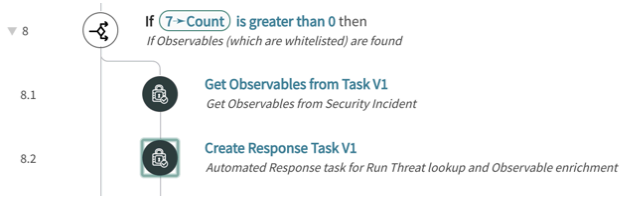
If you don't have an Active Directory integration, replace this step with a manual task for the security analyst to work with the IT team to block the user and move forward with the rest of the steps in the playbook.

4. In Step 4, the observables for the security incident are retrieved.
5. In Step 5, the observables are identified.
6. If no observables are found, a manual response task is created in Step 6 and the flow ends.

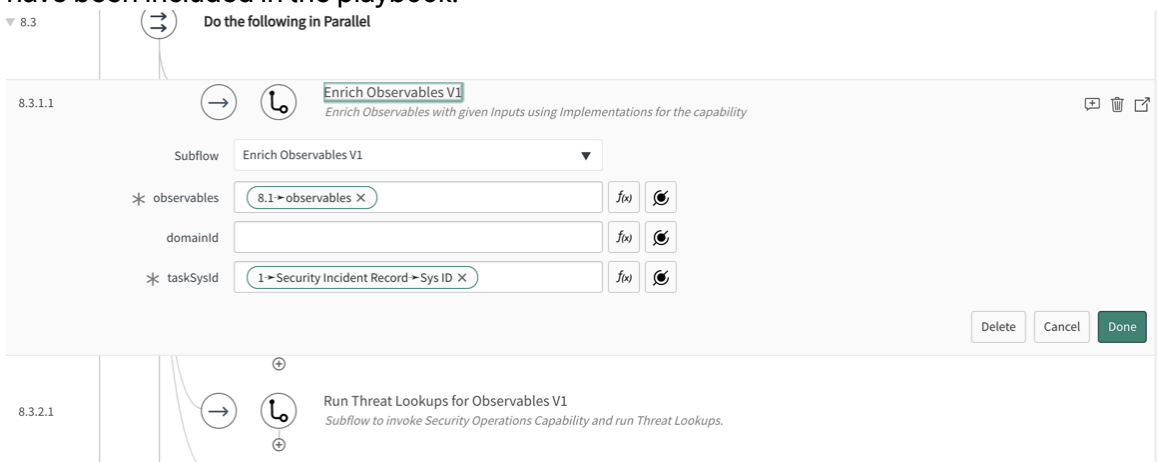
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. If observables are found in Step 7, observables that aren't allowed list are identified.
8. If at least one of the observables is not allowed list, the following steps are performed:
   a. Steps 8.1 and 8.2 are executed. Observables are retrieved and an automated response task is initiated.

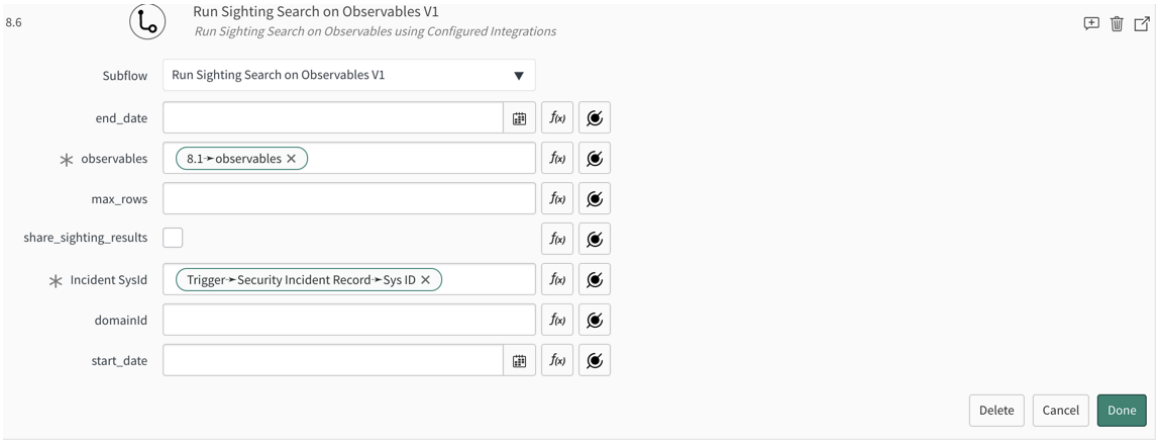


   b. After the automated task has been created, Step 8.3 (8.3.1.1 and 8.3.2.1) is run and the Enrich Observables and Threat Lookup integrations are executed. Note that these are subflows that have been included in the playbook.



   c. In Step 8.4, after the integrations have been completed, the security incident record is updated.
   d. In Step 8.5, a new response task is created to indicate the next automated task that will take place.
   e. In Step 8.6, the Sighting Search integration will be run on the observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



f. After the Sighting Search subflow has been completed, in Step 8.7, the security incident is updated.

g. In Step 8.8, the observables are checked to see if they are malicious.

h. If the observables are not malicious, and if the user account is active, an automated email is sent to the user to reconfirm the unsuccessful login attempts. A manual response task is created to identify the observables and add them to the security incident. The playbook then ends at this stage.

i. If the observables are malicious, three response tasks are created:

i. An automated email is sent to the user to confirm **(Yes or No)** the unsuccessful login attempts. If the user responds Yes:

1. The security incident status is updated to **Contain**.

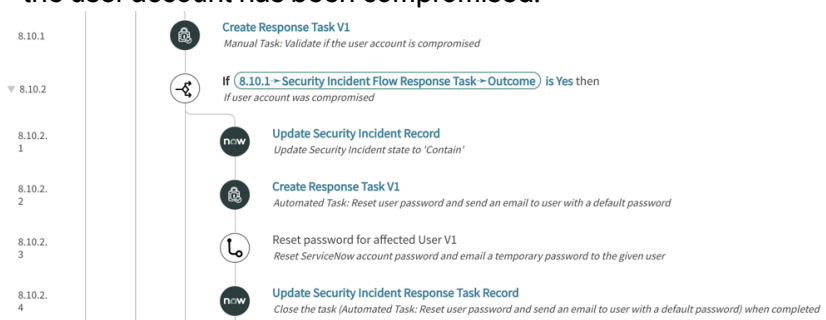
2. An automated email is sent to the user to reset the password.

3. The Reset Password subflow is initiated and an email is sent to the user when the task has been completed.

Note: The Reset Password step is provided as a guideline. The steps in the flow reset the password for the user's account in the ServiceNow System. But the process to reset the password may be different depending on your environment. You can check with your Active Directory integration to reset the password of users automatically. If you don't have an Active Directory integration, replace this step with a manual task for the security analyst to work with the respective IT team to reset users password and move forward with the rest of the steps in the playbook, upon completing the respective task.

ii. If the user responds No, an automated email is sent to the user to reconfirm the response. The security analyst has to manually take appropriate actions.

iii. If the user doesn't respond to the automated email, the security analyst must update the security incident manually and provide a response. A manual task is created to validate if the user account has been compromised.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. In Step 8.10.3, the security incident is state is updated.
10. In Step 8.10.4, an automated task is created to verify if the Create Block Requests for Malicious IPs and URLs capability implementation is available. If the capability implementation is available, the Create Block Requests subflow is executed. If this isn't available, the security incident is updated and a worknote is posted to indicate that the capability implementation isn't available.
11. In Step 9, the security incident is updated and the state is set to **Review**.
12. In Step 10, a response task is created for the user to complete the post-incident review before closing the task.

Playbook for Child Security Incident Automation

Duplicate security incidents are categorized as child security incidents and are rolled up to the parent security incidents.

The Child Security Incident Automation playbook helps reduce the time required to investigate and close duplicate security incidents. This playbook automatically rolls up specific unique artifacts of the child security incident (observables, affected users, CIs) to the parent security incident.

Prerequisites

Role required:

- sn_si.admin
- flow_designer

Spoke: Install Security Operations Spoke (sn_sec_spoke)

Key capabilities

The Child Automation playbook covers the following capabilities:

1. Moves the security incident to the **Analysis** stage.
2. Eliminates duplicates and adds (rolls up) the affected users and CIs to the parent security incident.
3. Adds observables from the child incident to the parent security incident.
4. Closes or cancels the child security incident when the parent security incident is closed.

Capabilities required

For more information, see the ServiceNow store.

Security analyst experience

To understand how to resolve security threats in a step-by-step manner, see Resolve security threats with the playbook.

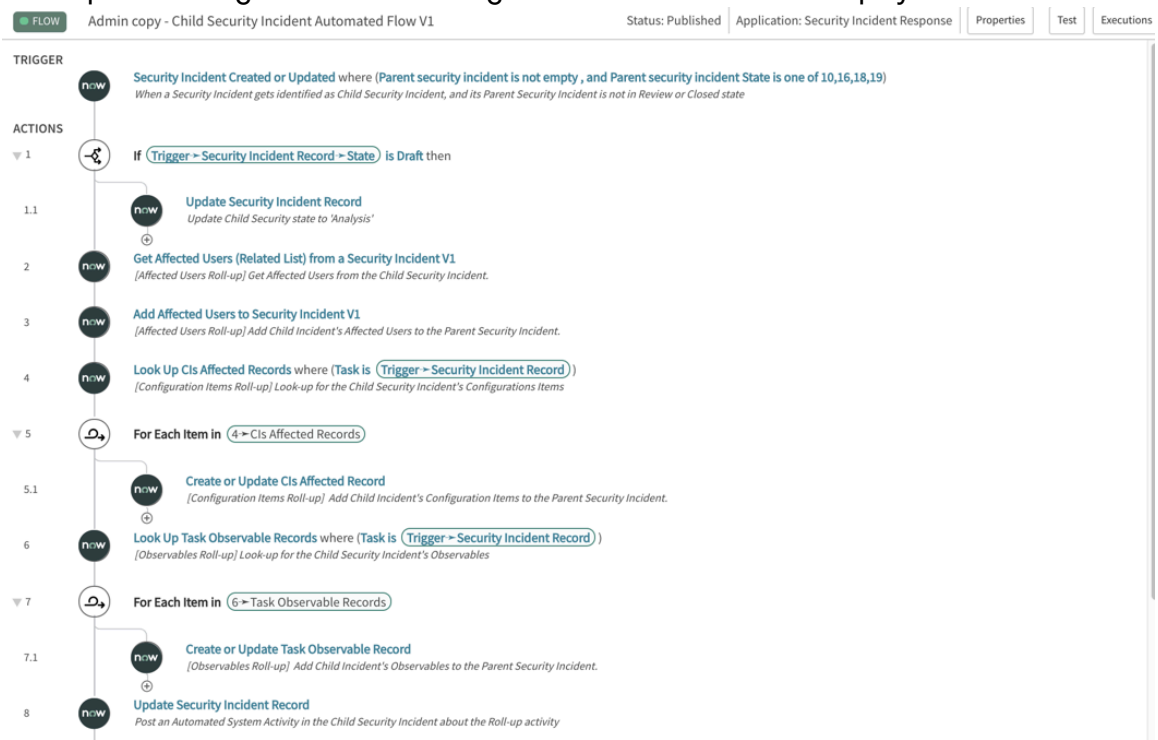
Deeper understanding of the Child Security Incident Automation playbook with Flow Designer capabilities

Getting Started

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **Flow Designer** > **Designer** and click on the Failed Login playbook.
3. Make a copy of the Child Security Incident Automation playbook and make the necessary modifications. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).
4. Make the necessary modifications according to your requirement. (This is an optional step. Follow this step only if you plan to customize or make specific changes to the flow).
5. Activate the playbook.
   - Activate the main flow to use the playbook available with the base system.
   - Activate the copied flow after making any modifications according to your requirements.

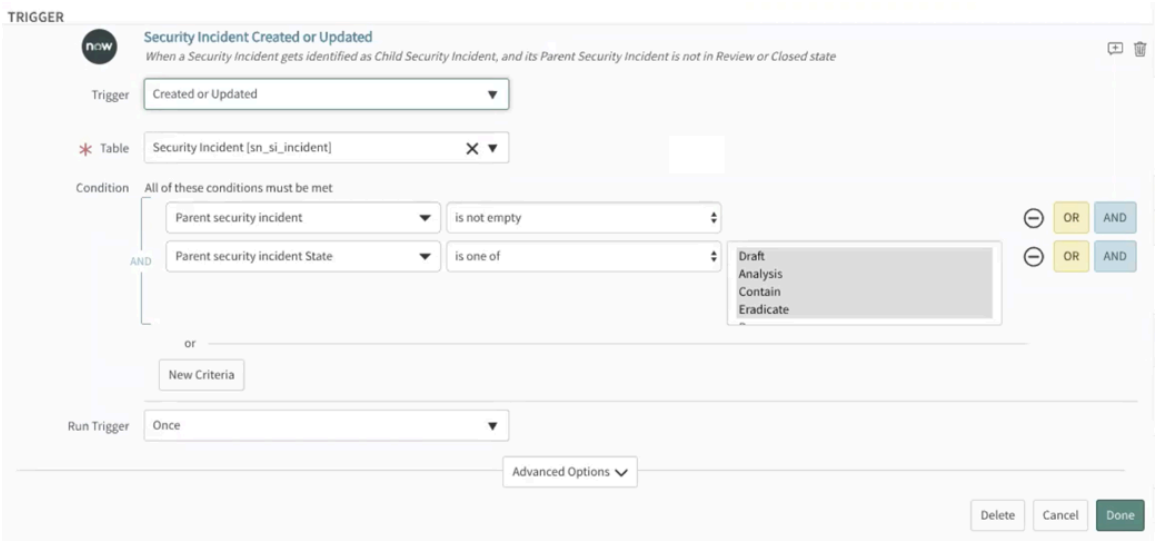
The following image shows a copy of the Child Security Incident Automation playbook. Review the steps below to get an understanding of the various actions in the playbook.



This playbook is triggered when:

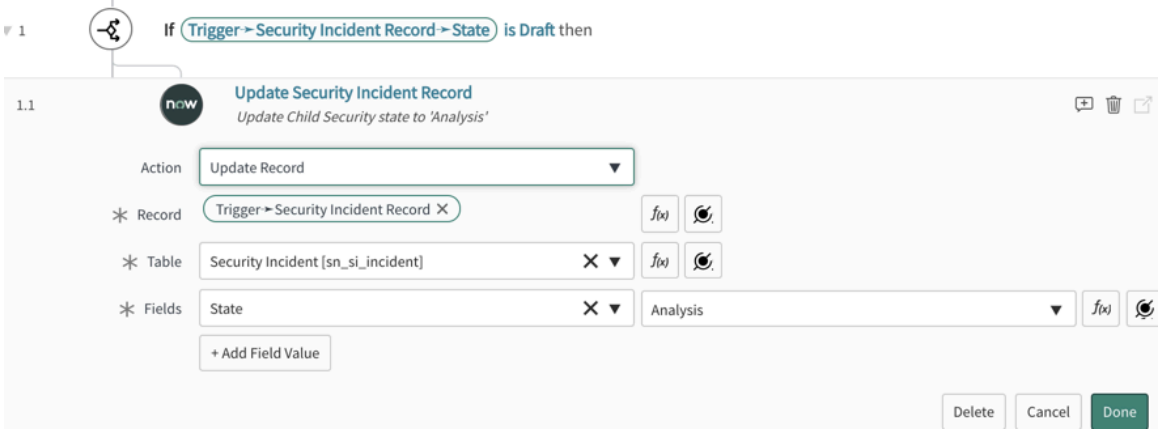
- The parent security incident field isn’t empty.
- The parent security incident is in Draft, Analysis, Contain, or Eradicate state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

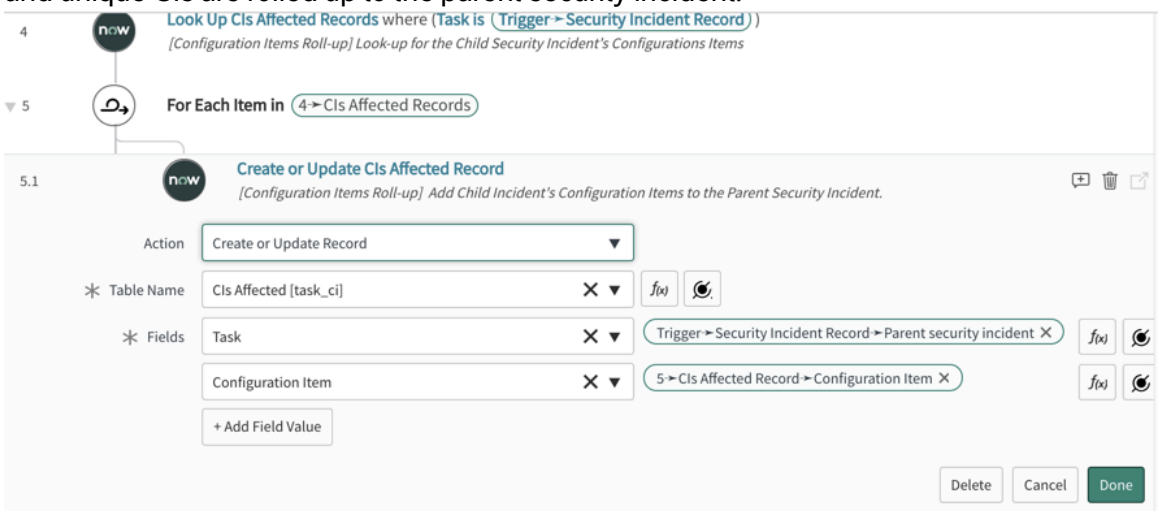


The following steps walk you through the actions and tasks that are available in the Child Security Incident Automation playbook.

1. When the playbook starts executing, in Step 1, if the security incident is in a Draft state, it's updated and set to the Analysis state.

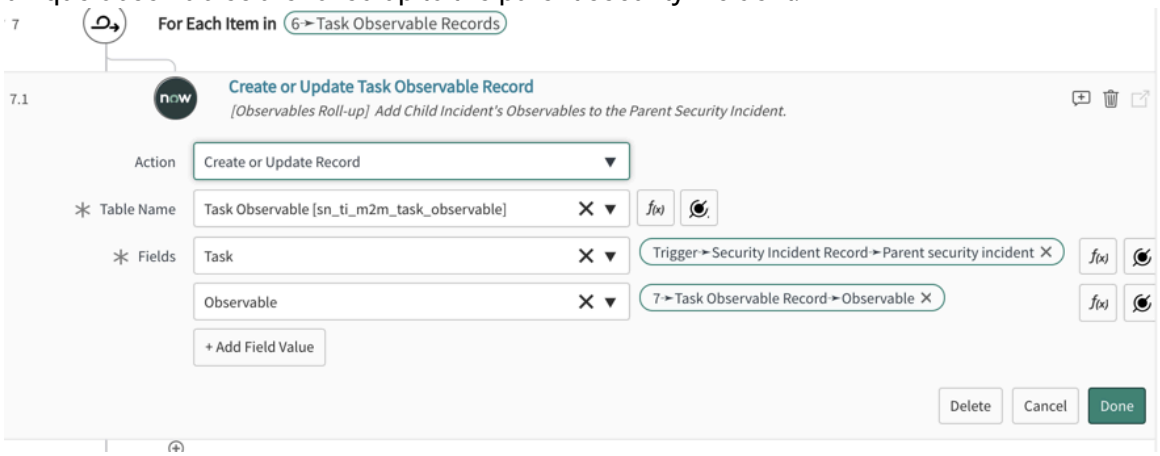


2. In steps 2 and 3, affected users for the security incident are retrieved and rolled up to the parent security incident. Any duplicate users are eliminated.
3. In steps 4 and 5, configuration items associated with the child security incident are retrieved and unique CIs are rolled up to the parent security incident.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In steps 6 and 7, observables associated with the child security incident are retrieved and unique observables are rolled up to the parent security incident.



5. In steps 8 and 9, automated worknotes are posted to the parent and child security incidents indicating that the affected users, configuration items, and observables have been rolled up from the child to the parent security incident.

Playbook for Office 365 - Malicious File Detected

This playbook provides systematic remediation steps for investigating malicious files detected in Office 365.

When malicious files are detected in Office 365, you can use the 365 - Malicious File Detected playbook in the Flow Designer for guidance and help optimize the investigation of these malicious files.

Set up the Office Malicous File Detected playbook

Use the following steps to set up the Office Malicous File Detected playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

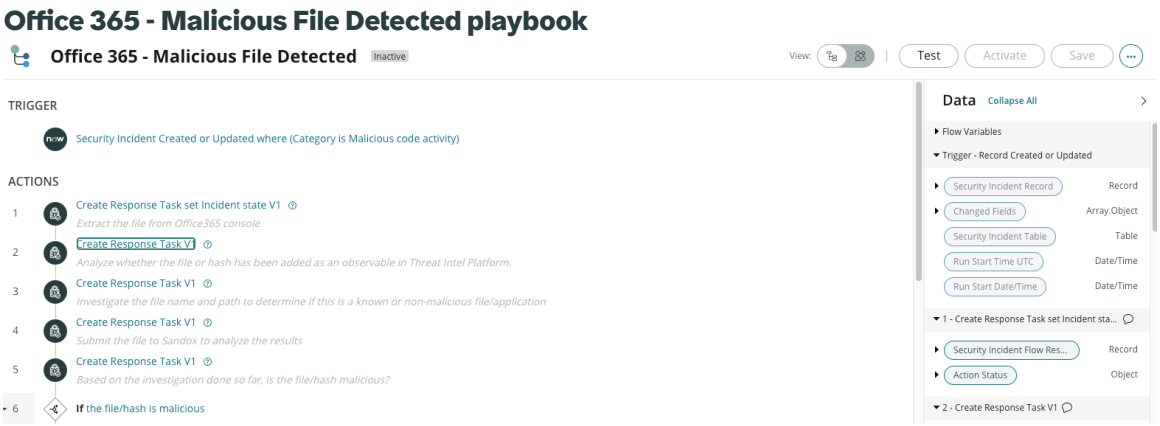
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

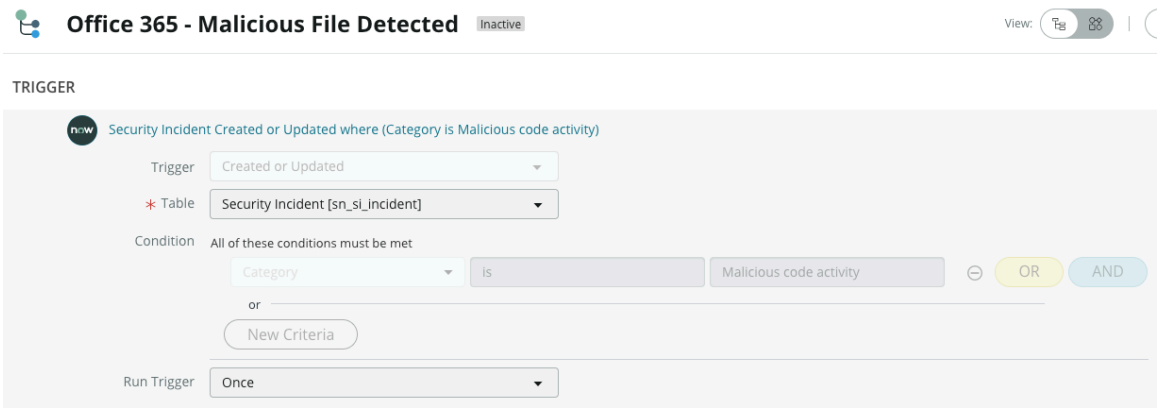
1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Office 365 - Malicious File Detected** playbook.
3. **Optional:** You can create a copy of the Office 365 - Malicious File Detected playbook flow and make the necessary modifications.

   To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.
   This playbook is triggered and associated with the security incident when the **Category** is **Malicious code activity**.



Use the Office 365 Malicious File Detected playbook

Use this playbook to investigate malicious files detected in Office 365. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Office 365 Malicious File Detected playbook.

Before you begin

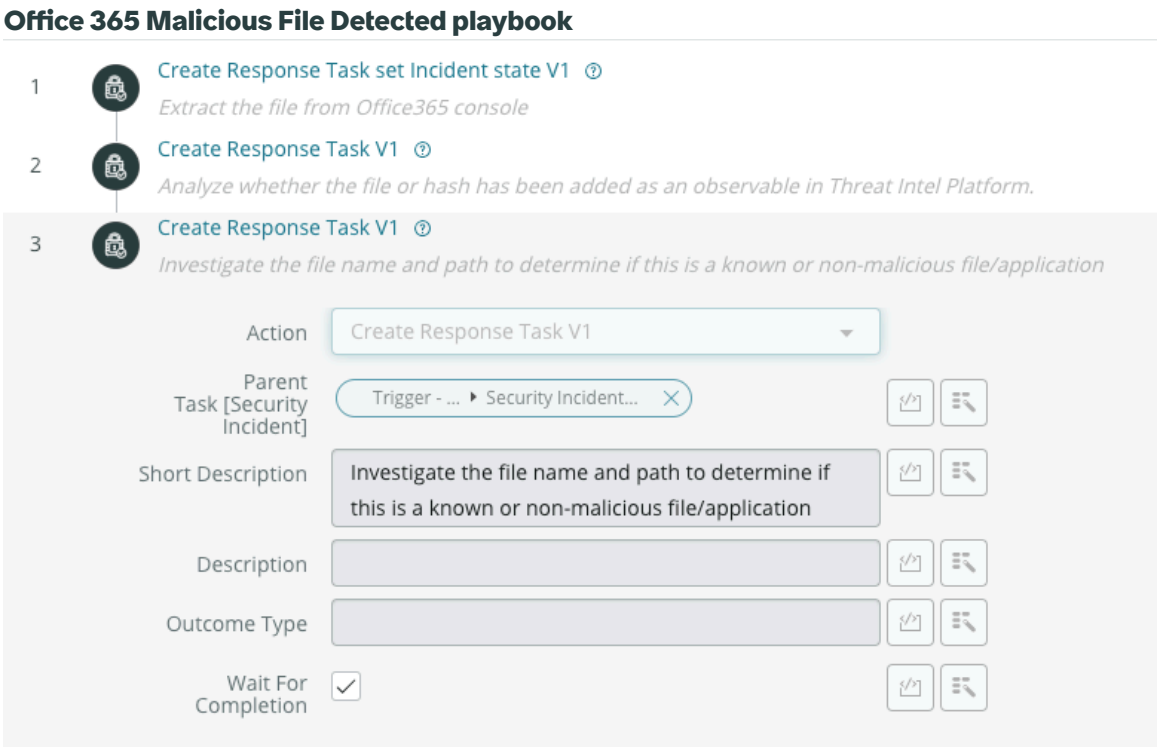
Role required:

- sn_si.admin
- flow_designer

Procedure

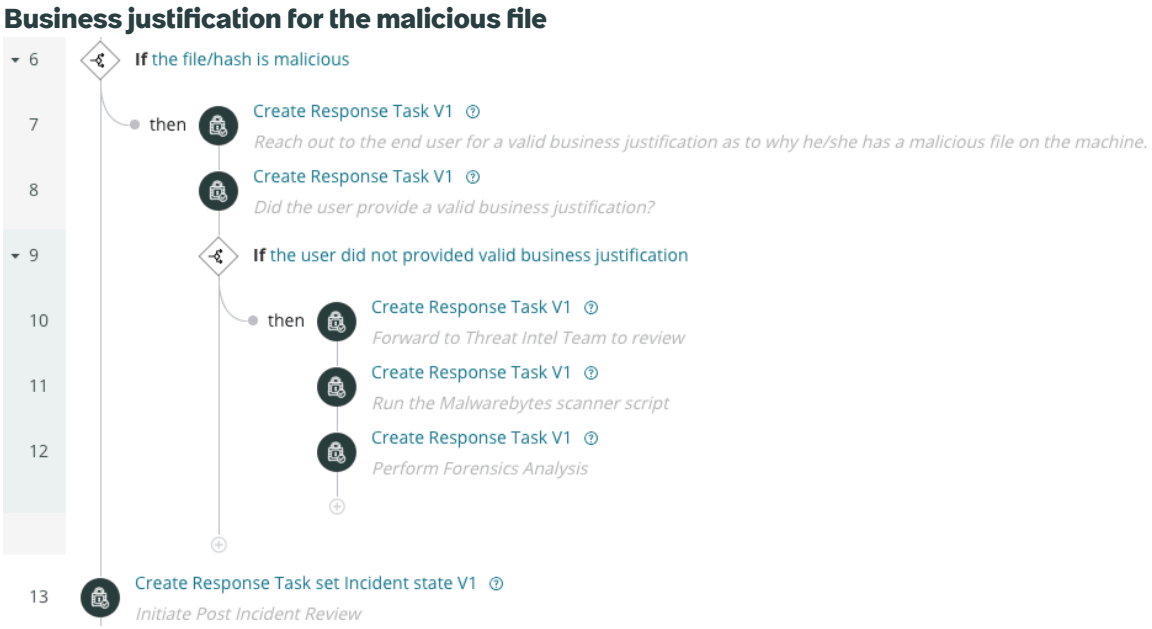
1. When the playbook is triggered and starts executing, in Action 1, you need to extract the malicious file from the Office 365 console.
2. In Action 2, you need to analyze whether the file or hash has been added as an observable in the Threat Intel Platform.
3. In Action 3, you need to investigate the file name and path to determine whether it is a known or non-malicious file/application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In Action 4, you need to submit the file to Sandbox for analyzing the results.
5. In Action 5, based on the investigation done so far, you need to check whether the file or hash is malicious or not.
   If the file or hash isn't malicious, a manual response task is created in Action 5 and the flow ends.
6. In Action 6, if the file or hash is malicious, then Actions 7 and 8 are executed.
7. In Action 7, you need to reach out to the end user for a valid business justification as to why they have a malicious file on the device.
   If the file or hash is malicious, you can use the pre-existing Email Template in the playbook to email the end user asking for clarification.
8. In Action 8, you need to check whether the end user provided a valid business justification or not.
   If the end user provided a valid business justification, a manual response task is created in Action 5 and the flow ends.
9. In Action 9, if the user didn't provide a valid business justification then Actions 10, 11, and 12 are executed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



10. In Action 10, since there was no valid business justification, you can forward the malicious file or hash to the Threat Intel Team for review.
11. In Action 11, you need to run the Malware bytes scanner script to check if the file or hash is malicious.
12. In Action 12, you need to perform a Forensic Analysis to check if the file or hash is malicious.
13. In Action 13, a response task is created for the user to complete the post-incident review before closing the task.

Playbook for Repeat Detection

This playbook helps you determine if the incident response has been provided on an exact or similar phishing report in the past and automatically works on the new report similarly.

The Repeat Detection playbook checks if the newly reported phishing incident resembles a past incident. When the repeat detection is identified, the matched security incident and the resolution details are provided to the analyst, who can use it on the newly reported incident, resulting in a quick remediation of the security incident.

Set up the Repeat Detection playbook

Use the following steps to set up the Repeat Detection playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*). You have an option to modify the following system properties:

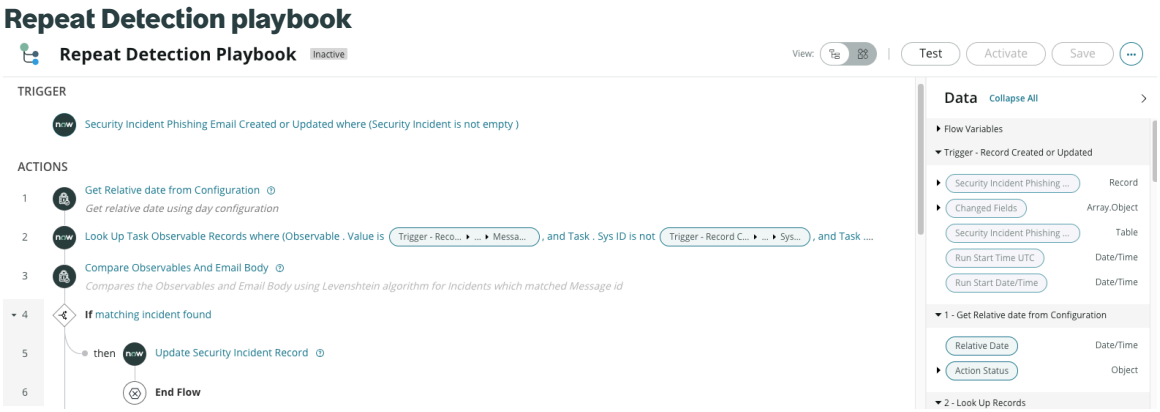
- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

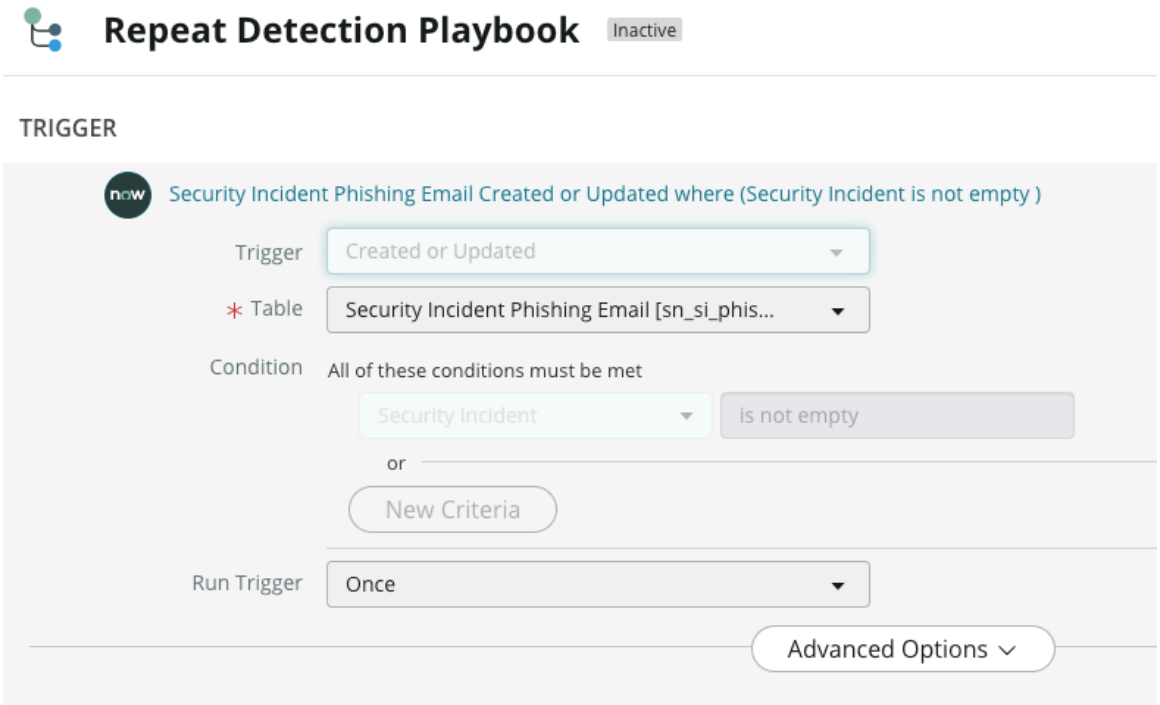
1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Repeat Detection** playbook.
3. **Optional:** You can create a copy of the Repeat Detection playbook flow and make the necessary modifications.

   To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered when the **Security Incident is not empty**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the Repeat Detection playbook

Use this playbook to investigate if the incident response has been provided on an exact or similar phishing report in the past and automatically works on the new report similarly. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Repeat Detection playbook.

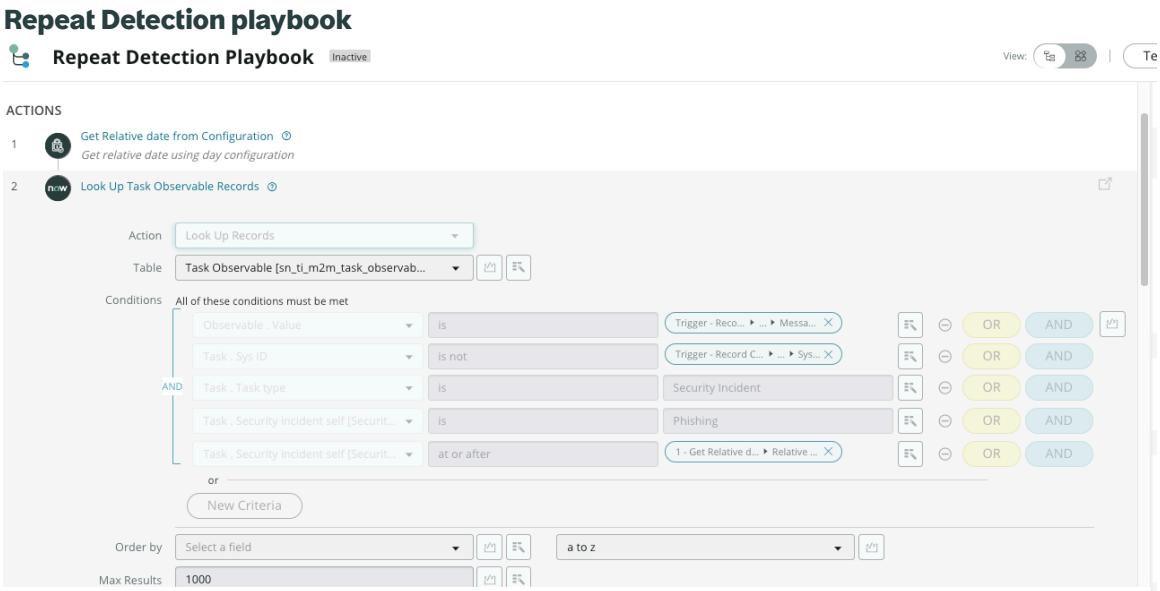
Before you begin

Role required:

- sn_si.admin
- flow_designer

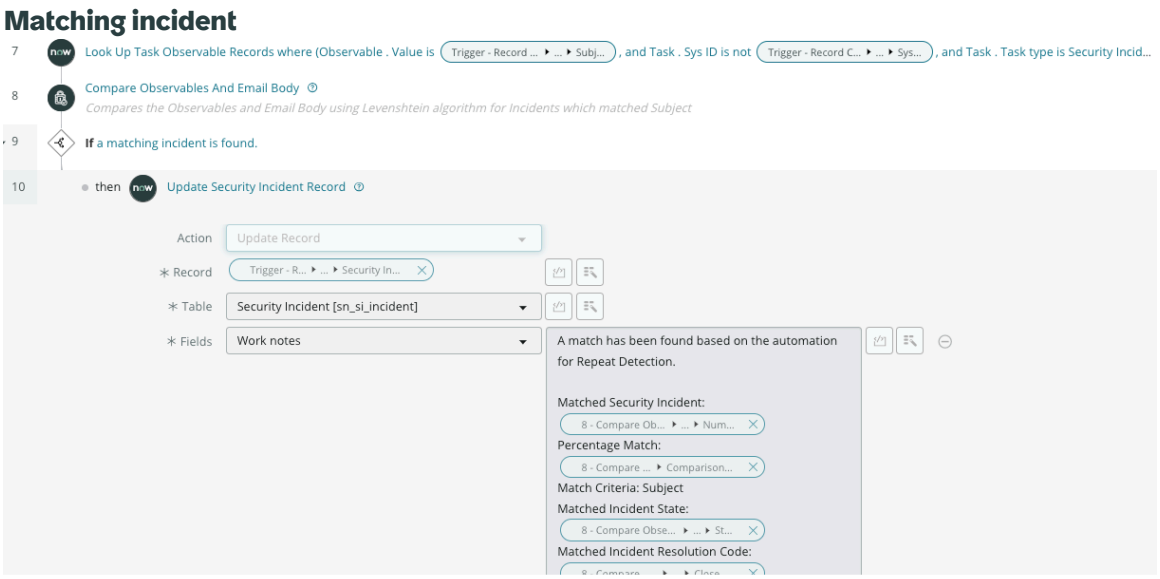
Procedure

1. When the playbook is triggered and starts executing, in Action 1, the playbook retrieves the relative date of the security incident using the day configuration.
2. In Action 2, the playbook looks up the Task Observable records on the table *sn_ti_m2m_task_observable* that match the incident based on the Message ID.



3. In Action 3, the playbook compares the Task Observables and Email body using the Levenshtein algorithm for incidents that matched the Message ID.
4. In Action 4, based on the investigation done so far, the playbook checks whether the matching incident is found based on the Message ID or not.
   In Action 5, if the matching incident is found, the playbook automatically updates the worknote that a match has been found based on the automation for Repeat Detection. In Action 6, the flow ends.
5. If the matching incident is not found, then in Action 7, the playbook looks up the Task Observable records on the table *sn_ti_m2m_task_observable* that match the incident based on the Subject.
6. In Action 8, the playbook compares the Task Observables and Email body using the Levenshtein algorithm for incidents that matched the Subject.
7. In Action 9, the playbook checks whether the matching incident is found or not.
   In Action 10, if the matching incident is found, the playbook automatically updates the worknote that a match has been found based on the automation for Repeat Detection. In Action 11, the flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. In Action 12, the playbook looks up the Task Observable records on the table *sn_ti_m2m_task_observable* that match the incident based on the Address.
9. In Action 13, the playbook compares the Task Observables and Email body using the Levenshtein algorithm for incidents that matched the Address.
10. In Action 14, the playbook checks whether the matching incident is found based on the Address or not.
    In Action 15, if the matching incident is found, the playbook automatically updates the worknote that a match has been found based on the automation for Repeat Detection. In Action 16, the flow ends.

Playbook for Spoofed Emails (using the same Display name)

This playbook provides systematic remediation steps to investigate Spoofed Emails, which get triggered when spoofed names for emails are sent to the organization's employees.

Set up the Spoofed Emails playbook

Use the following steps to set up the Spoofed Emails playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

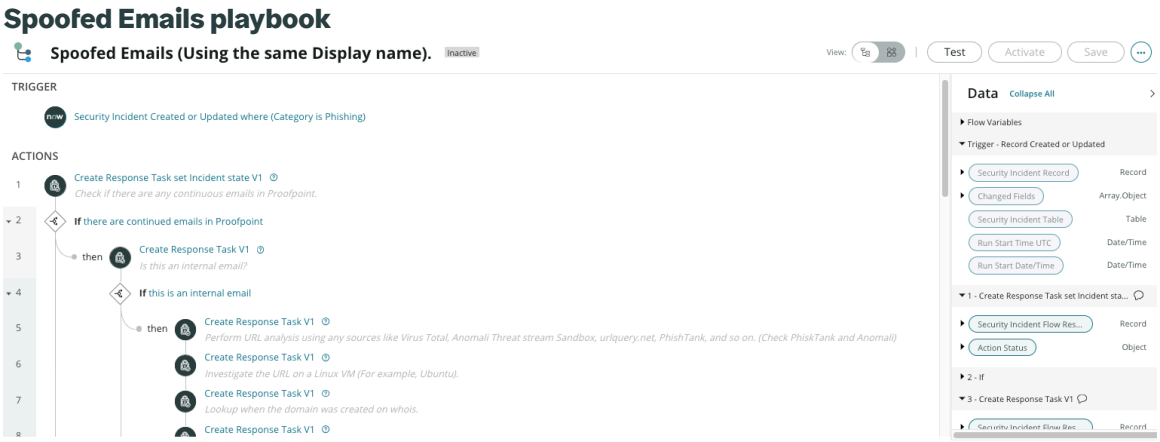
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Spoofed Emails (using the same Display name)** playbook.
3. **Optional:** You can create a copy of the Repeat Detection playbook flow and make the necessary modifications.

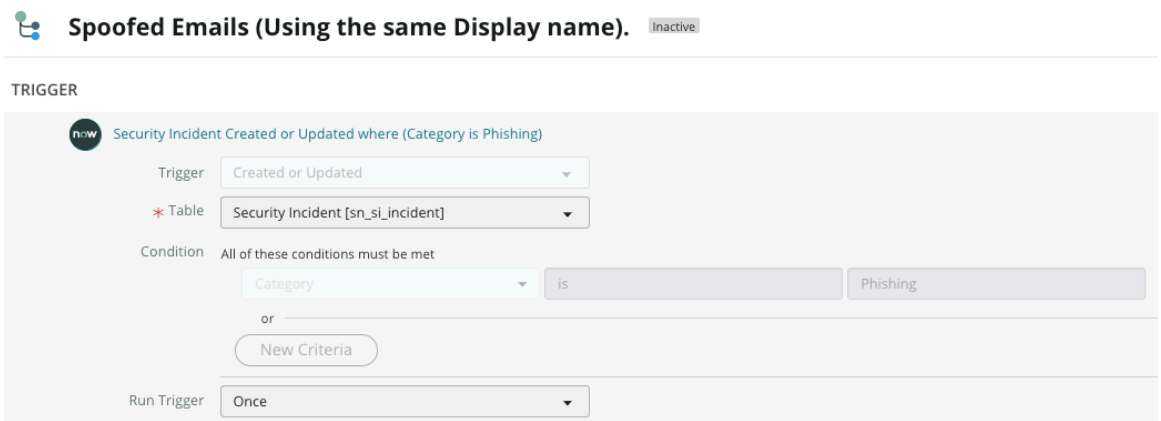
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered and associated with the security incident when the **Category** is **Phishing**.



Use the Spoofed Emails (using the same Display name) playbook

Use this playbook to investigate Spoofed Emails, which get triggered when spoofed names for emails are sent to the organization's employees. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Spoofed Emails (using the same Display name) playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

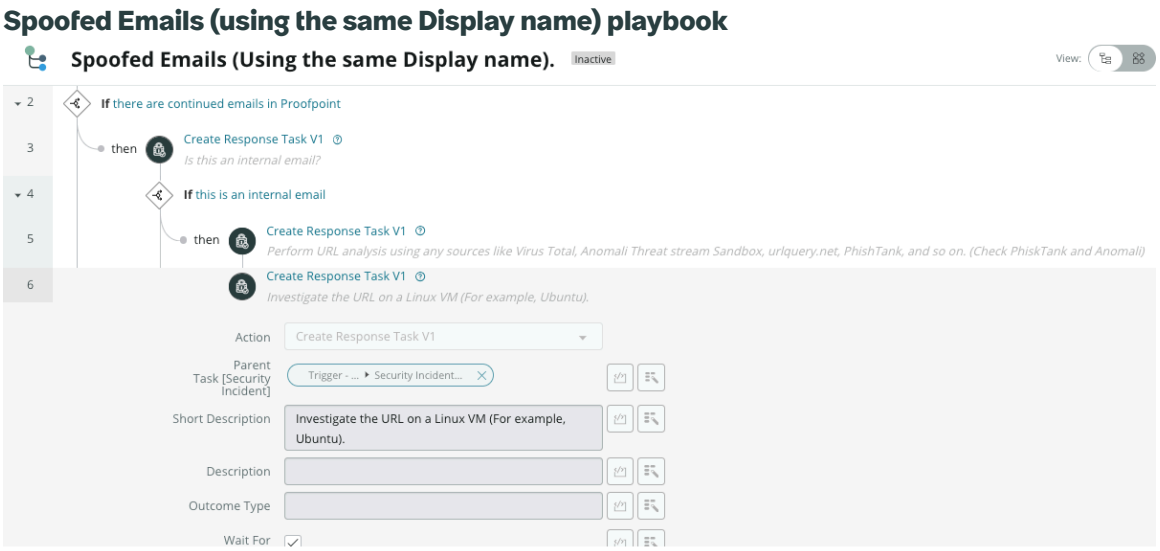
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. When the playbook is triggered and starts executing, in Action 1, you need to check if there are any continuous spoofed emails in Proofpoint.
2. In Action 2, if there are continuous emails in Proofpoint, then check whether this an internal spoofed email or not.
3. In Action 3, if this is an internal spoofed email, perform the following actions:

   a. In Action 5, you need to perform URL analysis using any sources like Virus Total, Anomali Threat stream Sandbox, urlquery.net, PhishTank (For example, check PhiskTank and Anomali).

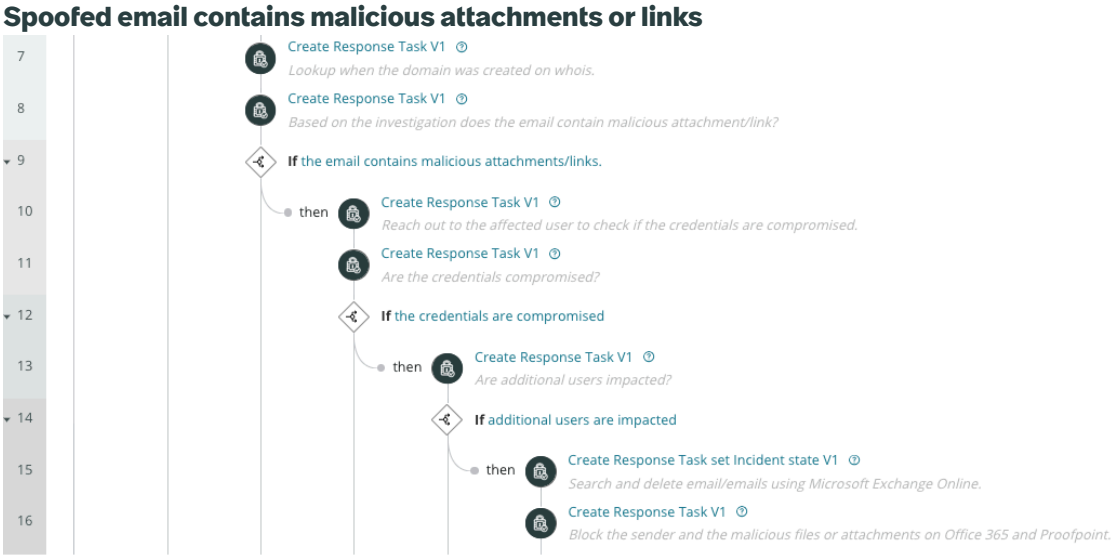
   b. In Action 6, you need to investigate the URL on a Linux VM (For example, Ubuntu).



   c. In Action 7, you need to look up when the domain was created on WHOIS.
   Look for recently registered domains (within the last week) that are suspicious and have a high probability of phishing attacks.

   d. In Action 8, based on the investigation done so far, you need to check whether this email contains a malicious attachment or link.
   If this email doesn't contain a malicious attachment or link, then the flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



e. In Action 9, if the email contains malicious attachments or links, perform the following actions.

i. In Action 10, you need to reach out to the affected user to check if the credentials are compromised. You can use the provided email template to contact the affected user.

ii. In Action 11, you need to check whether the credentials are compromised based on the email response. If the credentials weren't compromised, then the flow ends.

1. In Action 12, if the credentials are compromised, then in Action 13, you need to check if additional users are impacted. If no additional users are impacted, then the flow ends.

2. In Action 14, if additional users are impacted, then perform the following actions:

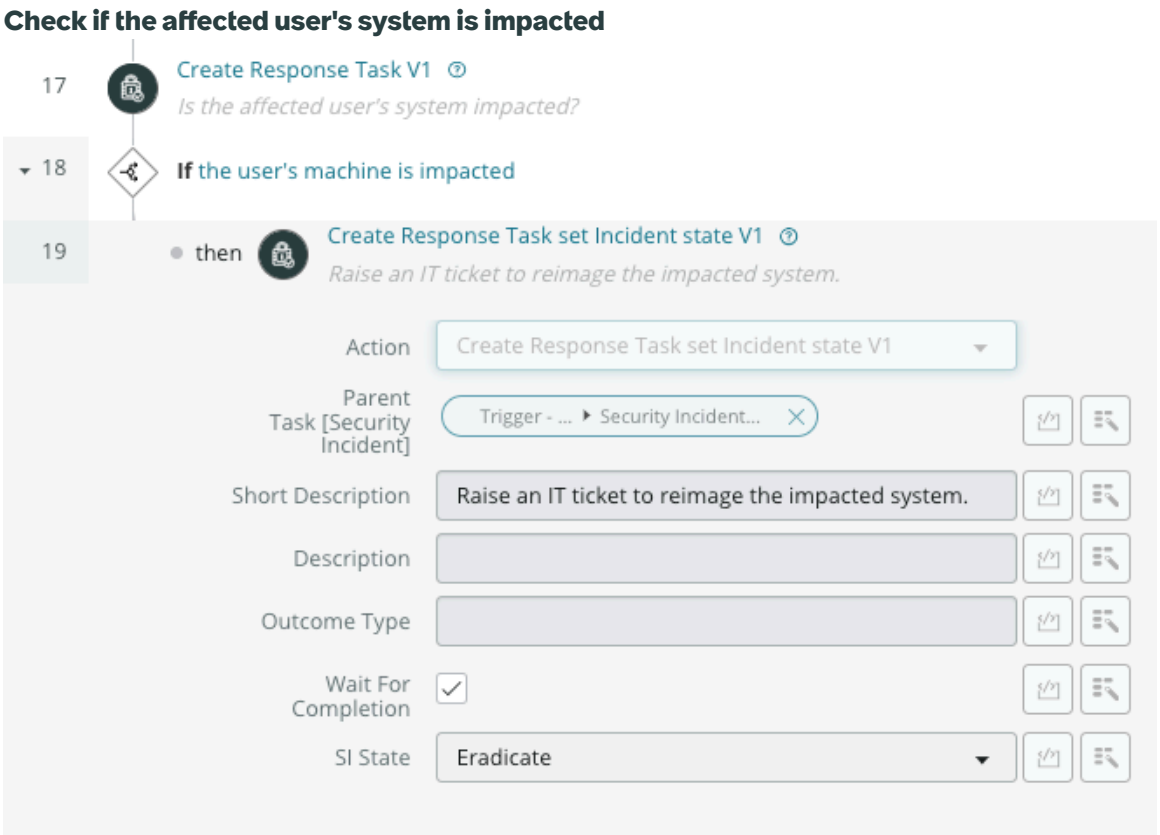
a. In Action 15, you need to search and delete emails using Microsoft Exchange Online.

b. In Action 16, you need to block the sender and the malicious files or attachments on Office 365 and Proofpoint.

4. In Action 17, if this isn't an internal spoofed email, then you need to check if the affected user's system is impacted.

5. In Action 18, if the user's system is impacted, then in Action 19, raise an IT ticket to reimage the impacted system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. In Action 20, a response task is created for you to complete the post-incident review before closing the task.

Playbook for Endpoint Detection

This playbook provides systematic remediation steps to investigate malware alerts triggered on a host or endpoint (For example, a malicious file detection).

When CrowdStrike alerts are triggered on a host or endpoint, you can use the Endpoint Detection playbook in the Flow Designer for guidance and help optimize the investigation of these malicious files.

Set up the Endpoint Detection playbook

Use the following steps to set up the Endpoint Detection playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

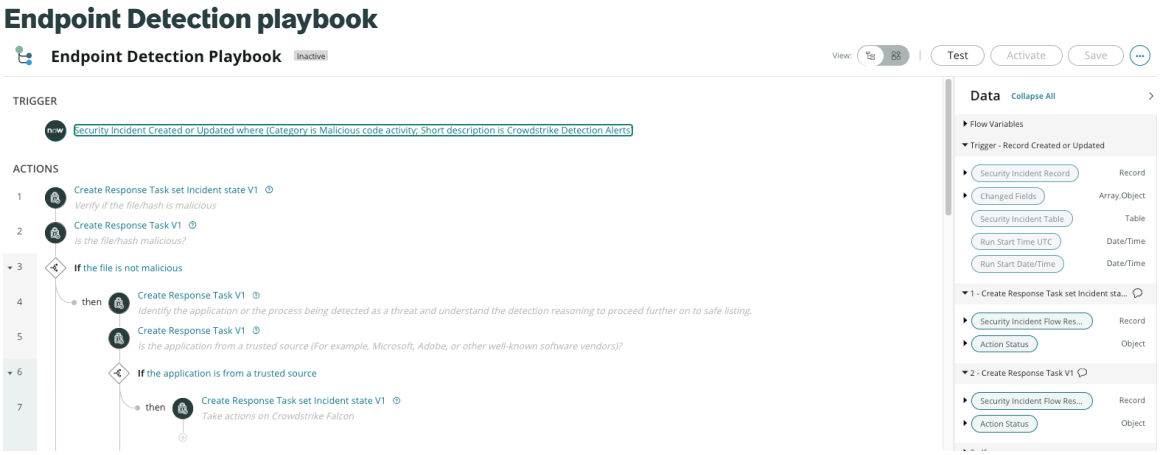
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

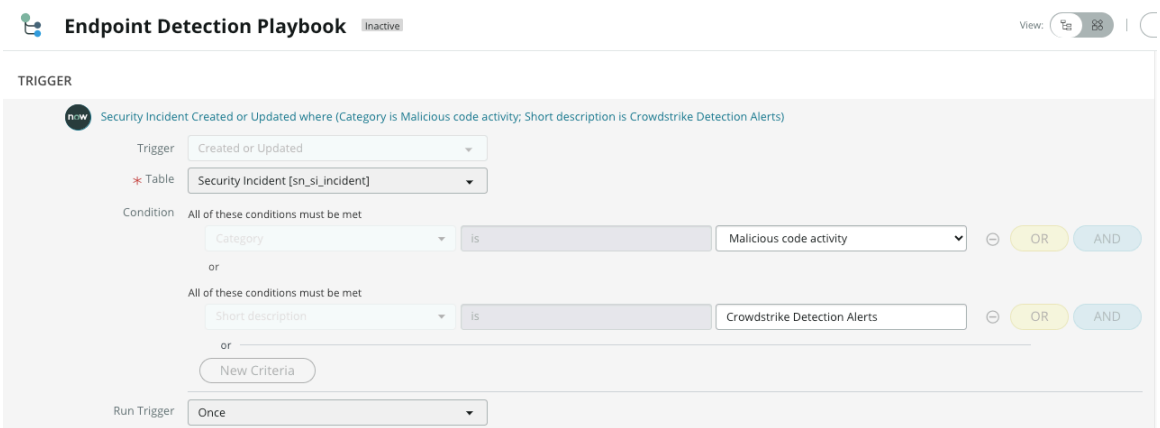
1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Endpoint Detection** playbook.
3. **Optional:** You can create a copy of the Endpoint Detection playbook flow and make the necessary modifications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.
   This playbook is triggered and associated with the security incident when the following conditions are met:
   - **Category** is **Malicious code activity**.
   - **Short description** is **CrowdStrike Detection Alerts**.



Use the Endpoint Detection playbook

Use this playbook to investigate malware alerts triggered on a host or endpoint. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Endpoint Detection playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

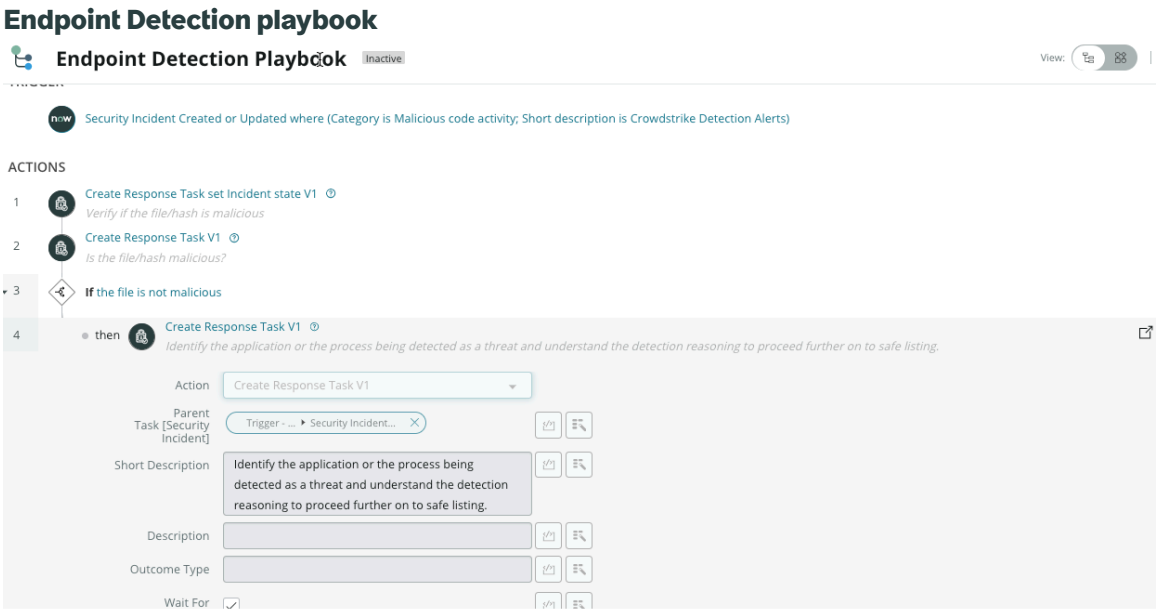
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. When the playbook is triggered and starts executing, in Action 1, you need to verify if the file or hash is malicious by analyzing the Threat lookup results in SIR and gathering intel from VirusTotal, WildFire, ThreatCrowd, etc.
2. In Action 2, you need to check whether the file or hash is malicious or not.
3. In Action 3, if the file or hash is malicious, perform the following actions:

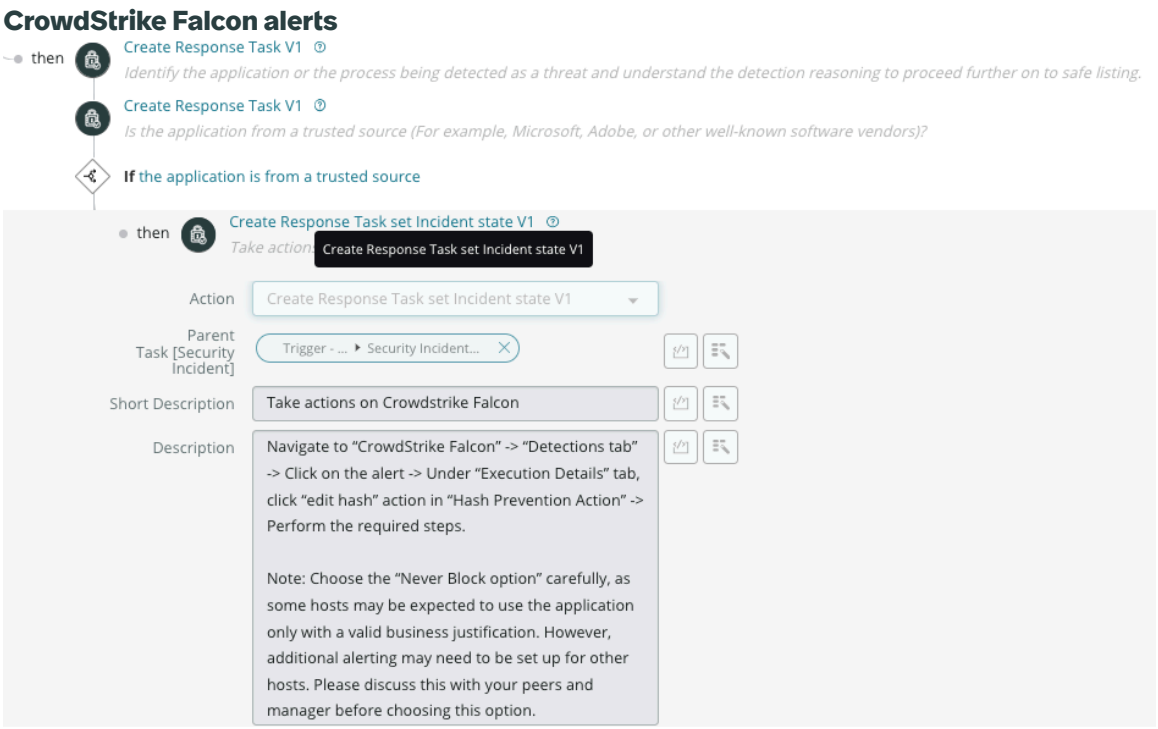
   a. In Action 4, you need to identify the application or the process being detected as a threat and gather information about the detection reasoning to proceed further on to safe listing.



   b. In Action 5, you need to check whether the application is from a trusted source (For example, Microsoft, Adobe, or other well-known software vendors).

   c. In Action 6, if the application is from a trusted source, then you need to take action on the CrowdStrike Falcon alerts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



d. In Action 7, perform the following actions:

i. Navigate to **CrowdStrike Falcon** > **Detections** tab.

ii. Click on the CrowdStrike Falcon alert.

iii. Under the Execution Details tab, click **Edit Hash** action in Hash Prevention Action.

iv. Perform the required steps.

> **Note:** Choose the **Never Block** option carefully, as only certain hosts may be allowed to use the application with a valid business justification. However, additional alertings may need to be set up for other hosts.

e. In Action 8, if the application isn't from a trusted source, then you need to choose whether you want to waive the file or application from the device locally.
In Action 10, if you want to waive the file or application from the device locally, perform the following actions:

i. In Action 11, navigate to the **Quarantined Files** tab, and filter the endpoint by searching for the device name.

ii. Select the file that needs to be waived locally, and click **Release**.

> **Note:**
>
> - The file still runs on this specific endpoint. However, detection and quarantine continue to happen on all other hosts.
> - To bulk release the quarantine file on multiple hosts, select the appropriate file name and status. Click on **Select**, and select **Release**.

In Action 12, if you don't want to waive the file or application from the device locally, you can redirect the user to the IT Support for requesting installation of the approved applications.

4. In Action 14, if the file or hash isn't malicious, perform the following actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In Action 15, you need to determine if the file/hash is high risk or low risk based on the user's role (department or position that handles sensitive information), the type of application (ransomware, rootkit, etc.), and the impact of the application (how many users were impacted).

b. In Action 16, if the file is a high-risk file, then perform the following actions:

i. In Action 17, review the results with the Threat Intel Team.

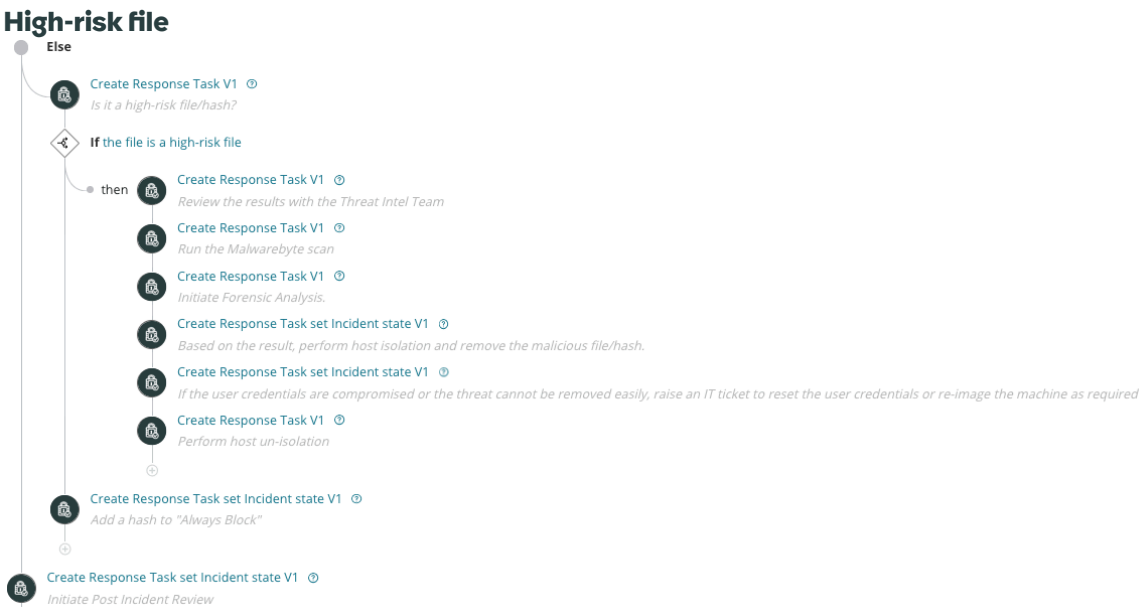
ii. In Action 18, run the Malware byte scan on the file.

iii. In Action 19, initiate Forensic Analysis.

iv. In Action 20, based on the result of the Forensic Analysis, perform host isolation and remove the malicious file/hash.

v. In Action 21, if the user credentials are compromised or the threat can't be removed easily, raise an IT ticket to reset the user credentials or reimage the machine as required.

vi. In Action 22, perform host unisolation.



c. In Action 23, if the file isn't a high-risk file, then perform the following actions:

i. Navigate to **CrowdStrike Falcon** > **Configurations** tab.

ii. From the Configurations tab, navigate to **Prevention Hashes** > > **Upload Hash** > **Add the Hash**.

iii. Choose the required OS, and select **Always Block**.

5. In Action 24, a response task is created for the user to complete the post-incident review before closing the task.

Playbook for Possible Password Spray

This playbook provides systematic remediation steps to investigate password spray alerts triggered by multiple failed logins (too many authentication failures from more than one IP address for the same user).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up the Possible Password Spray playbook

Use the following steps to set up the Possible Password Spray playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

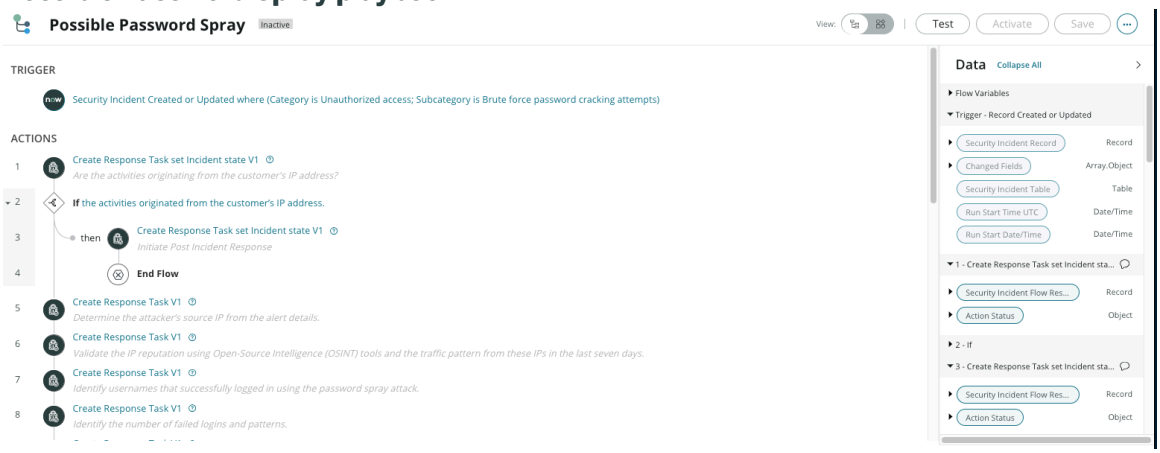
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Possible Password Spray** playbook.
3. **Optional:** You can create a copy of the Possible Password Spray playbook flow and make the necessary modifications.

   To create a copy of the playbook's flow, click the  icon and select **Possible Password Spray**. Perform this step only if you plan to customize or make specific changes to the flow.

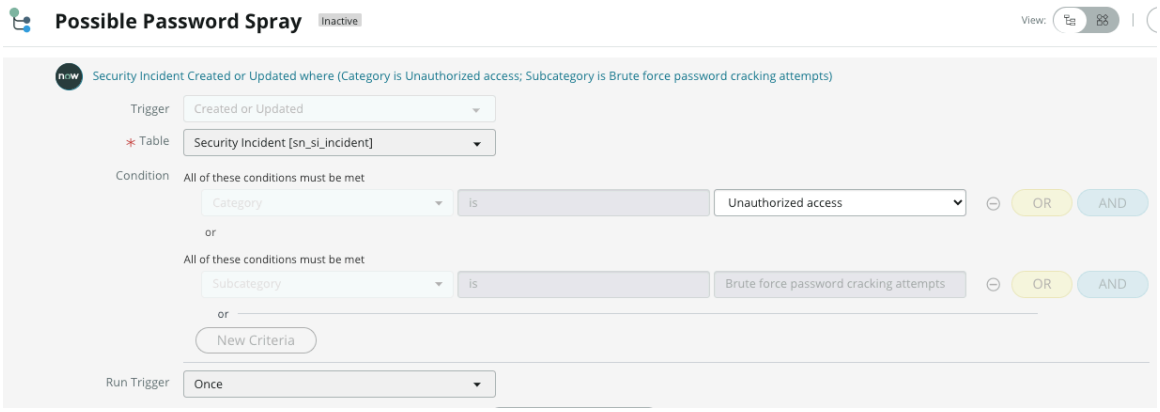
Possible Password Spray playbook



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.
   This playbook is triggered and associated with the security incident when the following conditions are met:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Category** is **Unauthorized access**.
- **Sub-category** is **Brute force password cracking attempts**.



Use the Possible Password Spray playbook

Use this playbook to investigate password spray alerts triggered by multiple failed logins (too many authentication failures from more than one IP address for the same user). The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Possible Password Spray playbook.

Before you begin

Role required:

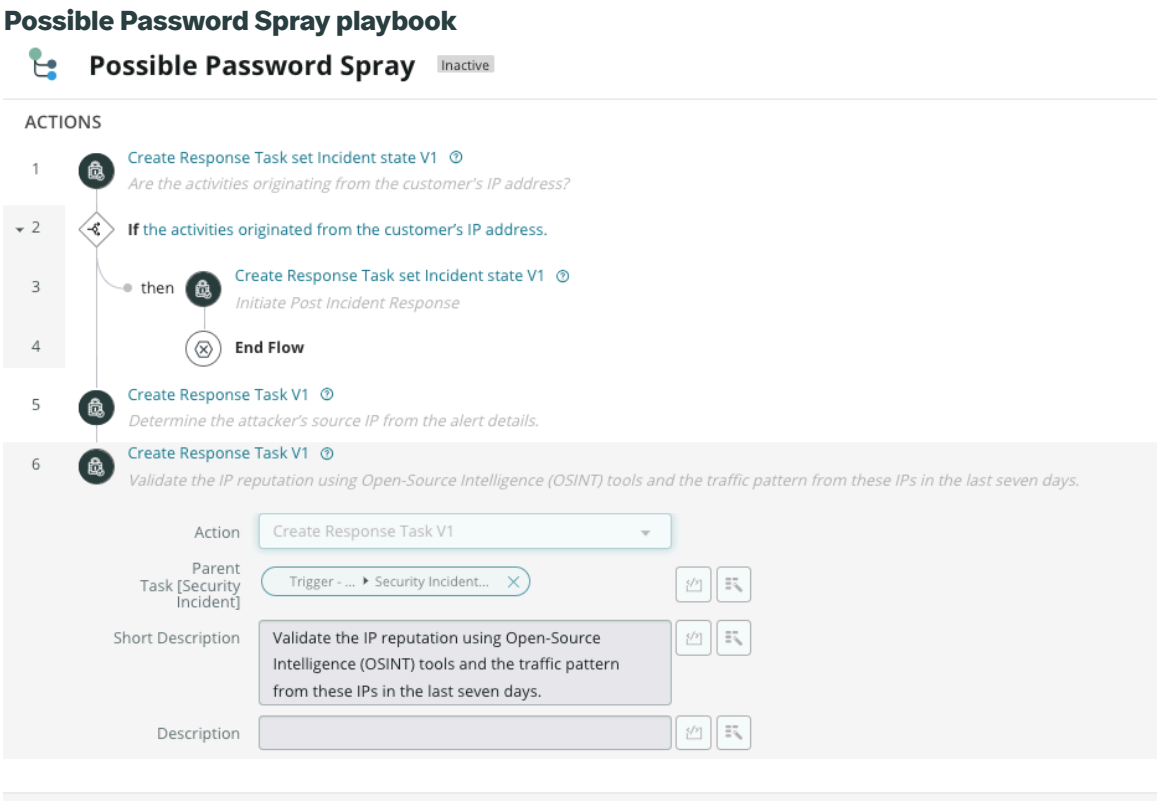
- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. When the playbook is triggered and starts executing, in Action 1, you need to check whether the activities are originating from the customer's IP address.
   Identify the IP addresses performing the Password Spray attack. For example, use the TXIDs (Transaction IDs) from the alert and look them up against the F5 logs.
2. In Action 2, if the activities originated from the customer's IP address, then perform the following actions:
   a. In Action 3, you need to initiate a post-incident review of the Possible Password Spray attack.
   b. In Action 4, the flow ends.
3. In Action 5, if the activities didn't originate from the customer's IP address then determine the attacker's source IP from the alert details.
4. In Action 6, you need to validate the IP reputation using Open-Source Intelligence (OSINT) tools and the traffic pattern from these IPs in the last seven days.

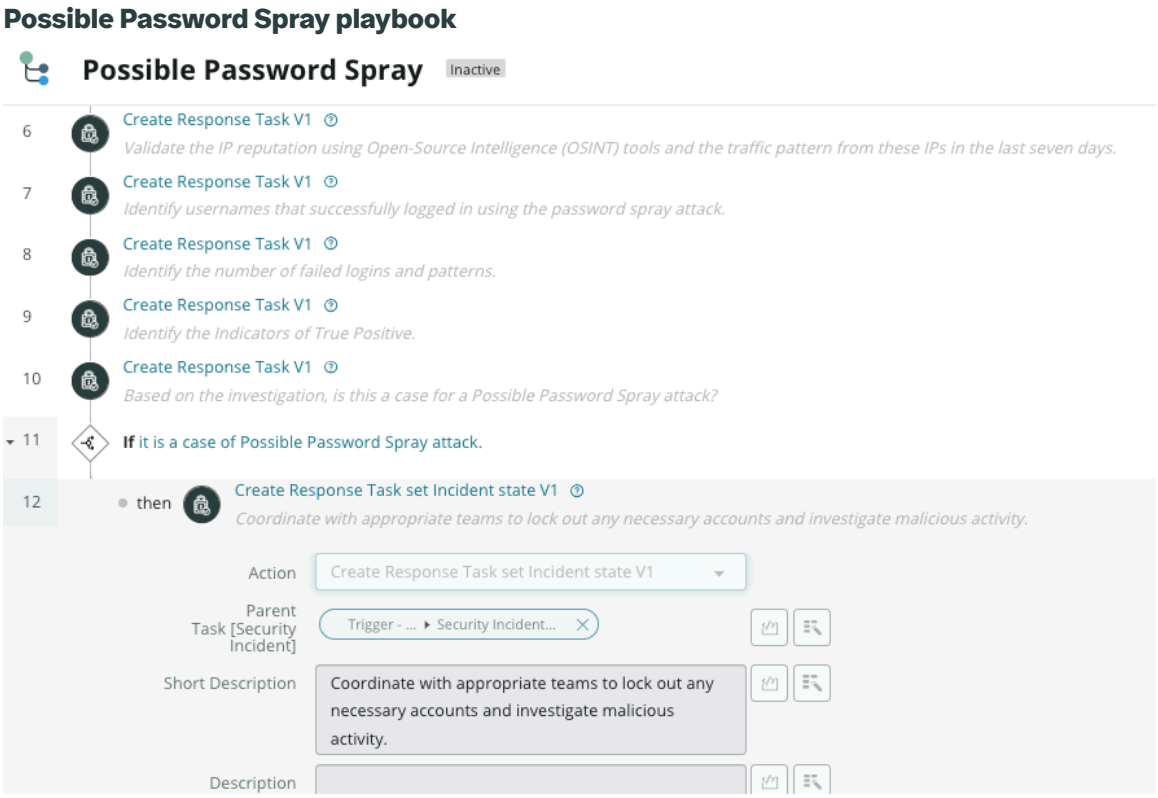
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. In Action 7, you need to identify the usernames that successfully logged in using the Password Spray attack.
6. In Action 8, you need to identify the number of failed logins and patterns.
7. In Action 9, you need to identify the indicators of true positive.
   - Check the traffic from the source IPs in the last 60 days. No historic traffic can be an indication of a true positive.
   - Check the username patterns having authentication failures and the count. The higher the count, the higher the probability that it's a true positive.
   - The username looks like a dictionary base (starting from A to Z) and might have common admin names like admin, sysadmin, root, and so on
   - The same username might have different patterns in the spray attack like the same alert might have failures for john.doe, johnd, jdoe, john_doe, jdoe7,etc., indicating attackers guessing the username pattern based on common use cases.
   - Notice the User Agent and URIs from the F5 logs in the step above, and see if the IOCs are related to the Red Condor alerts. If they match, then it's a true positive event.
8. In Action 10, based on the investigation done so far, you need to check whether this is a case of Possible Password Spray attack or not.
9. In Action 11, if this is case of Possible Password Spray attack, perform the following actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In Action 12, you need to coordinate with appropriate teams to lock out any necessary accounts and investigate malicious activity.



b. In Action 13, you need to initiate a post-incident review of the Possible Password Spray attack.

c. In Action 14, the flow ends.

10. In Action 15, you need to check whether this isn't a case of Possible Password Spray attack.
11. In Action 16, if this isn't a case of Possible Password Spray attack, perform the following actions:
    a. In Action 17, you need to document the findings so far.
    b. In Action 18, you need to initiate a post-incident review of the Possible Password Spray attack.
    c. In Action 19, the flow ends.
12. In Action 20, you need to consult with the peers and GIR manager for guidance.
13. In Action 21, a response task is created to complete the post-incident review before closing the task.

Playbook for T1003 - Detect Credential Dumping Tools

This playbook provides systematic remediation steps to investigate an incident involving credential dumping activities.

Set up the T1003 - Detect Credential Dumping Tools playbook

Use the following steps to set up the T1003 - Detect Credential Dumping Tools playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required:

- sn_si.admin
- flow_designer

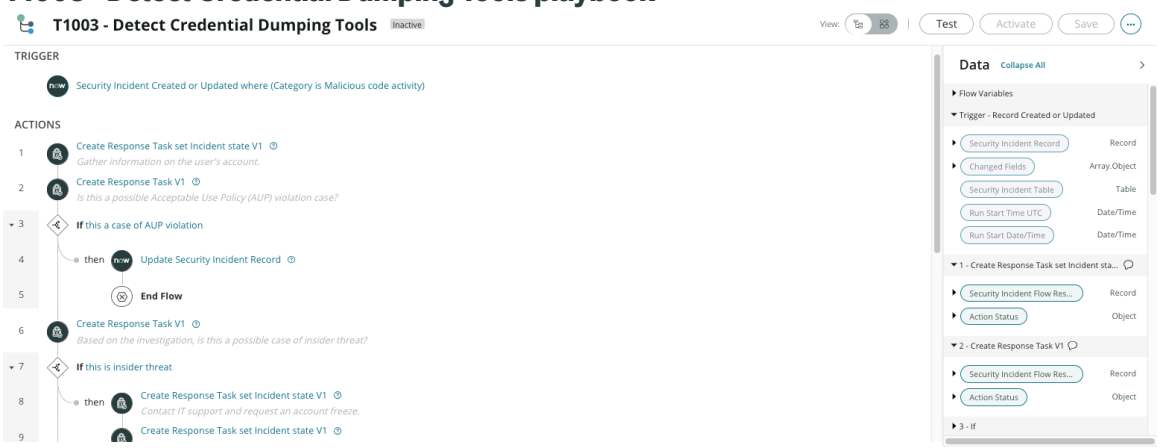
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **T1003 - Detect Credential Dumping Tools** playbook.
3. **Optional:** You can create a copy of the T1003 - Detect Credential Dumping Tools playbook flow and make the necessary modifications.

   To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

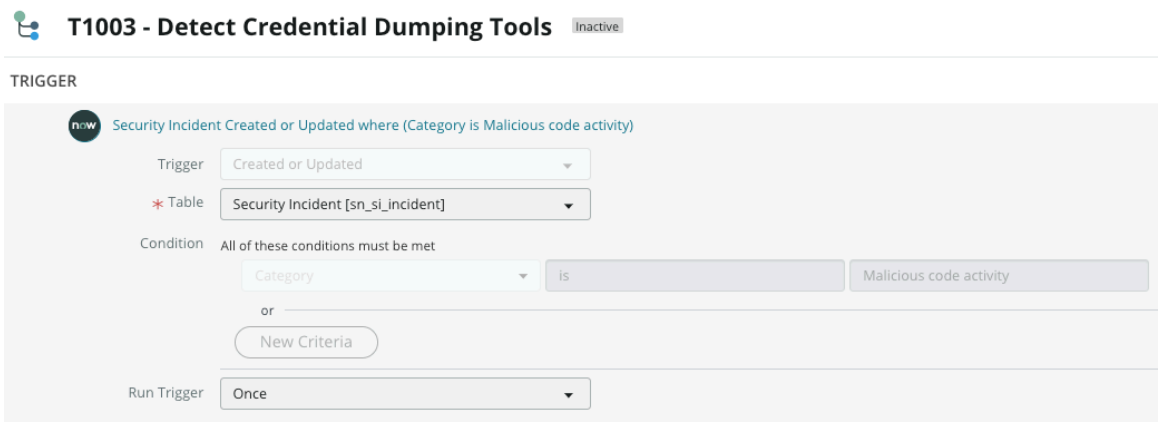
   T1003 - Detect Credential Dumping Tools playbook

4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Malicious code activity**.



Use the T1003 - Detect Credential Dumping Tools playbook

Use this playbook to investigate an incident involving credential dumping activities. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the T1003 - Detect Credential Dumping Tools playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

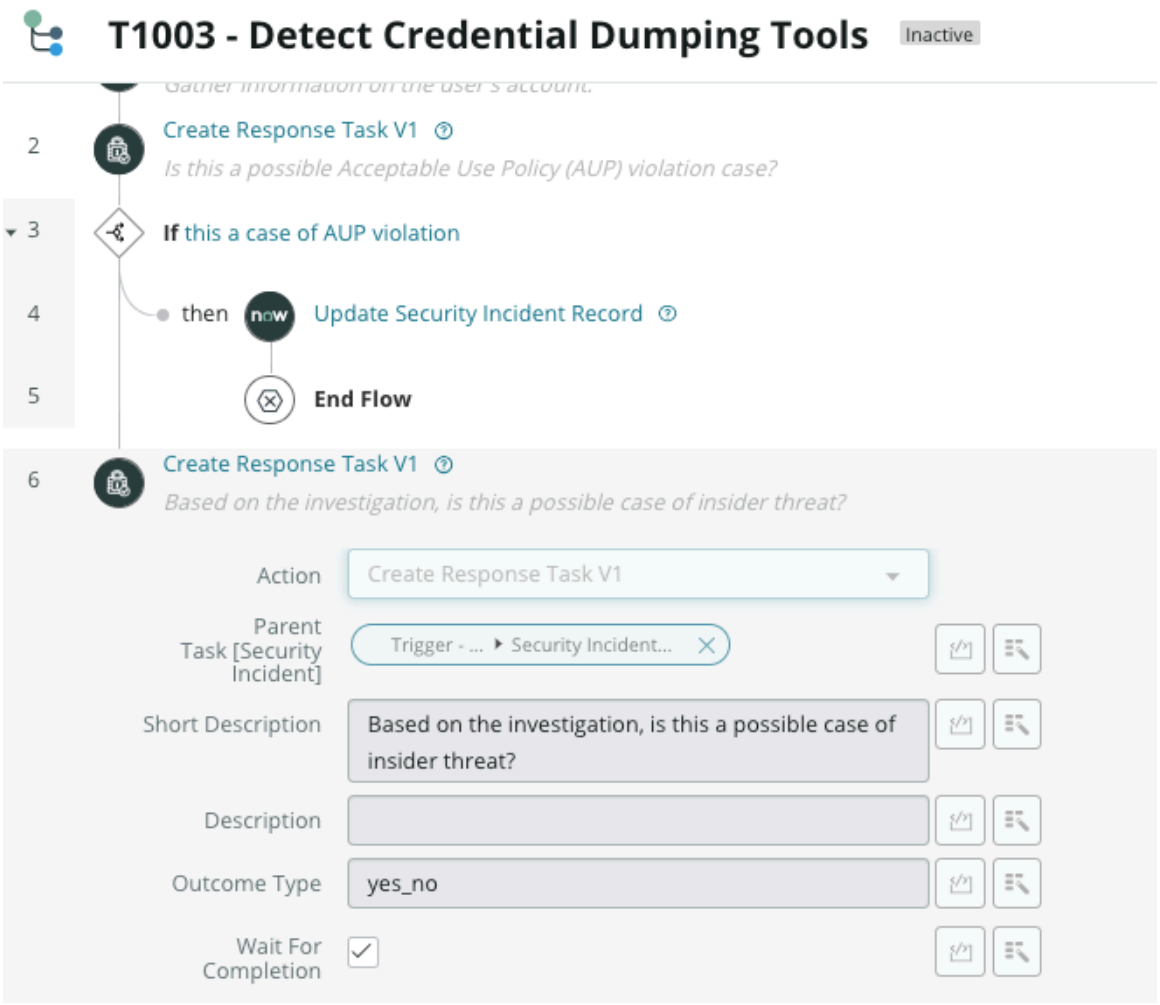
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. When the playbook is triggered and starts executing, in Action 1, you need to gather information on the user's account.
   - You need to check the host activity to look for any suspicious activities.
   - You need to identify the owner of the Server/Endpoint/VM and capture the data correlating to the tool.
   - You need to gather information on the user's other accounts.
2. In Action 2, you need to check whether this is a possible Acceptable Use Policy (AUP) violation case.
   You can do a peer review with the evidence gathered and consult with your regional Incident Manager whether to contact the user.
3. In Action 3, if this is a case of Acceptable Use Policy (AUP) violation, then perform the following actions:
   a. In Action 4, you need to update the security incident that this is a case of AUP violation
   b. In Action 5, the flow ends.
4. In Action 6, based on the investigation done so far, you need to check whether this is a possible case of insider threat or not.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

T1003 - Detect Credential Dumping Tools playbook



5. In Action 7, if this is a case of insider threat, perform the following actions:

a. In Action 8, you need to contact IT support and request an account freeze.

b. In Action 9, you need to block malicious IPs.

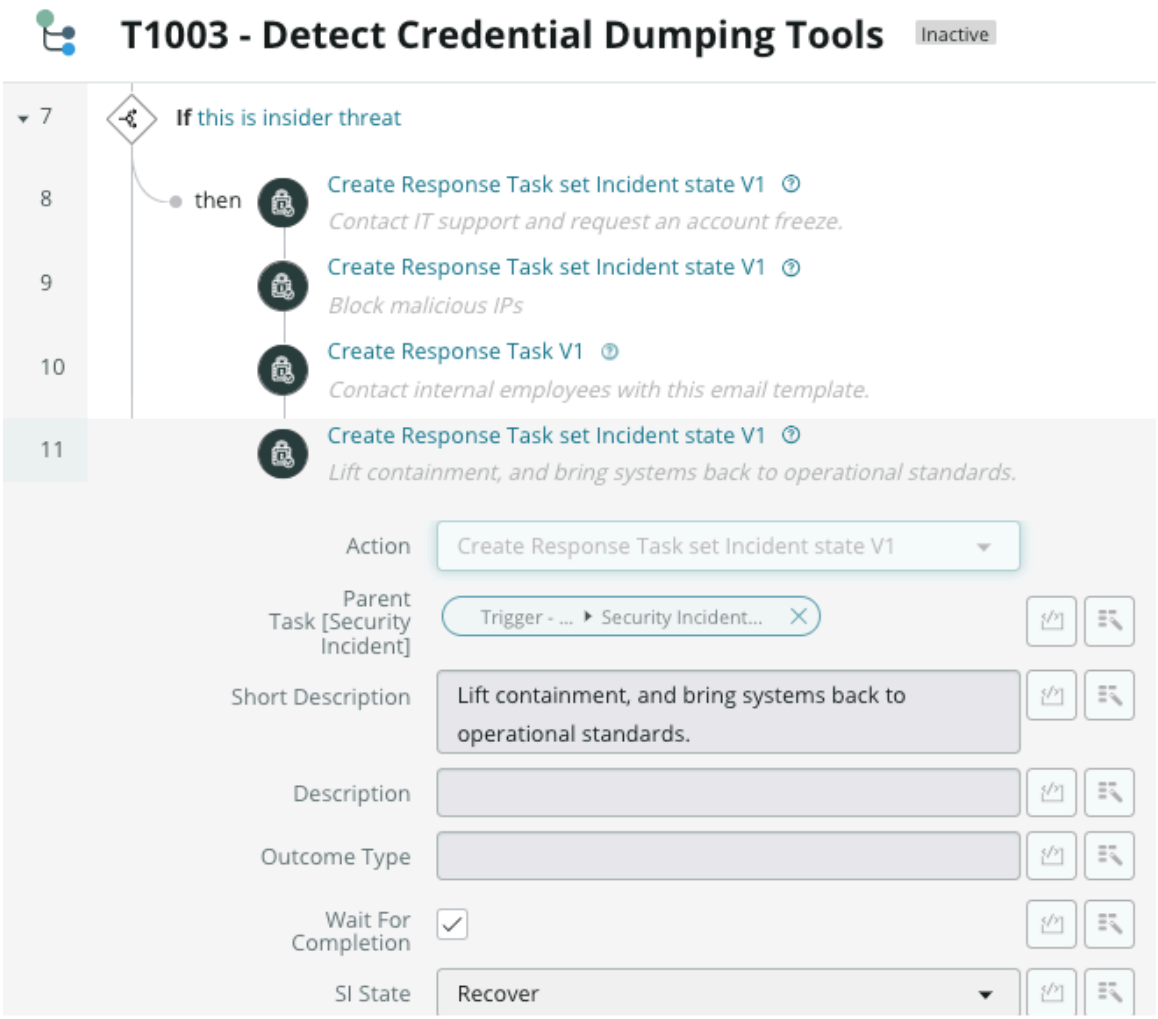
c. In Action 10, you need to contact internal employees through an email.
You can use the provided email template to contact your internal employees.

d. In Action 11, you need to lift the containment and bring the systems back to operational standards.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The flow ends.

Response tasks to lift the containment



6. In Action 12, if this isn't a case of insider threat, then in Action 13, you need to perform a peer review to determine if this needs to be added to the exclusion list.
   The flow ends.
7. In Action 14, a response task is created to complete the post-incident review before closing the task.

Playbook for Email Domain Spoofing Detection

This playbook helps with the early stage triage of user-reported phishing submissions by alerting the analyst to the possibility of a look-alike domain in the Phisher's email address.

The Email Domain Spoofing Detection playbook looks to find a similarity match between the Phisher's sender email domain with a trusted domain name exists in the observable repository. When a spoofed sender email domain match has been identified by the playbook, the analysts are alerted with a tag.

The workflow is created based on an existing playbook, which provides a consistent and efficient approach for incident investigation. Each decision point in the playbook has been converted into an outcome driven task and flow changes direction based on the outcome of such tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up the Email Spoof Detection playbook

Use the following steps to set up the Email Spoof Detection playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

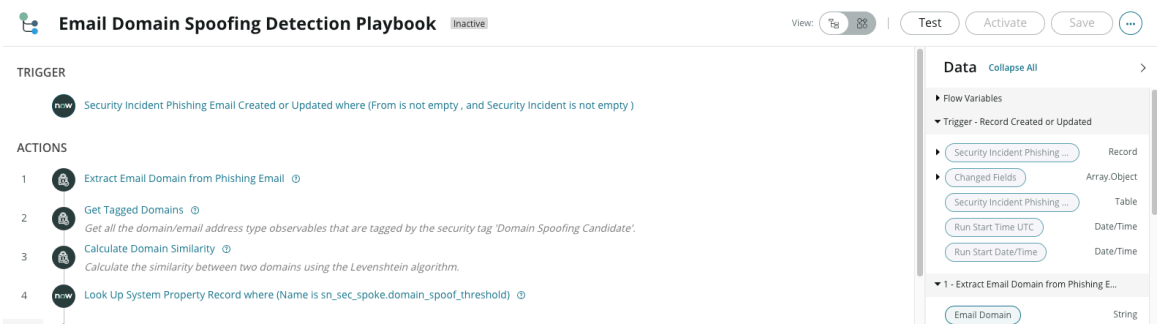
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Email Domain Spoofing Detection playbook** playbook.
3. **Optional:** You can create a copy of the Email Domain Spoofing Detection playbook flow and make the necessary modifications.

   To create a copy of the playbook's flow, click the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

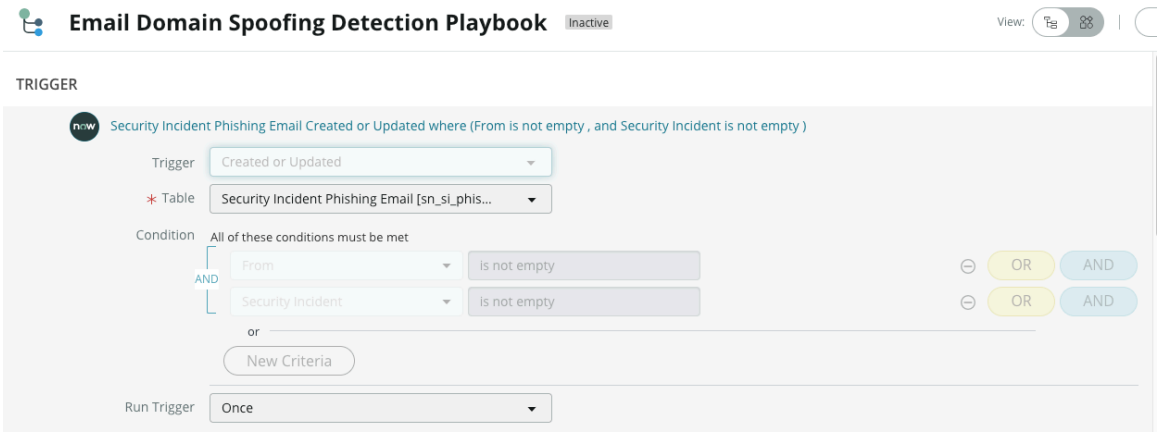
   Email Domain Spoofing Detection playbook

4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.
   This playbook is triggered and associated with the security incident when the following conditions are met:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **From** is not **empty**.
- **Security incident** is not **empty**.



Use the Email Domain Spoofing Detection playbook

Use this playbook to find a similarity match between the Phisher's sender email domain with a trusted domain name exists in the observable repository. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Email Domain Spoofing Detection playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

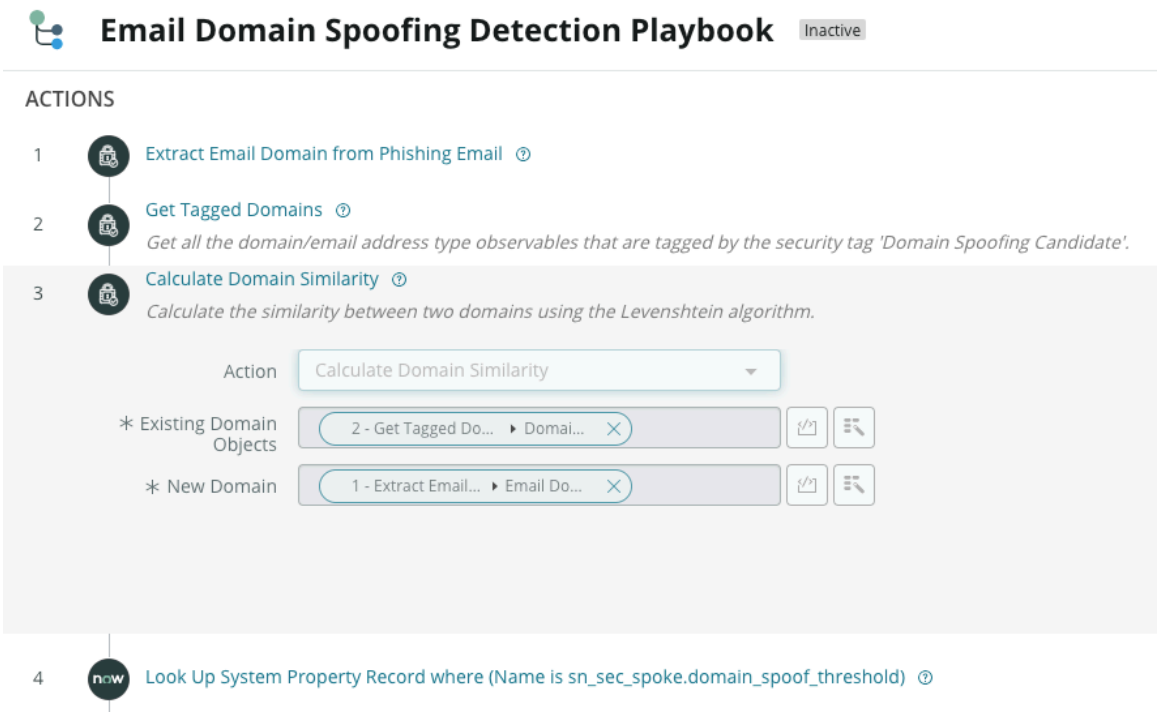
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. When the playbook is triggered and starts executing, in Action 1, the playbook extracts the email domain from the phishing email.
2. In Action 2, the playbook retrieves all the domain/email address type observables tagged by the security tag 'Domain Spoofing Candidate'.
3. In Action 3, the playbook calculates the similarity between the Get Tagged domain and Email domain using the Levenshtein algorithm.

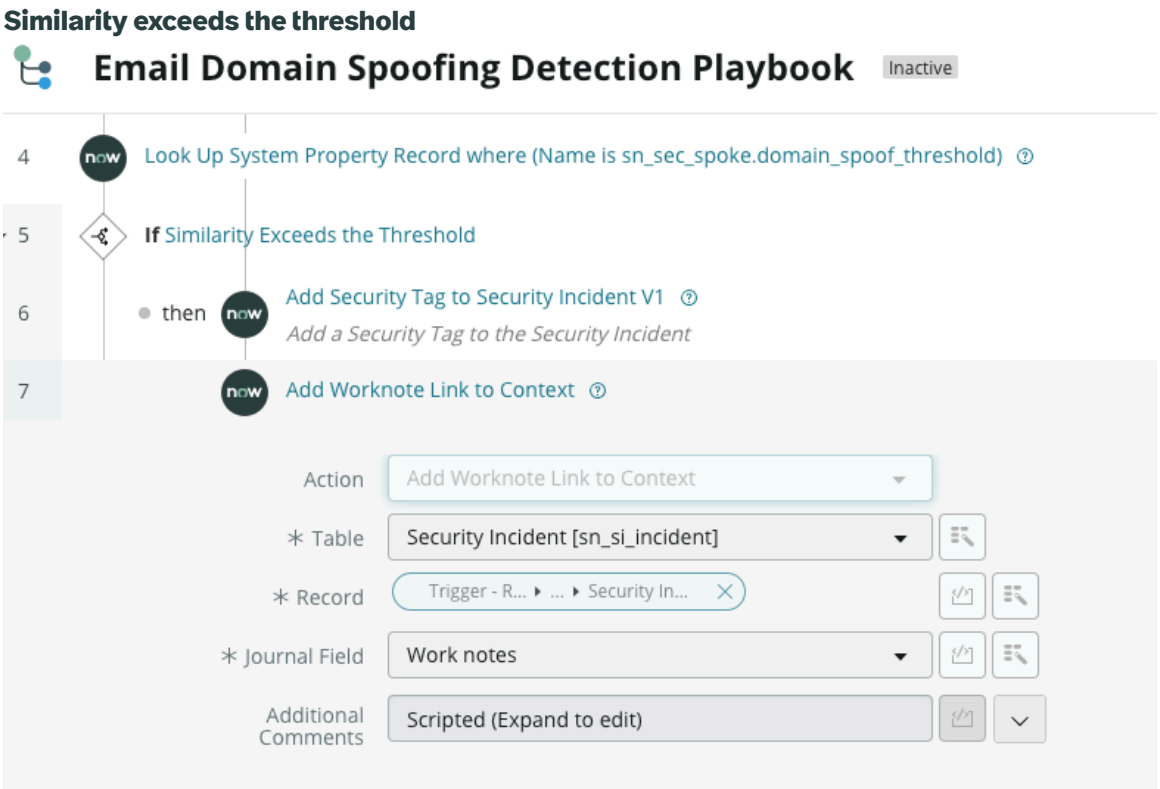
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Email Domain Spoofing Detection playbook



4. In Action 4, the playbook looks up for the System Property record based on the following conditions:
   - Name is sn_sec_spoke.domain_spoof_threshold, (OR)
   - Name is from a to z, and if multiple records are found then return only the first record.
5. In Action 5, based on the investigation done so far, the playbook checks if the similarity of the two domains exceeds the threshold or not.
   If the similarity of the two domains doesn't exceed the threshold, a manual response task is created in Action 5 and the flow ends. If the similarity of the two domains exceeds the threshold, then Actions 6 and 7 are executed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. In Action 6, the playbook adds the Email Domain Spoofing security tag to the security incident.
7. In Action 7, the playbook adds a worknote link to the context using the script option.
8. In Action 8, the flow ends.

Playbook for Typo Squatted Domain

This playbook provides systematic procedures for investigating misspelled domains and collaborating with the organization's legal department for take-downs. Typo Squatted domains are intentionally misspelled domain names that closely resemble legitimate ones. Attackers take advantage of spelling errors to lead them to an ill-intended website for financial exploitation or other malicious activities.

The Typo Squatted Domains are reported to the Security Operations Team from different sources like Digital risk protection solutions (Digital Shadows) and Threat intelligence platforms (Anomali Threatstream). After a security incident is created, this solution helps identify whether the domain is indeed a Typo Squatted Domain. If it's a Typo Squatted Domain, the analyst can report it to the legal team so that further actions can be taken.

The workflow is created based on an existing playbook, which provides a consistent and efficient approach for incident investigation. Each decision point in the playbook has been converted into an outcome-driven task and the flow changes direction based on the outcome of such tasks.

Set up the Typo Squatted Domain playbook

Use the following steps to set up the Typo Squatted Domain playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

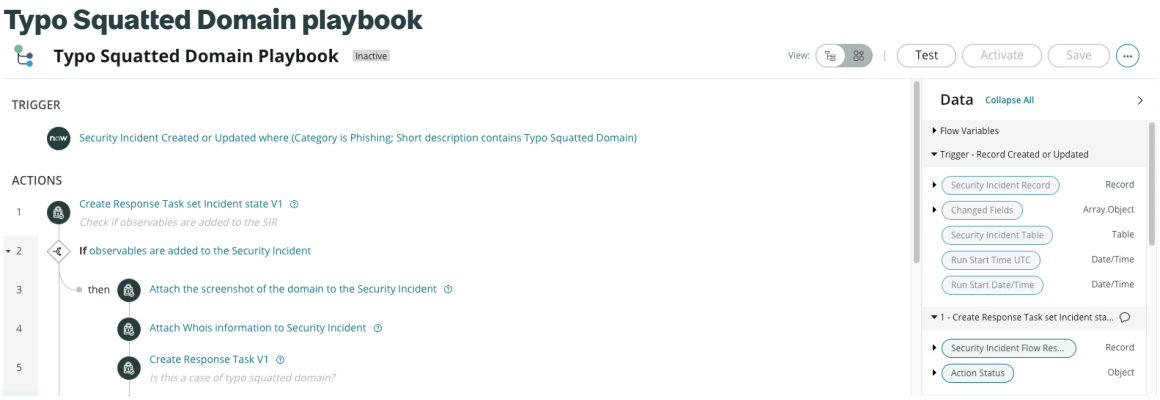
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Typo Squatted Domain** playbook.
3. **Optional:** You can create a copy of the Typo Squatted Domain playbook flow and make the necessary modifications.

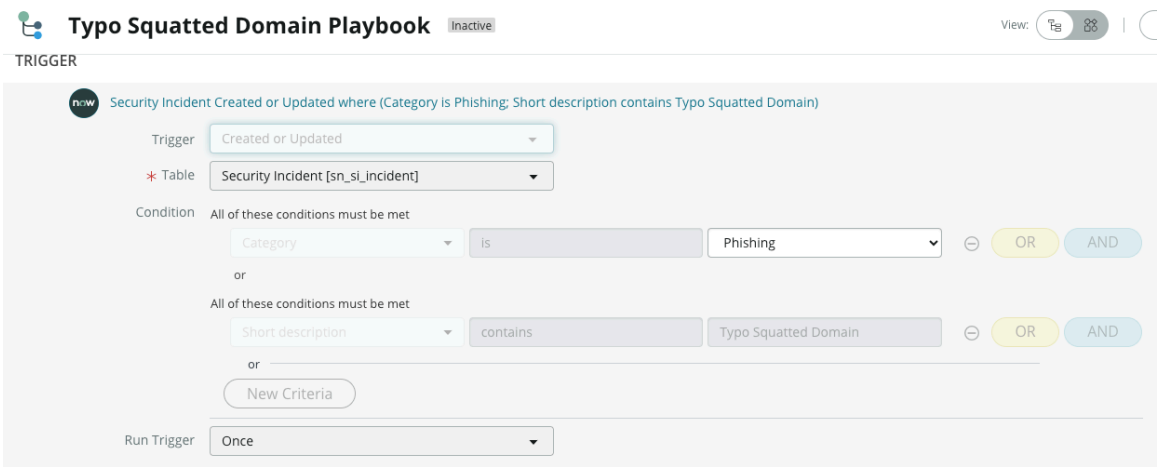
   (Optional) To create a copy of the playbook's flow, click the ••• icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.



4. Activate the playbooks.
   - Activate the main flow to use the playbook available in the base system.
   - Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered and associated with the security incident when the following conditions are met:

   - **Category** is **Phishing**.
   - **Short description** contains **Typo Squatted Domain**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the Typo Squatted Domain playbook

Use this playbook to investigate misspelled domains and collaborating with the organization's legal department for take-downs. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Typo Squatted Domain playbook.

Before you begin

Role required:

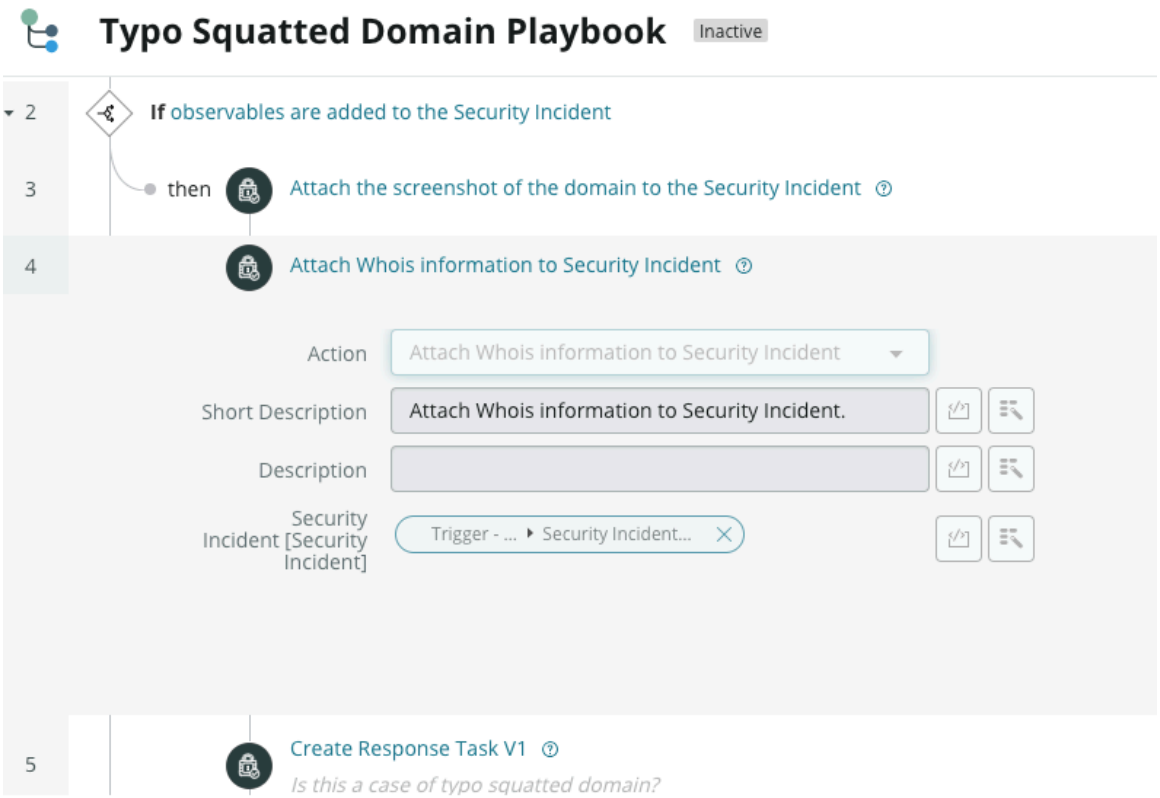
- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. When the playbook is triggered and starts executing, in Action 1, you need to check whether the observables are added to the Security Incident Response (SIR).
   If the observables aren't added to SIR, please add the observables before proceeding. If the observables aren't available, then Action 10 is executed and the security incident is closed.
2. In Action 2, if the observables are added to the security incident, then the following actions are executed.
3. In Action 3, you need to attach the screenshot of the Typo Squatted domain to the security incident.

Typo Squatted Domain playbook



4. In Action 4, you need to attach the Whois information to the security incident.
5. In Action 5, based on the investigation done so far, the playbook checks whether this is a case of Typo Squatted domain or not.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If this isn't a case of Typo Squatted domain, a manual response task is created in Action 5 and the flow ends.

6. In Action 6, if this is a case of Typo Squatted domain, then action 7 is executed.
7. In Action 7, you need to email and inform the Legal and other required teams that this is a case of Typo Squatted domain and take the necessary actions to eradicate it.
   If this isn't a case of Typo Squatted domain, a manual response task is created in Action 5 and the flow ends.

Case of Typo Squatted Domain



8. In Action 9, a response task is created for you to complete the post-incident review before closing the task.

Playbook for Credential Sniffing

This playbook provides system remediation steps to investigate an incident involving credential sniffing activities performed through the *sys_installation_exit* table in a ServiceNow instance.

The Credential Sniffing playbook provides a script field to process the Database (DB) logins, Single sign-on (SSO), and LDAP (Lightweight Directory Access Protocol) by using the records on the *sys_installation_exit* table. These privileged scripting fields enable listening of user requests and parameters to the instances during login, including user credentials such as username and password.

A malicious user may create a script to listen to the user requests and log these requests on the instance. The *sys_installation_exit* table on an instance defines the rules of processing the login and logout activities of all users on that instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up the Credential Sniffing playbook

Use the following steps to set up the Credential Sniffing playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

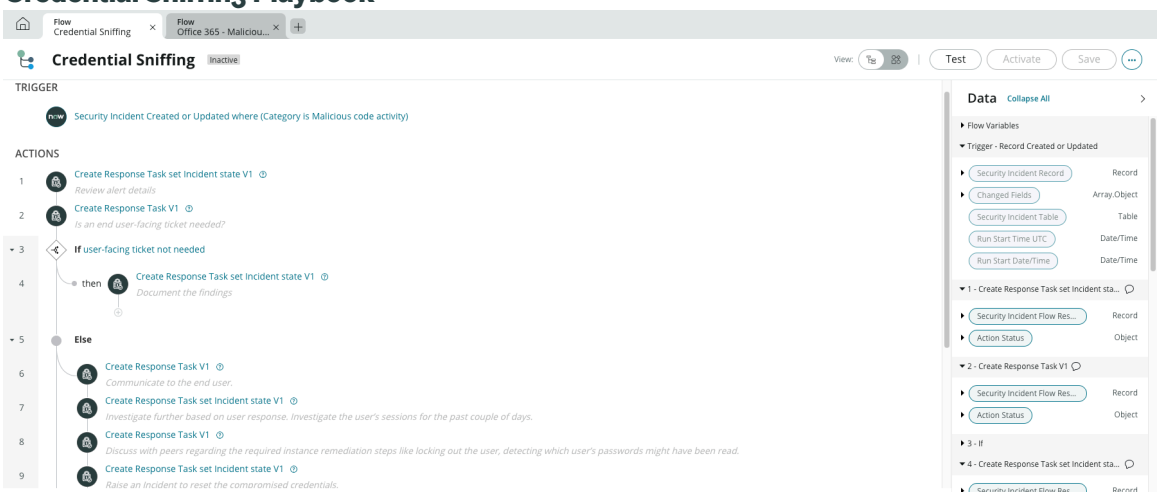
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Credential Sniffing** playbook.
3. **Optional:** Create a copy of the Credential Sniffing playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

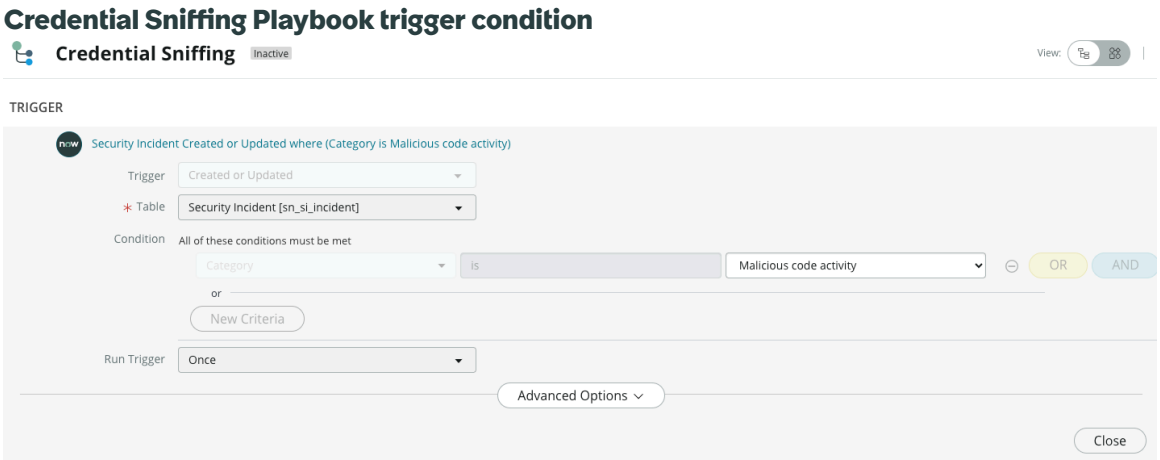
   Credential Sniffing Playbook

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Malicious code activity**.



Use the Credential Sniffing playbook

Use this playbook to investigate an incident involving credential sniffing activities performed through the *sys_installation_exit* table in a ServiceNow instance. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Credential Sniffing playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

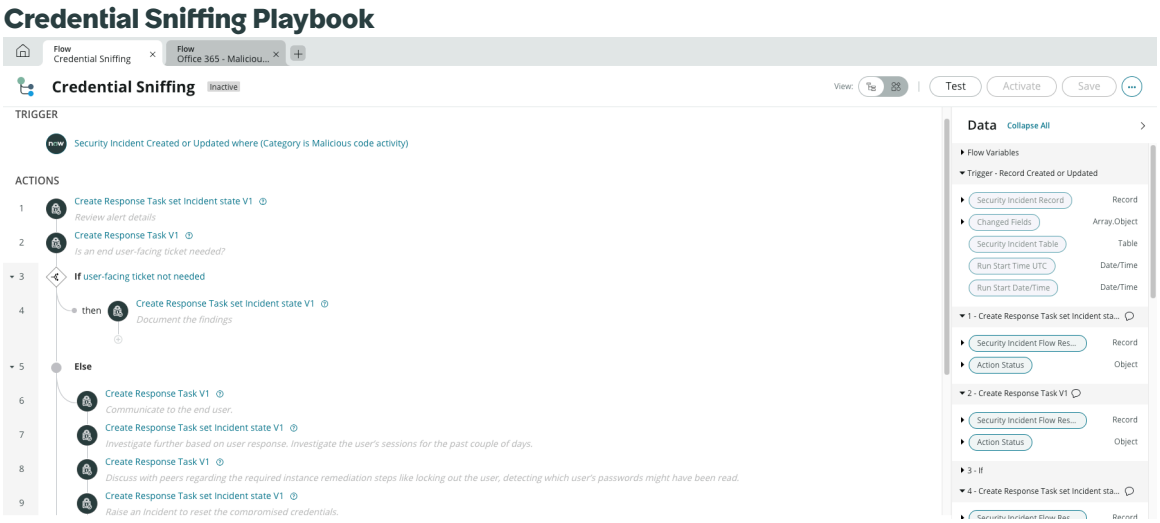
Procedure

1. When the playbook is triggered and starts executing, in Action 1, review the following alert details.
   - Instance
   - Session ID
   - Transaction ID
   - _raw: Provides the whole script.

     Example script:

     ```
     Var pass= request.getParameter("user_password");
     Gs.log(pass);
     ```
2. In Action 2, based on the data collected so far, check whether an end user ticket is required for this alert or not.
3. In Action 3, if the alert does not require an end user ticket, then in Action 4, document the findings so far.
   The flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In Action 5, if the alert requires an end user ticket, then perform the following steps:

   a. In Action 6, inform the end user that the alert requires an end user ticket.

   b. In Action 7, investigate further based on the user's response and the user's sessions during the last couple of days.

   c. In Action 8, discuss with peers about the remediation steps for the instance like locking out the user and detecting which user's passwords might have been read.

   d. In Action 9, raise an incident or ticket to reset the compromised user credentials.

   e. In Action 10, lift the containment and bring the systems back to operational standards
   The flow ends.

5. In Action 11, complete the post-incident review before closing the task.

Playbook for T1070 - Windows Events Logs Cleared

This playbook provides remediation steps to investigate incidents that track event types where the user removes security logs. Whenever the Security log is cleared, the events 517 and 1102 are logged regardless of the Audit System Event policy status.

This alert can track the following types of events:

- **Event 517**: The Primary username and Client username fields identifies the user who cleared the log. The Primary username corresponds to the system, and the Client username indicates the user who cleared the log.
- **Event 1102**: The Account Name and Domain Name fields identifies the user who cleared the log. The Logon ID enables you to correlate backwards to the log on event and other events logged during the same logon session.

Set up the T1070 - Windows Events Logs Cleared playbook

Use the following steps to set up the T1070 - Windows Events Logs Cleared playbook.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_si.admin
- flow_designer

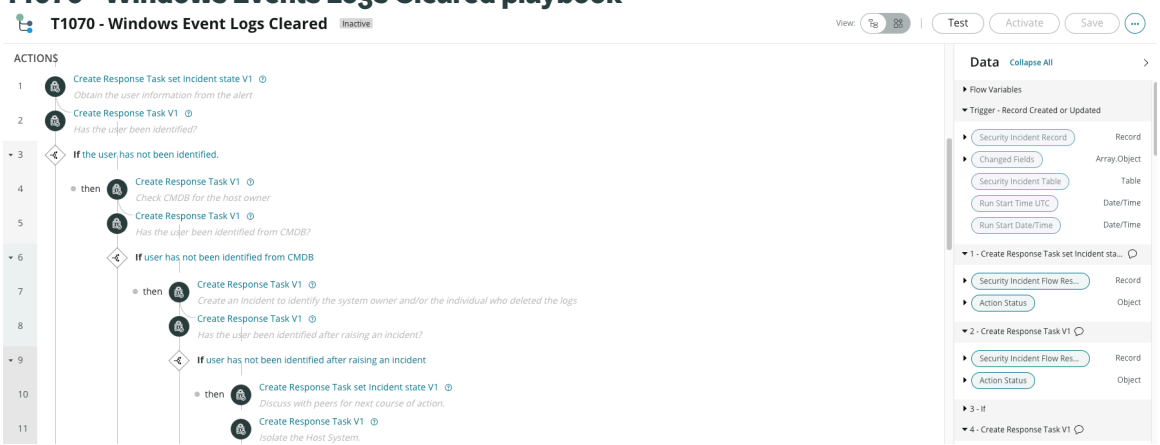
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **T1070 - Windows Events Logs Cleared** playbook.
3. **Optional:** Create a copy of the T1070 - Windows Events Logs Cleared playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

   T1070 - Windows Events Logs Cleared playbook

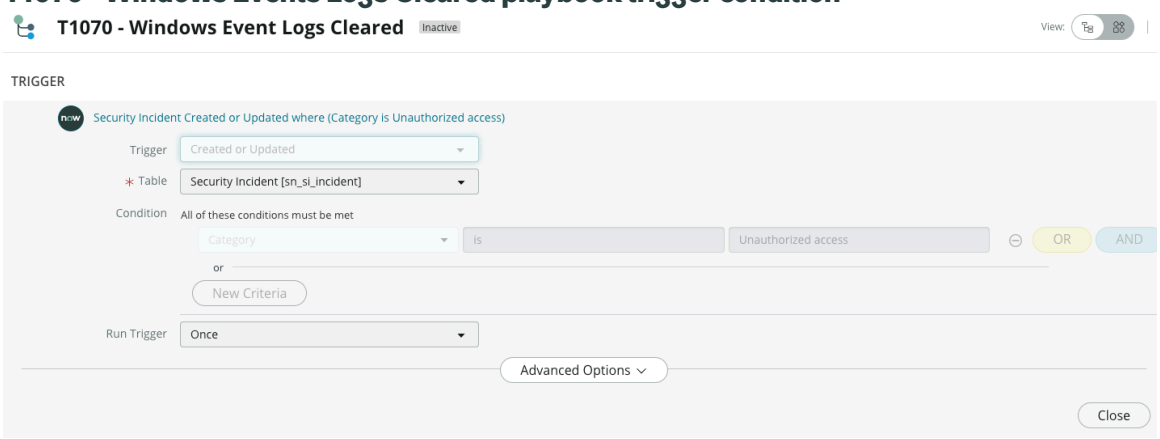
   

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Unauthorized access**.

T1070 - Windows Events Logs Cleared playbook trigger condition



Use the T1070 - Windows Events Logs Cleared playbook

Use this playbook to investigate incidents that track event types where the user removes security logs. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the T1070 - Windows Events Logs Cleared playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

Procedure

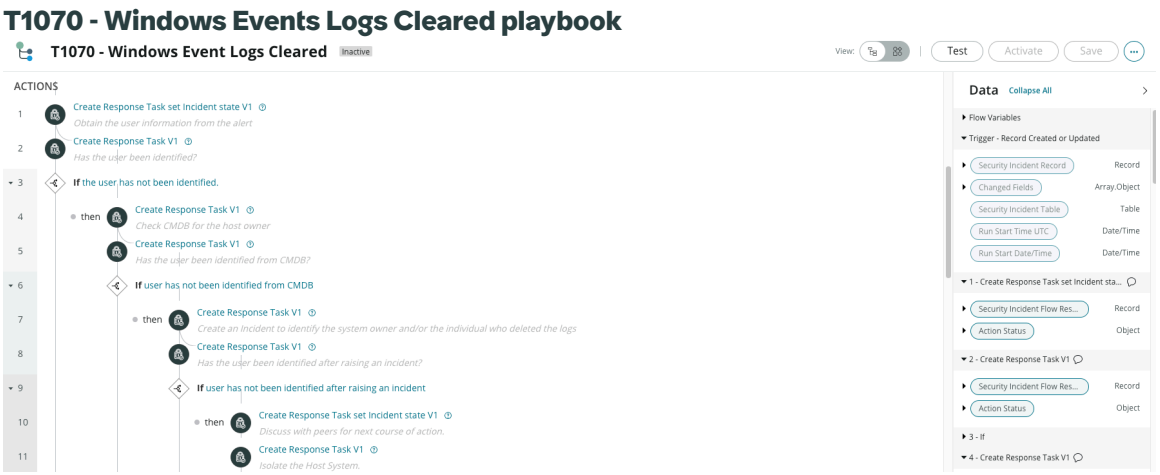
1. When the playbook is triggered and starts executing, in Action 1, obtain the user details from the alert.
2. In Action 2, check whether the user has been identified or not.
3. In Action 3, if the user has not been identified, perform the following steps:

   a. In Action 4, check the CMDB (Configuration management database) for the host owner details.

   b. In Action 5, check whether the user has been identified from the CMDB or not.

      If the user has been identified from the CMDB, a manual response task is created in Action 5 and the flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. In Action 6, if the user has not been identified from the CMDB, perform the following steps:

i. In Action 7, create an incident to identify the system owner and the individual who deleted the logs.

ii. In Action 8, check whether the user been identified after raising an incident or not.

If the user has been identified after raising an incident, a manual response task is created in Action 8 and the flow ends.

iii. In Action 9, if the user has not been identified after raising an incident, perform the following steps:

1. In Action 10, discuss the next course of action with peers.

2. In Action 11, isolate the host system.

3. In Action 12, remove any unwanted files that may have been created, and delete the rogue accounts.

4. In Action 13, lift the containment and bring the systems back to operational standards.

5. In Action 14, complete the post-incident review before closing the task.

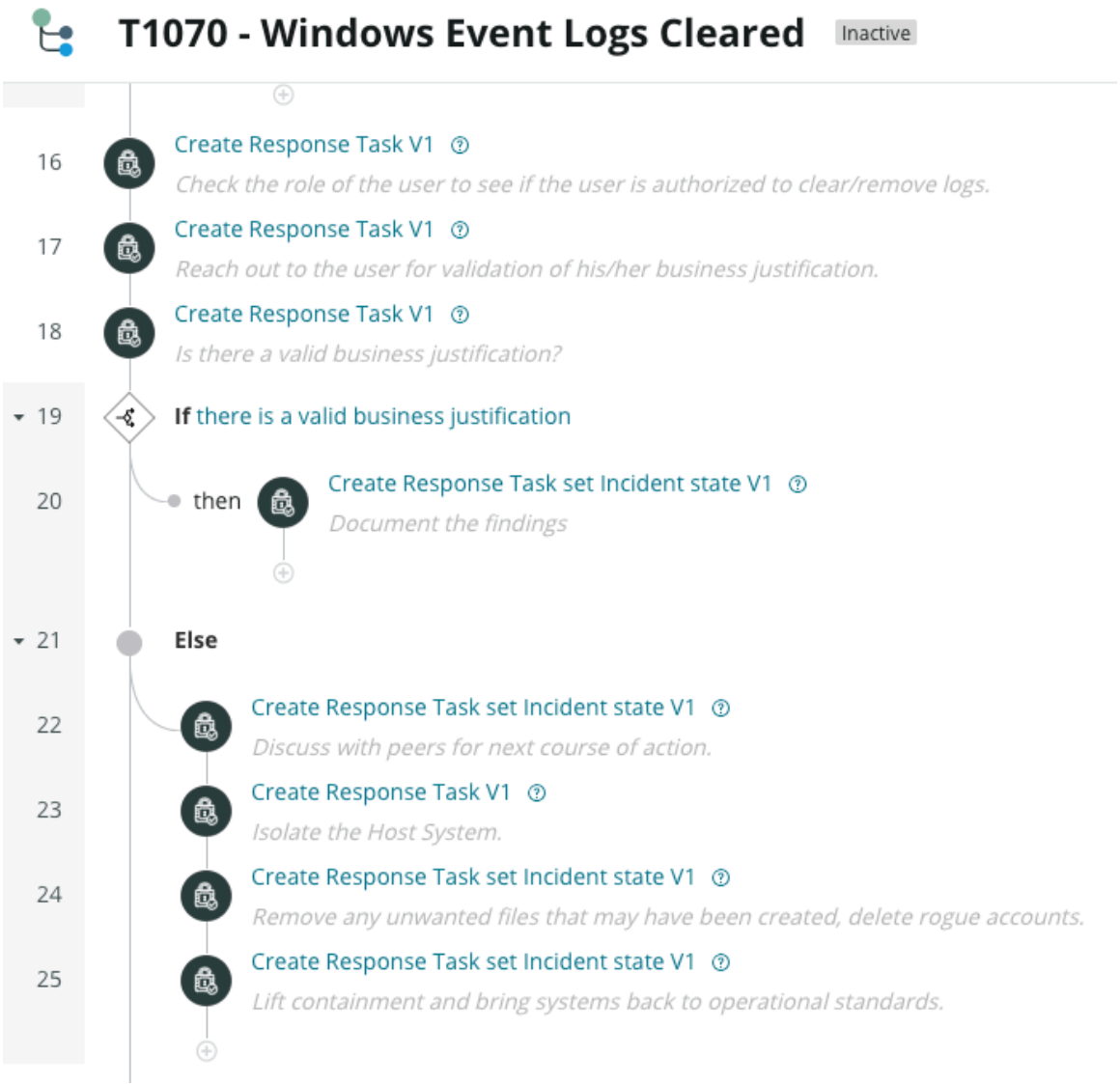
In Action 15, the flow ends.

4. In Action 16, if the user has been identified, then check the user's role to see if the user is authorized to clear or remove logs.

5. In Action 17, reach out to the user for validation of their business justification.
You can use the provided email template to contact the user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the T1070 - Windows Events Logs Cleared playbook



6. In Action 18, check whether a valid business justification is provided or not.
7. In Action 19, if there was a valid business justification provided, then in Action 20, document the findings so far.
   The flow ends.
8. In Action 21, if there was no valid business justification provided, perform the following steps:
   a. In Action 22, discuss the next course of action with peers.
   b. In Action 23, isolate the host system.
   c. In Action 24, remove any unwanted files that may have been created, and delete the rogue accounts.
   d. In Action 25, lift the containment and bring the systems back to operational standards.
      The flow ends.
9. In Action 26, complete the post-incident review before closing the task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Playbook for OSquery of External Address in /etc/hosts file

This playbook provides systematic remediation steps to investigate incidents that indicate that an internal hostname or domain has been assigned to an external IP address on the local DNS(/etc/hosts) of a Linux server.

Set up the OSquery of External Address in the /etc/hosts file playbook

Use the following steps to set up the OSquery of External Address in the /etc/hosts file playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

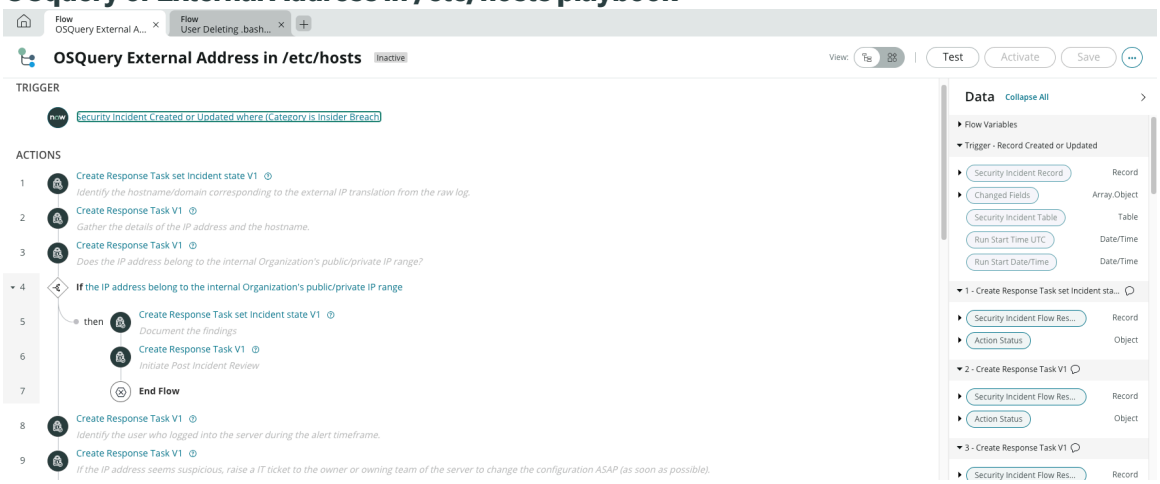
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **OSquery External Address in /etc/hosts** playbook.
3. **Optional:** Create a copy of the OSquery External Address in /etc/hosts playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

   OSquery of External Address in /etc/hosts playbook

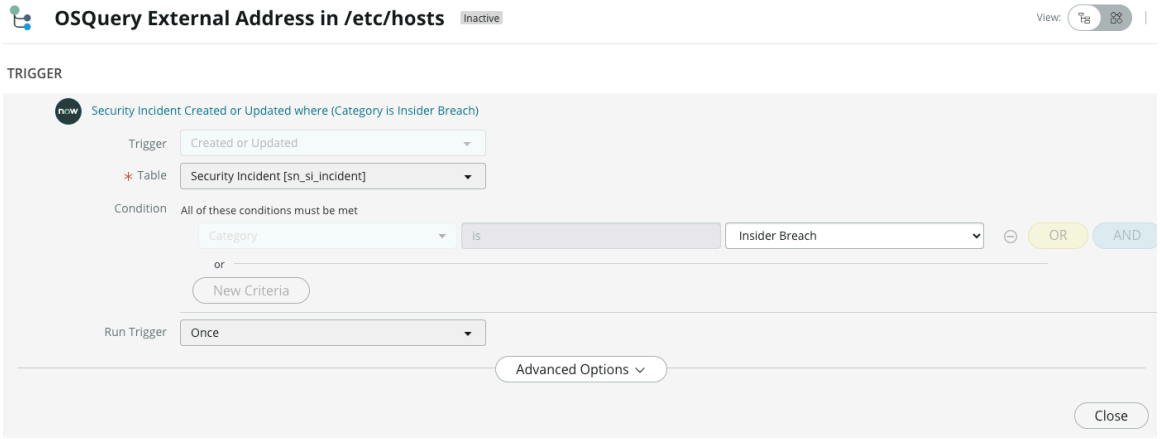
   

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Insider Breach**.

OSquery of External Address in /etc/hosts playbook trigger condition



Use the OSquery of External Address in the /etc/hosts file playbook

Use this playbook to investigate incidents that indicate that an internal hostname or domain has been assigned to an external IP address on the local DNS(/etc/hosts) of a Linux server. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the OSquery of external address in the /etc/hosts file playbook.

Before you begin

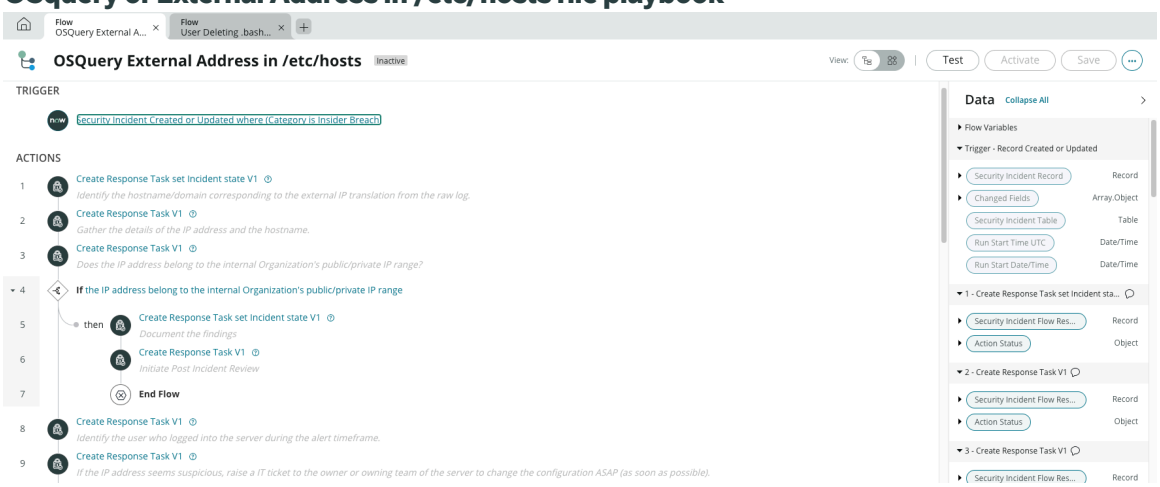
Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, identify the hostname or domain name corresponding to the external IP translation from the raw log.
2. In Action 2, gather the details of the IP address and the hostname.
3. In Action 3, check whether this IP address belongs to the internal organization's public/private IP range or not.

OSquery of External Address in /etc/hosts file playbook



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In Action 4, if the IP address belongs to the internal organization's public/private IP range, perform the following steps:

   a. In Action 5, document the findings so far.

   b. In Action 6, initiate a post incident review.
   In Action 7, after the post incident review, the flow ends.

5. If the IP address doesn’t belong to the internal organization's public/private IP range, then in Action 8, identify the user who logged in to the server during the alert timeframe.
6. In Action 9, if the IP address seems suspicious, raise an IT ticket to the owner or the server's team to change the configuration as soon as possible.
7. In Action 10, check whether there was any malicious activity on the server before and after adding the DNS entry.
8. In Action 11, check for any connections to the external IP address from the server.
9. In Action 12, document the findings so far.
10. In Action 13, check whether the owner or team information is available or not.
11. In Action 14, if the owner or team information is available, perform the following steps:

    a. In Action 15, reach out to the owner or the server’s team to see if they recognize the activity.
    You can use the provided email template to contact the owner or the server's team.

    b. In Action 16, check whether the owner or team provided a valid business justification or not.

    c. In Action 17, if the owner or team provided didn’t provide a valid business justification, then the flow ends.
    But, if the owner or team provided a valid business justification, perform the following steps:

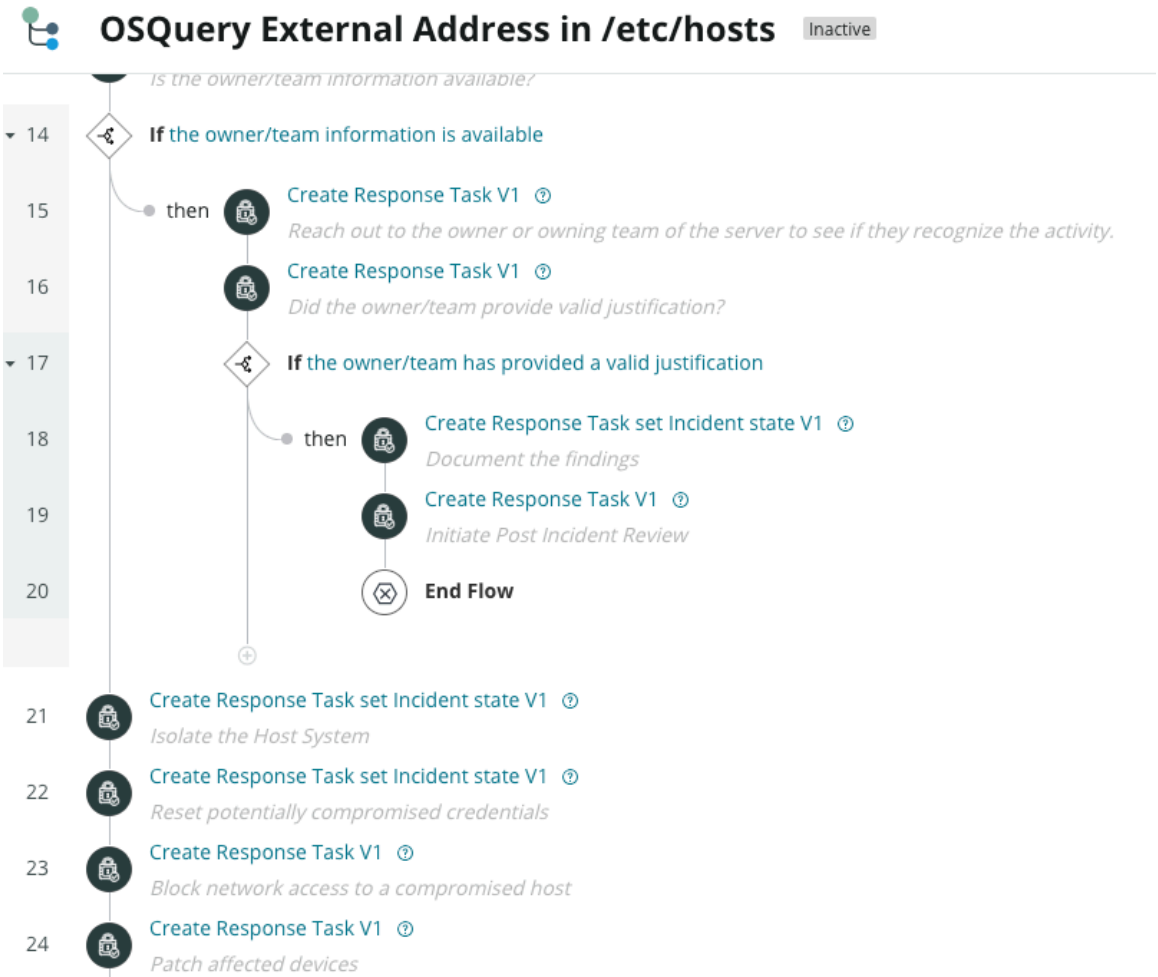
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

i. In Action 18, document the findings so far.

ii. In Action 19, initiate a post incident review.

In Action 20, after the post incident review, the flow ends.

Using the OSquery of External Address in /etc/hosts file playbook



12. In Action 21, if the owner or team information is unavailable, isolate the host system.
13. In Action 22, reset the potentially compromised credentials.
14. In Action 23, block the network access to the compromised host.
15. In Action 24, patch the affected devices.
16. In Action 25, lift containment and bring systems back to operational standards.
17. In Action 26, complete the post-incident review before closing the task.

Playbook for User Deleting Bash History - Cloud

This playbook provides systematic remediation steps to investigate incidents that indicate if someone was trying to remove the bash history (`.bash_history`) file from a Linux server.

Note: You need to mitigate this alert cautiously, as this alerts gets rarely triggered and it potentially indicates an insider threat.

Set up the User Deleting Bash History playbook

Use the following steps to set up the User Deleting Bash History playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required:

- sn_si.admin
- flow_designer

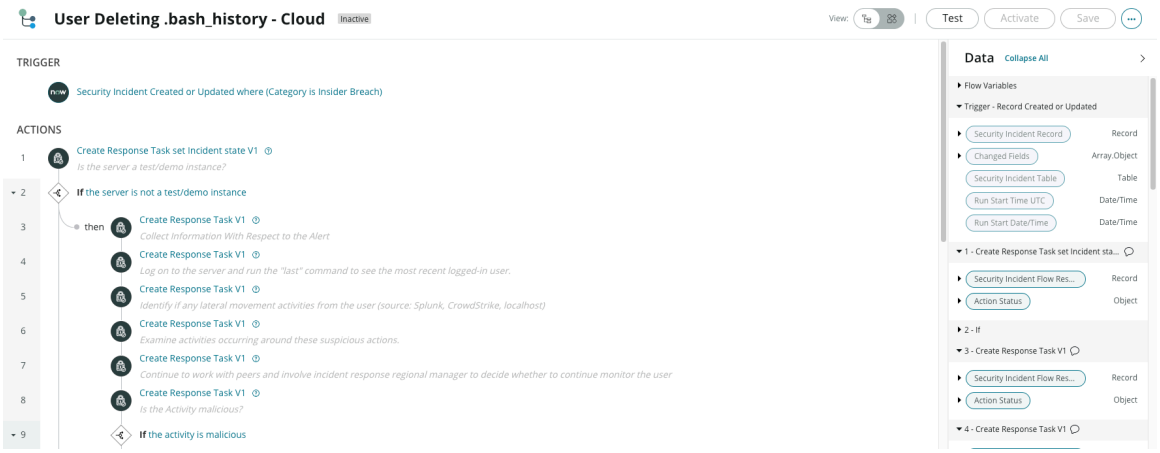
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **User Deleting .bash_history - Cloud** playbook.
3. **Optional:** Create a copy of the User Deleting .bash_history - Cloud playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

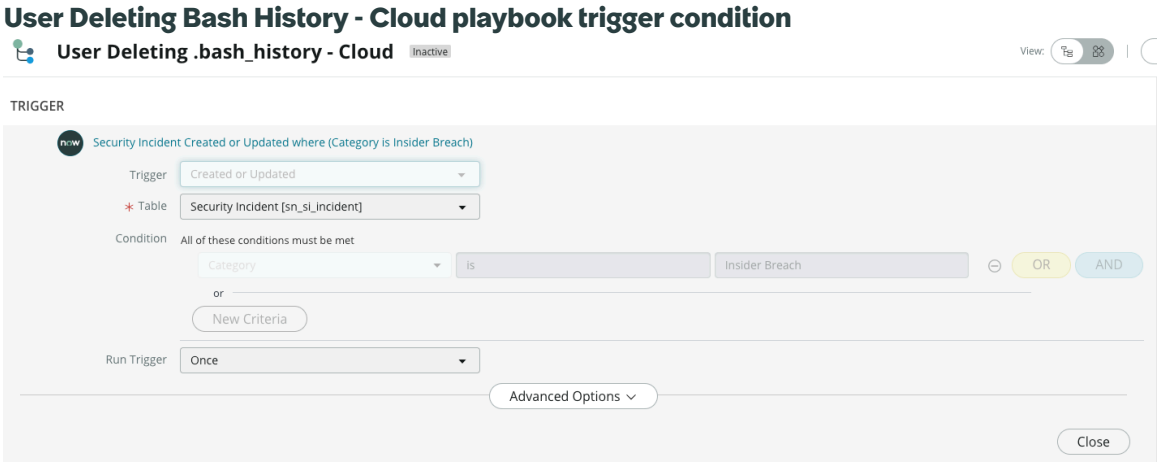
   User Deleting Bash History - Cloud playbook



4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Insider Breach**.



Use the User Deleting Bash History playbook

Use this playbook to investigate incidents that indicate if someone was trying to remove the bash history file from a Linux server. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the User Deleting the Bash History (*.bash_history*) playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, check whether the server is a test or demo instance.
2. In Action 2, if the server isn't a test or demo instance, perform the following steps:

   a. In Action 3, collect the following information for the alert:
      - Username
      - IP Address
      - Malicious commands attempting to delete bash history
      - All the commands run by the user, if available on the CrowdStrike logs.

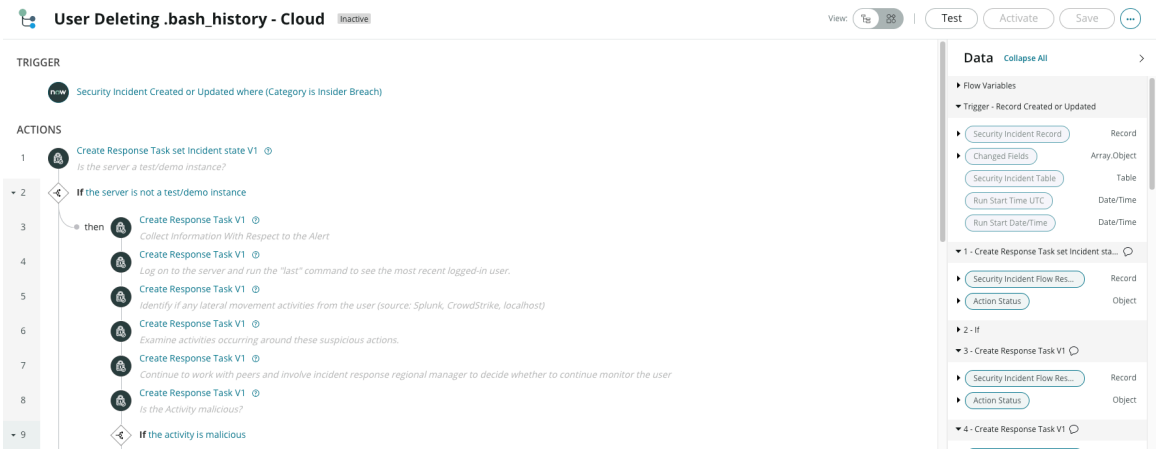
   b. In Action 4, log in to the server and run the *last* command to view the most recent logged-in user.

   c. In Action 5, identify if there were any lateral movement activities from the user (Source: Splunk, CrowdStrike, localhost).

   d. In Action 6, examine the activities occurring around these suspicious actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User Deleting Bash History playbook



e. In Action 7, continue working with peers and involve the incident response Regional Manager in deciding whether to continue monitoring the user.

f. In Action 8, determine whether the activity is malicious or not.

g. In Action 9, if the activity is malicious, perform the following steps:

i. In Action 10, during the investigation, contact IT Support and request an account freeze.

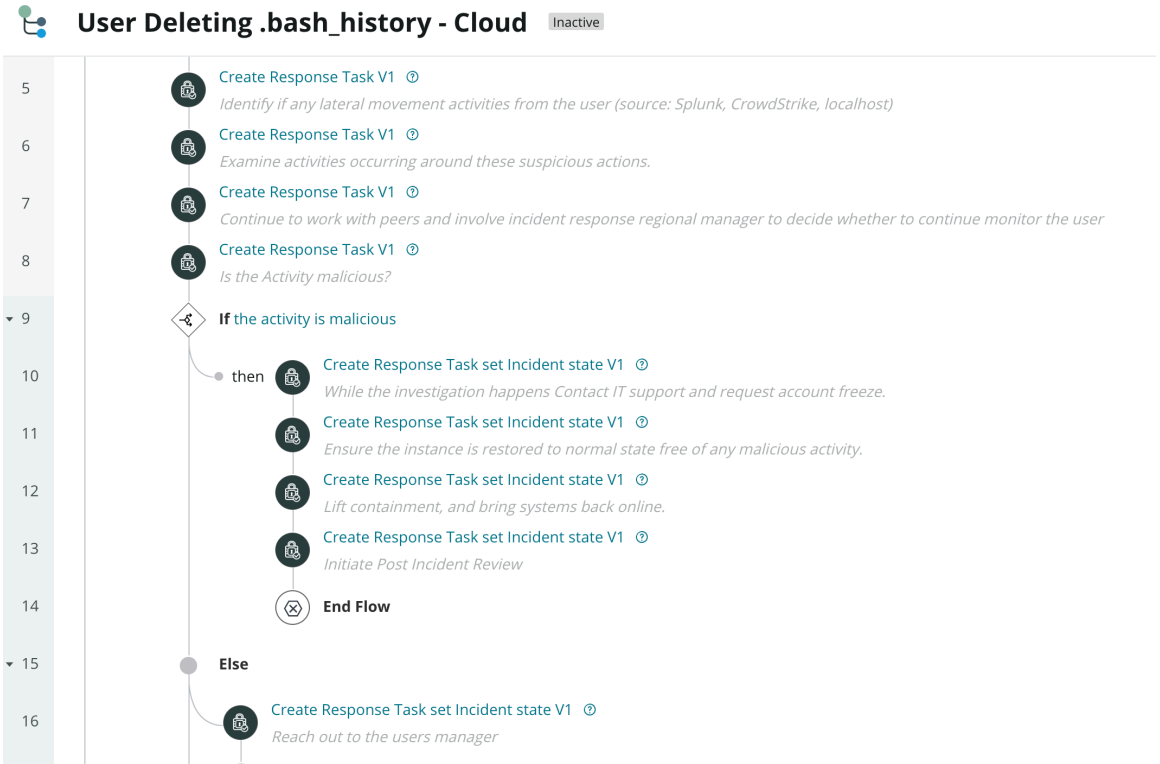
ii. In Action 11, ensure that the instance is restored to a normal state free of malicious activity.

iii. In Action 12, lift containment and bring systems back to operational standards.

iv. In Action 13, initiate a post incident review.

In Action 14, after the post incident review, the flow ends.

Using the User Deleting Bash History playbook



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

h. In Action 15, if the activity is not malicious, then in Action 16, reach out to the user's manager. You can use the provided email template to contact the user's manager and inform them about the recommended approach.

3. In Action 17, document the findings so far.
4. In Action 18, complete the post-incident review before closing the task.

Playbook for Successful VPN Attempts from the Service Accounts - Corp/Cloud

This playbook provides systematic remediation steps to investigate incidents that track successful login attempts from service accounts through VPN. Service accounts aren't supposed to have login events from a VPN, and such events could be indicators of either brute force or possible exposure of the account's credentials.

Set up the Successful VPN Attempts from the Service Accounts playbook

Use the following steps to set up the Successful VPN Attempts from the Service Accounts playbook.

Before you begin

Role required:

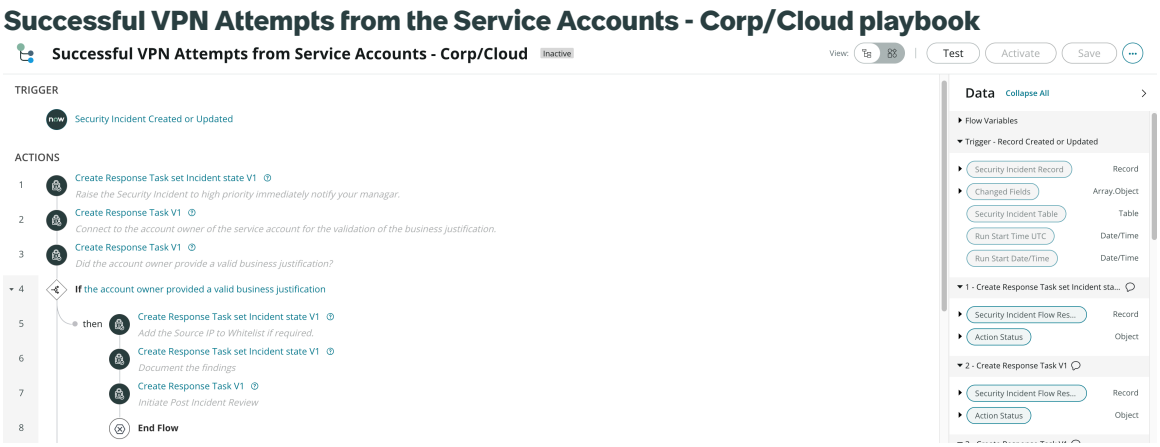
- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Successful VPN Attempts from the Service Accounts** playbook.
3. **Optional:** Create a copy of the Successful VPN Attempts from the Service Accounts playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.



4. Activate the playbooks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

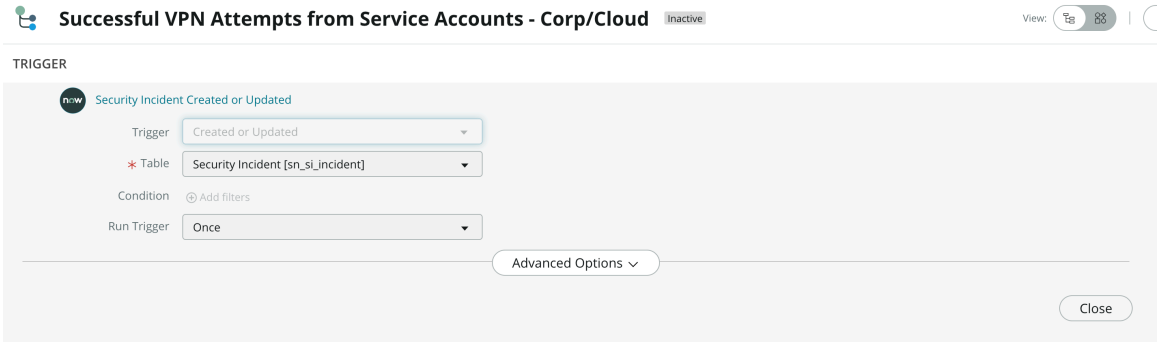
a. Activate the main flow to use the playbook available in the base system.

b. Activate the copied flows after making the required changes.

5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered and associated with the security incident when the security incident is created or updated based on your required conditions. For example, when **Category** is **Insider Breach**.

Successful VPN Attempts from the Service Accounts - Corp/Cloud playbook trigger condition



Use the Successful VPN Attempts from the Service Accounts playbook

Use this playbook to investigate incidents that track successful login attempts from service accounts through VPN. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Successful VPN Attempts from the Service Accounts playbook.

Before you begin

Role required:

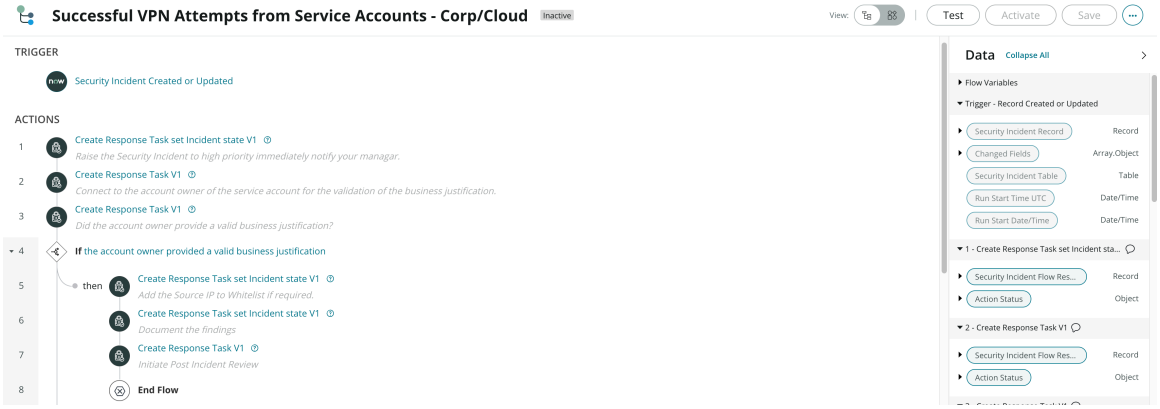
- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, raise the security incident to high priority and immediately notify your manager.
2. In Action 2, reach out to the service account's owner to validate the business justification. You can use the provided email template to contact the service account's owner to validate the business justification.
3. In Action 3, check whether the service account owner provided a valid business justification.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Successful VPN Attempts from the Service Accounts - Corp/Cloud playbook



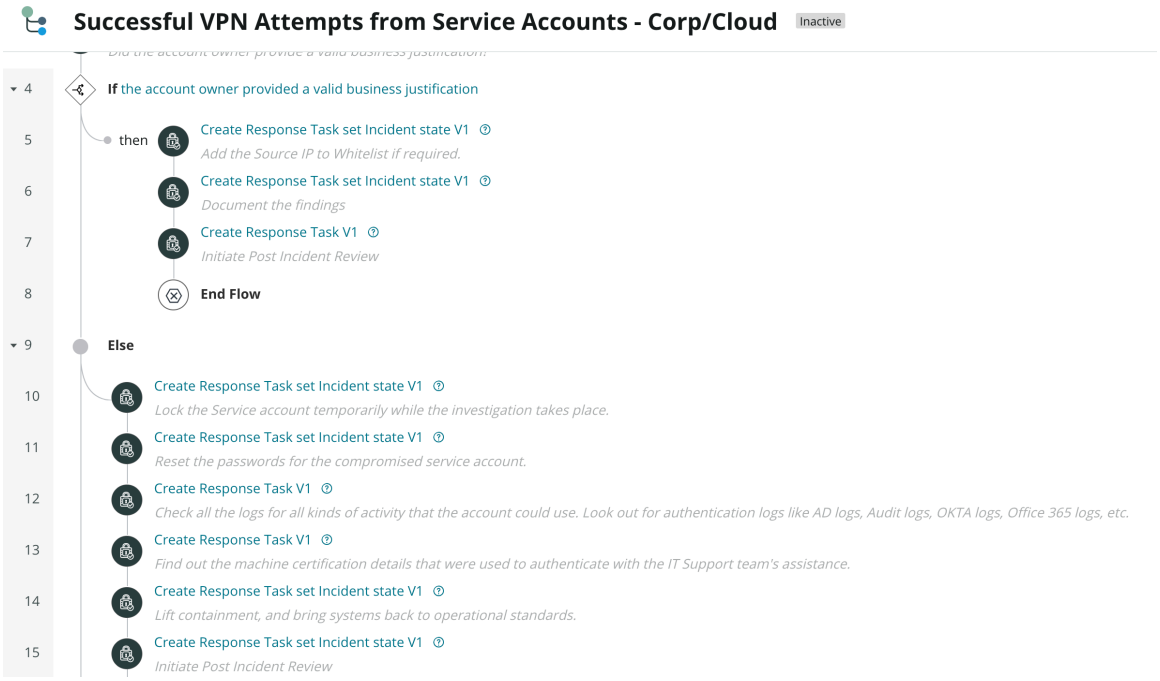
4. In Action 4, if the service account owner provided a valid business justification, perform the following steps:

   a. In Action 5, add the Source IP to the allow list if necessary.

   b. In Action 6, document the findings so far.

   c. In Action 7, initiate a post incident review.
   In Action 8, after the post incident review, the flow ends.

Using the Successful VPN Attempts from the Service Accounts - Corp/Cloud playbook



5. In Action 9, if the service account owner didn't provide a valid business justification, perform the following steps:

   a. In Action 10, temporarily lock the service account while the investigation occurs.

   b. In Action 11, reset the passwords for the compromised service account.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. In Action 12, check the logs for all kinds of activity the account could use.
Look out for authentication logs like Active Directory logs, Audit logs, Okta logs, Office 365 logs, and so on.

d. In Action 13, find the machine certification details used to authenticate with the IT Support team's assistance.

e. In Action 14, lift containment and bring systems back to operational standards.

f. In Action 15, complete the post-incident review before closing the task.

Playbook for Attempted Access to Deactivated Accounts

This playbook triggers when an employee whose account is terminated, disabled, or separated attempts to log in with their credentials. User's identity state in Sail point generally gets updated to disabled on their termination date.

30 days is the ideal time from the termination date for it to get updated to a separated state. You can use business logic in Sail point to delete the RSA accounts and remove the Active Directory (AD) group memberships after 30 days.

Set up the Attempted Access Deactivated Account playbook

Use the following steps to set up the Attempted Access Deactivated Account playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

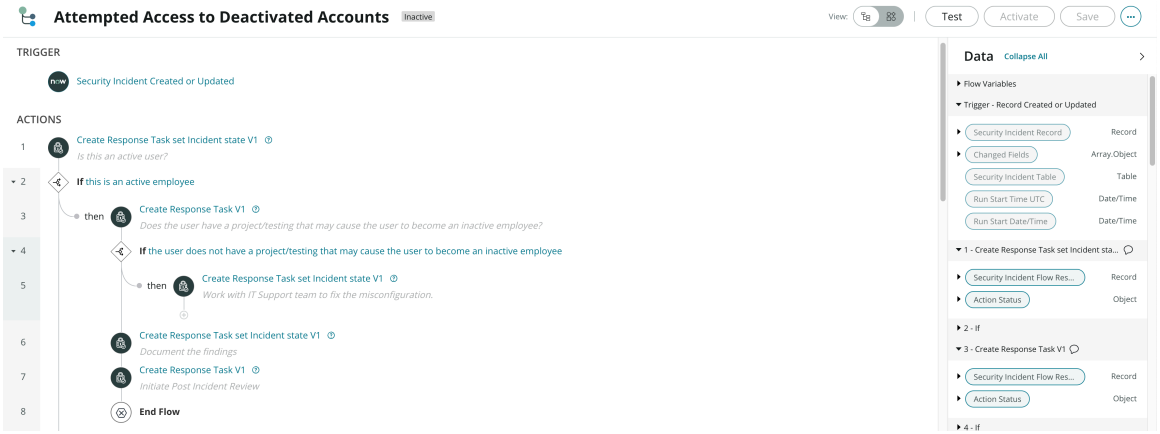
Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Attempted Access Deactivated Account** playbook.
3. **Optional:** Create a copy of the Attempted Access Deactivated Account playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

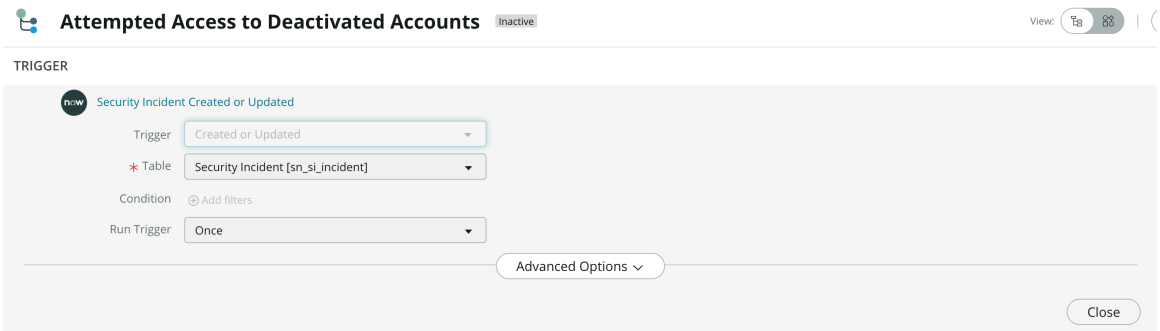
Attempted Access to Deactivated Accounts playbook



4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered when the security incident is created or updated based on your required conditions. For example, when **Category** is **Insider Breach**

Attempted Access to Deactivated Accounts playbook trigger condition



Use the Attempted Access to Deactivated Accounts playbook

Use this playbook when an employee whose account is terminated, disabled, or separated attempts to log in with their credentials. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Attempted Access to Deactivated Accounts playbook.

Before you begin

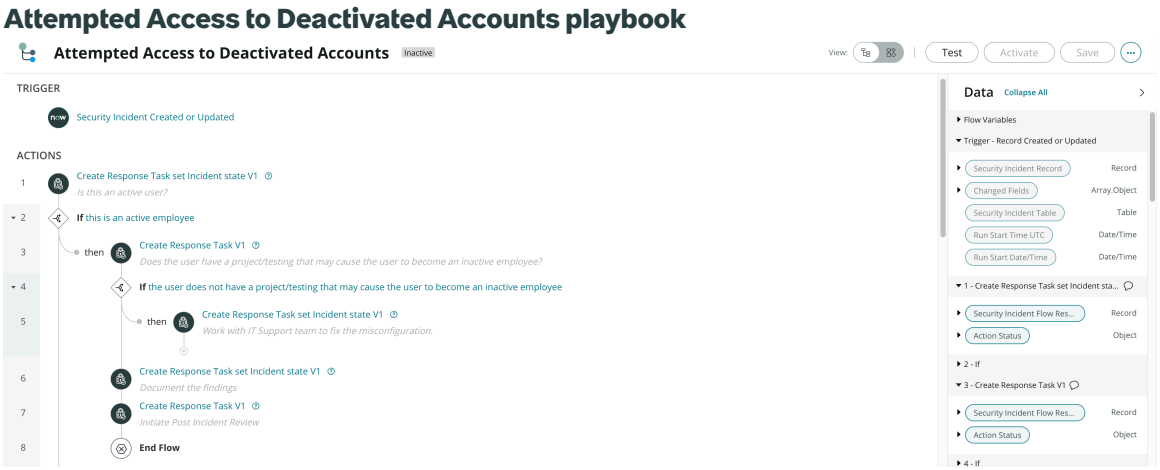
Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, check if the attempted access to the deactivated accounts were made by an active user.
2. In Action 2, check whether the attempted access to the deactivated accounts were made by an active employee.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. If the attempted access to the deactivated accounts were made by an active employee, perform the following steps:

   a. In Action 3, check if the user had a project or test case that caused the user to become an inactive employee.

   b. In Action 4, if the user did not have a project or test case that caused the user to become an inactive employee, then work with the IT Support team to fix the misconfiguration.
   The flow ends.

   c. In Action 5, if the user had a project or test case that caused the user to become an inactive employee, then perform the following steps:

      i. In Action 6, document the findings so far.

      ii. In Action 7, initiate a post incident review.

      In Action 8, after the post incident review, the flow ends.

4. In Action 9, if the attempted access to the deactivated account were not made by an active employee, perform the following steps:

   a. In Action 10, verify if the user had any successful logins.

   b. In Action 11, check when the employee was off-boarded.

   c. In Action 12, investigate the events on Splunk to examine the user's activities during the time period.

   d. In Action 13, based on the investigation so far, determine whether the user exfiltrated any data.

   e. In Action 14, if the user did not exfiltrate any data, perform the following steps:

      i. In Action 15, work with the IT Support team to terminate any active sessions and disable the accounts.

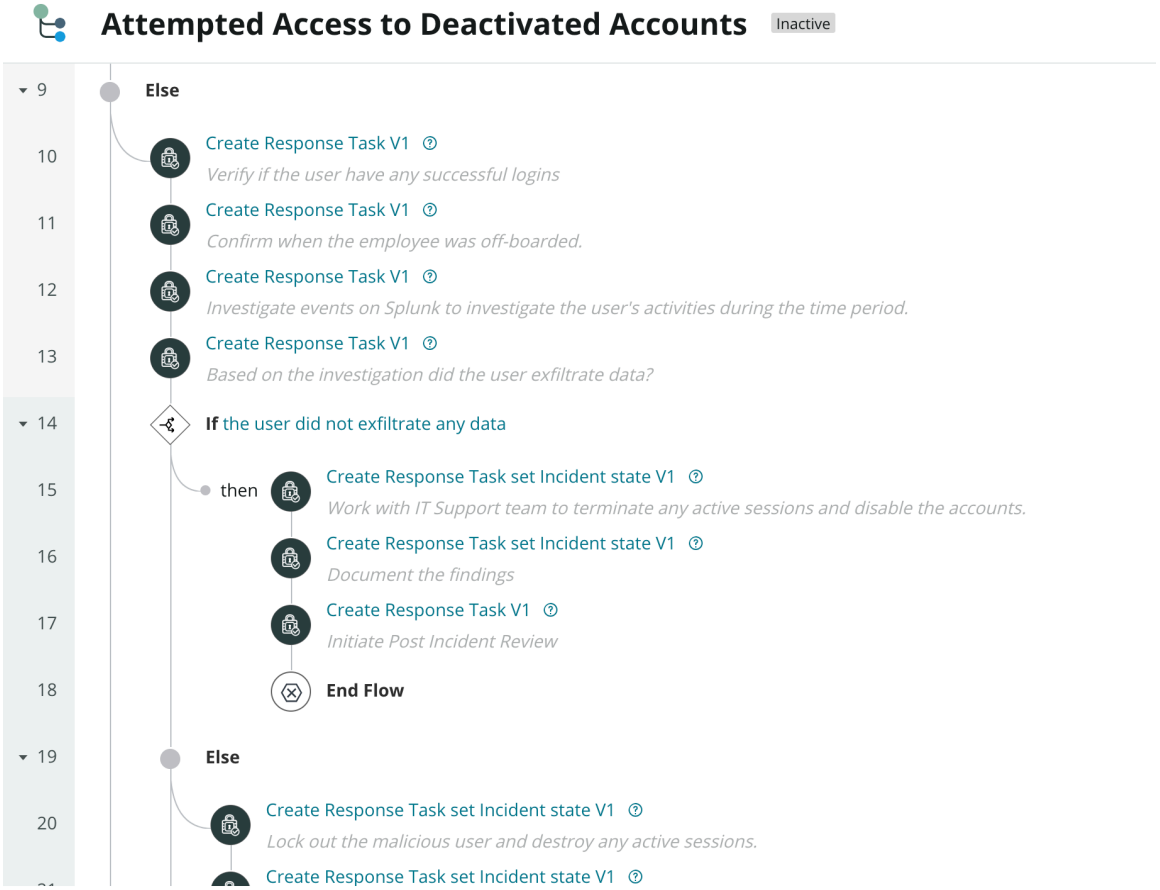
      ii. In Action 16, document the findings so far.

      iii. In Action 17, initiate a post incident review.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In Action 18, after the post incident review, the flow ends.

Using the Attempted Access to Deactivated Accounts playbook



5. In Action 19, if the user exfiltrated any data, perform the following steps:

   a. In Action 20, lock out the malicious user and destroy any active sessions.

   b. In Action 21, work with IT Support team to disable all accounts.

   c. In Action 22, ensure the resources are restored to the normal state and free of any malicious activity.
   You can reimage the resources if necessary.

   d. In Action 23, lift containment and bring systems back to operational standards.

   e. In Action 24, complete the post-incident review before closing the task.

Playbook for T1003 - Defense Evasion - Mimikatz DCShadow

This playbook provides systematic remediation steps to investigate incidents suspected to be caused by Mimikatz DCShadow. DCShadow is a feature in Mimikatz that simulates the behavior of a Domain Controller (a server controlling Active Directory) to inject its own data, bypassing most of the standard security controls (including SIEMs).

Mimikatz DCShadow helps the attacker establish a rogue Domain Controller (DC) that becomes part of the Active Directory (AD). Once registered, it can act as a legitimate DC and cause damage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up the T1003 - Defense Evasion - Mimikatz DCShadow playbook

Use the following steps to set up the T1003 - Defense Evasion - Mimikatz DCShadow playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

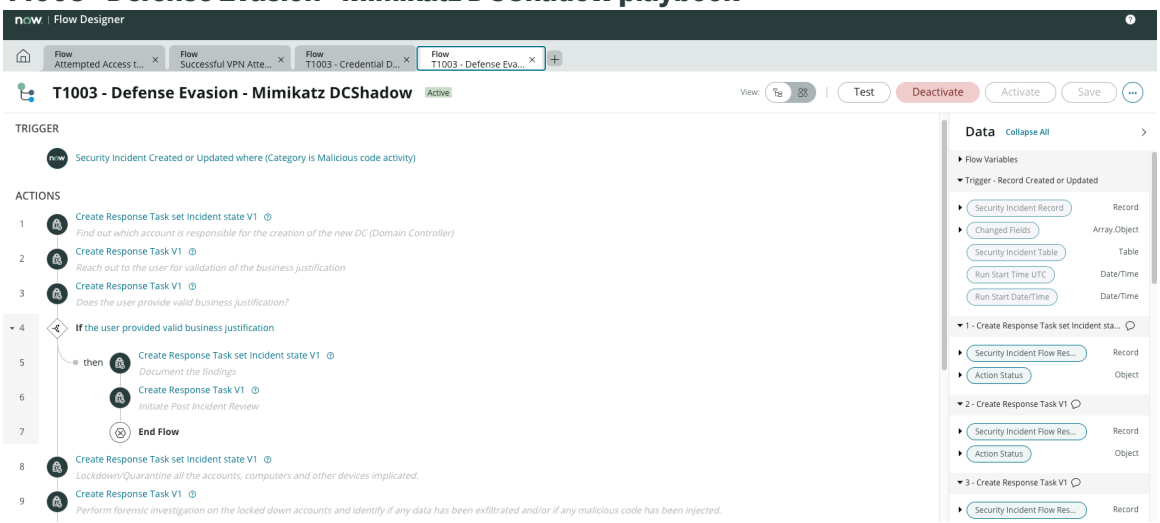
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **T1003 - Defense Evasion - Mimikatz DCShadow** playbook.
3. **Optional:** Create a copy of the T1003 - Defense Evasion - Mimikatz DCShadow playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

   T1003 - Defense Evasion - Mimikatz DCShadow playbook

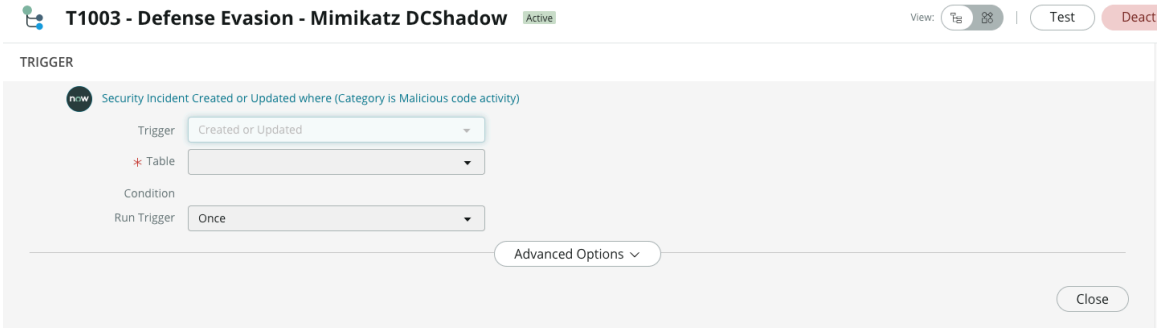
   

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Malicious code activity**.

T1003 - Defense Evasion - Mimikatz DCShadow playbook trigger condition



Use the T1003 - Defense Evasion - Mimikatz DCShadow playbook

Use this playbook to investigate security incidents suspected to be caused by Mimikatz DCShadow. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the T1003 - Defense Evasion - Mimikatz DCShadow playbook.

Before you begin

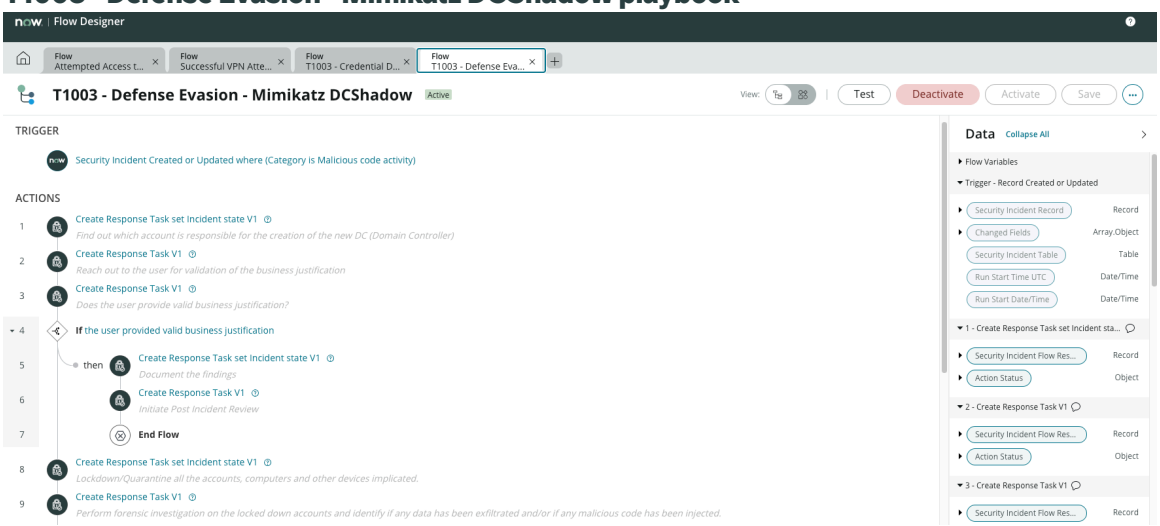
Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, find out which account is responsible for the creation of the new DC (Domain Controller).
2. In Action 2, reach out to the user to validate the business justification.
   You can use the provided email template to contact the user.
3. In Action 3, check whether the user provided a valid business justification.
4. In Action 4, if the user provided a valid business justification, perform the following steps:

T1003 - Defense Evasion - Mimikatz DCShadow playbook



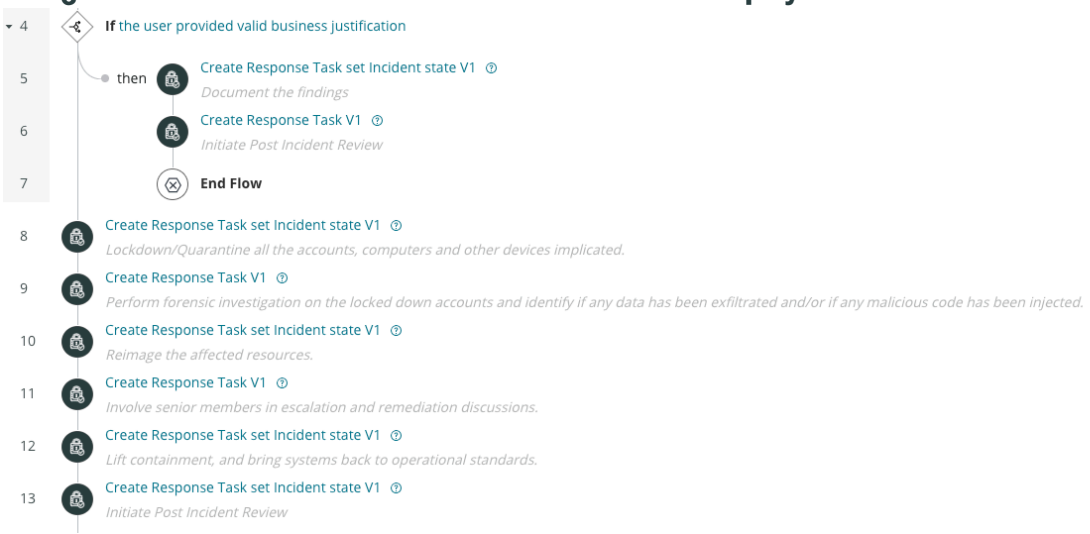
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In Action 5, document the findings so far.

b. In Action 6, initiate a post incident review.
In Action 7, after the post incident review, the flow ends.

5. In Action 8, if the user didn't provide a valid business justification, perform the following steps:

Using the T1003 - Defense Evasion - Mimikatz DCShadow playbook



a. In Action 9, lock down or quarantine all the accounts, computers, and other devices involved.

b. In Action 10, perform a forensic investigation on the locked-down accounts and identify if any data has been exfiltrated or any malicious code has been injected.

c. In Action 11, reimage the affected resources.

d. In Action 12, lift containment and bring systems back to operational standards.

e. In Action 13, complete the post-incident review before closing the task.

Playbook for T1003 - Credential Dumping - Mimikatz DCSync

This playbook provides systematic remediation steps to investigate incidents suspected to be caused by Mimikatz DCSync. This playbook triggers when one of the Mimikatz functions (`lsadump::dcsync`) is used. The function is typically used on attacked Domain Controllers (DC).

Mimikatz is a popular hacking tool that enables users to issue commands that help retrieve confidential data from the attacked system. The confidential data includes passwords, their hashes, and others.

Note: This is a high-fidelity alert, which is assumed to be rarely triggered. When it triggers, you should notify a senior team member or Manager immediately.

Set up the T1003 - Credential Dumping - Mimikatz DCsync playbook

Use the following steps to set up the T1003 - Credential Dumping - Mimikatz DCsync playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

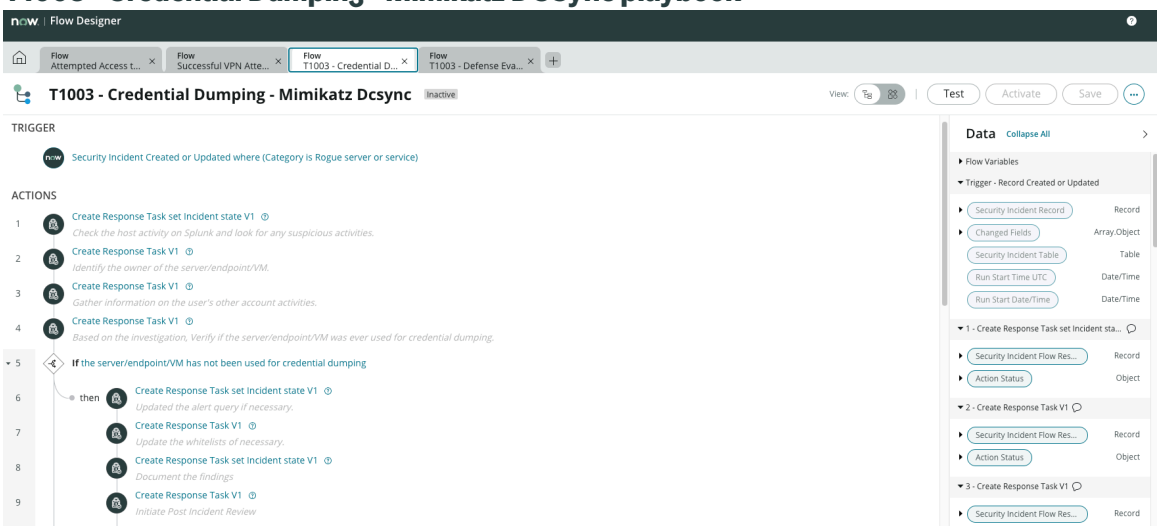
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **T1003 - Credential Dumping - Mimikatz DCsync** playbook.
3. **Optional:** Create a copy of the T1003 - Credential Dumping - Mimikatz DCsync playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

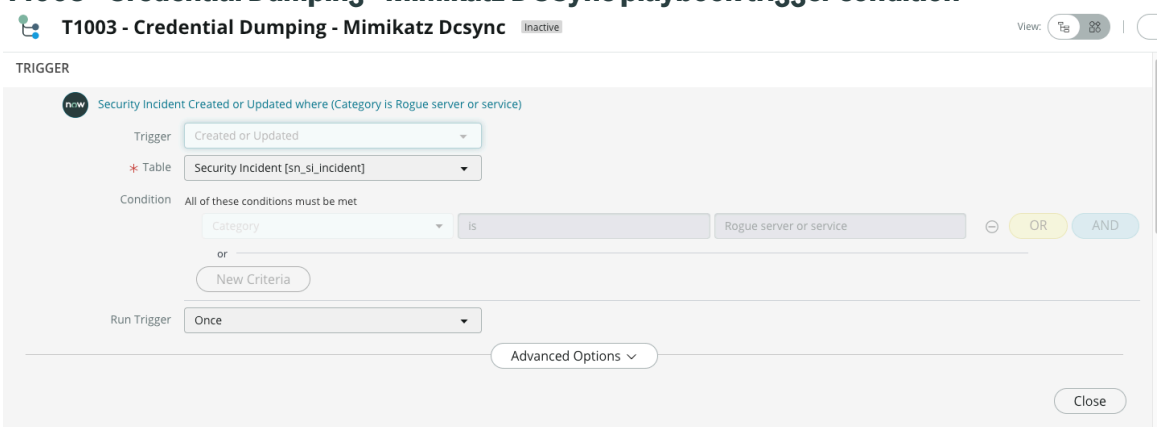
   T1003 - Credential Dumping - Mimikatz DCSync playbook

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

   This playbook is triggered and associated with the security incident when the **Category** is **Rogue server or service**.

   T1003 - Credential Dumping - Mimikatz DCSync playbook trigger condition

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the T1003 - Credential Dumping - Mimikatz DCsync playbook

Use this playbook to investigate incidents suspected to be caused by Mimikatz DCSync. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the T1003 - Credential Dumping - Mimikatz DCsync playbook.

Before you begin

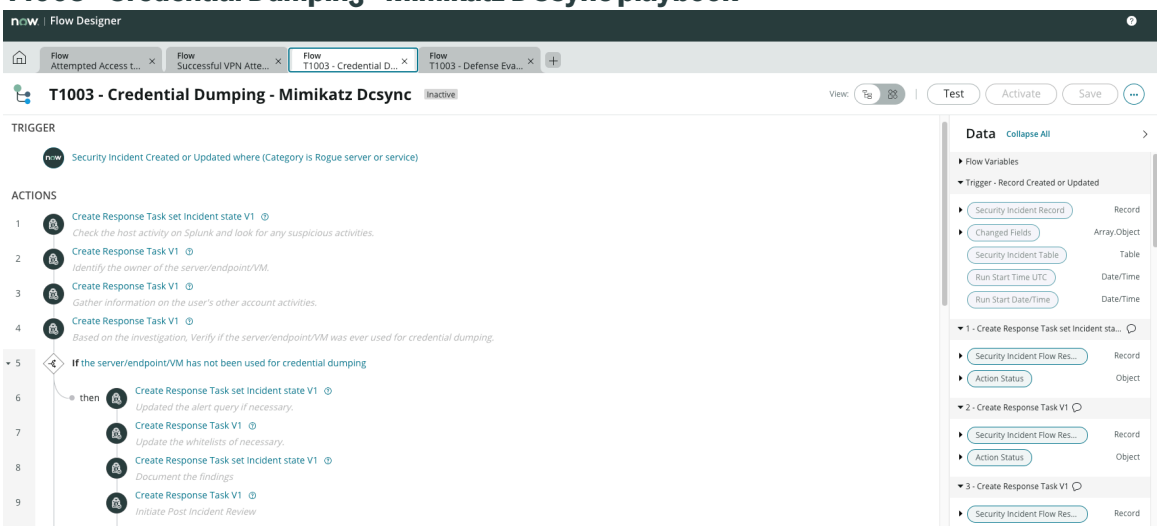
Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, check the host activity on Splunk and look for any suspicious activities.
2. In Action 2, identify the owner of the server/endpoint/VM.
   If the user is online, run the CrowdStrike EDR to gather a better scope of the system's activities.
3. In Action 3, gather information on the user's other account activities.
4. In Action 4, based on the investigation, verify if the server/endpoint/VM was ever used for credential dumping.
5. In Action 5, if the server/endpoint/VM wasn't used for credential dumping, perform the following actions:

T1003 - Credential Dumping - Mimikatz DCsync playbook



   a. In Action 6, update the alert query if necessary.

   b. In Action 7, update the allow list if necessary.

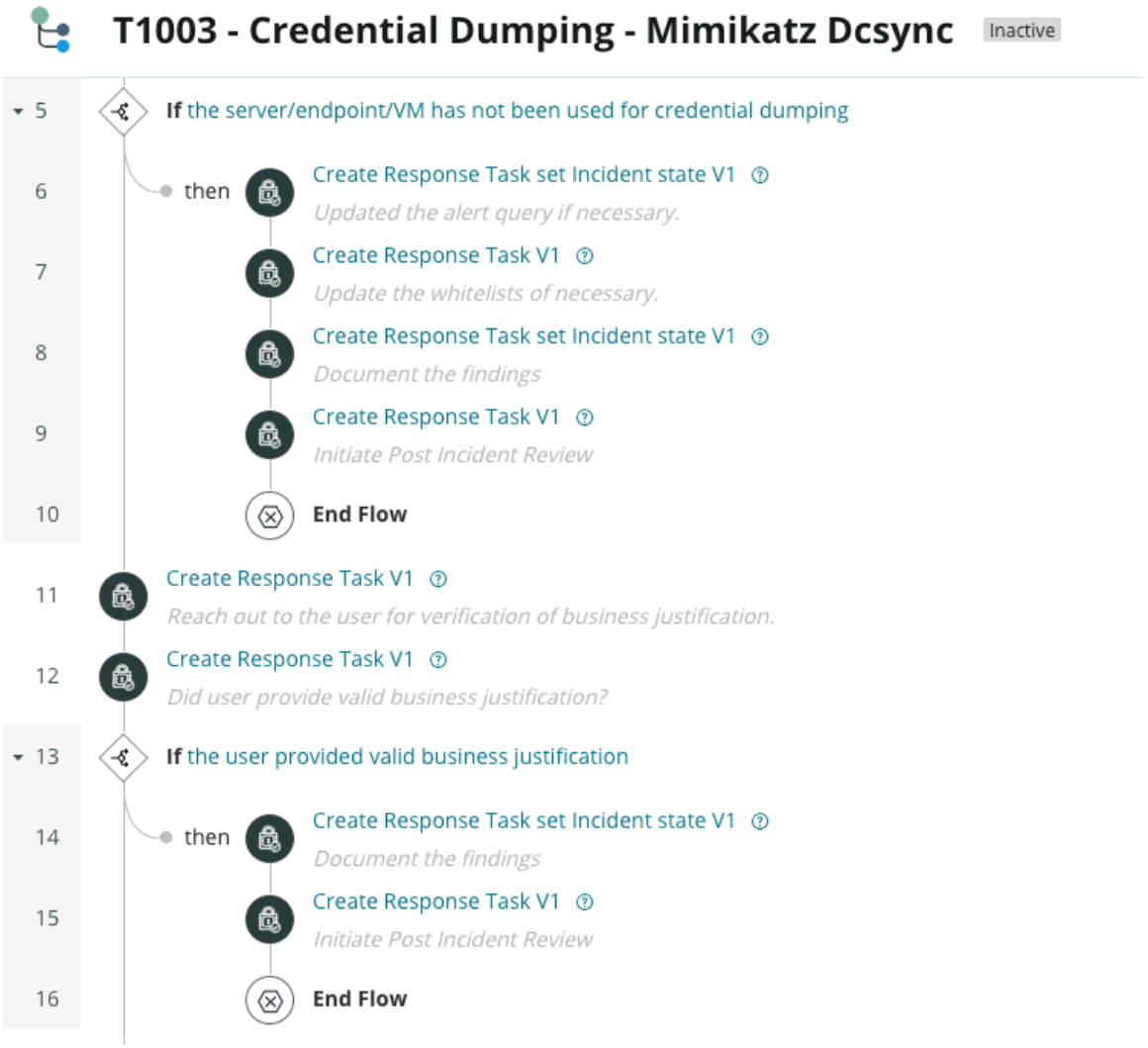
   c. In Action 8, document the findings so far.

   d. In Action 9, initiate a post incident review.
      In Action 10, the flow ends.

6. If the server/endpoint/VM was used for credential dumping, then in Action 11, reach out the user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the T1003 - Credential Dumping - Mimikatz DCsync playbook



7. In Action 12, reach out to the user to validate the business justification.
8. In Action 13, if the user provided a valid business justification, perform the following Actions:

   a. In Action 14, document the findings so far.

   b. In Action 15, initiate a post incident review.
   In Action 16, the flow ends.

9. If the user didn't provide a valid business justification, then in Action 17, quarantine the system.
10. In Action 18, remove any unwanted files that may have been created or deleted by the rogue accounts.
11. In Action 19, lift containment and bring systems back to operational standards.
12. In Action 20, complete the post-incident review before closing the task.

Playbook for Okta User Login Failures from Multiple IPs

This playbook provides systematic remediation steps to investigate incidents for user login failures on Okta.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Okta User Login Failures from Multiple IPs playbook provides instructions on analyzing the alert when ServiceNow account failures are observed on Okta from Multiple Non-ServiceNow IPs. The alert related to this playbook checks the Okta logs. It triggers an alert when login failure occurs for ServiceNow user IDs from more than three non-ServiceNow IP ranges in a 1-hour duration.

Set up the Okta User Login Failures from Multiple IPs playbook

Use the following steps to set up the Okta User Login Failures from Multiple IPs playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

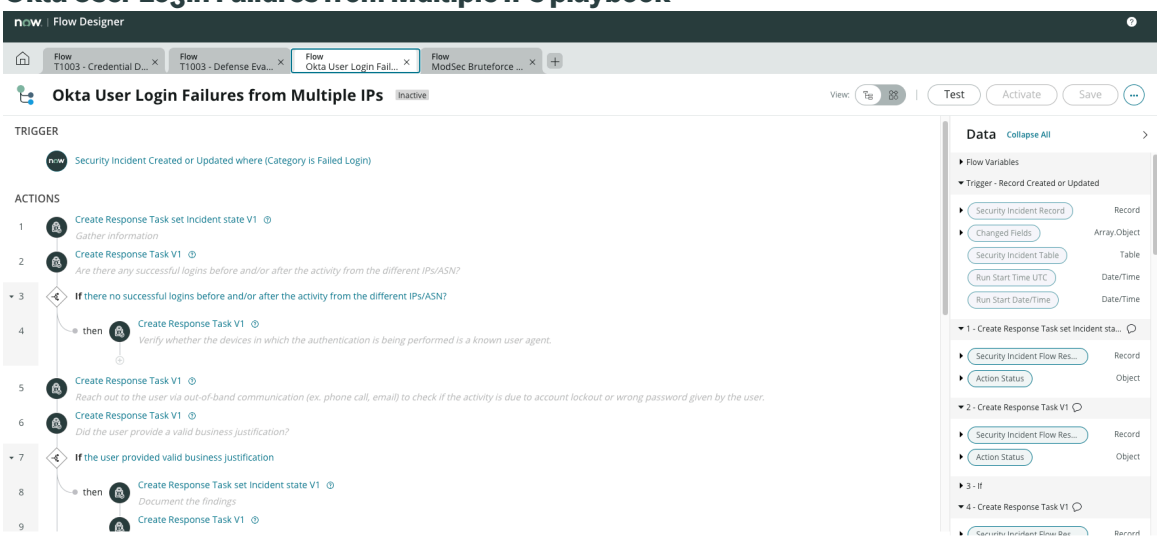
Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **Okta User Login Failures from Multiple IPs** playbook.
3. **Optional:** Create a copy of the Okta User Login Failures from Multiple IPs playbook flow and make the necessary modifications.

   (Optional) To create a copy of the playbook's flow, select the  icon and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

   Okta User Login Failures from Multiple IPs playbook

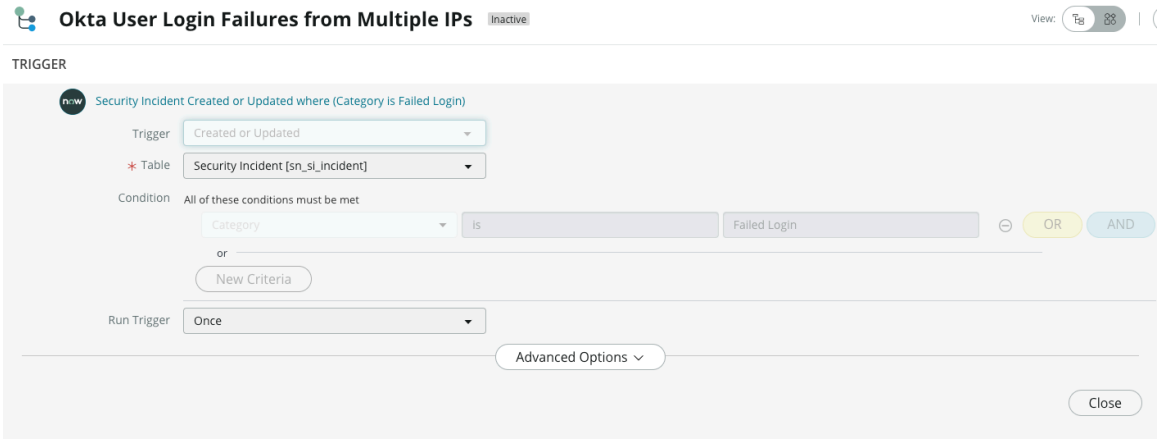
   

4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This playbook is triggered and associated with the security incident when the **Category** is **Failed Login**.

Okta User Login Failures from Multiple IPs playbook trigger condition



Use the Okta User Login Failures from Multiple IPs playbook

Use this playbook to investigate security incidents for user login failures on Okta. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the Okta User Login Failures from Multiple IPs playbook.

Before you begin

Role required:

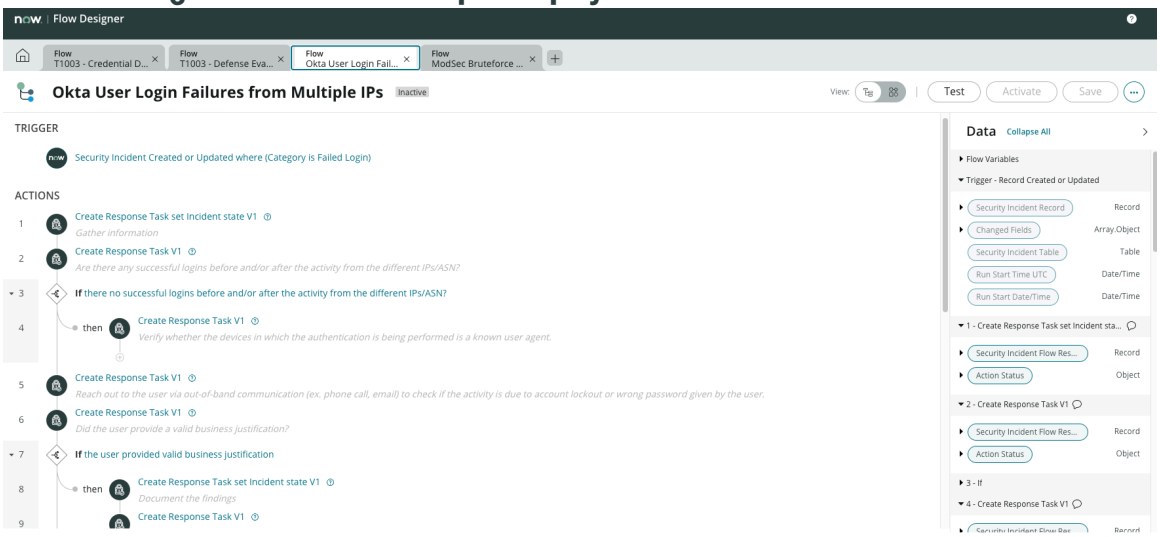
- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1, perform the following tasks:
   - Identify the user account that is being targeted.
   - Verify the IP subnet and check if they all belong to the same Autonomous System Number (ASN) owner.
2. In Action 2, check whether there were any successful logins before or after the activity from the different IPs/ASNs.
3. In Action 3, if there were no successful logins before or after the activity from the different IPs/ASNs, then in Action 4, verify whether the devices in which the authentication is being performed are known user agents.
   If the devices are authenticated by known user agents, then the flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Okta User Login Failures from Multiple IPs playbook



4. In Action 5, based on the investigation, reach out to the user through out-of-band communication (For example, phone call or email) to check if the activity is due to account lockout or a wrong password provided by the user.
5. In Action 6, check whether the user provided a valid business justification.
6. In Action 7, if the user provided a valid business justification, perform the following tasks.

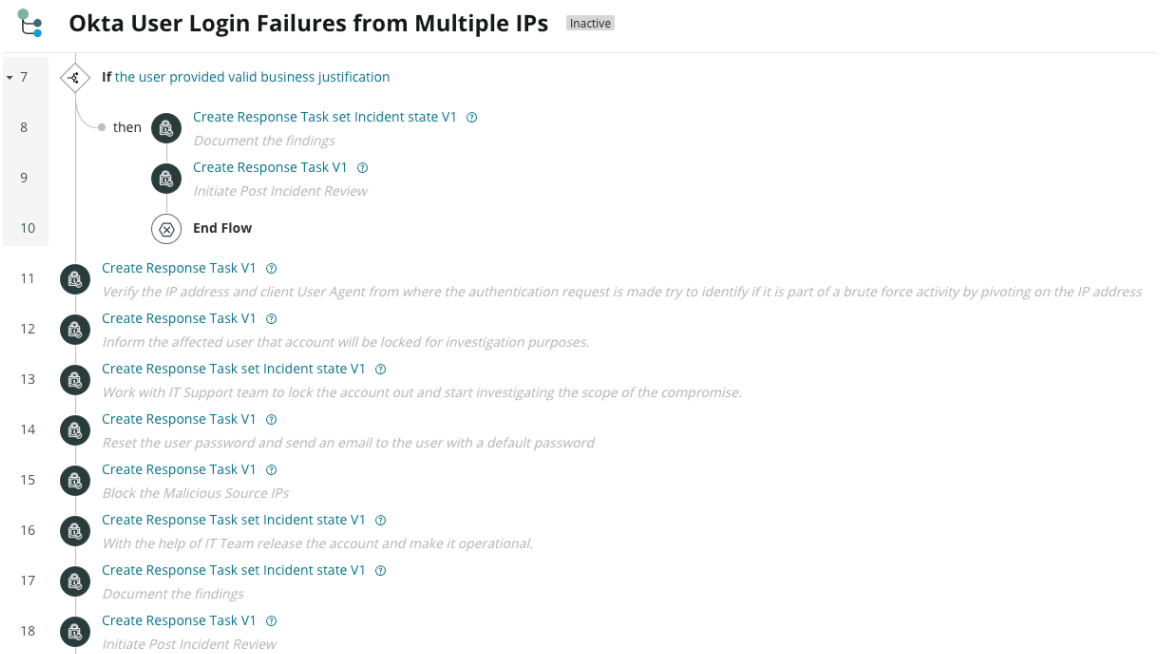
    a. In Action 8, create a response task to document the findings so far.

    b. In Action 9, create a response to initiate a post incident review.
    In Action 10, the flow ends.

7. In Action 11, verify the IP address and client user agent from where the authentication request is made and try to identify if it is part of a brute force activity by pivoting on the IP address.
8. In Action 12, inform the affected user that account will be locked for investigation purposes. You can use the provided email template to inform the affected user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the Okta User Login Failures from Multiple IPs playbook



9. In Action 13, work with the IT Support team to lock the account out and start investigating the scope of the compromise.
10. In Action 14, reset the user password and send an email to the user with the default password.
11. In Action 15, block the malicious Source IPs.
12. In Action 16, get help from the IT Support Team to the release the account and bring it back to operational standards.
13. In Action 17, document the findings so far.
14. In Action 18, complete the post-incident review before closing the task.

Playbook for ModSec Brute force by IP Burst

This playbook provides systematic remediation steps to investigate incidents of brute force attempts on the login pages from multiple IPs detected by ModSec. The event conditions could be set at the ModSec policy itself and will raise an alert at Splunk when the event is created at ModSec.

This playbook helps in detecting abnormal traffic counts on the login page. In this example, two successive bursts of more than 50 hits/minute should be from an IP to the login page, which indicates a brute-force attempt to log in.

Set up the ModSec Brute force by IP Burst playbook

Use the following steps to set up the ModSec Brute force by IP Burst playbook.

Before you begin

Role required:

- sn_si.admin
- flow_designer

Make sure you have installed Security Operations Spoke (*sn_sec_spoke*).

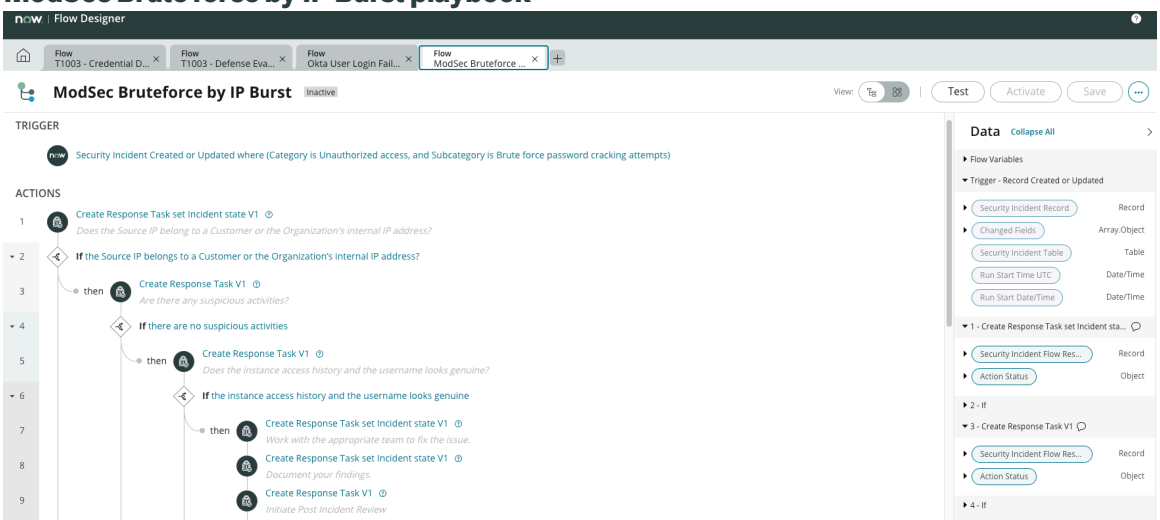
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Login as a user with sn_si.user and flow_designer roles.
2. Navigate to **All** > **Flow Designer** and select the **ModSec Bruteforce by IP Burst** playbook.
3. **Optional:** Create a copy of the ModSec Bruteforce by IP Burst playbook flow and make the necessary modifications.

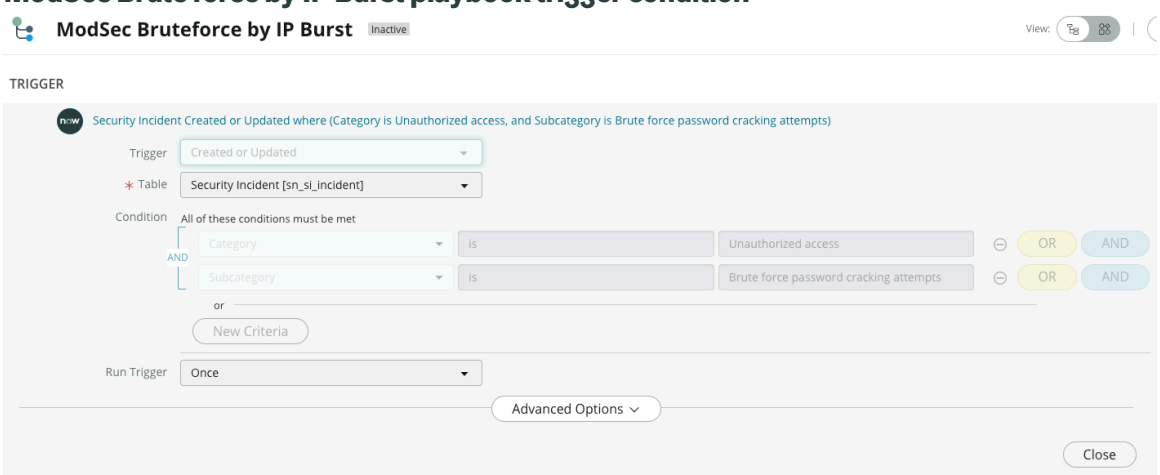
   (Optional) To create a copy of the playbook's flow, select the more actions menu icon ( ) and select **Copy flow**. Perform this step only if you plan to customize or make specific changes to the flow.

ModSec Brute force by IP Burst playbook



4. Activate the playbooks.
   a. Activate the main flow to use the playbook available in the base system.
   b. Activate the copied flows after making the required changes.
5. Set a **Trigger Condition** for the playbook.
   This playbook is triggered and associated with the security incident when the following conditions are met:
   - **Category** is **Unauthorized access**.
   - **Subcategory** is **Brute force password cracking attempts**.

ModSec Brute force by IP Burst playbook trigger condition



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the ModSec Brute force by IP Burst playbook

Use this playbook to investigate incidents of brute force attempts on the login pages from multiple IPs detected by ModSec. The following steps give you a walkthrough of the actions, tasks, and subflows that are available in the ModSec Brute force by IP Burst playbook.

Before you begin

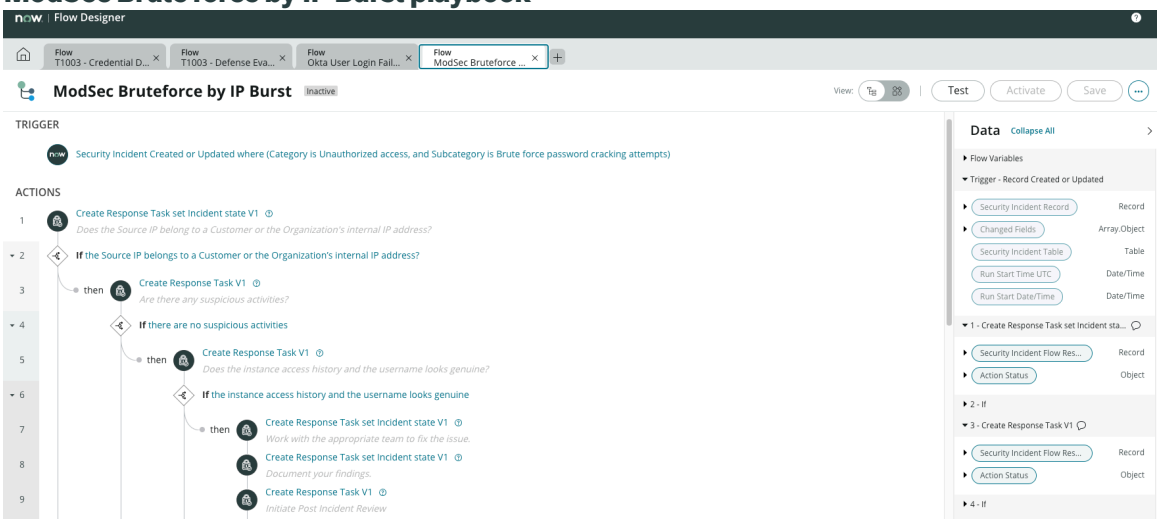
Role required:

- sn_si.admin
- flow_designer

Procedure

1. When the playbook is triggered and starts executing, in Action 1 check whether the Source IP belongs to a customer or to the organization's internal IP address.
2. In Action 2, if the Source IP belongs to a customer or to the organization's internal IP address, perform the following steps:

ModSec Brute force by IP Burst playbook



   a. In Action 3, check whether there were any suspicious activities.

      - Check the activity from the source IP in the last few days. If the IP had negligible traffic, it indicates an actual attack.
      - Check the spraying usernames. For example, check if the usernames are arranged in an alphabetic order.
      - Look for generic account names involved. For example, admin, sysadmin, root, administrator, and other application account names.

      If there are no suspicious activities, then the flow ends.

   b. In Action 4, if there were any suspicious activities, then in Action 5, check if the instance access history and the username look genuine.

      Check the *Appnode* logs for any indications of failure. There could be SAML, SSO, or LDAP fail events, which could be due to an operational issue.

      If the instance access history and the username don't look genuine, then the flow ends.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. In Action 6, if the instance access history and the username look genuine, then perform the following steps:

i. In Action 7, coordinate with the appropriate team to fix the issue.

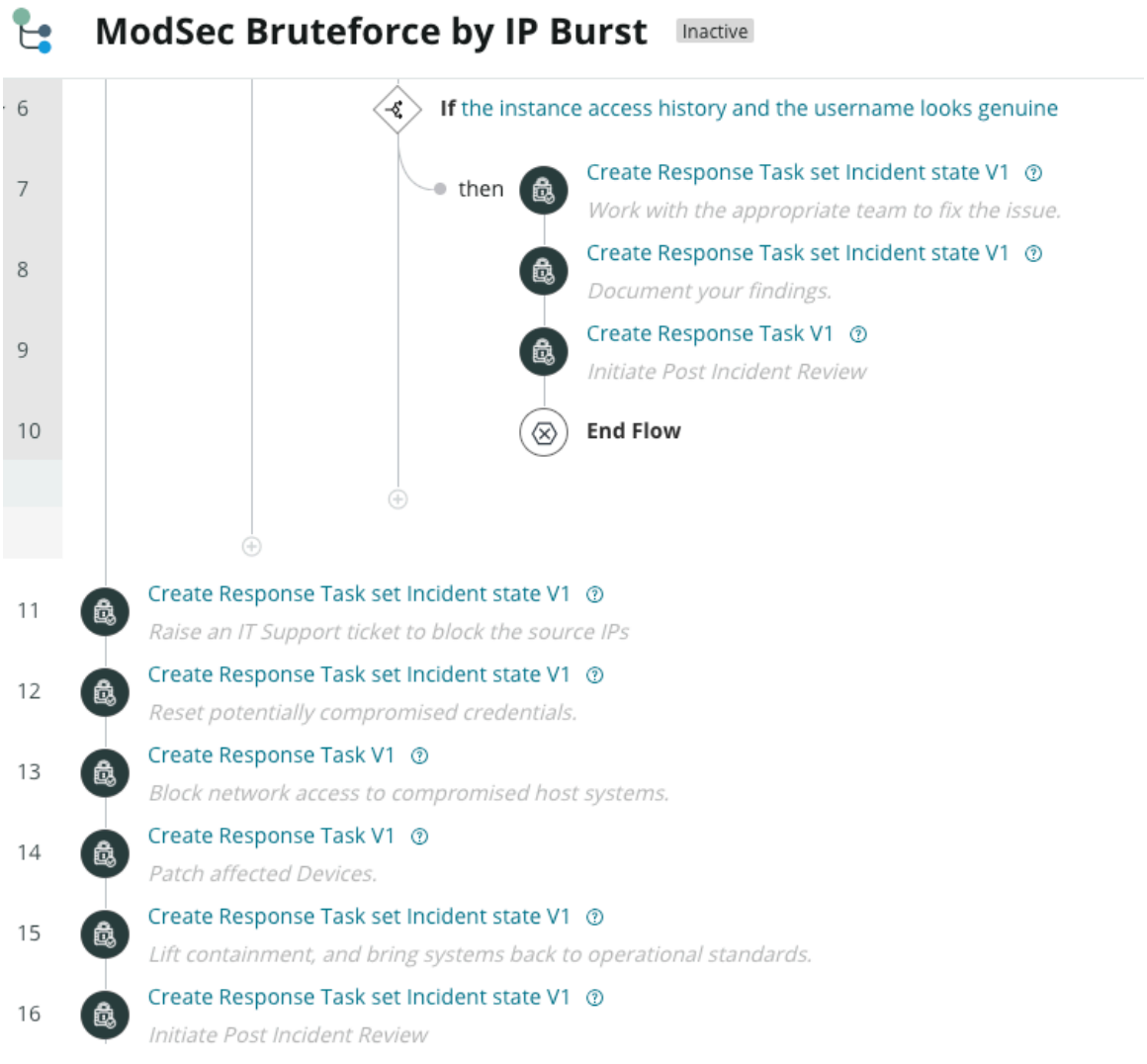
ii. In Action 8, document the findings so far.

iii. In Action 9, complete the post-incident review before closing the task.

In Action 10, the flow ends.

3. If the Source IP doesn't belong to a customer or the organization's internal IP address, then in Action 11, raise an IT Support ticket to block the source IPs.

Using the ModSec Brute force by IP Burst playbook



4. In Action 12, reset the potentially compromised credentials.
5. In Action 13, block the network access to compromised host systems.
6. In Action 14, patch the affected devices.
7. In Action 15, lift the containment and bring the systems back to operational standards.
8. In Action 16, complete the post-incident review before closing the task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response playbook actions

This section describes the actions provided in the Flow Designer action library.

Action Name	Description	Example scenario	
Add a security tag to the security incident	Use this action to add a security tag automatically using flow designer logic.	If the flow detects an IOC, the **IOC Detected** tag can be automatically added using this action. **Flow**:	• Input: security incident, security tag • Output: not applicable
Add observables to the security incident	Use this action to add observables to a selected security incident. • By default, the list of observables are separated by the comma (,) delimiter but this can be modified. You can specify another single special character as a delimiter. While adding observables, the type (URL, IP address, hash) is automatically set. • When the observables are added to the security incident, the type (URL, IP address, hash) is automatically set. • When the observables are being added, the Filter Allowed list Observables option identifies allowed list observables and does not add them to the security incident's observables related list. An automated system activity (response) is added to indicate that		• Input: ◦ security incident ◦ observables ◦ delimiter ◦ filter allowed list observables and post activity note • Output: not applicable

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action Name	Description	Example scenario	
	these observables have been removed.		

Get affected users (Related Lists) from multiple security incidents V1	Retrieves all the affected users listed in the Affected Users related list for the specified security incidents.	You may have parent security incidents with multiple child security incidents. Use this action to roll-up affected users from all the child security incidents to the corresponding parent security incidents. Only unique affected users are rolled-up and all duplicates are eliminated.	• Input: security incidents
			• Output:
			  ○ affected user
			  ○ count

Get affected users from multiple security incidents	Retrieves the primary affected user for the specified security incident. It does not include the affected users from the Affected User related list.	• While investigating a phishing security incident, send an email to the primary affected users (who reported the phishing incident) to confirm if any of the users clicked on the malicious links in the phishing email.
		• Update the parent security incident severity or risk score based on the count of primary affected users.
			• Input: security incidents
			• Output:
			  ○ affected users
			  ○ count

Get affected users (related list) from a security incident	Retrieves all the affected users listed in the Affected Users related list for a specified security incident.		• Input: security incidents
			• Output:
			  ○ affected users
			  ○ count

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action Name	Description	Example scenario	

Add affected users to security incident	Adds all affected users to a security incident.	Suppose you have a parent security incident with multiple child security incidents. You can use this action to roll-up affected users from all the child security incidents to the corresponding parent security incident. Only unique affected users are rolled-up and all duplicates are eliminated.	• Input:
			  ○ security incident
			  ○ user
			• Output: not applicable

Get configuration items of the affected users	Retrieves the configuration items (CIs) of all affected users.	In phishing or malware scenarios, you can use this action to update the Affected Configuration Items (CI) related list and investigate the CIs. You can then update the severity or risk score of the security incident based on the number of identified CIs.	• Input: users
			• Output:
			  ○ configuration items
			  ○ count

Get all child security incidents for a security incident	Retrieves all child security incidents related to a specific parent security incident.	Example scenario: Use this action to:
		• Update the status of the child security incidents when their corresponding parent security incidents status get updated.
		• Update the severity or risk score of the security incident automatically based on the number of child security incidents.
			• Input:
			  ○ security incident
			  ○ incident state
			• Output:
			  ○ child security incident
			  ○ count

Get configuration items for the observables (type IP address)	Retrieves all configuration items (CIs) for observables of type IP address.	An IP address observable can be associated with a configuration item. For example, the IP address of a server.	• Input: observable ip address • Output:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action Name	Description	Example scenario	
		If you use this action, you can retrieve information for the server.	○ configuration items ○ count
Is observable malicious	Confirms the presence of one or more malicious observables in a set of observables.	After the threat lookup has been completed and you have identified the presence of malicious observables, you can increase the severity or risk score of a security incident.	• Input: security incident • Output: malicious (true/false)
Send email to confirm user interaction	Sends email in response to a user response.	If a user tries multiple times to login to an application and fails, it results in a failed login scenario. In this case, an email is sent to the user to confirm whether the user attempted to login or not. Depending on the user response (Yes or No), different actions can be taken. **Flow**: Failed Login Manual playbook	
Filter out allowed list observables	Use this action to allow list observables from a given set of observables.	You can identify certain observables that can be ignored from a set of observables. These observables will not taken into account while resolving the security incident.	• Input: security incident • Output: ○ allowed list observables ○ count
Reset password for affected users	Use this action to reset password for affected users.	If a user account has been hacked or a user requests a password to be reset, an email is sent to the user to reset the password. **Flow**: Failed Login Manual playbook.	
Get user group for affected user	Retrieves the user group details of affected users.	In an organization, if two or more users report phishing emails, you can find	• Input: user • Output:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action Name	Description	Example scenario	
		out the group they belong to and identify if more users have been affected	○ user groups ○ count

Visual representation of Security Incident Response reporting

Security managers can use the high-level graphical interfaces such as maps, treemaps to pinpoint areas of concern.

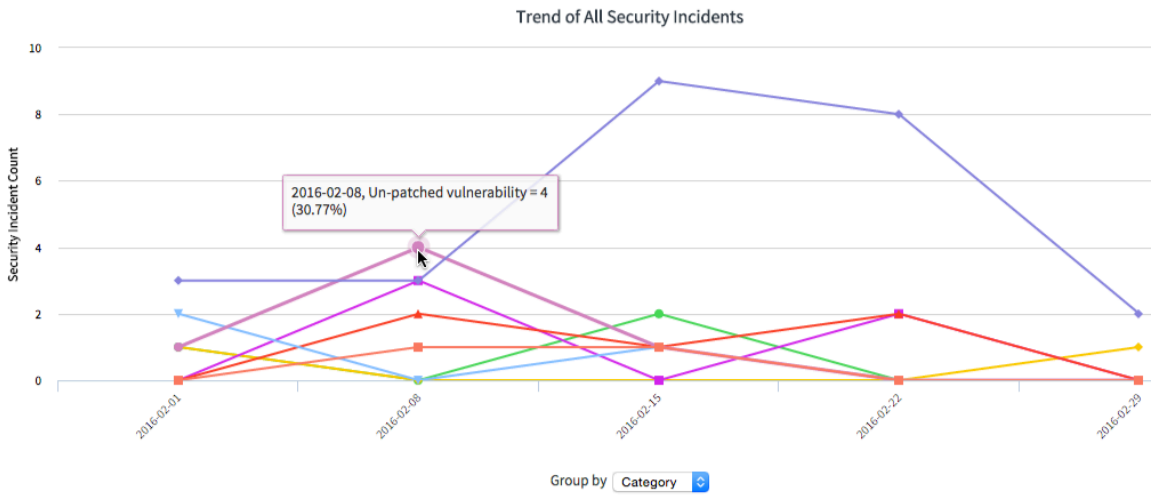
To view Security Incident Response Explorer dashboard in Security Incident Response Workspace in detail, see Viewing SIR Workspace Dashboards.

Security Incident Response Overview dashboard

The Security Incident Response Overview dashboard provides an executive view into security incident activity, providing trends and reports, and drill-downs into specific data.

The Overview module displays security incident information that is tailored to the role of the user. You can point to any part of a chart (bar, pie, data point, heatmap, and so on) to view general data specific to that part. See the following image. If you click any part of a report, a list opens to provide detailed information.

Trend of All Security Incidents



Security Incident Manager Overview

Users with the Security Incident Administrator and Security Incident Manager roles view the Security Incident Manager Overview. It contains the following reports in the base system.

Security Incident Manager Overview reports

Name	Visual	Description
Team Critical Security Incidents	Single score	The number of critical security incidents assigned to the team.
Team High Security Incidents	Single score	The number of high security incidents assigned to the team.
SLAs expiring within 24 hours	Single score	The number of SLAs that expire within the next 24 hours.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Manager Overview reports (continued)

Name	Visual	Description
Risk vs Severity	Heatmap	The distribution of security incidents assigned to the team by risk and severity.
Security Incidents by CI Class, last 3 months	Bar chart	The count of security incidents assigned to the team by configuration item class.
Trend of All Security Incidents	Trend	Plots the count of the number of security incidents received by category or priority.
Unauthorized Access Security Incidents	Bar chart	Displays the types of security incident categories received over time.
Average Time to Contain	Single score	The average time it takes to contain all security incidents.
Average Time to Contain Critical	Single score	The average time it takes to contain all critical security incidents.
Average Time to Identity	Single score	The average time it takes to identify all security incidents.

Security Analyst Overview

Users with the Security Incident Analyst role view the Security Analyst Overview. It contains the following reports in the base system.

Security Analyst Overview reports

Name	Visual	Description
My Critical Priority Work	Single score	The number of critical security incidents assigned to me.
My High Priority Work	Single score	The number of high security incidents assigned to me.
My SLAs expiring within 24 hours	Single score	The number of SLAs assigned to me that expire within the next 24 hours.
Security Incidents assigned to me	Bar chart	Security Incidents assigned to me by incident state or category.
Work assigned to me by Type	Bar chart	Security tasks (incidents, tasks, or requests) assigned to me by type or priority.
Security Incidents, Requests, Tasks assigned to me	List	A list of all security incidents, security requests, and tasks assigned to me.
Security Incident Location	Map	Regional location of the security incidents.
Count	Map	Number of security incidents per region.
Min/Max Count	Color Spectrum Bar	The minimum and maximum numbers of security incidents per region represented by a color spectrum bar.
Percentage of Count	Map	Percentage of the total incident count per region.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident CISO Overview with Security Incident Analytics activated

When the Security Incident Analytics plugin is activated, users with the Security Incident CISO and System Administrator roles view the Security Incident CISO Overview. The following CISO reports are provided in the base system.

Security Incident CISO Overview reports (with Security Incident Analytics activated)

Name	Visual	Description
New Security Incidents This Week	Single score	The number of new security incidents received in the current week.
Security Incidents Closed This Week	Single score	The number of security incidents closed in the current week.
New Security Incidents (Running 7 Days)	Single score	The number of security incidents opened within the last 7 days.
Security Incidents Closed (Running 7 Days)	Single score	The number of security incidents closed within the last 7 days.
Daily New Security Incidents vs Closed Security Incidents	Trend	New and Closed security incident counts over time by day.
Weekly New Security Incidents vs Closed Security Incidents	Trend	New and Closed security incidents over time by week.
Security Incident Close Code	Trend	Full count of closure codes over time.
Security Incident Business Impact	Treemap	Business services with security incidents with available groupings by business criticality.
Average Time to Contain (Weekly)	Trend	The 7-day average time it takes to contain a security incident over time.
Average Time to Eradicate (Weekly)	Trend	The 7-day average time it takes to eradicate a security incident over time.
Average Time to Identity (Weekly)	Trend	The 7-day average time it takes to identify a security incident over time.
Security Incident Location	Map	Regional location of the security incidents.
Count	Map	Number of security incidents per region.
Min/Max Count	Color Spectrum Bar	The minimum and maximum numbers of security incidents per region represented by a color spectrum bar.
Percentage of Count	Map	Percentage of the total incident count per region.

Security Incident CISO Overview without Security Incident Analytics activated

When the Security Incident Analytics plugin is not activated, users with the Security Incident CISO and System Administrator roles view the Security Incident CISO Reporting Overview. The following CISO reports are provided in the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident CISO Overview reports (without Security Incident Analytics activated)

Name	Visual	Description
New Security Incidents This Week	Single score	The number of new security incidents opened in the current week.
Security Incidents Closed This Week	Single score	The number of security incidents closed in the current week.
New Security Incidents (Running 7 Days)	Single score	The number of security incidents opened within the last 7 days.
Security Incidents Closed (Running 7 Days)	Single score	The number of security incidents closed within the last 7 days.
Weekly New Security Incidents	Trend	The new security incidents opened on a weekly basis.
Weekly Closed Security Incidents	Trend	The security incidents closed on a weekly basis.
Security Incident Close Codes	Trend	Security incident close codes over time.
Business Services with Security Incidents - Business Impact	Treemap	Business services with security incidents with available groupings by business criticality.
Average Time to Contain	Single score	The average time it takes to contain all security incidents.
Average Time to Contain Critical	Single score	The average time it takes to contain all critical security incidents.
Average Time to Identity	Single score	The average time it takes to identify all security incidents.

Note: The Security Incident Response base system includes Performance Analytics Solutions for displaying preconfigured best practice dashboards. The dashboards present important metrics for analyzing your Security Incident Response process, such as new security incidents or the average age of open security incidents. For more information and installation instructions, see Security Incident Response Platform Analytics Solutions.

Access Security Incident Response Explorer

You can access the Security Incident Response Explorer dashboard to view security incident activity in order to instantly pinpoint areas of concern and quickly resolve issues.

Before you begin

Roles required:

- sn_si.admin (to write)
- sn_si_basic (to read)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Self-Service** > **Homepage** or navigate to **Self-Service** > **Dashboards**.
2. Choose Security Incident Explorer from the reports list.



Result
The Security Incident Response Explorer dashboard appears.

What to do next
To view Security Incident Response Explorer dashboard in Security Incident Response Workspace in detail, see Viewing SIR Workspace Dashboards.

Security incident map

The security incident map provides data by geographical location. The world map is highlighted in every area in which an incident occurs. When the Security Incident Analytics plugin is activated, you can add the security incident map to the Security Incident Response overview. After it has been added, you can configure the map by modifying the map filters.

Add map to Security Incident Response overview

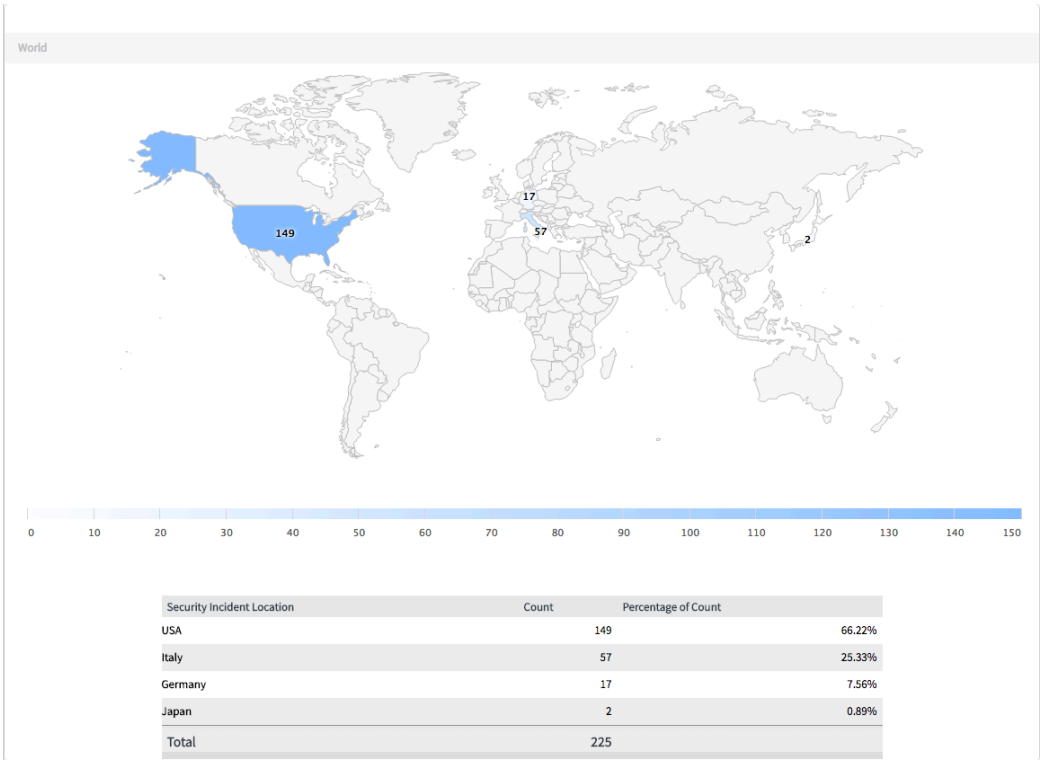
You can add the map to the Security Incident Response overview to view security incident data by geographical location. A map allows you to drill down to security incident information by location.

Before you begin
Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Security Incident** > **Overview**.
2. Click **Add content** in the top left corner of the page to open the widget selection control.
3. In the first selection box, click **Reports**.
4. In the second selection box, click **Security Incident**.
5. In the third selection box, click **Security Incident map**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. At the bottom of the screen, click the location on the screen you want to add to the report.
7. Close the **Add content** box.

Modify security incident map

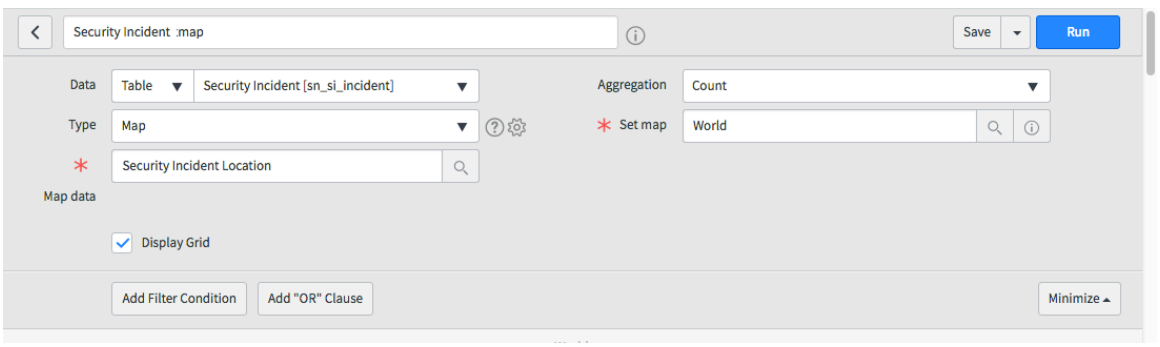
Administrators in the global domain, can modify how the security incident map handles security incidents using filters.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **Reports** > **Administration** > **All**.
2. Search for **Security Incident map**.
3. Click **Edit Report**.



4. Click **Add Filter Condition** to add or edit filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Run** to see the changes applied.
6. Click **Save**.

Security incident treemaps

When the Security Incident Analytics plugin is activated, you can add the security incident - service impact and security incident - real-time treemaps to the Security Incident Response overview. After they have been added, you can configure the treemaps by modifying treemap categories and indicators.

Add treemaps to the Security Incident Response overview

Treemaps display hierarchical (tree-structured) data as a set of nested rectangles. Each branch of the tree is given a rectangle, which is then tiled with smaller rectangles representing subbranches. Treemaps allow you to display security incident information in a dynamic, engaging way.

Before you begin

Role required: sn_si.admin

Procedure

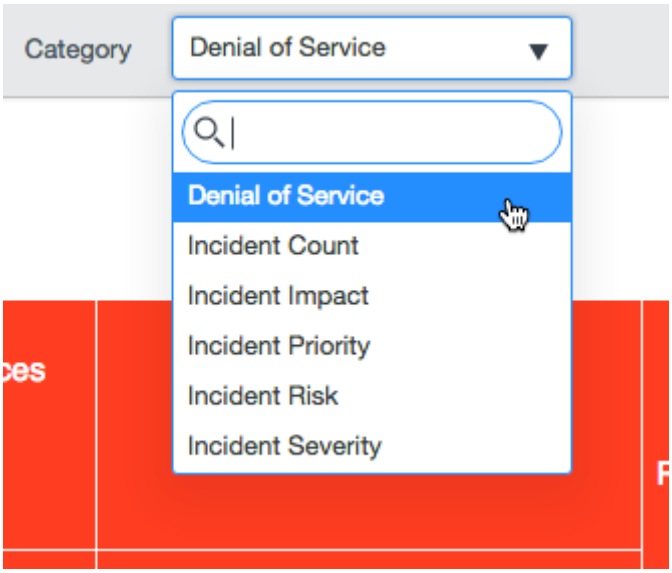
1. Navigate to **All** > **Security Incident** > **Overview**.
2. Click **Add content** in the top left corner of the page to open the widget selection control.
3. In the first selection box, click **Treemap**.
4. In the second selection box, select the treemap you want to insert from the following list:
   - Security Incident - Service Impact
   - Security Incident - Real time
   - Security Incident - Business Impact
   - Vulnerability Significance

   Note: The Business Impact treemap appears on the Security Incident Response homepage by default. The Service Impact and Real time treemaps require that the Security Incident Analytics plugin are activated.

5. In the third selection box, select the level of granularity of information you want retrieved for the selected treemap.

   Note: For the Security Incident - Service Impact treemap, select **Security Incident** in the third selection box. This selection provides a drop-down list with multiple data categories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. At the bottom of the screen, click the location on the screen you want to add the gauge.
7. Close the **Add content** box.

Create or update a treemap category

You can modify the predefined categories for the security incident treemaps or create categories as needed.

Before you begin

Role required: sn_si.admin

The treemaps use performance analytics as the data source. The Performance Analytics module requires a separate plugin.

About this task

In the base system, treemap categories such as Incident Risk, Denial of Service, and Incident Severity are included. You can modify these categories or define more categories as needed.

Procedure

1. Navigate to **All** > **Security Incident** > **Administration**, and open the treemap definition you want to configure categories for:
   - **Service Criticality Reporting Definition**
   - **Real-time Definition**
2. **Optional:** Change the treemap definition name.
   In the base system, the default name for the service impact treemap definition is **Security Incident**. The default name for the real-time treemap definition is **Security Incident - Real time**.
3. Unless you are using a custom-built treemap, do not change the **PA Indicator Group** value.
4. To deactivate the treemap definition, clear the **Active** check box.
   If, for example, you deactivate the Denial of Service category from the system impact dashboard, that treemap category is not available.
5. In the **Treemap Categories** related list, select a category to modify or click **New** to create a new category.
6. Fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Treemap Category form

Field	Description
Name	The name that is displayed for the category in the **Categories** list above the treemap.
Order	The order that the category appears in the **Categories** list above the treemap.
Treemap	The name of the treemap that uses this category.
Color	The color displayed for this category in the treemap.
Active	Select to activate this category.
Description	A description of the category.
Visible by all roles	Select to make this category visible to all users regardless of their role.
Roles	If you did not select the **Visible by all roles** check box, select the roles able to view this category.

7. Click **Submit** or **Update**.

Create or update a treemap indicator

You can modify the predefined indicators for a treemap category or create new indicators. For each indicator, you can configure its data source and specify how lists of security incidents are opened from treemaps that are viewed with the indicator.

Before you begin

Role required: sn_si.admin

The treemaps use performance analytics as the data source. The Performance Analytics module requires a separate plugin.

Procedure

1. Open the treemap definition that you want to configure indicators for.

Treemap definition	Action
Service impact treemap	Navigate to **Security Incident** > **Administration** > **Service Impact Definition**.
Real-time treemap	Navigate to **Security Incident** > **Administration** > **Real-time Definition**.

2. In the **Treemap Categories** related list, select the category that you want to configure indicators for.
3. In the **Treemap Indicators** related list, select an indicator to modify or click **New** to create a new indicator.
4. Fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Treemap Indicator form

Field	Description
Name	The name that is displayed for the indicator in the **Indicators** list on the service impact dashboard.
Short description	A description that is displayed for the indicator in the **Indicators** list above the treemap.
Result limit	The maximum number of results allowed. The upper limit is 100.
Result Precision	The number of digits to display after the decimal point. This field is displayed for the real-time treemap definition only.
Active	Check box to activate this indicator.
Category	The category name entered on the previous screen.
Direction	Indicates whether the tile on the treemap is minimized or maximized. This field is displayed for the real-time treemap definition only.
Unit	The unit of measure to be used for the metric. This field is displayed for the real-time definition only.
Automatic Refresh Interval	How frequently to refresh the treemap.
Order	The order the indicator appears in the **Indicators** list above the treemap.

5. Click the **Data Source Configuration** tab and configure one of the following data source options for the indicator.

Option	Action
Performance analytics	Select **Performance Analytics** from the **Data source** field, then make the following entries: ○ **Indicator:** The indicator used to group the PA data. ○ **Default breakdown:** The default break down used to break the selected PA indica tor into multiple parts.
Custom script	Select **Custom Script** from the **Data Source** field. Then use the HTML editor to customize the script as needed. The result of running

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Action
	the script must be an array in order for the in formation to display in the treemap.
Query conditions	Select **Query Condition** from the **Data Source** field, and then make the following en tries: ○ **Query table:** The base table to be queried. ○ **Aggregate type:** The type of aggregate (SUM, COUNT, AVG, MIN, MAX) to be used. ○ **Aggregate field:** The field to be used by the query. ○ **Group by:** The field to sort the queried data. **Note:** To enhance the query, click **Add Filter Condition** and **Add "OR" Clause**.

6. Click the **Click Through** tab, and specify how lists of security incidents are opened from the treemap.
   a. In the **Click through URL navigation type** field, select whether you want the list of security incidents to open in a new window, in the same window, or in a dialog box.
   b. **Optional:** In the **Click through URL script** field, modify the sample script if needed.
7. Click **Submit** or **Update**.

Add vulnerability significance charts to an overview

If the Vulnerability Response plugin is activated, you can add vulnerability significance definition charts and other visualizations to the Overview.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to the Overview page to which you want to add the vulnerability significance gauge.
2. Click **Add content** in the top left corner of the page to open the widget selection control.
3. In the three selection boxes, make the selections depending on the gauge (tree map or score report) you want to add:
   - To add the Vulnerability Significance tree map, make these selections:
     - Treemap
     - Vulnerability Significance
     - Vulnerability Significance
   - To add the Vulnerability Significance score report, make these selections:
     - Performance Analytics
     - Score
     - Services with Vulnerability Significance

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click the location on the screen you want to add the gauge.
5. Close the **Add content** box.

Major Security Incident Management

The ServiceNow® Major Security Incident Management application tracks the progress of Major Security Incident (MSI) from discovery to analysis, propose, promote, and link security incidents, and closure.

Major Security Incident Management

Explore  Learn about how analysts, administrators, and managers use Major Security Incident Management (MSIM)	**Configure**  Plan and configure your implementation	**Integrate**  Extend MSIM capabilities by integrating with other Microsoft applications
Administer  Administration tasks on how to tag incident records and configure labels	**Use**  Propose, promote, link, and reject major security incident records through the workspace management	**Status Reports**  Monitor incident related tasks and improve processes through metrics, trend charts, and reports
Additional Capabilities  Configure information to roll up records		

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request apps on Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Request a Security Operations app on Store

If you are a new Security Operations customer on Rome or later, visit the ServiceNow Store website to view the available apps and information on how to submit requests to the store.

More resources

Visit the Major Security Incident Management forum on the ServiceNow Community.

Exploring Major Security Incident Management

Explore Major Security Incident Management to understand how the application works in terms of tracking high priority critical security incidents, which are identified as a threat to the organization.

Use this section to learn the key features, various roles involved in working with major security incident records. This section also helps you understand on how to get started with the application, prerequisites, and plugins required to work with the application.

Major Security Incident Management

Track and manage various activities that are typically part of resolving a major security incident through Major Security Incident Management. Through an intuitive workspace, incident managers and those working on an incident can propose and promote incidents to major incidents, track major security incident activities, and easily collaborate with colleagues.

Overview

The major security incident management capabilities work in conjunction with the existing security incident response product capabilities. This includes an ability for a security analyst to escalate a standard security incident to a major security incident, so that the new product capabilities are available to support the remediation process.

After you install on your ServiceNow instance, a security incident analyst can:

- Propose a security incident to major security incident candidate to initiate a review process on the need to create a major security incident.
- Directly promote a security incident to a major security incident without the need for an additional review process.
- Reject a security incident that is proposed as a major security incident (MSI).
- Link a security incident as a child incident to the major security incident (MSI) so that all security incidents can be worked.

Key features

Major Security Incident Management (MSIM) improves the major security incident remediation process with the following features:

- Dedicated workspace for managing major security incidents designed for the major security incident manager user role.
- Organize response tasks across multiple 'child' security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Automate creation of collaboration folders and chat communication channels after a major security incident is created, as well as archival as part of incident closure.
- File explorer component to organize and track the collection of artifacts (files) related to the major security incident via a Microsoft SharePoint integration.
- Chat channel manager and activity stream components to manage communications across multiple security, IT, and functional groups via a Microsoft Teams integration.

Workspace Components

The Major Security Incident Management product contains several new workspace components and user interface pages that deliver the key features functionality:

- Dedicated workspace for managing major security incidents specifically designed for the major Security Incident Manager user role.
- Organize response tasks across multiple child security incidents.
- Automate creation of collaboration folders and chat communication channels after a major security incident is created, as well as archival as part of incident closure.
- File explorer component to organize and track the collection of artifacts (files) related to the major security incident via a Microsoft SharePoint integration.
- Chat channel manager and activity stream components to manage communications across multiple security, IT, and functional groups via a Microsoft Teams integration.

Supported Major Security Incident Management versions

Major Security Incident Management (MSIM) requires ServiceNow AI Platform® Rome version.

This feature supports Microsoft Teams, which is a chat-centered workspace in the Microsoft Office 365 suite. Earlier Microsoft Teams was a separate installation from Microsoft Office 365 applications.

Supported ServiceNow AI Platform versions

This feature is supported on Rome and later releases.

The following Security Operations applications are the standard Security Incident Response plugins that will likely be installed for most of the users if they're using already Security Incident Response (SIR). If not installed, you must install and activate from ServiceNow Store. Install and then activate one application at a time in the order mentioned to ensure a smooth installation:

1. Security Incident Response: com.snc.si_dep is the dependent plugin. Installing this plugin activates the other Security Operations applications.
2. Security Integration Framework
3. Security Support Common
4. Security Support Common Orchestration

Get started with MSIM

Review the following information before you start working with Major Security Incident Management.

Role required: sn_msi.workspace_admin.

For an easy installation and configuration of the Major Security Incident Management application, you may have to verify if the following plugins are activated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: An update set (KB1289784) is available within the Major Security Incident Management Quick Start Guide to help users with an easy configuration set up, you need to import the update set after you complete the application installation. Follow the procedure detailed in the Quick Start Guide (Step 2) under the Supporting documents section within the MSIM application, which is on ServiceNow Store.

Prerequisite

Task	Description
Before you begin with the application, ensure that you have the required dependent plugins.	As a first step, install: • ServiceNow IntegrationHub Installer (com.glide.hub.integrations) • ServiceNow® Integration Hub Runtime (com.glide.hub.integration.runtime). • ServiceNow® Integration Hub Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow® Integration Hub Action Template - Data Stream (com.glide.hub.action_type.datastream) • ServiceNow® Integration Hub Flow Designer - Dynamic Inputs (com.glide.hub.dynamic_inputs) **Note:** If you don't have the necessary privileges for any of the listed ServiceNow® Integration Hub plugins, then raise a support ticket to install those prerequisite applications.
Verify that you have required access to install Microsoft SharePoint Spoke and Microsoft Teams Graph Spoke. **Note:** The above listed are the primary dependent applications to get started with Major Security Incident Management.	Before you install Microsoft SharePoint Spoke and Microsoft Teams Graph Spoke, make sure you have required access to the ServiceNow Integration Hub applications. **Note:** Microsoft SharePoint Spoke and Microsoft Teams Graph spoke are dependent applications to ServiceNow® Integration Hub applications.

Checklist for MSIM setup

Before using the ServiceNow® Major Security Incident Management (MSIM) application, download the application from the ServiceNow® Store.

Track your progress with the setup, installation, and configuration from the following table.

Note: The roles assigned for Major Security Incident Management application are listed in the further following sections, for more information, see Major Security Incident Management roles.

Use the following checklist to guide you through the end-to-end steps to install and configure Major Security Incident Management application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist

Setup task	Description
Verify that the Major Security Incident Management application is installed and activated from the ServiceNow® Store.	Major Security Incident Management v1.1.1 is available on ServiceNow® Store. Follow these instructions: downloading an application from the ServiceNow Store.
Verify that the following applications are installed in the given order.	The following applications will be installed by default after you install Major Security Incident Management application in the current application release version: • File Explorer Core for Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connector for Security Operations v1.1.1 • File Explorer Component for Security Operations v1.0.0 • Microsoft Teams Chat Connector for Security Operations v1.0.0 • Chat core for Security Operations v1.0.0 • Major Security Incident Response v1.1.1 • Collab Chat EVAM card for MSIM workspace v1.0.0 (This application is set up only for the UI visualizations in the application background for Major Security Incident Management workspace) • Task Organizer UI Component for Major Security Incident Management workspace 1.0.0 • Security Incident Response v12.8.1
Verify that the user roles are assigned to Major Security Incident as appropriate.	The following roles are involved throughout the incident life-cycle of Major Security Incident remediation process: • MSI Administrator [sn_msi.workspace_admin] • MSI Manager [sn_msi.workspace_manager] • MSI Responder [sn_msi.workspace_responder] For more detailed information on each role, see Major Security Incident Management roles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
Verify that you have successfully setup Microsoft SharePoint v1.0.0 configuration.	Microsoft SharePoint manages sites, folders, files, groups, and users in Microsoft SharePoint. Add Microsoft SharePoint data to your ServiceNow® instance. To do this, you must have to setup Graph and Rest connections. For information, see Microsoft SharePoint spoke v1.1.2 documentation on how to setup REST and Graph connections Configuration. Establish Graph and REST connection to connect to your ServiceNow® instance from Microsoft SharePoint.
Verify that you have created a Microsoft SharePoint site to create a document library.	Create a Microsoft SharePoint site, if required or you can use an existing site to create the document library.
Verify that you have created a document library under the Microsoft SharePoint site.	Create a dedicated document library under a new or existing Microsoft SharePoint site.
Verify that required permissions are provided to the users and assigned to the required user groups in the Microsoft SharePoint.	Manage access from Microsoft SharePoint site to different users and user groups.
Verify that you have created and configured Microsoft SharePoint Drive and necessary configuration settings.	To verify the drive configurations, setup Microsoft SharePoint File Explorer Connector, Folder, and File Actions and Folder Templates: • Configure File Explorer Repository Drive: Create connection from Microsoft SharePoint to ServiceNow® instance. • Configure Folder and File Action Settings: Configure and control the individual Folder and File Actions displayed on the File Explorer Component. • Create Folder Templates: Configure to create unique folders for different Major Security Incident types.
Verify that you have successfully established a connection to Microsoft Teams Chat Connector application.	To establish Microsoft Teams Chat Connector application connection with ServiceNow® instance, follow the procedure explained here: Establish MS Teams Graph connection on ServiceNow AI Platform.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
Verify that you have configured Microsoft teams with ServiceNow AI Platform® instance and created connections and credentials configurations.	To verify Microsoft Teams configuration with ServiceNow® instance, follow the procedure as explained here: • Establish MS Teams Graph connection on ServiceNow AI Platform • Create a chat channel template
Verify that the Major Security Incident Administration - Configuration settings are successful.	As an MSI Administrator, you must be able to: • Determine whether security analysts can propose and promote the incident and link other security incidents. • Enable or disable the notifications when an incident is proposed or promoted. Ability to edit default template messages. • Configure security tags that appear on the security analyst interface to differentiate the incidents that have been proposed as a major security incident candidate or promoted to a major security incident.
Verify that the Major Security Incident Administration - Notifications settings are successful.	As an MSI Administrator, trigger email notifications when a security incident is proposed and are sent to all those users and groups who are configured to the notifications list. For more information, see Set notification preferences for MSIM.

Major Security Incident Management roles

Assign roles to ensure that users can perform all necessary actions within the MSIM application.

Roles for Major Incident Management

Role Type	Role	Description
MSI Administrator	sn_msi.workspace_admin	Can I install and configure Major Incident Management and set up the dependent applications such as File Explorer (FE), Microsoft Teams and Chat Channel configuration, Workspace setup, and MSI Administration: Configurations and Notifications setup. How to set up:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roles for Major Incident Management (continued)

Role Type	Role	Description

		• File Explorer (FE) component:
		  ○ Configure file repository.
		  ○ Configure file and folder actions, which are provided on the File Explorer component of the Collaboration tab in the Major Security Incident Management workspace.
		  ○ Create the root folders and subfolders, and provide access to the subfolders.
		• Chat channel management
		  ○ Activate and configure Microsoft Teams by validating Microsoft Teams connection.
		  ○ Create chat teams and chat channels, and add users and assign users to the various user groups.
		• MSI Administration:
		  ○ Configurations: Configure the security analysts actions, notifications sent when incidents are proposed and promoted, and display tags for the security incidents.
		  ○ Notifications: Automate email notification process and user notifications when a security incident is either proposed or promoted as a major security incident.

MSI Manager	sn_msi.workspace_manager	• View access to the major security incident management configuration settings page. Restricted from modifying any of the configuration settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roles for Major Incident Management (continued)

Role Type	Role	Description
		• View and edit incident record data in the **Details**, **Collaboration**, and **Task Organizer** tabs of the Major Incident Management workspace. • Promote the security incident to a major security incident. • Configure file and folders actions available on the File Explorer component on the **Collaboration** tab of the Major Incident Management workspace. • Linking and unlinking additional records to Major Security Incidents from the workspace.
MSI Responder	sn_msi.workspace_responder	• Optional role to view, edit, and respond to major security incidents in the **Details** and **Tasks** tabs of the Major Incident Management workspace. • Linking and unlinking additional records to Major Security Incidents from the workspace.

Integrating Major Security Incident Management

Extend the capabilities of Major Security Incident Management and connect with ServiceNow AI Platform instance by integrating with Microsoft applications.

Important: An update set (KB1289784) is available within the Major Security Incident Management Quick Start Guide to help users with an easy configuration set up, you need to import the update set after you complete the application installation. Follow the procedure detailed in the Quick Start Guide (Step 2) under the Supporting documents section within the MSIM application, which is on ServiceNow Store.

Integrate Major Security Incident Management with Microsoft SharePoint

Integrate your Microsoft SharePoint with Major Security Incident Management.

Register a new application at Azure portal for SharePoint connections

Register a new application at Azure portal for Microsoft SharePoint integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: admin, Azure admin

Procedure

1. Sign in to Microsoft Azure portal using your Microsoft account as Azure admin.
2. Navigate to **Azure Services** > **Application Registration** > **New Registration**.

   Note: In case if you don't find, navigate to **Azure Services** and search for **App Registration**.

3. Enter the name of the application.
   For example, Microsoft SharePoint graph.
4. Select **Supported account types: Accounts in this organizational directory only (Service Now only - Single tenant)**.
5. Select **Web** type from the drop down list under the Redirect URI (optional) field.
6. Enter ServiceNow AI Platform® instance redirect URL in the allowed redirect URL field.
   For example, `https://<InstanceName>.service-now.com/oauth_redirect.do`.
7. Click on **Register** and make sure the page is displayed with **Overview** section.
8. Make a note of the Client ID and Tenant ID from **Essentials** section of the Overview page.
9. Under **API Permissions**, add the Microsoft Graph permission:
   a. Click **Add a permission**.
   b. Select **Microsoft Graph**.
   c. Select **Application Permissions**.
   d. From the **Sites** list, select **Sites.Selected** permission.
   e. Click **Add permissions**.
10. Under **API Permissions**, add the SharePoint permission:
    a. Click **Add a permission**.
    b. Select **SharePoint**.
    c. Select **Application Permissions**.
    d. From the **Sites** list, select the **Sites.Selected** permission.
    e. Click **Add permissions**.
11. After adding the permissions, click on#**Grant admin consent**.
    All the permissions are now admin consented.

Use certificates for authentication

Request an access token with a certificate credential.

Before you begin

1. You can either use a self-signed certificate or CA issued certificate. You can create a self-signed certificate by executing the PowerShell script as outlined in Setting up an Azure AD app for app-only access. The script generates two files: .PFX file and .CER file.

   Note: Ensure that you are aware of the password that is used to encrypt private key to generate the .PFX file and .CER file.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Use the .PFX file to create a Java Key Store (JKS) file.

   Note: Ensure that you are aware of the password that is used to generate JKS file from the .PFX file.

Role required: admin

Procedure

1. Navigate to **App registrations** in Azure AD portal.
2. Click **Certificates & secrets** from the **Manage** section.
3. In the **Certificates** tab, click **Upload Certificate**.
4. On the form, fill these values.

Field	Description
Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt	.CER file you had generated using the PowerShell script.
Description	Description of the certificate.

5. Click **Add**.
   The certificate is uploaded and its details are displayed under the **Certificates** tab.
6. Copy the **Thumbprint** value of the uploaded certificate.

   Note: The **Thumbprint** value is a hexadecimal value.

7. Encode the **Thumbprint** value to a Base64 value and record the value for later use.

   Note: You can use a Hexadecimal to Base64 (Hex to Base64) converter tool to encode the **Thumbprint** value to a Base64 value.

Configure Microsoft SharePoint with Major Security Incident Management

Set up Major Security Incident Management with Microsoft SharePoint connection.

Before you begin

Role required: admin

Procedure

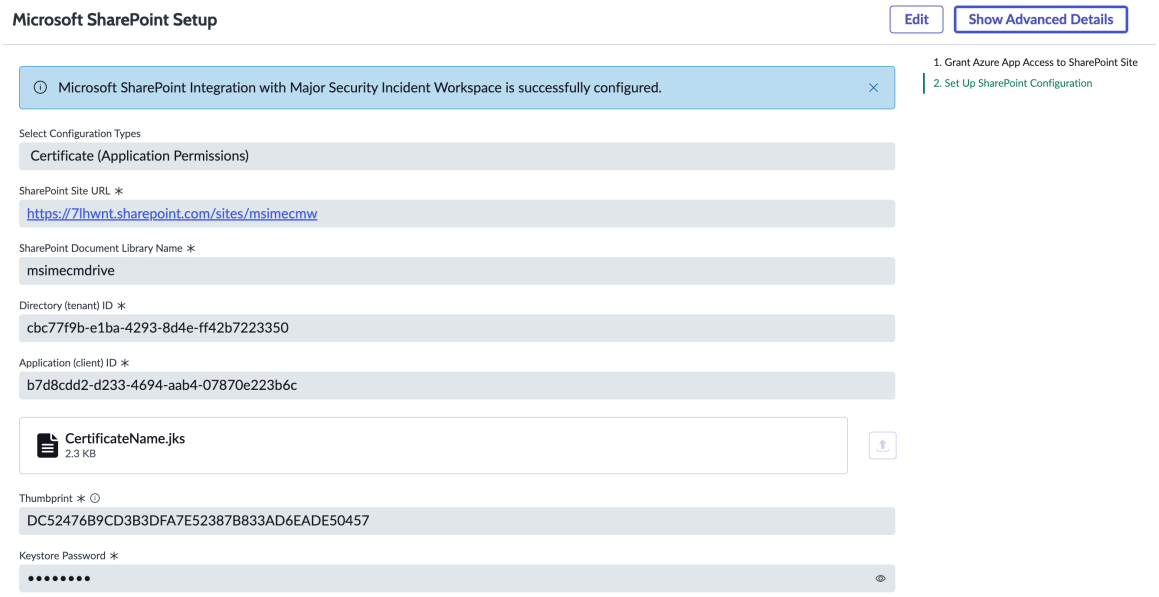
1. Navigate to **Workspaces** > **Major Security Incident Management** > **Administration**.
2. Select **Document Collaboration**, and then **Microsoft SharePoint Setup**.
3. Select **Grant Azure App Access to SharePoint Site** from the context menu.
4. Grant access to your registered application using one of the following methods: Curl Commands, Azure CLI or PowerShell.

   Note:

   - The Azure administrator must provide the access configuration.
   - Grant the Sites.FullControl.All permission to the registered application.
   - Remove the Sites.FullControl.All permission when the access is successfully granted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select **Set Up SharePoint Configuration** from the context menu.
6. Select a configuration type in **Select Configurations Types**, and configure the following.
   - Certificate (Applications Permissions)



SharePoint settings for certificate

Field	Description
SharePoint Site URL	The Microsoft SharePoint Site URL.
SharePoint Document Library Name	Name of the Microsoft SharePoint document library.
Directory (tenant) ID	The unique identifier of your Azure Active Directory instance.
Application (client) ID	The unique identifier of your registered application in Azure.
Upload Certificate	The certificate file for the authentication.
Thumbprint	The thumbprint for the certificate.
Keystore password	The keystore password to access the certificate's thumbprint.

   - Client Secret (Applications Permissions)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



SharePoint settings for Client Secret

Field	Description
SharePoint Site URL	The Microsoft SharePoint Site URL.
SharePoint Document Library Name	Name of the Microsoft SharePoint document library.
Directory (tenant) ID	The unique identifier of your Azure Active Directory instance.
Application (client) ID	The unique identifier of your registered application in Azure.
Client Secret	The secret string of the application used for requesting a token.

7. Select **Configure & Get OAuth Token**.
   A login prompt appears to provide your Microsoft account details.
8. Provide your Microsoft account details and login.
   A successful message appears and the connection is established.

Integrate Major Security Incident Management with Microsoft Teams

Integrate your Microsoft Teams with Major Security Incident Management.

- Register a new application at Azure portal for Microsoft Teams connections
- Configure Microsoft Teams connection with Major Security Incident Management

Register a new application at Azure portal for Microsoft Teams connections

Register a new application at Azure portal for Microsoft Teams integration and grant access to the Azure app.

Before you begin

Note: If you want, you can use the same application that you created for SharePoint to establish the Microsoft Teams Graph connection.

Role required: admin, Azure admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Sign in to Azure portal using your Microsoft account.
2. Navigate to **Azure Services** > **Application Registration** > **New Registration**.
3. Enter name of the application.
   For example, Microsoft Teams Graph.
4. Select **Supported account type: Accounts in this organizational directory only (Service Now only - Single tenant)**.
5. Select **Web** type from drop down list under the Redirect URL.
6. Enter ServiceNow AI Platform® instance redirect URL in the allowed redirect URL field.
   For example, `https://<<InstanceName>>.service-now.com/oauth_redirect.do`
7. Click on **Register** and make sure the page is displayed with **Overview** section.
8. Make a note of the Client ID and Tenant ID from the **Essentials** section in the **Overview** page.
9. You can either follow Step 6.1 or Step 6.2 to complete the procedure of establishing a connection on your ServiceNow instance.

Configure Microsoft Teams connection with Major Security Incident Management

Set up Major Security Incident Management with Microsoft Teams connection.

Before you begin

Prerequisite: Make sure that you have registered an application in Azure Active Directory with required delegate permissions.

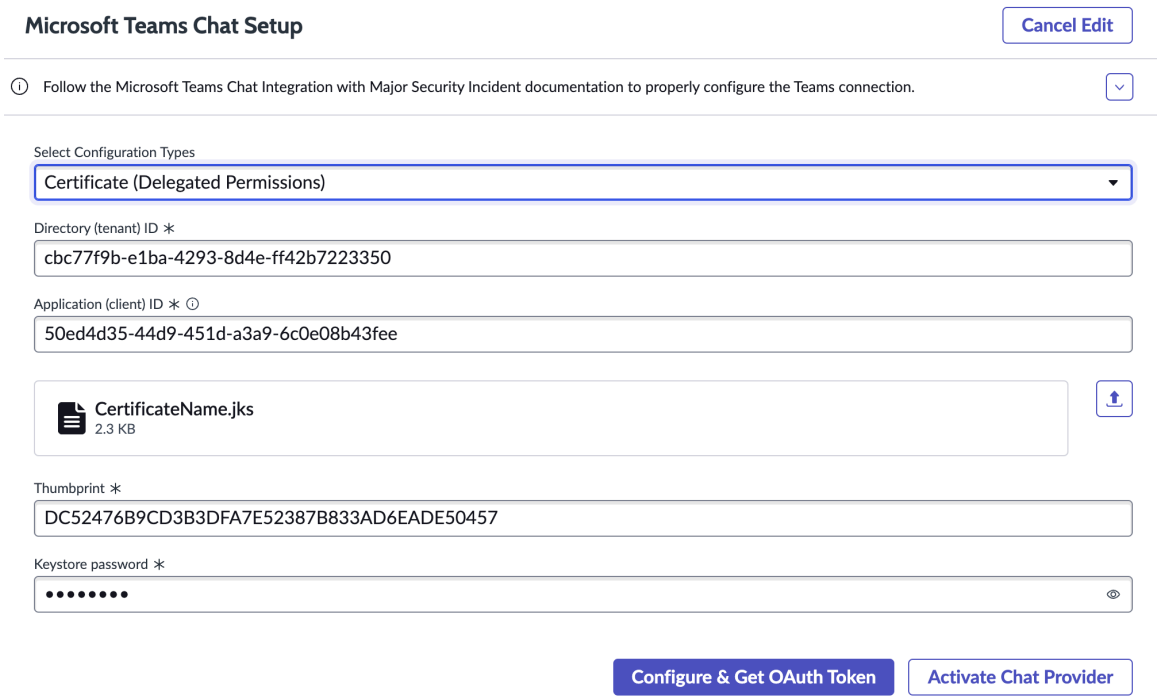
Role required: admin

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Administration**.
2. Select **Chat Collaboration**, and then **Microsoft Teams Setup**.
3. Select a configuration type in the **Select Configurations Types** field, and configure the following.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Certificate (Delegated Permissions)

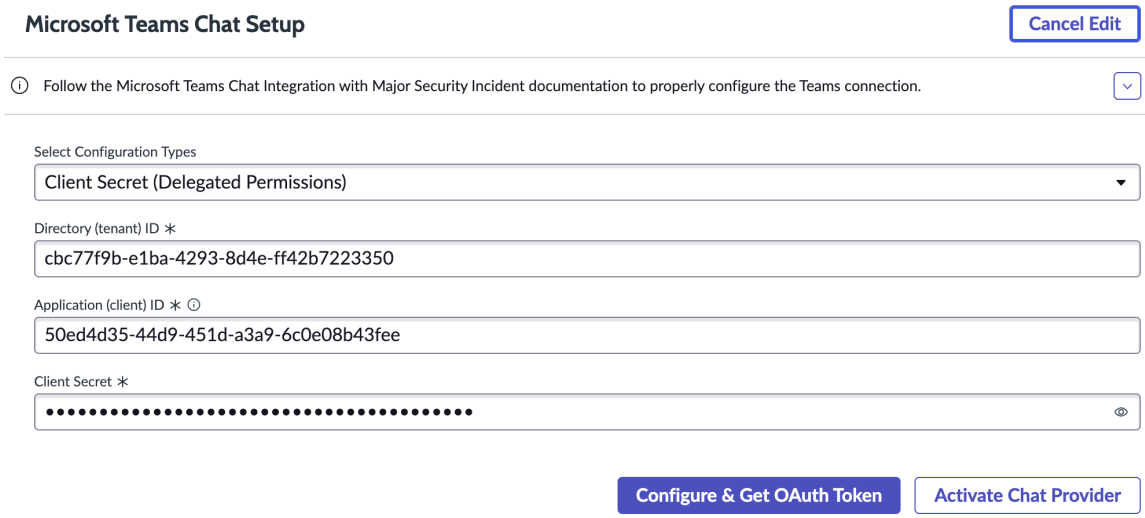


Microsoft Teams settings for Certificate

Field	Description
Directory (tenant) ID	The unique identifier of your Azure Active Directory instance.
Application (client) ID	The unique identifier of your registered application in Azure.
Upload Certificate	The certificate file for the authentication.
Thumbprint	The thumbprint for the certificate.
Keystore password	The keystore password to access the certificate's thumbprint.

- Client Secret (Delegated Permissions)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Microsoft Teams settings for Client Secret

Field	Description
Directory (tenant) ID	The unique identifier of your Azure Active Directory instance.
Application (client) ID	The unique identifier of your registered application in Azure.
Client Secret	The secret string of the application used for requesting a token.

4. Select **Configure & Get OAuth Token**.
   A login prompt appears to provide your Microsoft account details.
5. Provide your Microsoft account details and login.
   A successful message appears and the connection is established.
6. Select **Activate Chat Provider** to enable Microsoft Teams connection.
7. **Optional:** Select **Show Advanced Details** to view the configuration details.

Establish MS Teams Graph connection on ServiceNow AI Platform

Integrate ServiceNow AI Platform instance and Microsoft Teams account by establishing a Microsoft Teams Graph connection.

Before you begin

If you want, you can use the same application that you created for SharePoint to establish the Microsoft Teams Graph connection.

Role required: admin, Azure admin

Register a new application on Azure for Microsoft Teams Graph Connection

Procedure

1. Sign in to Azure portal using your Microsoft account.
2. Navigate to **Azure Services** > **Application Registration** > **New Registration**.
3. Enter name of the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, Microsoft Teams Graph.

4. Select the respective **Supported account types** option whichever is applicable to your organization.
   For example, select **Accounts in this organizational directory only (Service Now only - Single tenant)** option.

   Note: For information on supported account types, see Register an application with the Microsoft identity platform.

5. Select **Web** type from drop down list under the Redirect URL.
6. Enter ServiceNow AI Platform instance redirect URL in the allowed redirect URL field.
   For example, https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Click **Register** to register your new application and make sure the page is displayed with **Overview** section.

Using Certificates for authentication

Request an access token with a certificate credential.

Before you begin

1. You can either use a self-signed certificate or CA issued certificate. You can create a self-signed certificate by executing the PowerShell script as outlined inSetting up an Azure AD app for app-only access. The script generates two files: .PFX file and .CER file.

   Note: Ensure that you are aware of the password that is used to encrypt private key to generate the .PFX file and .CER file.

2. Use the .PFX file to create a Java Key Store (JKS) file.

   Note: Ensure that you are aware of the password that is used to generate JKS file from the .PFX file.

Role required: admin

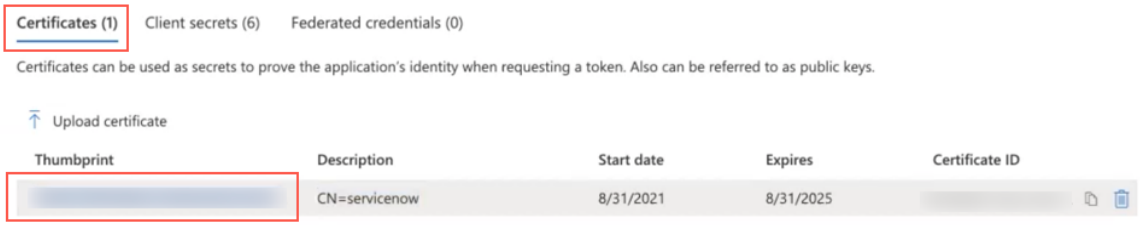
Procedure

1. Navigate to **App registrations** in Azure AD portal.
2. Click **Certificates & secrets** from the **Manage** section.
3. In the **Certificates** tab, click **Upload Certificate**.
4. On the form, fill these values.

Field	Description
Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt	.CER file you had generated using the PowerShell script.
Description	Description of the certificate.

5. Click **Add**.
   The certificate is uploaded and its details are displayed under the **Certificates** tab.
6. Copy the **Thumbprint** value of the uploaded certificate.
   The **Thumbprint** value is a hexadecimal value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Encode the **Thumbprint** value to a Base64 value and record the value for later use.

> **Note:** You can use a Hexadecimal to Base64 (Hex to Base64) converter tool to encode the **Thumbprint** value to a Base64 value.

Attach a Java Key Store certificate for MS Teams

Enable the JWT Bearer Grant token authentication by attaching a valid Java Key Store (JKS) certificate.

Before you begin

Login to your ServiceNow instance to perform the following procedure.

- Valid Java Key Store certificate
- Role required: admin

Procedure

1. Navigate to **System Definition** > **Certificates**.
2. Open the record **Microsoft Teams Connector Certificate**.
   Ensure to use the default record **Microsoft Teams Connector Certificate** only.
3. Enter the password associated with the JKS file in **Key store password**.
4. Click the attachments icon ( ) and attach the JKS certificate you had generated.
   For more information, see Configure OAuth application in Microsoft Azure.
5. Click **Validate Stores/Certificates**.
6. Click **Update**.

Configure the JWT signing key for MS Teams

Create a JSON Web Token (JWT) signing key to assign to your Java Key Store certificate.

Before you begin

Role required: admin

Procedure

1. Navigate to **System OAuth** > **JWT Keys**.
2. Open the record **Microsoft Teams Connector JWT**.
3. Enter the password that is used to encrypt private key to generate the .PFX file and .CER file in **Signing Key Password**.
4. Click **Update**.

Configure the JWT provider for MS Teams

Add a JSON Web Token (JWT) provider to your ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- Copy and record the value of **Application (client) ID** and **Directory (tenant) ID** of the application you had registered in the Azure portal.



- Role required: admin

Procedure

1. Navigate to **System OAuth** > **JWT Providers**.
2. Open the record **MS Teams Connector JWT Provider**.
3. Enter values for **iss**, **sub**, and **aud** in the Standard Claims related list.

Field	Value
aud	Microsoft Online URL in this format: `https://login.microsoftonline.com/<tenant-id>/oauth2/token`. Replace `<tenant-id>` with **Directory (tenant) ID** value of your application had registered in the Azure portal.
iss	**Application (client) ID** of the application you had registered in Azure portal.
sub	**Application (client) ID** of the application you had registered in Azure portal.

4. Click **Update**.

Establish a connection using certificates

Establish a connection between newly created Microsoft Teams graph application using certificates.

Before you begin

Role required: admin

Procedure

1. Navigate to **Connections & Credentials** > **Connections & Credentials Aliases**.
2. Open **Microsoft Teams Spoke**.
3. Modify the field value **Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template** and save the form.

> **Note:** This template contains the delegated API permission required for the MSTeams integration.

4. From the Related Links section, click Create **New Connection & Credential**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Any unique Name.
Connection URL	Connection URL. For example, https://graph.microsoft.com
API Version	Version of the API. For example, v1.0
Authorization URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/authorize
Token URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/token
Token Revocation URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/revoke
OAuth Client ID	Client ID.
OAuth Client Secret	You can enter any value. **Note:** This is not important as you will be using the certificate-based authentication.

5. Click **Create and Get Oauth Token**.
   An error message is displayed prompting 401- unauthorised.
6. Reload the form and open the record in the Connections related list.
7. Enter the Base64 encoded **Thumbprint** value in the **Encoded Certificate Thumbprint** attribute in the **Attributes** section.

   Note: The Thumbprint value is a hexadecimal value. You can use a Hexadecimal toBase64 (Hex to Base64) converter tool to encode the Thumbprint value to a Base64 value.

8. Navigate to **System OAuth** > **Application Registry**
9. Open **MSIM Microsoft Teams Connector Authorization Code** record.
10. Modify the OAuth API Script: **OAuthUtilJWTMSTeamsConnector**.
11. Navigate to **Connections & Credentials** > **Credentials**.
12. Open the record **MSIM Microsoft Teams Connector Credential**.
13. From Related Links, click **Get OAuth Token**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

On success, the following API permissions are added to the Azure application.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Using Client Secret value

Use client secret value to configure the Graph application registry record.

Before you begin

Role required: admin

Procedure

1. Navigate to **App registrations** in Azure AD portal.
2. Click **Certificates & secrets** from the **Manage** section.
3. Click **New client secret**.
4. Copy and make a note of the created client secret from the **Value** field.

Establish a connection using client secret

Establish a connection between newly created Microsoft Teams graph application with ServiceNow AI Platform instance.

Before you begin

Role required: admin

Procedure

1. Navigate to **Connections & Credentials** > **Connections & Credentials Aliases**.
2. Open **Microsoft Teams Spoke**.
3. Modify the field value **Configuration Template: MSIM Microsoft Teams ConnectorAuthorization Code Template** and save the form.

   Note: This template contains the delegated API permission required for the MSTeams integration.

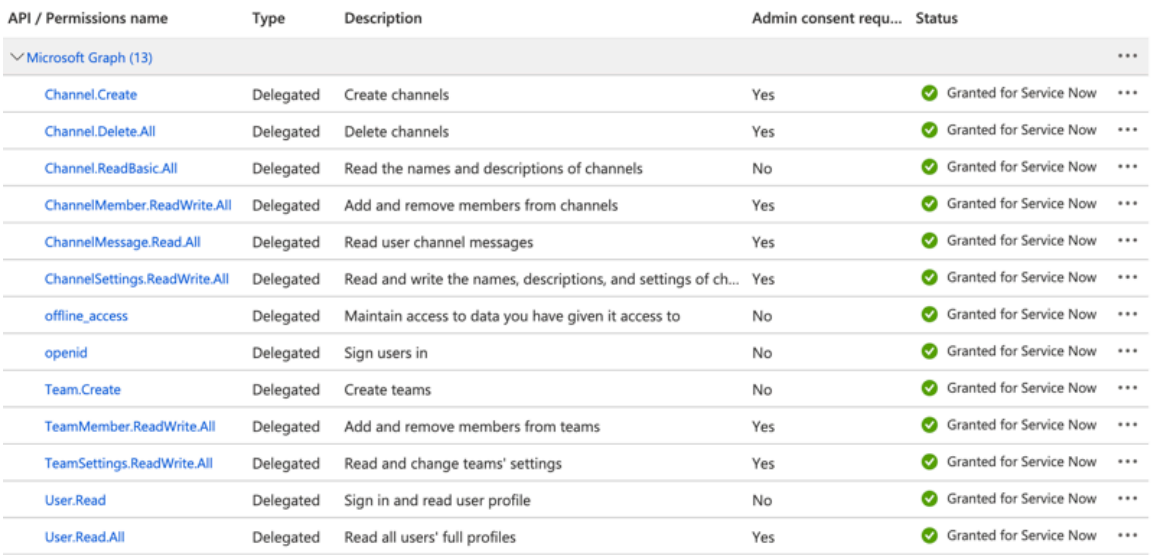
4. From the Related Links section, click Create **New Connection & Credential**.

Name	Any unique Name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Connection URL	Connection URL. For example, https://graph.microsoft.com
API Version	Version of the API. For example, v1.0
Authorization URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/authorize
Token URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/token
Token Revocation URL	https://login.microsoftonline.com/<<tenant ID>/oauth2/v2.0/revoke
OAuth Client ID	Client ID.
OAuth Client Secret	Client secret.

5. Click **Create and Get Oauth Token**.
   On success, the following API permissions are added to the Azure application.



API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Activate MS Teams chat connector for MS Teams Graph Spoke user

If you are an existing user, then follow the procedure in this section to activate Microsoft Teams chat connector.

Before you begin

Role required: admin

Procedure

If you are an existing Microsoft Teams Graph Spoke user, follow the below steps:

- Navigate to your registered application on Azure portal which is used by Microsoft Teams Graph Spoke.
- Navigate to **API Permissions** section to configure the required API permissions.
- Click **Add a permission**.
- Select **Microsoft Graph**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To use the Microsoft Teams Connector application, you need to add two more delegated permissions to your application from the Azure portal: "ChannelMember.ReadWrite.All" and "TeamMember.ReadWrite.All".
- After adding the above required permissions, click on **Grant admin consent**.

Configure MS Teams on *ServiceNow AI Platform* Instance for an existing user:

- Navigate to **Connection & Credential Aliases**.
- Select **Microsoft Teams Spoke** record.
- Select the Credential record associated with Microsoft Teams Spoke.
- Click **Get OAuth Token**. A confirmation message displays that the OAuth Refresh token is available.

As an existing user, you have now completed integrating Microsoft Teams chat connector application with Microsoft Teams Graph API.

Major Security Incident Management Conference Call Integration

With Major Security Incident Management conference calls integration, you can collaborate with your customers and peer agents to resolve customer issues using the video and screen sharing options in Microsoft Teams, Cisco Webex, or Zoom from the MSIM application.

The Major Security Incident Management Conference Call integration enables you to integrate the conference communication channel with the Notify communication channel by managing and initiating a Microsoft Teams, Cisco Webex, or Zoom meeting directly from the Major Security Incident Management application.

As an MSI Manager, you can use the MSIM Conference Call integration to initiate Microsoft Teams, Cisco Webex or Zoom meetings. Integrate the Major Security Incident Management Conference Call with the third-party service providers as a communication channel to meet with the stakeholders to resolve the major security incidents.

Key Features

The Major Security Incident Management Conference Call integration provides the following key features:

- MSI Managers can initiate a Microsoft Teams, Cisco Webex, or Zoom conference call directly from the major security incident.
- Invite additional participants to the call.
- View call recordings and chat details.
- Sends invites to participants through emails and Microsoft Teams chat.

Start a conference call

Start a conference call from a task or a major security by inviting one or more users to join a conference call. The conference call would start only when at least two participants join.

Before you begin
Role required: sn_msi.workspace_manager

Make sure you've done the following on the ServiceNow® instance:

- Installed and activated the Notify plugin (com.snc.notify).
- Installed the Notify UI Components for Configurable Workspaces app.
- Installed and activated the Visual Task Board plugin (com.devsnc.snb_vtb).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see Request IntegrationHub.

About this task

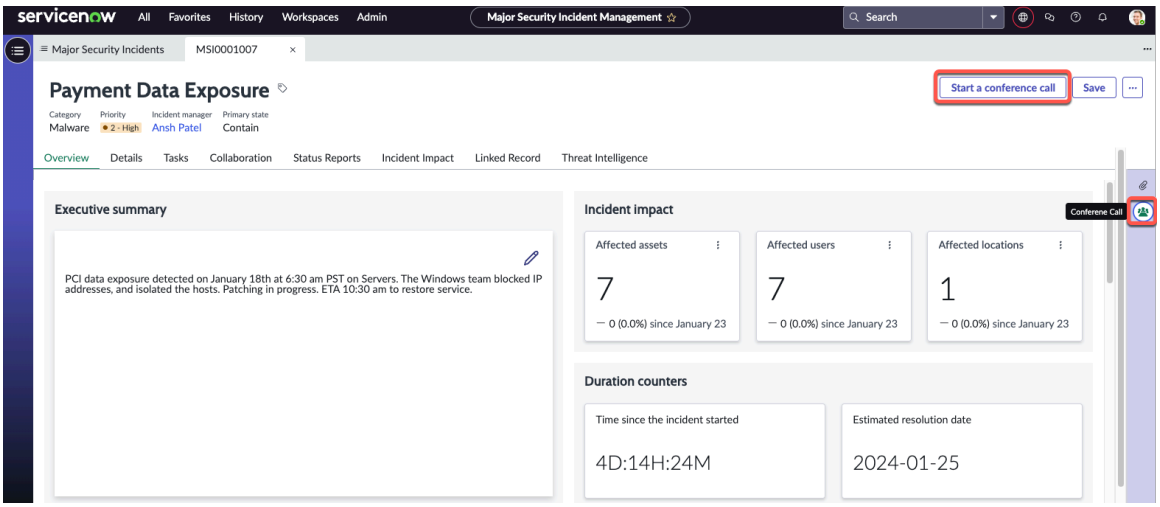
The call participants can include the following:

- Users who have been assigned specific responsibilities.
- Ad hoc or on-demand contacts
- Other third-party contacts

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select a major security incident.
3. Select the **Start a conference call** action.
4. You can also start a conference call by selecting the icon on the right-context menu and selecting the + icon.
   The Start conference call pop-up appears.

MSIM Conference call



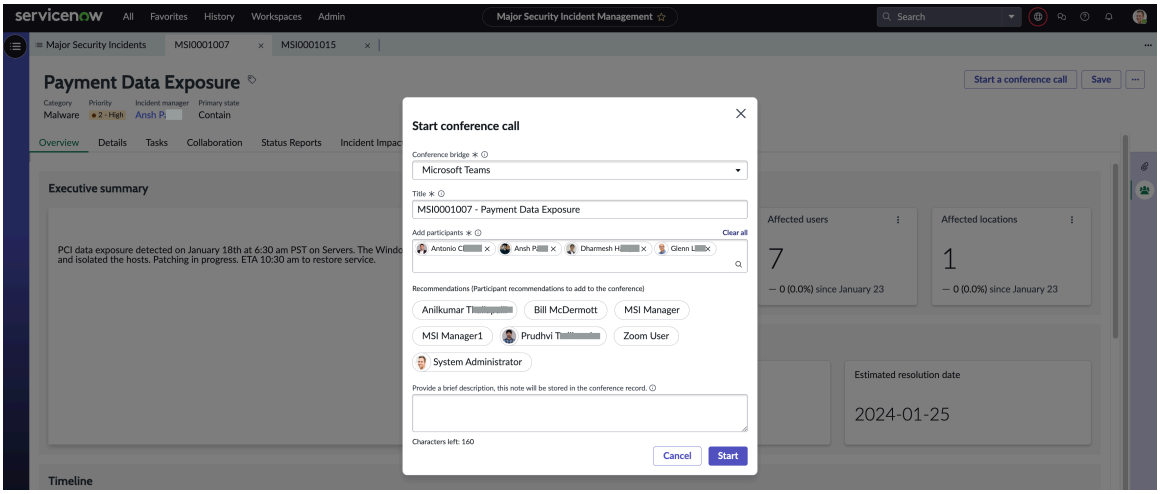
5. In the Conference bridge field, choose a **Conference bridge** that you want to connect from. For example, Microsoft Team, Zoom, or Cisco Webex.
6. In the Title field, provide a title that describes the reason for the conference call.
7. In the Add participants field, select the participants for the conference call.
   You can use the search option to find and add the required participants or select the participants from the **Recommendations** list, which provides participant recommendations to add to the conference call.

   The user (host) who initiates the conference call is automatically added to the list of selected participants. All the users associated with the major security incident are available by default under the **Recommendations** list.

   Note: Make sure the participants that you select have a valid email address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Start a conference call



8. After selecting the participants, provide a brief description of the reason for starting the conference call in the Description field.
   The description that you provide will be added to the conference record.
9. After the participant list is finalized, select **Start**.
   The conference call starts in the selected conference bridge. All the participants are notified through email, and they're also notified through the respective conference bridge that was selected.
10. Select the **Click here** option on top of the major security incident to join the conference call.
    The participants can use the link from the email notification or the notification from the selected conference bridge to join the call.
11. Open the associated major security incident to view the conference call details.
    When the final participant leaves the conference, the conference call ends or select **End call** to end the conference call.

Add participants to a conference call

Add participants to a conference call using the search option on the **Start conference call** pop-up to find and add the required participants. You can also add participants by selecting the participants from the Recommendations list, which provides participant recommendations to add to the conference call.

Before you begin

Role required: sn_msi.workspace_manager

About this task

The user (host) who initiates the conference call is automatically added to the list of selected participants. All the users associated with the major security incident are available by default under the Recommendations list.

The call participants can include the following:

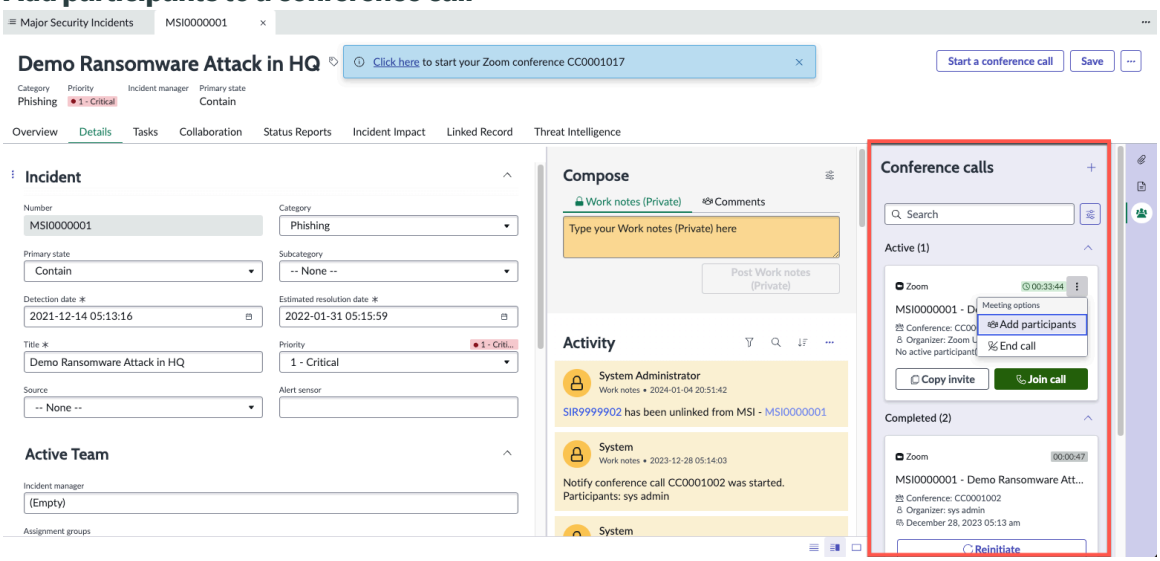
- Users who have been assigned specific responsibilities.
- Ad hoc or on-demand contacts
- Other third-party contacts

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select the major security incident that you're trying to resolve on the conference call.
3. Select the icon on the right-context menu to view the details of the conference calls. This includes details like conference bridge name, organizer name, date, time, duration of the call, active and inactive participants.
4. Select next to the active conference call and select the **Add Participants** option.

Add participants to a conference call



5. You can use the search option to find and add the required participants or select the participants from the **Recommendations** list, which provides participant recommendations to add to the conference call.
6. After selecting the participants, provide a brief description of the reason for starting the conference call in the Description field.
   All the participants are notified through email, and they're also notified through the respective conference bridge that was selected. The participants can use the link from the email notification or the notification from the selected conference bridge to join the call.
7. Alternatively, you can add participants by selecting the **Copy invite** option on the Conference calls section on the right-context menu, and you can share with the required participants.

Mute participants in a conference call

As an MSI manager or a conference call host, you have the option to mute a particular participant or all the participants on the conference call.

Before you begin

Role required: sn_msi.workspace_manager

Before starting this procedure, verify that there's an active conference call with one or more participants.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select the major security incident that you're trying to resolve on the conference call.
3. Select the  icon on the right-context menu to view the details of the conference calls.
4. Select **Join call** on the active conference bridge.
5. After joining the conference call, select a participant that you want to mute and select **Mute** on the conference bridge.
6. To mute all participants on the conference call, select **Participants** in the meeting controls and select **Mute All**.

View conference call details

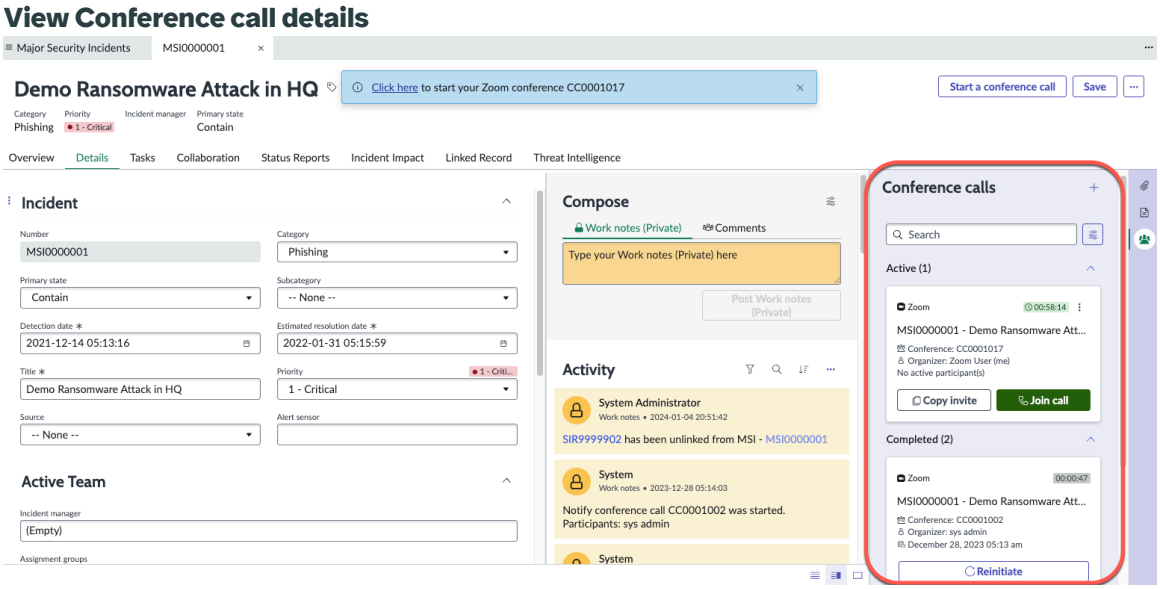
Conference calls are listed as system activities in the Activity section of the major security incident and also listed in the Conference calls related list. You can view details like Conference bridge name, organizer name, date, time, duration of the call, active and inactive participants.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select the major security incident that you're trying to resolve on the conference call.
3. Select the  icon on the right-context menu to view the details of the conference calls. This includes details like conference bridge name, organizer name, date, time, duration of the call, active and inactive participants.



4. You can use the search option to look for a particular conference call. There can be several calls for the same major security incident.
5. To add participants to a conference call, select next to the active call conference call and select the **Add Participants** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. You can also add participants by using the **Copy invite** option and sharing the link with the required participants.
7. To join a conference call, navigate to the Active section and select the **Join call** option of the required conference call.
8. To end a conference call, select ⋮ next to the active conference call and select the **End call** option.
9. To restart a conference call, navigate to the Completed section and select the **Reinitiate** option of the required conference call.

Integrate MSIM Conference Calls with Microsoft Teams

The Conference Call Microsoft Teams integration enables you to manage and initiate a Microsoft Teams conference call directly from a major security incident.

Key Features

- Start and end Microsoft Teams conference calls directly from major security incidents or a task from the major security workbench.
- Manage a Microsoft Teams conference call by adding or removing participants.

Prerequisites

Verify you've installed the following Integration Hub plugins on your ServiceNow instance.

- Notify plugin (com.snc.notify)
- Microsoft Teams Communications spoke plugin (sn_msteams_com_spk).
- Azure Active Directory User Mapping plugin (sn_now_azure).
- Notify UI Components for Configurable Workspaces

For more information, see Request IntegrationHub.

Configuration

- To configure the MSIM Conference Call Microsoft Teams integration using the pre-configured app, see Integrate Notify connector pre-published app with Microsoft Teams.
- To configure the MSIM Conference Call Microsoft Teams integration using the self-configured app, see Integrating Notify connector self-configured app with Microsoft Teams.

Use the MSIM Conference Call Microsoft Teams integration

The following steps give you a walkthrough of how you can manage and initiate a Microsoft Teams conference call directly from a major security incident.

Before you begin

Role required: sn_msi.workspace_manager

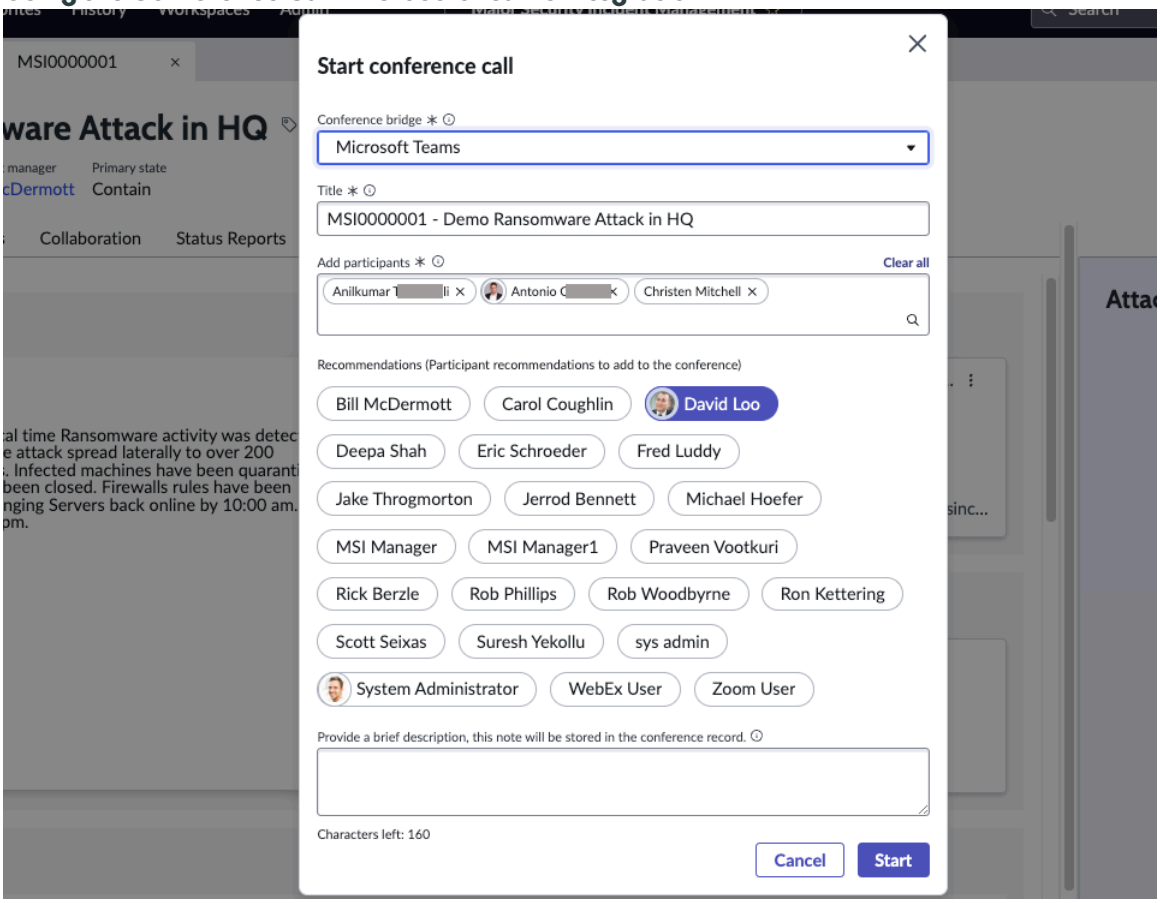
Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select a major security incident.
3. Select the **Start a conference call** action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. You can also start a conference call by selecting the  icon on the right-context menu and selecting the + icon.
   The Start conference call pop-up appears.
5. Choose **Microsoft Teams** as the conference bridge that you want to connect from.
6. In the Title field, provide a title that describes the reason for the Microsoft Teams conference call.

Using the Conference Call Microsoft Teams integration



7. In the Add participants field, select the participants for the Microsoft Teams conference call. You can use the search option to find and add the required participants or select the participants from the **Recommendations** list, which provides participant recommendations to add to the Microsoft Teams conference call.

   The user (host) who initiates the Microsoft Teams conference call is automatically added to the list of selected participants. All the users associated with the major security incident are available by default under the **Recommendations** list.

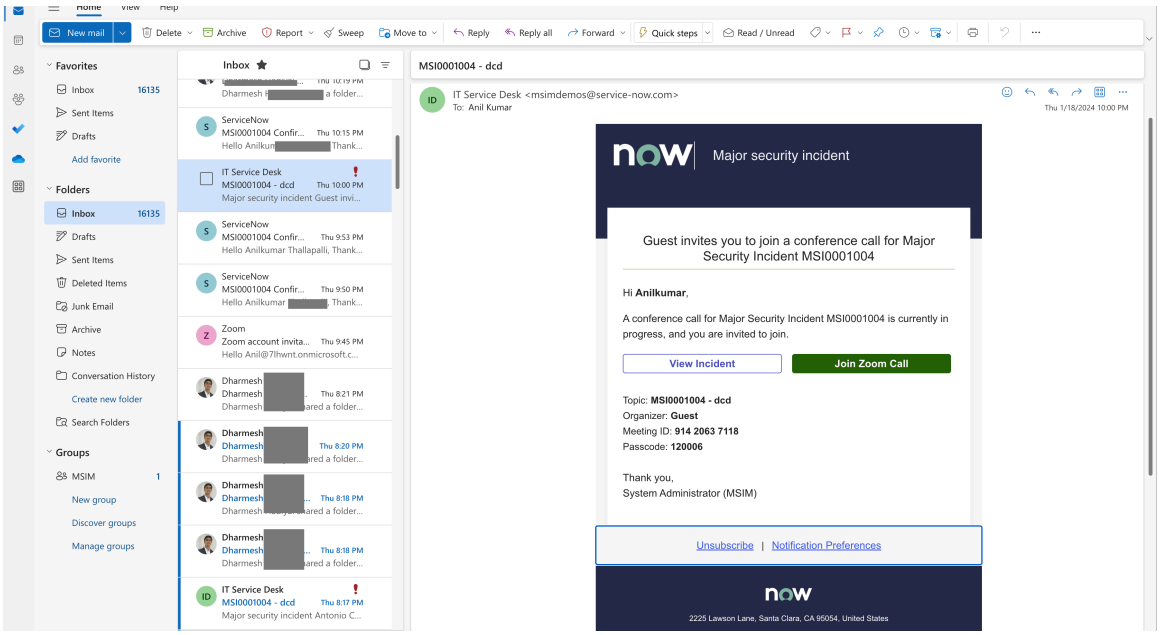
   Note: Make sure the participants that you select have a valid email address.

8. After selecting the participants, provide a brief description of the reason for starting the conference call in the Description field.
   The description that you provide will be added to the conference record.
9. After the participant list is finalized, select **Start**.
   The conference call starts in the Microsoft Teams app. All the participants are notified through an email from the MSIM app and the other notification is sent through a bot on the Microsoft Teams app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Select the **Click here** option on top of the major security incident to join the conference call on the Microsoft Teams app.
    The participants can use the link from the MSIM email notification or the notification from the Microsoft Teams app to join the call.

Email notification



11. Open the associated major security incident in the MSIM workspace to view the conference call details.

    When the final participant leaves the call, the conference call ends or select **End call** in the Conference call section to end the conference call.

Integrate MSIM Conference Calls with Zoom

The Conference Call Zoom integration enables you to manage and initiate a Zoom conference call directly from a major security incident.

Key Features

- Start and end Zoom meetings directly from any task record such as a major security incident, or a change or even from the major incident workbench.
- Manage Zoom meetings by adding or removing participants.
- Track and report meeting details such as meeting duration and attendees for further analysis.

Prerequisites

Verify you've installed the following Integration Hub plugins on your ServiceNow instance.

- Notify plugin (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify UI Components for Configurable Workspaces

For more information, see Request IntegrationHub.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration

To configure the MSIM Conference Call Zoom integration using the Notify communication channel, see Configure Notify Zoom connector in Notify.

Use the MSIM Conference Call Zoom integration

The following steps give you a walkthrough of how you can manage and initiate a Zoom conference call directly from a major security incident.

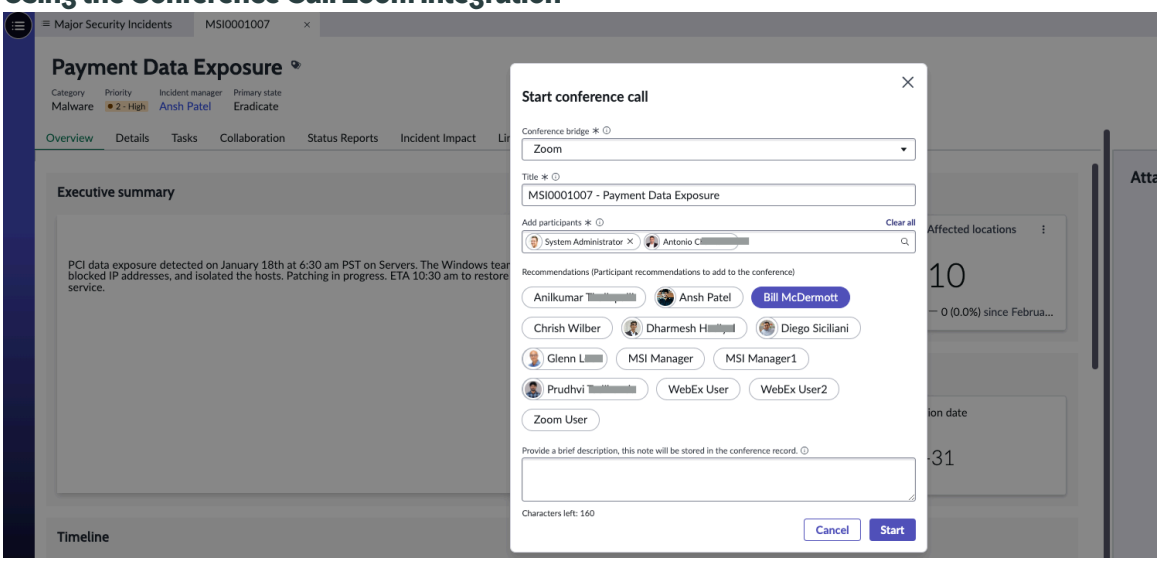
Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select a major security incident.
3. Click the **Start a conference call** action.
4. You can also start a conference call by clicking the  icon on the right-context menu and selecting the + icon.
   The Start conference call pop-up appears.
5. Choose **Zoom** as the conference bridge that you want to connect from.
6. In the Title field, provide a title that describes the reason for the Zoom conference call.

Using the Conference Call Zoom integration



7. In the Add participants field, select the participants for the Zoom conference call.
   You can use the search option to find and add the required participants or select the participants from the **Recommendations** list, which provides participant recommendations to add to the Zoom conference call.

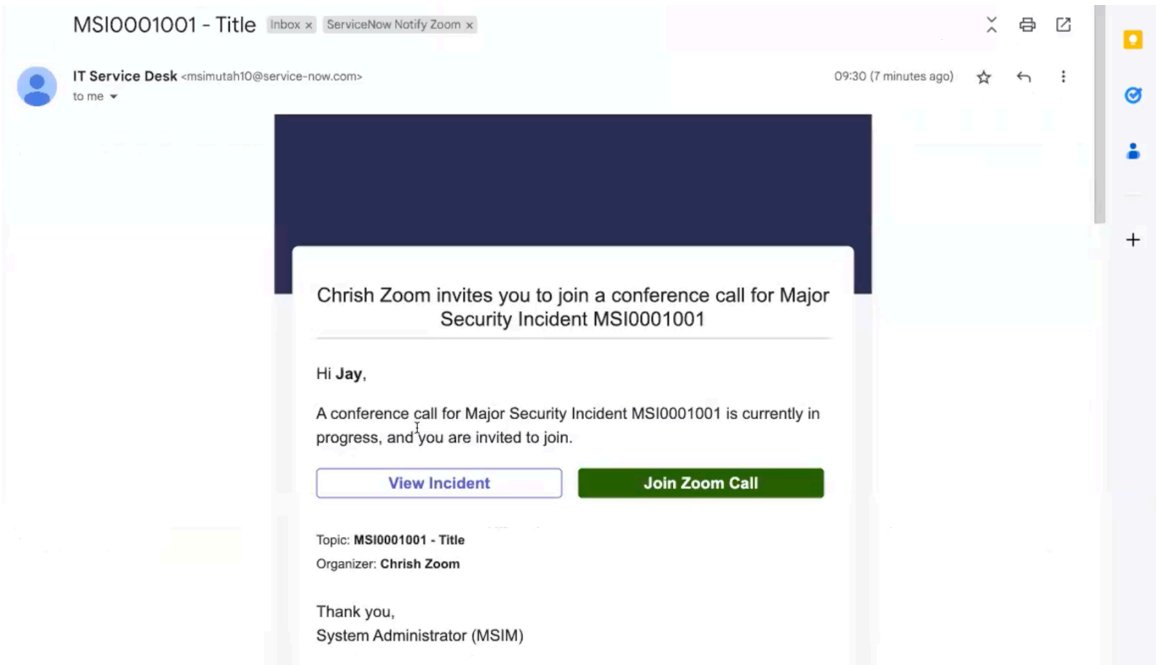
   The user (host) who initiates the Zoom conference call is automatically added to the list of selected participants. All the users associated with the major security incident are available by default under the **Recommendations** list.

   Note: Make sure the participants that you select have a valid email address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. After selecting the participants, provide a brief description of the reason for starting the conference call in the Description field.
   The description that you provide will be added to the conference record.
9. After the participant list is finalized, click **Start**.
   The conference call starts in the Zoom app. All the participants are notified through two emails, one email is sent to the participants from the MSIM app and the other email is sent from the Zoom conference bridge.
10. Select the **Click here** option on top of the major security incident to join the conference call on the Zoom app.
    The participants can use the link from the MSIM email notification or the notification from the Zoom app to join the call.

Email notification



11. Open the associated major security incident in the MSIM workspace to view the conference call details.

    When the final participant leaves the call, the conference call ends or select **End call** in the Conference call section to end the conference call.

    If the conference call was recorded, then the recording will be available in the Conference call section of the associated major security incident after sometime.

Integrate MSIM Conference Calls with Cisco Webex

The MSIM Conference Call Cisco Webex integration enables you to manage and initiate a Cisco Webex conference call directly from a major security incident.

Key Features

- Start and end Cisco Webex meetings directly from major security incidents.
- Manage a Cisco Webex meeting by adding or removing participants.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prerequisites

Verify you've installed the following Integration Hub plugins on your ServiceNow instance.

- Notify plugin (com.snc.notify)
- Notify Cisco Webex Connector (sn_notify_webex)
- Cisco Webex Teams Spoke (sn_cisco_teams_spk)
- Notify UI Components for Configurable Workspaces

For more information, see Request IntegrationHub.

Configuration

To configure the MSIM Conference Call Cisco Webex integration using the Notify communication channel, see Configure Notify Cisco Webex Connector.

Use the Conference Calls Cisco Webex integration

The following steps give you a walkthrough of how you can manage and initiate a Cisco Webex conference call directly from a major security incident.

Before you begin

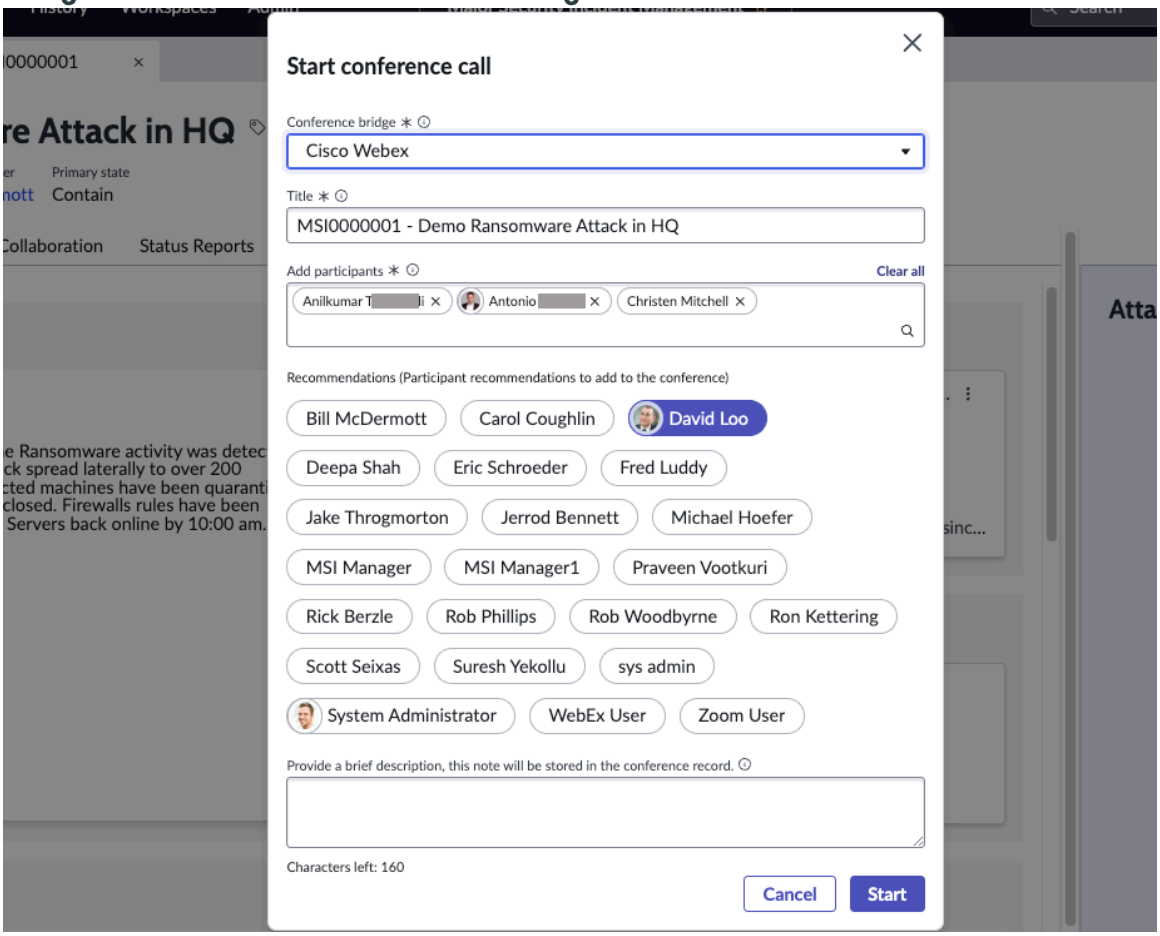
Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management**.
2. From the Major Security Incident list, select a major security incident.
3. Select the **Start a conference call** action.
4. You can also start a conference call by selecting the  icon on the right-context menu and selecting the + icon.
   The Start conference call pop-up appears.
5. Choose **Cisco Webex** as the conference bridge that you want to connect from.
6. In the Title field, provide a title that describes the reason for the Cisco Webex conference call.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the Conference Call Cisco Webex integration



7. In the Add participants field, select the participants for the Cisco Webex conference call.
   You can use the search option to find and add the required participants or select the participants from the **Recommendations** list, which provides participant recommendations to add to the Cisco Webex conference call.

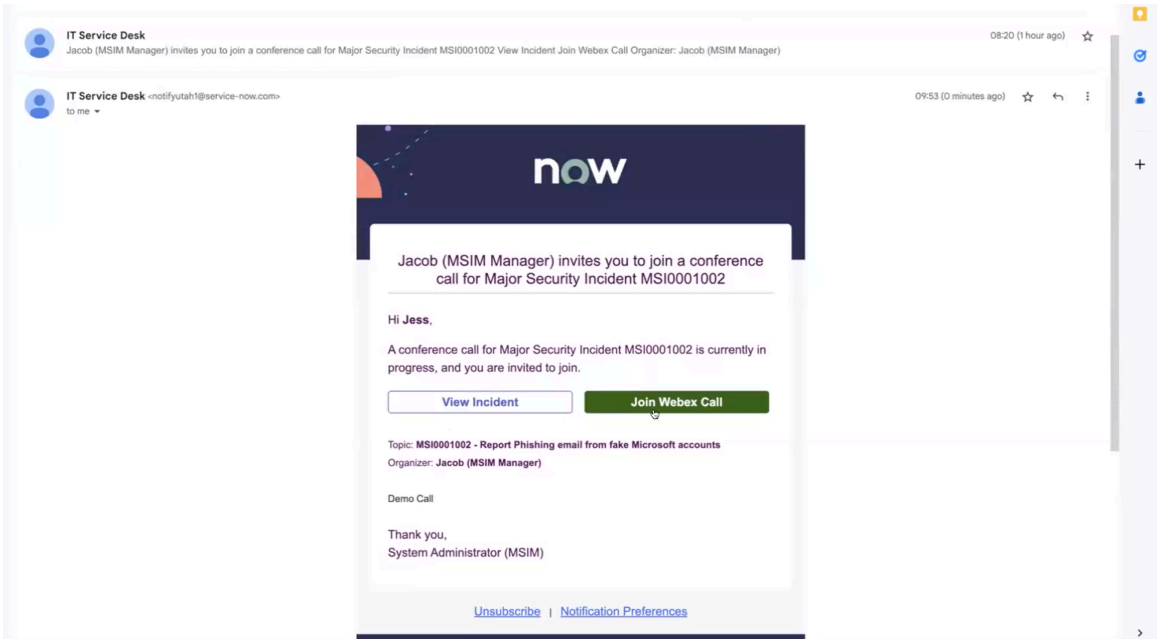
   The user (host) who initiates the Cisco Webex conference call is automatically added to the list of selected participants. All the users associated with the major security incident are available by default under the **Recommendations** list.

   Note: Make sure the participants that you select have a valid email address.

8. After selecting the participants, provide a brief description of the reason for starting the conference call in the Description field.
   The description that you provide will be added to the conference record.
9. After the participant list is finalized, select **Start**.
   The conference call starts in the Cisco Webex app. All the participants are notified through two emails, one email is sent to the participants from the MSIM app and the other email is sent from the Cisco Webex conference bridge.
10. Select the **Click here** option on top of the major security incident to join the conference call on the Cisco Webex app.
    The participants can use the link from the MSIM email notification or the notification from the Cisco Webex app to join the call.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Email notification



11. Open the associated major security incident in the MSIM workspace to view the conference call details.

    When the final participant leaves the call, the conference call ends or select **End call** in the Conference call section to end the conference call.

    If the conference call was recorded, then the recording will be available in the Conference call section of the associated major security incident after sometime.

Configuring Major Security Incident Management

Install and configure Major Security Incident Management application.

Important:

- To get quickly started with Major Security Incident Management configuration, you can refer to the Major Security Incident Management (MSIM) Quick Start Guide on the ServiceNow Store.
- After installing the Major Security Incident Management app, ensure that you import the update set in KB1289784 to load the partially pre-configured files.

Use this section to learn how to set up the necessary configurations required to work with Major Security Incident records by integrating with other external Microsoft applications to establish connections with ServiceNow instance.

Configure File Explorer Component

The File Explorer workspace component organizes and tracks the collection of artifacts (files) related to a major security incident. It is designed to support integration with any third-party file hosting provider such as Microsoft SharePoint in the Major Security Incident Management workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- File Explorer Component: Provides a graphical user interface to display the file system and allows the users to perform file operations.
- File Explorer Core: Provides an abstraction layer that allows the File Explorer component to display the file system and perform various file operations without knowing anything about the underlying connector that is used to communicate with external repositories.
- File Explorer Microsoft SharePoint Connector application: Provides the implementation modules required to track and fetch files/folder metadata from a Microsoft SharePoint document library and perform file operations.

The File Explorer Core component provides a base infrastructure required for the different file sharing connector applications to define its connection properties.

You must install and configure the file repository drive and file repository provider by adding the connection properties to pull the files metadata from a file hosting provider location.

For this current version of the File Explorer, these instructions include configuring and subscribing to a retrieving file metadata such as Microsoft SharePoint file and folder updates, file operations, and logging file activity. A designated Microsoft SharePoint document library and related drive configuration will be required to create individual folders that are specific to a major security incident.

File Explorer also allows connector applications such as Microsoft SharePoint. You can use this example to configure its file operation implementations such as **Download** or **Rename** folder and file actions will be enabled in the File Explorer workspace component. These actions are enabled and executed using the integrated flow designer sub flows. For more information, see Folder and File Action Settings.

File Explorer configuration includes the following setup:

- Configure File Explorer Repository Drive
- Configure Folder and File Action Settings
- Create Folder Templates

Get Started with File Explorer

Review the following information before you start working with File Explorer Component.

Review the following information before you start establishing the connection with Microsoft SharePoint, creating folder and file actions, and creating folder templates for the file explorer component.

Prerequisites

Name	Description
Microsoft SharePoint spoke, version 2.0.2 for ServiceNow® IntegrationHub.	Use **sn_sp_spoke** plugin ID to search and install Microsoft SharePoint spoke. Installing this plugin provides flows and actions to automate collaboration, document management, and user access rights in Microsoft SharePoint.
File Explorer Component v1.1.0	Use **sn_file_explorer** plugin ID to search and install File Explorer Component v1.1.0

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Prerequisites (continued)

Name	Description
	Installing this plugin provides a graphical user interface to browse the file system, which is available in the file explorer core.
File Explorer Core for Security Operations v1.1.1	Use **sn_fe** plugin ID to search and install File Explorer Core. Installing this plugin provides base infrastructure to integrate with any third-party file hosting provider.
Microsoft SharePoint File Explorer Connector for Security Operations v1.1.1	Use **sn_fe_sharepoint** plugin ID to search and install Microsoft SharePoint File Explorer Connector. Installing this plugin will manage the Microsoft SharePoint Files/Folders using File Explorer.

Configure File Explorer Repository Drive

The Microsoft SharePoint connector provides various capabilities to be implemented in Microsoft SharePoint File Explorer features by managing and tracking the file metadata.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Major Security Incident** > **File Explorer** > **File Repository Configuration**.
2. Fill the following fields as described in the following table:

Field Name	Field Description
Name	Name of the file repository record that identifies the usage. For example, MSIM.
Provider	Name of the provider that is the third-party file hosting repository provider. For example,Microsoft SharePoint.
Properties	
Site URL Path	Enter a Microsoft SharePoint URL with a specific site path. Provide only the relative path to the site and a complete site URL may not be required. For example, Sites/MSIM.
Document Library Name	Create a document library under the Microsoft SharePoint site and provide the same document library name here.

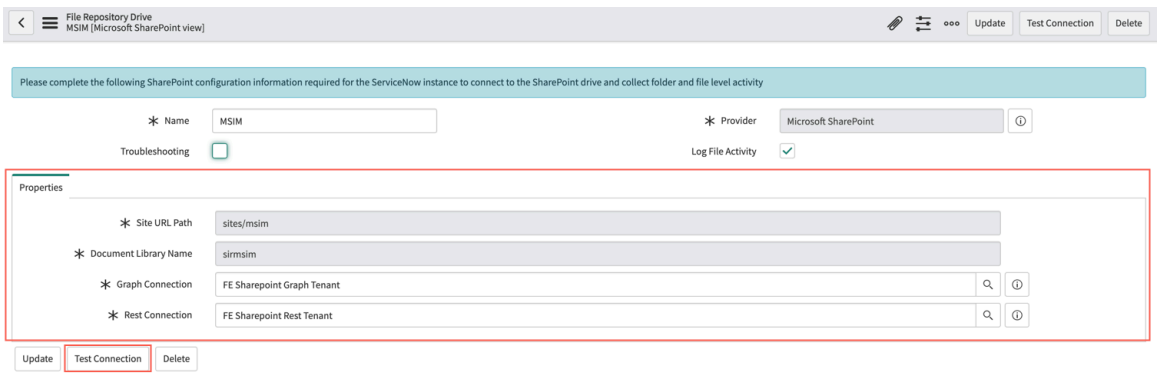
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Field Description
	This would be the same document library that you created in the Microsoft SharePoint Connector Drive setup.
Graph Connection	Select the File Explorer Graph tenant record. For more information on the tenant connection configuration, see Microsoft SharePoint spoke.
Rest Connection	Select the File Explorer REST tenant record. For more information on the tenant connection configuration, see Microsoft SharePoint spoke.

3. Select **Save**.
4. Click **Test Connection** tab to test the connection and validate the file repository drive configuration properties.

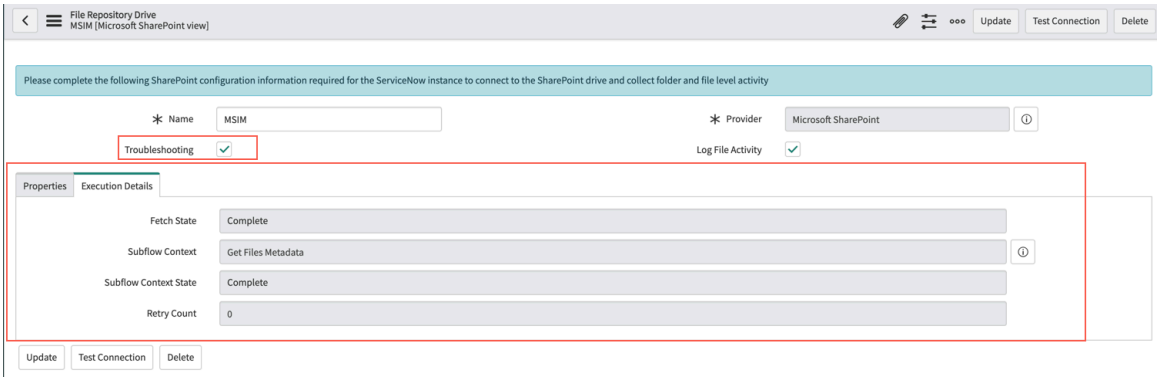
   Note: Before **Activating** the file repository, make sure that the corresponding document library at Microsoft SharePoint doesn't have any folder or file data.

5. Click **Activate** to activate the file repository.



6. Select the **Troubleshooting** check box to verify the file repository **Execution Details** and verify the **Fetch State** is complete and make sure that the Microsoft SharePoint Drive Subscriptions is created and state is complete.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: Using the **Test Connection** button, either MSI Administrator or MSI Manager can only validate the file repository configuration.

Configure Folder and File Action Settings

Configure the folder and file actions you would like to be enabled from the File Explorer component on the Major Security Incident Management workspace, using the Folder and File Action Settings setup page. As an MSI Administrator, you can control the individual Folder and File Actions displayed on the File Explorer Component.

Before you begin

Following are the implemented file operations capabilities in the file explorer component using the ServiceNow® flow designer:

File Operations Capabilities

File Operation	Description
Open in Microsoft SharePoint	Opens new browser tab to display Microsoft SharePoint document library file view
Create Folder	Ability to create additional ad hoc folders after the major security incident is created.
Rename Folder	Ability to rename the folders created.
Move File	Allows you to move files between folders in File Explorer component of workspace, resulting in movement of files in Microsoft SharePoint
Locate File	Shows folder location when using the **Recents** view of the File Explorer.
Delete File	Delete the file.
Delete Folder	Delete the folder.
Download File	Downloads the file within the existing MSIM Workspace browser tab for quick viewing.
Rename File	Renames the file.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

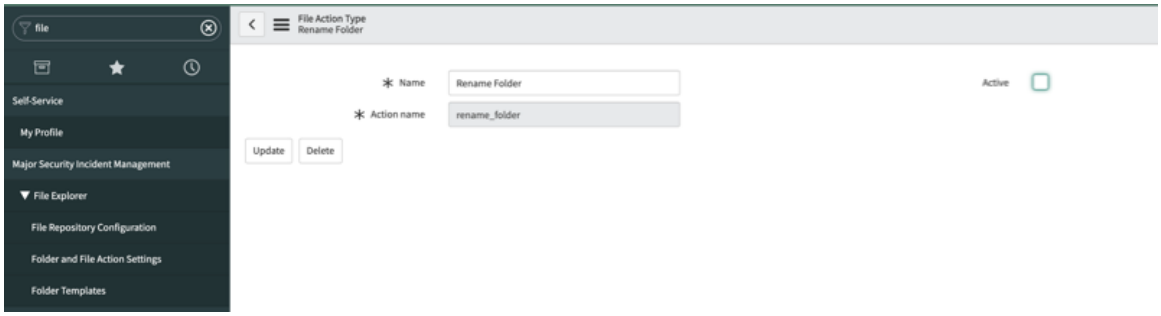
1. All actions listed are currently enabled by default. You will need to edit the **File Action Settings** if you do not want certain actions to appear. All the settings are currently global for all users, which means no ability to enable actions for a subset of the users that have a specific role.
2. **Revoke User Access** and **Add Permissions** actions are system related actions. It is recommended not to modify these file actions.

The following sample procedure describes one of the file operations capabilities to disable any specific folder and file action during the configuration of the File Explorer Repository. This procedure is applicable to all other actions that may need to be edited:

Role required: sn_msi.workspace_admin

Procedure

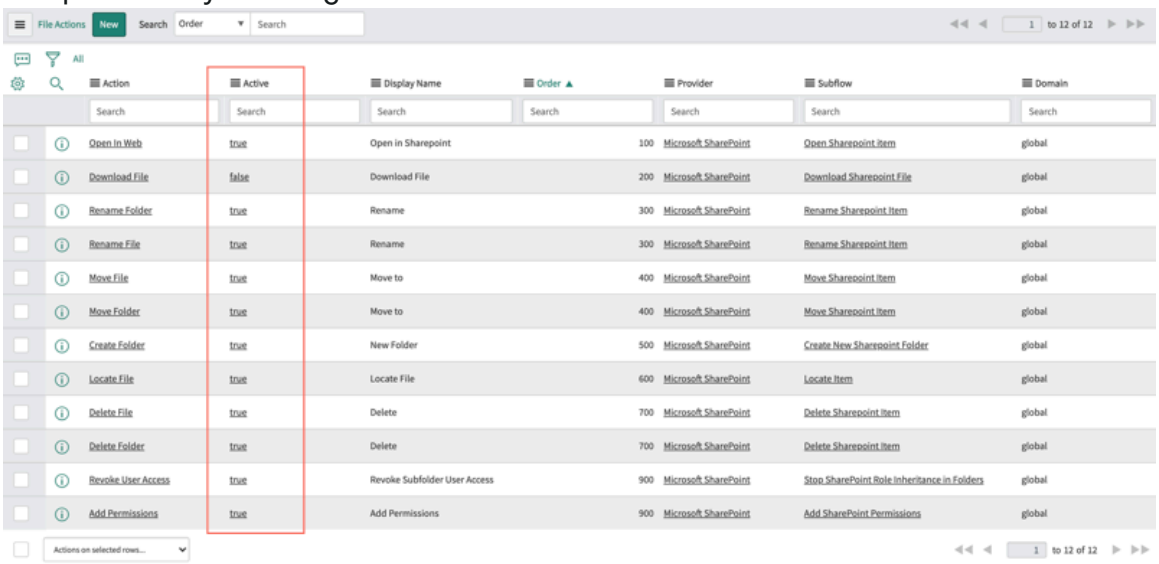
1. Navigate to **Major Security Incident Management** > **File Explorer** > **Folder and File Action Settings**.
2. Select the desired record to enable or disable the folder or file action respectively.
3. Deselect the **Active** check box to disable the folder and file action.



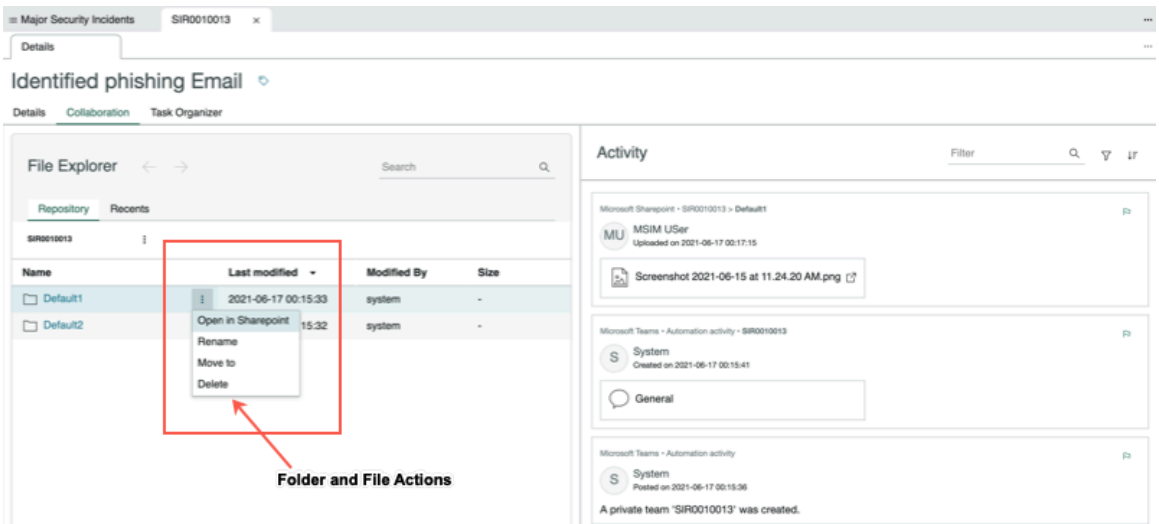
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. **Update** the drive record.

Note: You can also perform the file action directly from the list of displayed file operations by choosing the **Active** column values to either True or False.



If the file action performed is disabled then the action will not be displayed on the **Collaborations** tab of the **Major Security Incident Management** workspace.



Create Folder Templates

Use Folder Templates to automatically create unique folders for different Major Security Incident types. The folder templates within the File Explorer Component are used to create a base folder structure for the security incident in the Microsoft SharePoint.

Before you begin

As an MSI Administrator, you define the initial folder structure necessary to allow collaboration across different incident responder groups and assign appropriate access privileges at a sub folder level. Multiple configurations can be created for different Major Security Incident types using a condition builder for specific Major Security Incident field values, which includes allowing access to different users and user groups at each sub folder level.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: These folder templates are used by all major security incidents that meet the conditions specified in the condition builder. It is recommended that you consider using incident field variables, such as the incident number or category, to create unique root folder names that distinguish one set of subfolders with common folder names for one major security incident from similar folders with these names that are part of a different major security incident.

The defined Folder Templates configuration is applied to the major security incident only when the condition is matched.

Note: A base system configuration (without any sub folders), is applied to all the security incidents. You may either edit this default configuration to include specific subfolders or create a new configuration based on a specified set of major security incident field values. For example, category = malicious code activity.

Role required: sn_msi.workspace_admin

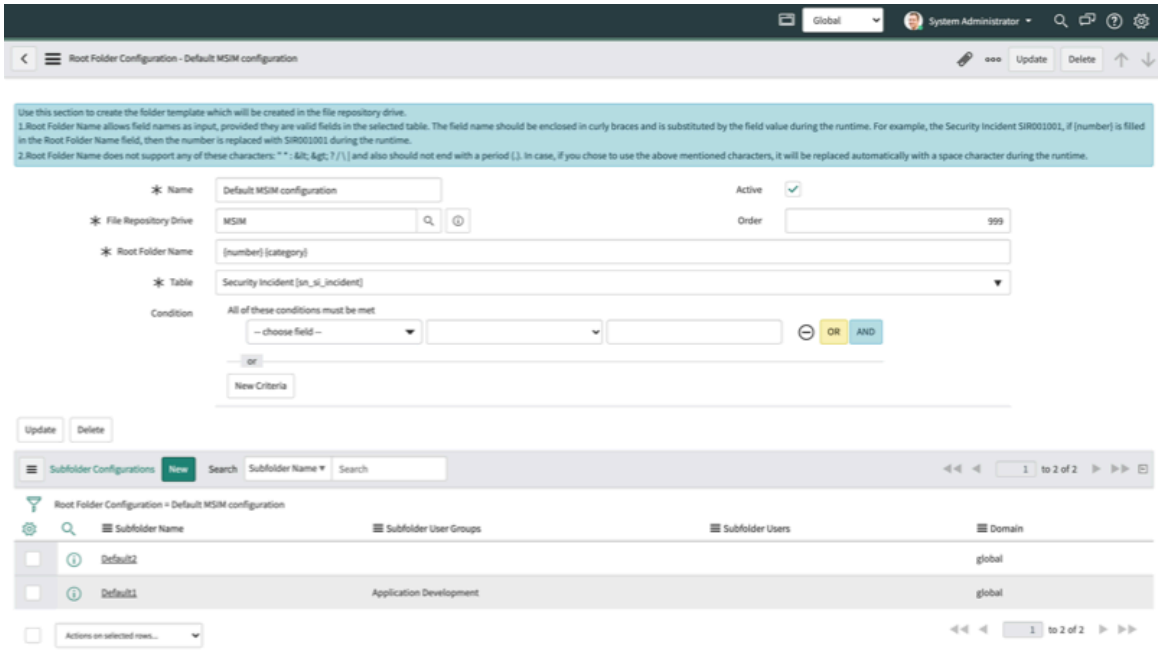
Procedure

1. Navigate to **All** > **Major Security Incident Management** > **File Explorer** > **Folder Templates**.
2. Click **New** for Root Folder Configuration.
3. On the form, fill the fields.

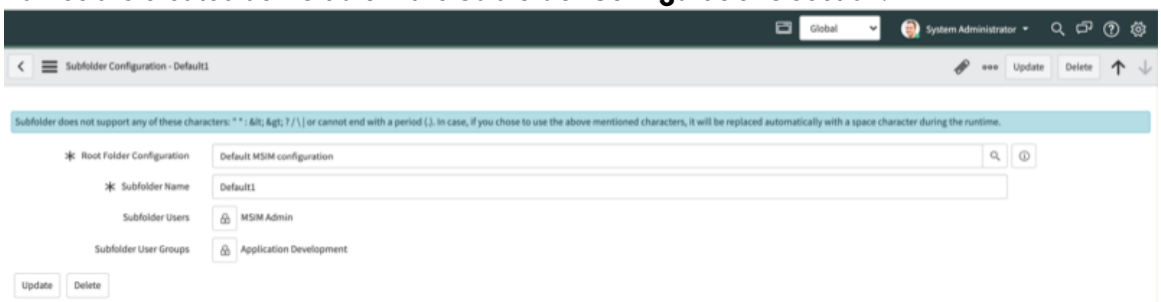
Field Name	Description
Name	Name of the folder template.
File Repository Drive	
Root Folder Name	Name of the Root Folder which will appear in Microsoft SharePoint as well as the File Explorer and should probably include incident field variables such as the major security incident number and category so that one major security incident can be distinguished from another one.
Table	

4. Define the security incident **Condition** values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. **Update** the record.
   The sub folders are created with the defined values.
6. Click the desired **Sub folder**.
   If you don't create a sub folder with an appropriate name then the sub folders names are created as **Default** in the **Subfolder Configurations** section.



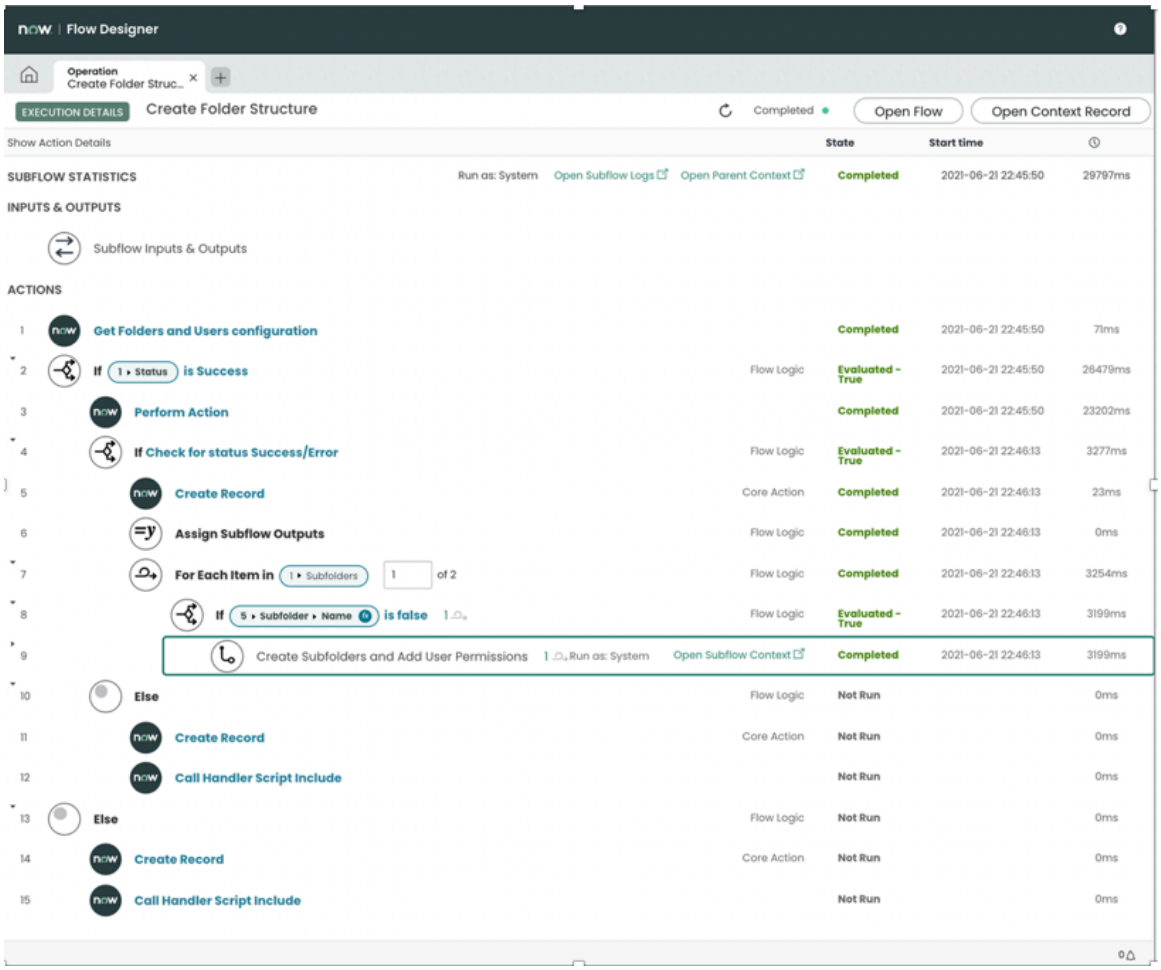
The same folder structure will be created automatically in the Microsoft SharePoint using the same access privileges that are configured on the **Folder Templates** page.

Note:

- **Root Folder Name** allows field variable names as input, provided they are valid fields in the selected table. The field name must be enclosed in curly braces and is substituted by the field value during the flow execution runtime. For example, the Security Incident SIR001001, if {number} variable is configured in the **Root Folder Name** field, then the number is replaced with SIR001001 during the runtime.
- **Root Folder Name** does not support any of these characters: " * : < > ? / \ | and also, should not end with a period (.). If you use the above mentioned characters, they will be replaced automatically with a space character during the runtime.
- If the **Root Folder** and **Sub folder** name exceeds the defined limit (256 characters) then the folder name is truncated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Following is the run time execution of Create Folder Structure subflow:



File Explorer Activity Stream in Workspace

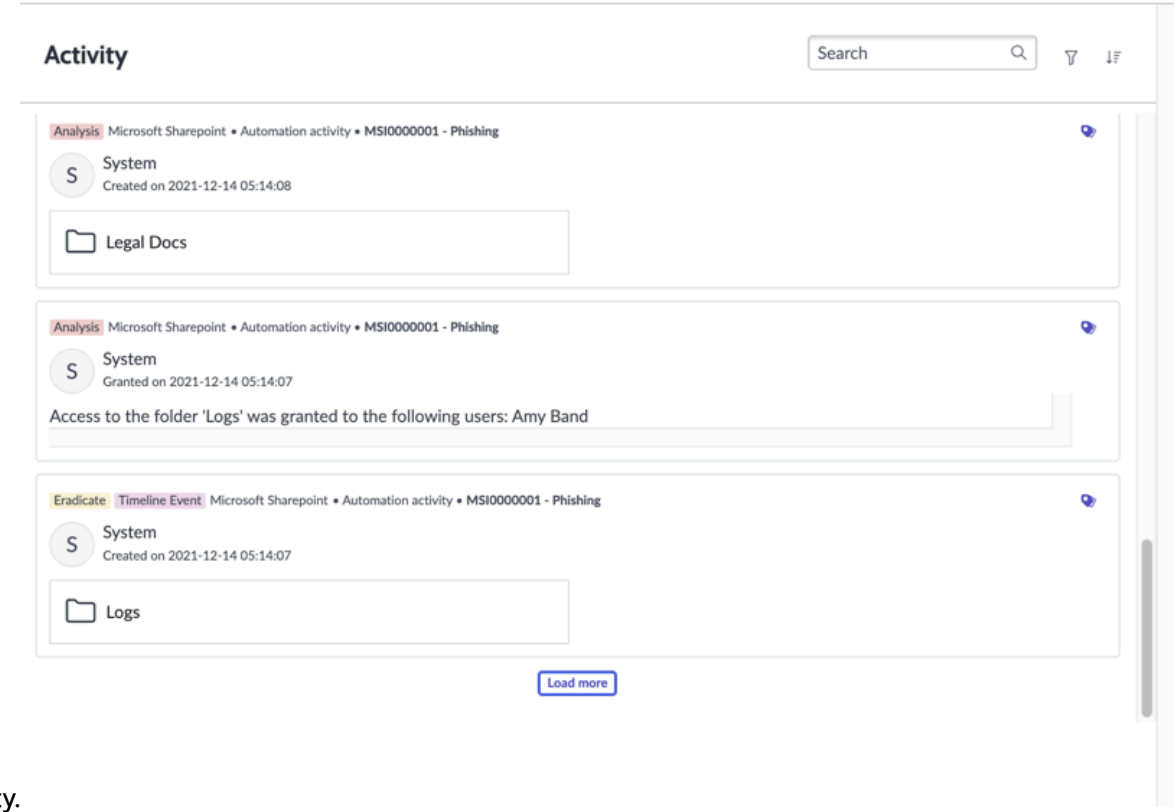
Use the File Explorer section from the Major Security Incident Management workspace to display the folders and files, the sequence those were created in Microsoft SharePoint document library.

The activity stream lists all the automation activity postings whenever any folder and file activity, or logs that occur during the Major Security Incident resolution. The activity stream structure is aligned in the same format of the Microsoft SharePoint library which shows the folders that were created and which users or user groups were assigned to those folders.

Activity Stream enables the workspace mangers and other user or user group(s) to communicate and collaborate effectively, list down the activities that were performed on Microsoft SharePoint folders and files, monitor the status of the incident, post the notes or add additional comments they have on the incident

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

record. The workspace mangers can pick up and work based on the last updated



activity.

File Explorer troubleshooting

The troubleshooting section can help you resolve some of the technical issues that you may encounter when setting up File Explorer component.

Refer to the following section on the scheduled jobs, system properties, and File Explorer flow designer subflows in detail.

Scheduled jobs for File Explorer

Scheduled Jobs are automated jobs that are run to process the notifications from Microsoft SharePoint, ingest the files metadata into ServiceNow instance and renew the file repository subscriptions on a recurring schedule.

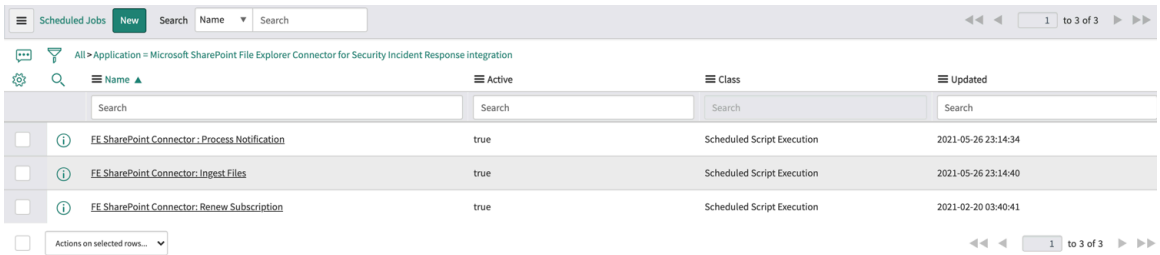
Scheduled Jobs are automated jobs which are run in the background to:

- process the notifications from Microsoft Microsoft SharePoint.
- ingest the files metadata into ServiceNow AI Platform instance.
- renew the subscription with Microsoft SharePoint document library to receive notifications.

Job	Description
Microsoft SharePoint File Explorer Connector: Process Notification	Runs every 30 seconds and responsible for reading the notifications which indicates any change occurred on the subscribed document library and marks the state of drives (sn_fe_file_repo_drive) as pending.
Microsoft SharePoint File Explorer Connector: Ingest Files	Runs every 30 seconds and primarily responsible for processing the drives (sn_fe_file_repo_drive) which are in pending

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Job	Description
	state and pulls the delta file changes from the configured Microsoft SharePoint document library since the last pull.
Microsoft SharePoint File Explorer: Renew Subscription	Runs every 10mins and responsible for renewing the Microsoft SharePoint document library subscription a day before its expiry date. Usually, these subscriptions expire in 30 days.



Available File Explorer system properties

Following are the available Microsoft SharePoint File Explorer connector system properties.

System properties

Property Name	Description
sn_fe_sharepoint.max_retry_count	Controls the frequency of attempts that Microsoft SharePoint connector application tried to pull the failed drive or renew the failed subscription. The default frequency value is set to 50.
sn_fe_sharepoint.retry_after_seconds	Time interval between each attempt to pull the failed drive or renew the subscription. The default value is set to 900 sec or 15 mins.
sn_fe_sharepoint.max_subscription_expiration_time	Maximum subscription expiry period in number of days for Microsoft SharePoint. The default expiry period is set to 30 days.

File Explorer Flow Designer Subflows

Following are the Flow Designer subflows which are installed with Microsoft SharePoint File Explorer connector.

Subflows

Name	Description
Add Microsoft SharePoint Permissions	Grants edit permission for a specific folder to specific users.
Create Drive Subscription	Subscribes with a configured Microsoft SharePoint document library to receive notifications about any updates occurs on the document library.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Subflows (continued)

Name	Description
Create New Microsoft SharePoint Folder	Creates a new Microsoft SharePoint folder under a given parent folder.
Delete Microsoft SharePoint Item	Deletes Microsoft SharePoint files and folders.
Download Microsoft SharePoint File	Returns the download URL of Microsoft SharePoint files
Get Files Metadata	Subscribes and pulls the changes from Microsoft SharePoint document library.
Move Microsoft SharePoint Item	Moves the Microsoft SharePoint files/folders to the destination folder
Open Microsoft SharePoint Item	Returns the web URL of Microsoft SharePoint file/folder to open in a browser.
Renew Drive Subscription	Renews the subscription with Microsoft SharePoint document library.
Create Folder Structure	Follows the folder template configurations and creates the folder structure on Microsoft SharePoint document library.

Configure Microsoft Teams

Easily integrate and collaborate with Microsoft Teams to resolve Major Security Incident to view and filter collaboration chat activities.

Configuring and subscribing to a Microsoft Teams chat environment, retrieving chat conversations from within specified channels, and archiving the Team and associated channels are included as part of the incident closure process. A designated Microsoft Teams environment and related Microsoft Teams Graph API configuration is required to create individual channels that are specific to a Major Security Incident.

To configure Microsoft Teams, activate Teams as the chat provider. You can then create chat channels for the various stakeholders and groups communicating about activities and track chat conversations to resolve the Major Security Incident. The Microsoft Teams and Microsoft Graph API configuration includes:

- Establish MS Teams Graph connection on ServiceNow AI Platform
- Activate MS Teams as a chat provider
- Create a chat channel template
- View Chat Message Activity

Get started with Microsoft Teams

Review the following information before you start working with Microsoft Teams as a connector application.

Make sure that the following plugins are installed, before you start establishing, activating, and validating Microsoft Teams set up connections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required plugins

Name	Description
Chat integration with Security Incident Management	Use **sn_chat_collab_core** plugin ID to search and install Microsoft Teams Chat. Installing this plugin allows you to track the chat activity for third-party applications such as Microsoft Teams (or Slack and other third-party chat applications).
Microsoft Teams Chat Connector for Security Incident Management	Use **sn_ms_teams_connector** plugin ID to search and install Microsoft Teams Chat Connector for Major Security Incident Management. Installing this plugin allows you to track the chat activities using the collaboration component specific to Microsoft Teams.
Microsoft Teams Graph spoke	Installing this plugin establishes a Graph spoke connection with Microsoft Teams. For more information, see Microsoft Teams Graph spoke

Activate MS Teams as a chat provider

Activate Microsoft Teams by validating the Microsoft Teams Connection.

Before you begin

Role required: sn_msi.workspace_admin

Once the connection is activated and validated, an information message is displayed that the Provider connection is validated successfully. You can modify the channel configuration by adding and removing users, and possibly adding more channels or renaming existing channels.

Procedure

1. Navigate to **Major Security Incident Management** > **Chat Provider Configuration**.
2. Select **Microsoft Teams record**.
3. Click **Validate Connection**.
   A confirmation message displays that, Provider connection is validated successfully.
4. Select **Active** check box to activate the provider record.
   A confirmation message displays that the provider connection is validated successfully.
5. **Save** the form after you activate the chat provider configuration.
   With this connection between Microsoft Teams and ServiceNow AI Platform Instance is successfully established.

Create a chat channel template

Configure Chat Teams and Channel Templates to create chat teams and channels to collaborate, track the chat conversations, and add users and user groups to those Chat Channels. These Channel templates are created in the Microsoft Teams when a major security incident is promoted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_msi.workspace_admin

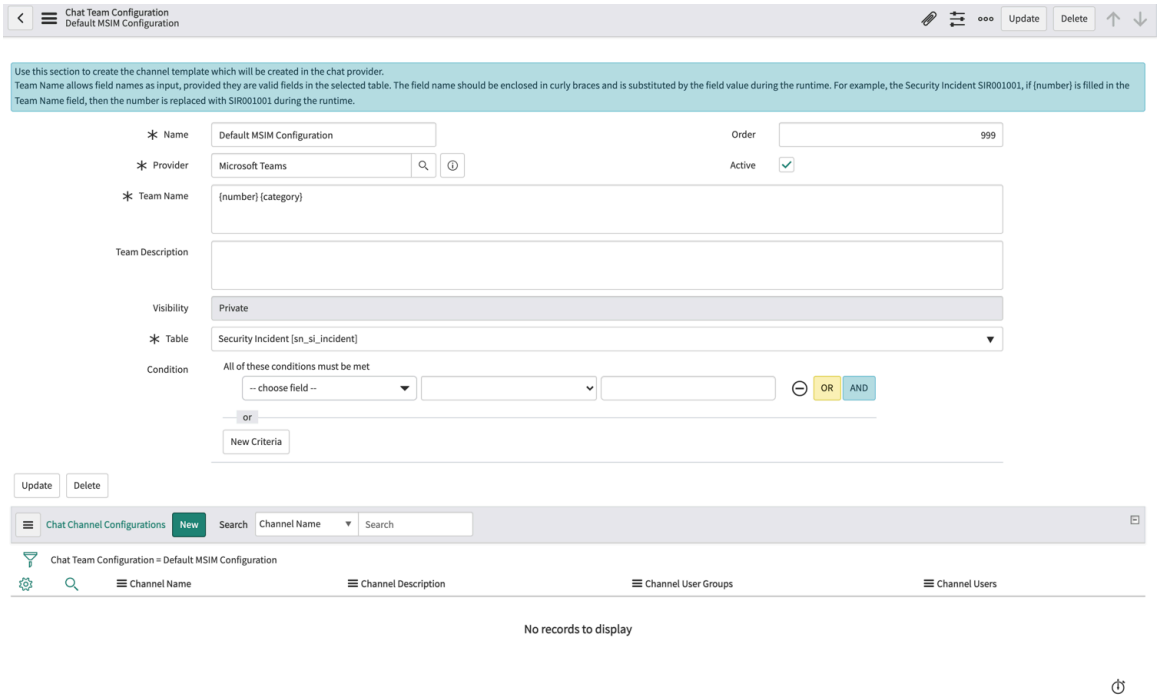
Procedure

1. Navigate to **Major Security Incident Management** > **Chat Channel** > **Channel Templates**.
2. On the Chat Channel Configuration form, click **New** in the form header.
3. On the form, fill in the fields.

Chat Team Configuration form

Field	Description
Name	Name of the folder.
Provider	Microsoft Teams.
Team Name	Name for the team, for example in the format, {number}-{category}. **Note:** The team name provided here will be used across all Major Security Incident records. To ensure that the actual Microsoft Team Name is displayed in MS Teams application and has a unique name value for different Major Security Incidents, it is recommended that you use an incident field value which is unique such as the incident number - {number}. As shown in the screen shot example, the {number} followed by a separator '-' and the {category} field variable would provide a unique number and description of the major security incident that Microsoft Teams is created for, for example {number} - {category}.
Team Description	Optional description of the team.
Table	Major Security Incident (sn_msi_incident).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



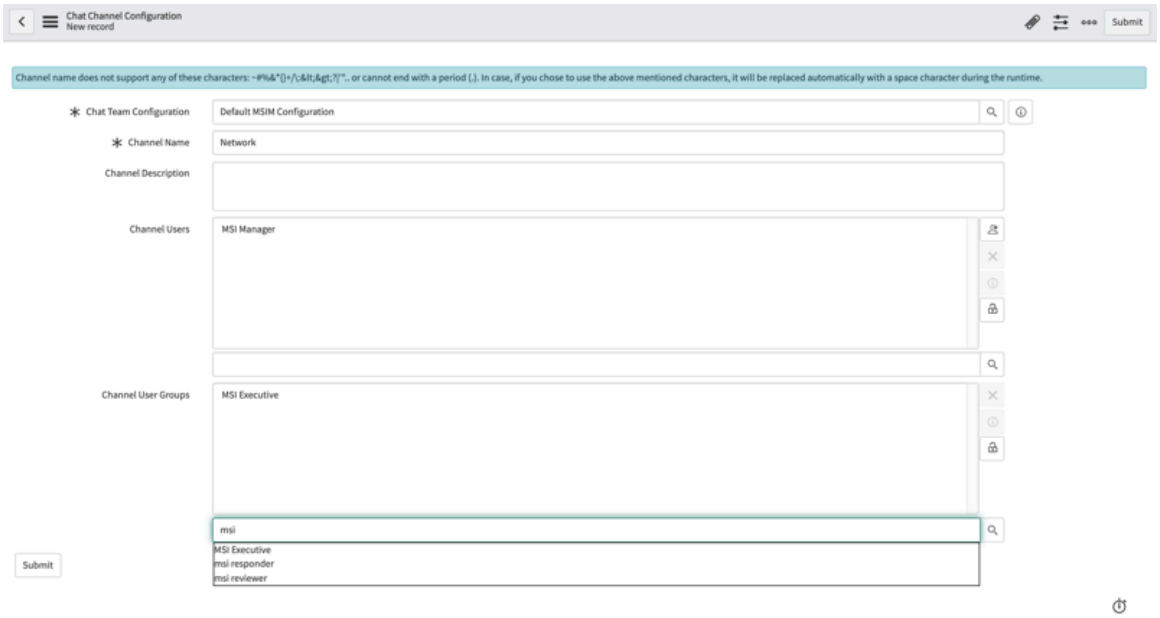
4. Click **Submit**.
5. Navigate to Chat Channel Configuration section.
6. Click **New** to create a new Chat Channel Configuration.
7. Enter the **Chat Team Configuration** and **Channel Name**.

> **Note:** The new channel that you had created here will be your channel name in Microsoft Teams as well. You can search for the same channel and add your conversations.

8. Add the **Channel Users** and **Channel User Groups** from the lookup list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. **Submit** the new chat channel configuration record.



Result

The chat channel is now created and the users are assigned to those chat channel groups. You can view the collaboration chat activities both in Microsoft Teams and in the Collaboration activity stream of the MSIM Workspace with the organized chat channel hierarchy structure as configured in the Chat Channel provider configuration.

View Chat Message Activity

Chat message activity is recorded and displayed on the Collaboration tab of the Major Security Incident Management workspace.

The chat message activity includes all the chat conversations occurred between the participants, different user groups.

MS Teams Chat Connector Troubleshooting for MSIM

Refer to Microsoft Teams chat connector troubleshooting section on the scheduled jobs, system properties, and Microsoft Teams flow designer subflows.

Verify chat connector process scheduled jobs in any case if you don't see the collaboration chat messages are posted on Microsoft Team and on the external collaboration activity stream of the MSIM workspace.

Scheduled Jobs for Microsoft Teams

Scheduled jobs are automated jobs that are run to process the notifications from Microsoft Teams chat connector and renew the Microsoft Teams subscriptions on a recurring schedule.

Role required: admin.

- **MS Teams Chat Connector: Process Notification**

  For each chat message event, a notification will be received which will have the Resource ID and the notification which are stored in a table. A schedule job is run for every 30 seconds to pick unprocessed notifications and query Microsoft Teams API to get the actual message contents, which are further stored in a different table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **MS Teams Chat Connector: Renew Subscriptions**

  For each channel within the team, subscriptions are created to get notified of the created, updated, and deleted events. This subscription is active only for 60 minutes. The subscriptions are renewed every 25 minutes through the Microsoft Teams Connector: Renew Notification schedule job.

Microsoft Teams Chat Connector Functional Flow

View this section to understand the Microsoft Teams related flow designer subflows used to administer the Chat Channel(s) creation and user access from Major Security Incident.

Before you begin

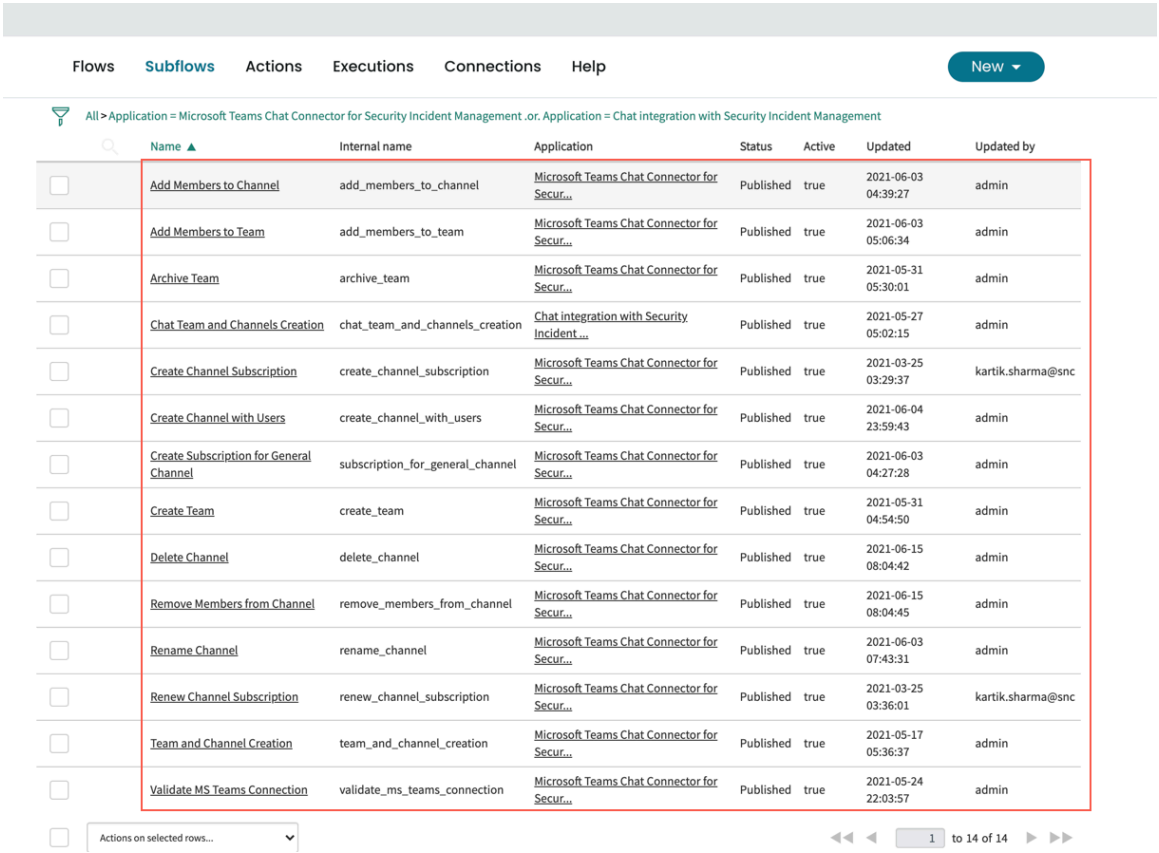
Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Flow Designer**.
2. Add Members to Channel
3. Add Members to Team
4. Archive Team
5. Chat Team and Channels Creation
6. Create Channel Subscription
7. Create Channel with Users
8. Create Subscription for General Channel
9. Create Team
10. Delete Channel
11. Remove Members from Channel
12. Rename Channel
13. Renew Channel Subscription
14. Team and Channel Creation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

15. Validate MS Teams Connection



Configure Slack chat connector for major security incidents

Integrate and collaborate with Slack to resolve Major Security Incident to view and filter collaboration chat activities.

Configuring and subscribing to a Slack chat environment, retrieving chat conversations from within specified channels, and archiving the Slack and associated channels are included as part of the incident closure process. A designated Slack environment and related Slack API configuration is required to create individual channels that are specific to a Major Security Incident.

To configure Slack, activate Slack as the chat provider. You can then create chat channels for the various stakeholders and groups communicating about activities and track chat conversations to resolve the Major Security Incident. The Slack and Slack API configuration includes:

- Get started with Slack chat connector configuration
- Activate Slack as a channel provider
- Create a chat channel template for Slack
- View chat message activities in Slack

Get started with Slack chat connector configuration

Review the following information before you start working with Slack as a connector application.

Make sure that the following plugins are installed, before you start establishing, activating, and validating Slack set up connections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required plugins

Name	Description
Slack Chat Connector for Security Incident Management	Use **sn_slack_connector** plugin ID to search and install Slack Connector for Major Security Incident Management. Installing this plugin allows you to track the chat activities using the collaboration component specific to Slack.
Slack spoke	Installing this plugin establishes a spoke connection with Slack. For more information, see Slack Spoke

Create a chat channel template for Slack

Configure Chat Teams and Channel Templates to create chat teams and channels to collaborate, track the chat conversations, and add users and user groups to those Chat Channels. These Channel templates are created in Slack when a major security incident is promoted.

Before you begin
Role required: sn_msi.workspace_admin

About this task
The new channel that you create will be your channel name in Slack as well. You can search for the same channel and add your conversations.

Procedure
1. Navigate to **All** > **Major Security Incident Management** > **Chat Channel** > **Channel Templates**.
2. Select **Slack channel configuration** to view the Slack configuration details.
3. Select the **Active** check box to activate the Slack Chat Channel configuration.
4. In the Team Name field, provide the MSI number and code name.

   By default, all Slack channels will be prefixed with the incident number. For example, `MSI000000 - {channel name}`. You can change the prefix to any field of your choice in this format: `{field_name}`.

   Note: The team name provided here will be used across all Major Security Incident records. To verify that the actual Slack is displayed in Slack application and has a unique name value for different Major Security Incidents, it's recommended that you use an incident field value, which is unique such as the `MSI000000 - {channel name}`.

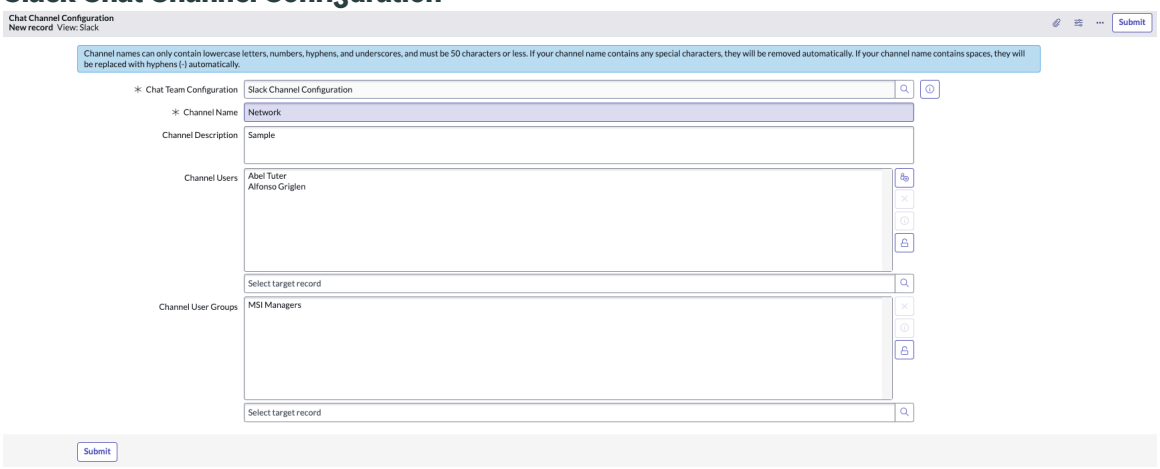
5. Right-click the configuration, and select **Save**.
6. Navigate to the Chat Channel Configuration section.
7. Select **New** to create a new Chat Channel Configuration.
8. On the form, fill the fields.

Field	Description
Chat Team Configuration	Name of the Chat Team configuration. For ex ample, Slack channel configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Channel Name	Name of the channel. For example, legal. **Note:** ○ Channel names can only contain low ercase letters, numbers, hyphens, and underscores and must be 50 char acters or less. If your channel name contains special characters, they're removed automatically. If your chan nel name contains spaces, they are re placed automatically with hyphens (-). ○ The new channel that you create here will be your channel name in Slack as well. You can search for the same channel and add your conversations.
Channel Description	Unique description for the channel.
Channel Users	Select the **Unlock Channel Users** icon, and add the users who can access this channel from the lookup list. Select the **Lock Channel Users** icon to lock the selected list of channel users.
Channel User Groups	Select the **Unlock Channel User Groups** icon, and add the user groups who can access this channel from the lookup list. You can also use the **Add me** icon to add yourself. Select the **Lock Channel User Groups** icon to lock the selected list of channel user groups.

Slack Chat Channel Configuration



9. Select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result

The chat channel is now created and the users are assigned to those chat channel groups. You can view the collaboration chat activities both in Slack and in the Collaboration activity stream of the MSIM Workspace with the organized chat channel hierarchy structure as configured in the Chat Channel provider configuration.

Activate Slack as a channel provider

Activate Slack by validating the Slack connection.

Before you begin

Role required:

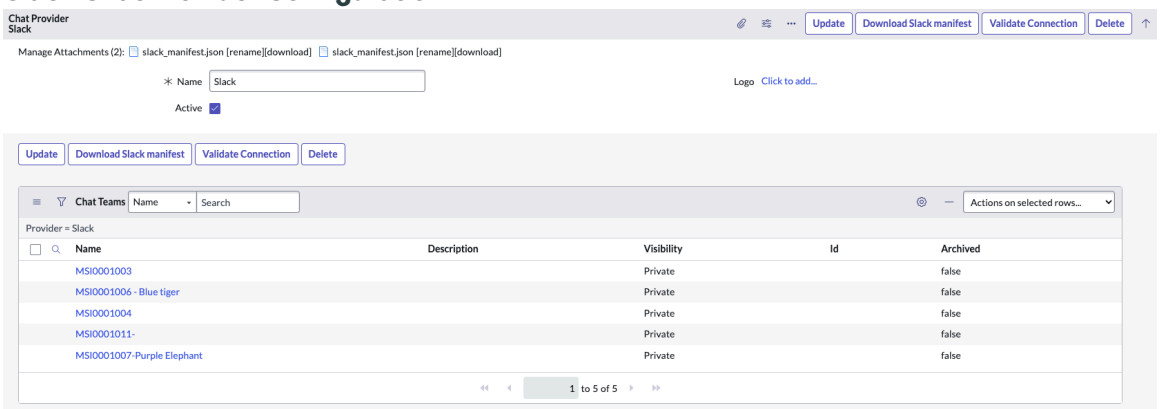
- sn_msi.workspace_admin - Write
- sn_msi.chat_collab_provider - Read

Once the connection is activated and validated, an information message is displayed that the Provider connection is validated successfully. You can modify the channel configuration by adding and removing users, and possibly adding more channels or renaming existing channels.

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **Chat Channel** > **Chat Provider Configuration**.
2. Select **Slack** to open the Slack chat provider configuration.

Slack Chat Provider Configuration



3. Select **Download Slack manifest** to download the `slack_manifest.json` file.
   The `slack_manifest.json` file contains the complete configuration for the Slack setup and enables you to configure Slack automatically. You need to upload this JSON file into the Slack configuration.
4. Open the `slack_manifest.json` file, and perform the following steps:

   a. Go to the `api.slack.com/apps` URL on your web browser.

   b. Select **Create New App** action.

   c. In the Create an app pop-up, choose the **From an app manifest** option.

   d. In the Pick a workspace to develop your app pop-up, choose a workspace from the list and select **Next**.
   For example, MSIM Slack Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. In the Enter app manifest below pop-up, select the **JSON** tab, and copy paste the code from the `slack_manifest.json` file.

f. Select **Next**.

g. In the Review summary & create your app pop-up, select **Create**.
Now your app has been created.

h. In the Basic Information page, select **Install to Workspace**.
The Slack integration bot requests your permission to access the MSIM Slack Workspace.

i. Select **Allow**.

j. In the App Credentials section, fill in the details by navigating back to the ServiceNow instance.

k. Select **All** > **Slack Configurations**.
You need the sn_msi.workspace_admin role for this action.

l. Select a **Signing Secret** property.

m. Copy the Signing Secret and paste it in the App Credentials section of Slack.

n. In the ServiceNow instance, navigate to **All** > **Flow Designer**.

o. Navigate to **Connections** > **Slack** > **View Details** > **Configure**.

p. On the form, fill the fields.

Field	Description
Connection Name	Name of this connection. For example, Slack.
Connection URL	URL of this connection. For example, https://slack.com
Credential Name	Name of the credentials. For example, Slack credentials.
OAuth Name	Name of the OAuth. For example, Slack OAuth.
OAuth Client ID	The Client ID that was generated for the account that you created in Slack.
OAuth Client Secret	The Client secret for the account that you created in Slack.
OAuth Redirect URL	OAuth redirect instance name. For example, msimslack.service-now.com/oauth_redirect.do

q. Select **Configure and Get OAuth Token**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Slack integration bot requests your permission to access the MSIM Slack Workspace.

r. Select **Allow**.
The OAuth Access token is available and will expire on <YYYY-MM-DD> <HH:MM:SS>.

5. Navigate to **All** > **Major Security Incident Management** > **Chat Channel** > **Chat Provider Configuration**.
6. Select the **Active** check box to activate the Chat Provider record.
7. Select **Validate Connection** to test the connection.
A confirmation message displays that the Provider connection is validated successfully.
8. Right-click the record and select **Save**.
After that the connection between Slack and ServiceNow AI Platform instance is successfully established.
9. Navigate to **api.slack.com/apps** > **Features** > **OAuth & Permissions**.

a. Verify if all the scopes are correct.

b. Navigate to **Features** > **Event Subscriptions**.

c. In the Request URL field, select **Retry**.
You can see a verified message.

d. Select **Save**.

View chat message activities in Slack

Chat message activity is recorded and displayed on the Collaboration tab of the Major Security Incident Management workspace.

Before you begin
Role required: sn_msi.workspace_admin

About this task
The chat message activity includes all the chat conversations occurred between the participants, different user groups. For more information, see Manage Chat Channels communications using Slack.

Major Security Incident Management administration

Plan and configure your Major Security Incident Management implementation.

You can configure the following aspects of Major Security Incident Management administration:

Enable proposal, promotion, and linking of major security incidents

Enable users to decide to propose or promote incidents as major security incidents. Easily track all incidents related to a major security incident by enabling security incidents to be linked to the parent or child incident.

Before you begin
Role required: sn_msi.workspace_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Configurations**.
2. Enable users to propose a security incident to a major security incident by selecting the **Propose Major Security Incident** check box in the SIR/VR Workspace Actions section.
3. Enable users to promote a security incident to a major security incident by selecting the **Promote to Major Security Incident** check box.
4. Enable linking a security incident to a major security incident so they can be tracked together by selecting the **Link to Major Security Incident** check box.
5. Select **Update**.

Tag security incidents as major security incidents

Tag or label the security incidents or vulnerable records to a major security incident when the incident is proposed or promoted. If a security incident is proposed then the incident record is referred as major security incident candidate. When a security is promoted then the incident record is referred as Major Security Incident with state as Accepted.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Configurations**.
2. Enable **Display Labels** check box to label the proposed incident candidate as major security incident by selecting the **Label Name - Propose As Candidate** lookup field and select Major Security Incident Candidate in the **SIR/VR Workspace Labels** section.
3. Enable **Display Labels** check box to label the promoted incident candidate as major security incident by selecting the **Label Name - Promotion to Major Security Incident** lookup field and select Major Security Incident in the **SIR/VR Workspace Labels** section.
4. Select **Update**.

Configure labels for major security incidents

Configure labels in major security incident management to create custom labels and filter the external collaboration activities and tasks in the activity stream. The different types of implemented labels are State labels and timeline labels.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Configurations**.
2. Enable **Display Labels** check box to enable labeling different incident states such as Analysis, Contain, Eradicate, Recover, Review, Timeline Event in the **MSIM Workspace Labels (Display on Collaboration Activities and Tasks)** section.
3. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure labels for major security incidents

Configure different types of labels to better filter and also indicate the incident states. Major security incident labels provide the flexibility to label the collaboration activities and tasks of the incident records.

Before you begin

Role required: sn_msi.workspace_admin

You can select or deselect the labels using the labels icon that is available on the Activity stream section of the Collaboration and Task organizer section of the MSIM workspace.

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **MSI Labels**.
2. Click **New** to create a new label.
3. Fill the form with **Label Name** and **Label Color**.
4. Click **Create Label**.
5. As a part of the base system, the following are the configured labels for each incident state and you can't modify the label name or color:
   - Analysis
   - Contain
   - Eradicate
   - Review
   - Recover
   - Timeline Event

Note: You can modify the custom labels and its properties.

Configure timeline categories for major security incidents

Configure and assign Timeline categories such as Threat, Response, or Custom to your major security incidents using the Timeline section on the Overview tab.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Timeline categories**.
   The following timeline categories are provided as a part of the base system:
   - **Custom**.
   - **Response**.
   - **Threat**.
2. To modify an existing Timeline event category, perform the following steps:
   a. Select a Timeline event category from the list.
   b. You can modify the name of the Timeline event category.
   c. You can modify the Event Color and select another color for your Timeline event category.
   d. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To create a new Timeline event category, perform the following steps:
   a. Select **New**.
   b. In the Name field, enter a name for the Timeline event category.
   c. In the Event Color field, choose a color for the event timeline category using the drop-down list.
   d. Select **Submit**.

Set notification preferences for MSIM

Automate the email notification process and notify the users when a security incident is either proposed or promoted to a major security incident candidate.

Role required: sn_msi.workspace_admin.

The notifications are triggered only when a security incident is proposed and sent to all those users and groups who are configured to the notifications list. By default, the email notification is received by the user who had proposed the security incident as a major security incident candidate.

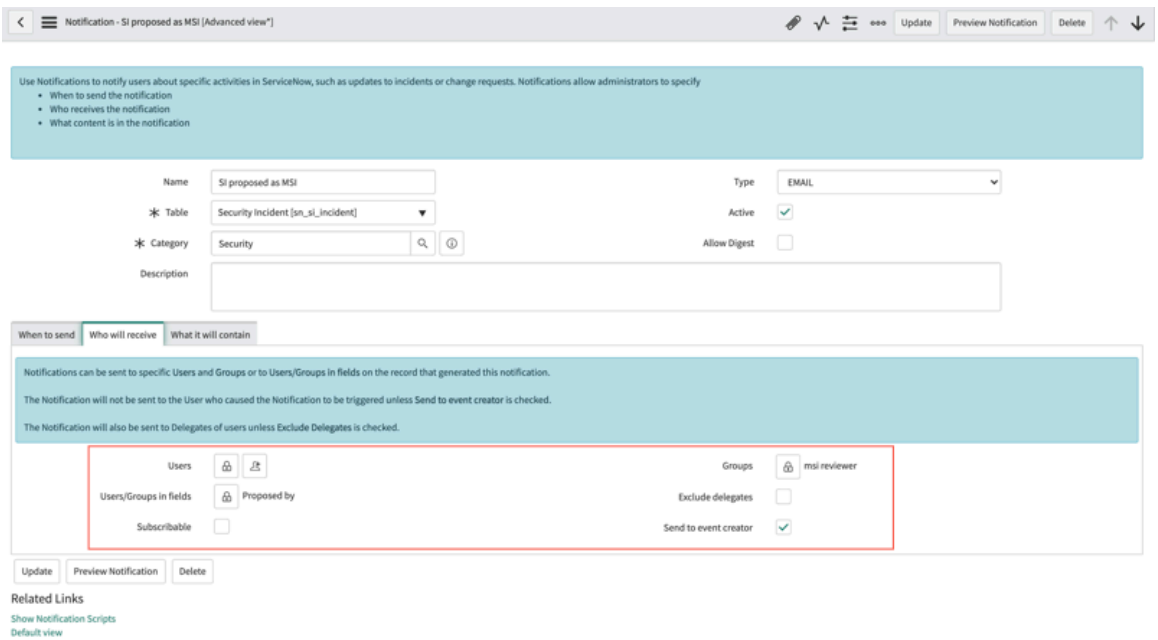
Notification: Security Incident proposed (SI) as Major Security Incident (MSI)

Who will receive:

- By default, **MSI Reviewers** group name is created and any user who is added to this group will be privileged to be a **MSIM Manager** and the users who are under that group will receive the notification emails.
- Any specific user who is added to the **Users** list will also receive the notification emails.

What will it contain:

If you want to modify the email contents such as body of the email which includes the Subject or Message HTML, you must have the System Administrator role access or assigned as System Administrator and not an MSI Administrator.



Notification: Security Incident promoted (SI) as Major Security Incident (MSI)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

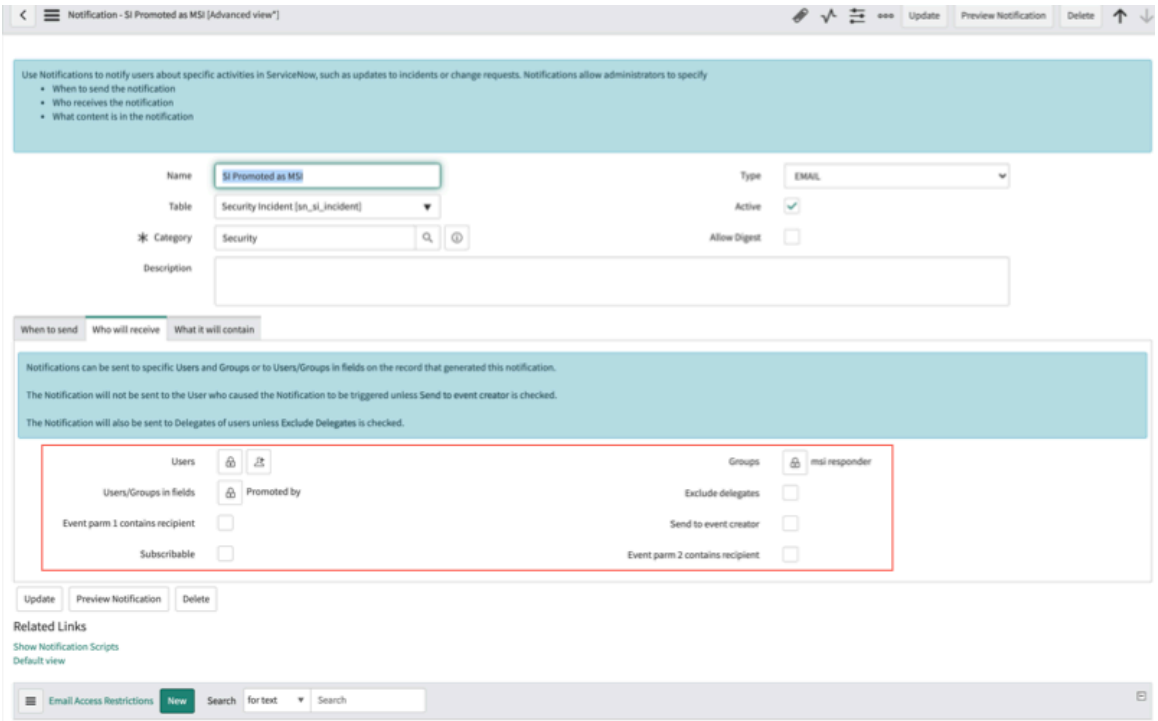
This notification is triggered when a security incident is promoted and when the File Explorer and Microsoft Teams base structure is created. By default, this notification is received by the user who had promoted the security incident to a major security incident.

Who will receive

- By default, a **Group** by name **MSI Responder** is created and any user who is added to this group will be privileged to have **MSIM Responder** role and all the users who are under that group will receive the notification email.
- Any specific user who is added to the **Users** list will also receive the notification emails.

What will it contain

If you want to modify the email contents such as body of the email, which includes the Subject or Message HTML, you must have the System Administrator role access or assigned as System Administrator and not an MSI Administrator.



Configure MSI closure activities

Establish actions that will occur automatically when a major security incident is closed. Increase security by automatically archiving and removing access to folders containing resolution information.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Configurations**.
2. Archive chat communications related to resolve the incident by selecting the **Archive Collaboration Channels** check box in the Automated Closure Actions section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Remove folders containing material related to resolving the incident by selecting the **Remove Collaboration Folders** check box.
4. Select **Update**.

Major Security Incident Management workspace

Major Security Incident Management provides a dedicated workspace for managing major security incidents specifically designed for the Major Security Incident manager.

Easily collaborate on activities that help resolve major security incidents by sharing and viewing files and folders, viewing and updating incident tasks, and communicate with those working on the incident through dedicated chat channels.

Major Security Incident Management (MSIM) provides a mechanism to track and resolve major security incidents. MSIM works in conjunction with the existing security incident and vulnerability response product capabilities and improves the major security incident remediation process with the following features:

- Dedicated workspace for managing major security incidents specifically designed for the major security incident manager user role.
- Organize major security incident response tasks, including tasks tracked on linked security incidents and vulnerability groups.
- Automate creation of collaboration folders and chat communication channels once a major security incident is created, as well as archival as part of incident closure.
- File explorer component to organize and track collection of artifacts (files) related to the major security incident via a Microsoft SharePoint integration.
- Chat channel manager and activity stream components to manage communications across multiple security, IT, and functional groups via a Microsoft Teams integration.
- Summary reporting of major security incident impact and progress metrics, including rollup of affected assets, users, locations, and team resources, as well timeline of significant incident milestones.

Use the MSIM Workspace to track and resolve major security incidents:

1. View the trend charts and progress of the major security incident.
2. Track and organize Microsoft SharePoint files activity via the MSIM Workspace.
3. Track and organize Microsoft Teams chat activity via the MSIM Workspace.
4. View and update incident details via the MSIM Workspace.
5. Filter collaboration activities in the MSIM Workspace Activity stream.

Using Major Security Incident Management

Managers can use Major Security Incident Management workspace to view the proposed, promoted, linked, and rejected incident records and track their related activities.

Propose, promote, and link incident records

Propose or promote security incidents as major security incidents when incidents are identified as critical threat to the organization.

Once Major Security Incident Management is installed on your ServiceNow instance, you can handle the transition of security incidents to major incidents as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Propose a security incident to major security incident candidate to initiate a review process.
- Directly promote a security incident to a major security incident without a review process.
- Reject a security incident proposed as a major security incident.

You can also link a security incident as a child incident to the major security incident so that all related security incidents can be tracked together.

Propose as a Major Security Incident

Propose a security incident to a major security incident.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **Lists**.
2. Select the security incident in the related category that you want to propose as a major security incident.
3. Select the **More Actions** icon and select **Propose as Major Security Incident**.
4. In the Propose as Major Security Incident dialog box, fill in the fields.
   a. **Detection Date**: Date when the major security incident was first created or proposed.
   b. **Justification**: Provide the justification for proposing the incident.
   c. **Potential impact**: Indicate the impact of the incident.
5. Select **Propose**.

Result

The incident is proposed and the following actions occur:

- In the security incident record, a verification banner message is displayed and the defined Major Security Incident tag appears.
- The record appears in the Major Security Incident related list in the incident record, with the state listed as Proposed, and in the MSIM Workspace Candidates list.
- The Activity section in the MSIM Workspace shows that the security incident has been proposed to be promoted as a major security incident.
- A message is sent to those in the defined notification list that contains a link to the incident record and the Details tab for the incident.

Promote to a Major Security Incident

Promote a security incident to a major security incident or reject promoted proposals through the Major Security Incident Management (MSIM) Workspace.

Before you begin

Role required: sn_msi.workspace_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Security Incident Response Workspace** > **Security Incidents** > **Lists**.
2. Select the security incident in the related category that you want to promote as major security incident.
   Review the details of the security incident in the Details section or view extended details in the incident record in a separate tab by clicking **View more details**.
3. Select the **More Actions** icon and select **Promote to Major Security Incident**.
4. In the Promote Major Security Incident dialog box, fill in the fields.

   a. **Detection Date**: Date when the major security incident was first created or proposed.

   b. **Estimated resolution date**: The estimated resolution date by when the major security incident is estimated to be resolved.

   c. **Code name**: Select the code name for the major security incident.
   For example, Blue Tiger.

   d. **Category**: Select the category for the major security incident.
   For example, Misconfiguration.

   e. **Justification**: Provide the justification for proposing the incident.

   f. **Potential impact**: Indicate the impact of the incident.

5. Select **Propose**.
6. Either promote the security incident or reject the promotion proposal.
   - To promote the incident, click **Promote to Major Security Incident**.
   - To reject the promotion proposal, click **Reject as Major Security Incident**.
7. Select **Save**.

Result

- If you rejected the promotion proposal, the incident is not promoted and the incident entry moves to the Rejected tab.
- If you promoted the incident, the incident entry moves to the Open tab and the security record displays a tag indicating that it is a major security incident.
- The decision is listed in the Activity section of the MSIM Workspace.

Once an incident is promoted, the default configuration is applied.

- A folder structure is created based on the folder template configuration.
- Chat channels are created based on the channels configuration.
- An email message is sent to the designated users. The default notification contains a link to the major security incident and details of the incident. The designated users also now have access to the collaboration resources, so the notification also includes the Microsoft Team name and a link to Microsoft SharePoint folders related to the incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Link to Major Security Incident

Link security incidents to a major security incident.

Before you begin

Role required: sn_msi.workspace_admin

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**.
2. Select the security incident in the related category that you want to link to the major security incident.
3. Select the **Additional Actions** icon and select **Link to Major Security Incident**.
4. Select the major security incident to which you want to link.
   a. In the dialog box, select the Lookup using list icon.
   b. Select the major security incident you want to link to.
   c. Select **OK**.
5. Select **Propose**.

Result

The proposal is submitted and the following actions occur:

- In the security incident record, a verification banner message is displayed and the defined Major Security Incident tag appears next to the **Select security tag** field.
- In the **Details** tab for the major security incident in Major Security Incident Management, the record number drop-down list includes both incidents.
- The record appears in the incident record's Major Security Incident related list, with the state listed as Proposed.
- A message is sent to those in the defined notification list that contains a link to the incident record and the Details tab for the incident.
- The **Activity** section in the MSIM Workspace shows that the security incident has been added as a child security incident to the major security incident with a link.

Using MSI List view in the MSIM workspace

With the list view in the MSIM workspace, you can view proposed, promoted, and rejected major security incidents.

Before you begin

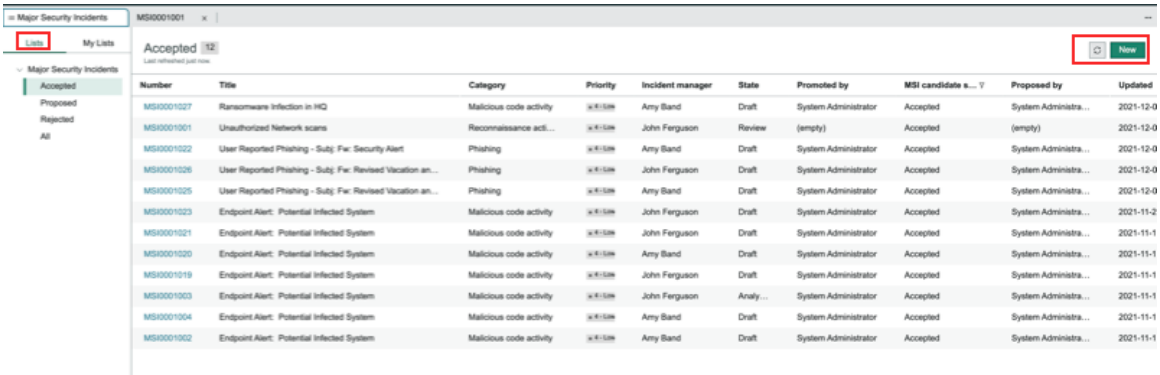
Role required: sn_msi.workspace_manager

You can also create new incidents using the **New** button available in the top right corner of the workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Major Security Incident Management** > **MSIM Workspace**.
2. Select the Lists tab to display the Lists view.



3. Select **My Lists** to create your own list of major security incidents.
4. Refer to the following table for what you can do from the list view:

Task	Description
My Lists	Create new MSI records lists and view the lists that you have created.
Set filters for a column on a list	Select a column and expand the vertical dots menu to view options that further filter the data in the column.
Filter out items or match items from a row in a column	Select a cell in a column and refine the data displayed by choosing one: ○ Show Matching - Display only items that match the selected item in the column. ○ Filter Out - Filter out the items from the column that match the selected item in the respective column.
Refresh List	Refresh the lists and view the complete lists that was updated.
New	Create a new MSI record.

View Major Security Incident impact metrics

Provides up-to-date summary reporting of the impact and progress of major security incidents, which is an important aspect of managing a major security incident using the new workspace.

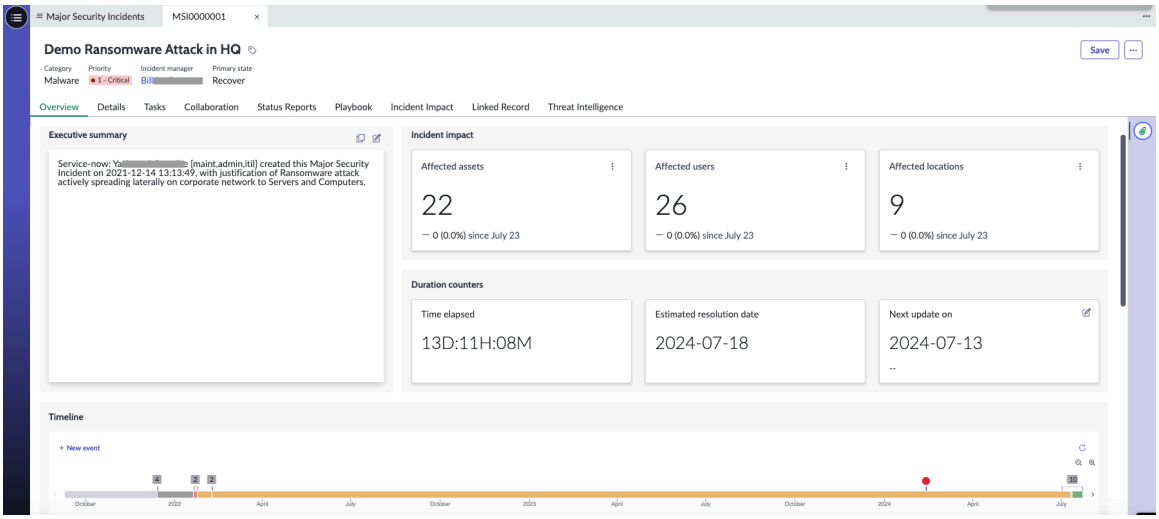
The **Overview** tab provides the relevant metrics to manage both the scope and progress of the incident, including a rollup of affected assets, users, locations, and team resources, as well as the timeline of significant incident milestones.

Timeline provides a horizontal view of key events and milestones that have occurred as part of the specific major security incident resolution. The timeline component is displayed on top of all the Major Security Incident Management workspace tabs with an ability to collapse and expand for viewing as required. The events data represented will be updated and refreshed whenever designated milestone events or milestones are added or updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Each event or milestone is indicated with a different timeline event type option to identify the number and type of events or milestones. For example NOW record updates, collaboration activities. In addition, the time range period for the different major security incident states is tracked automatically and displayed using color-coded ranges displayed along with the duration of each incident state.

MSIM Overview tab



Executive Summary and Incident Impact

Task	Description
Executive Summary	A brief summary of the major security incident along with the user name, user role, and timestamp details. • You can modify the Executive Summary by selecting the **Edit** icon. After you make the required changes, select the **Update** option. • To copy the Executive Summary and paste it to a major security incident, select the **Copy** icon and paste the summary to the required major security incident.
Incident Impact	These components display the impacted resources based on a rollup of all active tasks and linked incidents with identified assets, users, locations, and assigned team members. The impacted resources are: • **Affected assets** • **Affected users** • **Affected locations** Selecting the number values enables you to drill down and navigate to the impacted assets, users, and location details and displays the related tasks on the **Incident Impact** tab of the workspace.

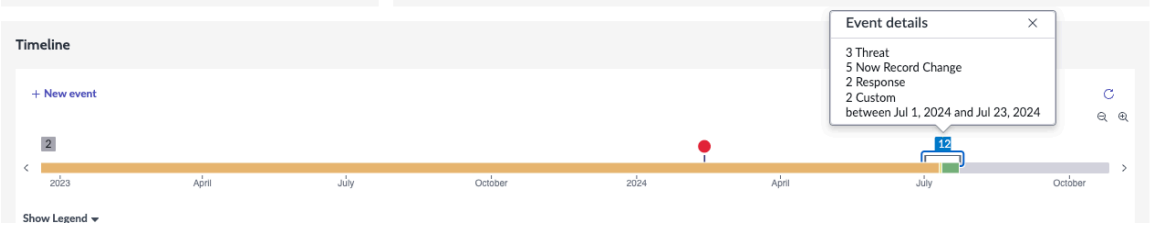
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Executive Summary and Incident Impact (continued)

Task	Description
	Based on your selected incident impact type link, the related incident details such as task type and its description, assignment group and incident state are displayed in the **Incident Impact** tab of the MSIM workspace.
Duration counters	These components display the duration of the major security incident. The impacted resources are: • **Time elapsed**: Displays the time elapsed from the time that the major security incident is detected. • **Estimated resolution date**: Displays the estimated resolution date by when the major security incident is estimated to be resolved. • **Next update on**: The date and time of the next update for resolving the major security incident. For example, 5:00 pm EST on March 25, 2024. You can modify the **Next update on** by selecting the **Edit** icon. Select the new date and time, and select **Update**.

You can enable or disable viewing of certain event types for both timeline indicators and timeline ranges accordingly using the filter toggle buttons.

Timeline



Refer to the following table for additional capabilities available with the timeline component.

Timeline component additional capabilities

Task	Description
New Event	Creates new custom events and associates these events to the MSI record. This helps in creating events for both past and future dates that might not otherwise get captured via a labeled task, record state change, or labeled collaboration activity, which are displayed by default on the timeline.
Refresh	Refreshes the Timeline events to display the latest updates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Timeline component additional capabilities (continued)

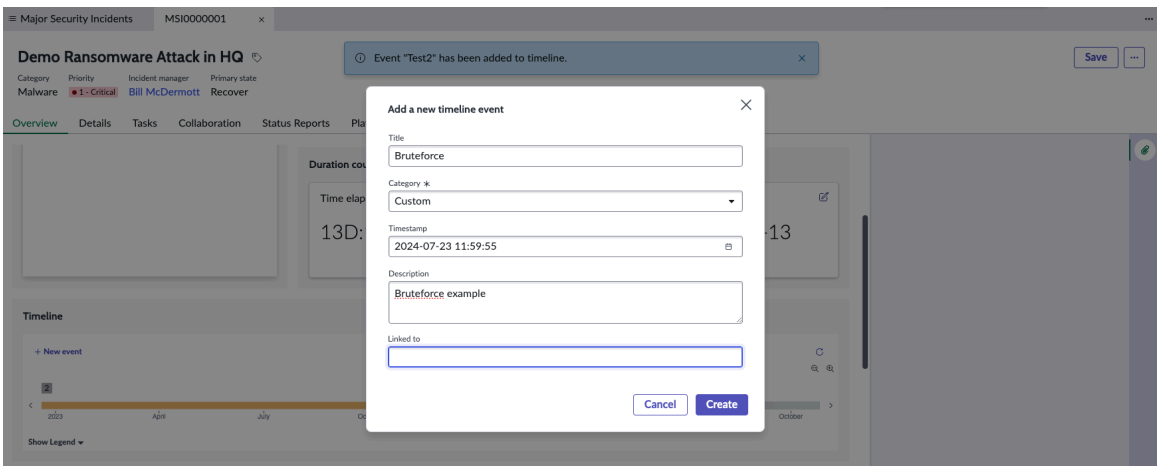
Task	Description
Timeline Indicators	Lists the various types of events such as Now Record field changes, Labeled Collaboration Activities, and Other (custom), along with the icons and total number of events that occurred with respect to each event type indicator. The slide indicator enables you to enable or disable all events for a specific event type.
Show Legend	Select to display the drop-down legend with different types of timeline indicators.
Timeline progress bar	Displays the overall progress of the incident via designated timeline events or milestones that are occurred within the different timeline ranges displayed. You can also link an Event type to an Event category. After you link it, the Event details get updated at both places on the timeline.
Timeline ranges	Displays various incidents state types and duration as the incident progresses throughout the full major security incident life-cycle. Enable or disable a specific event based on the incident state.

Create a Timeline event

To create a new Timeline event, perform the following steps:

1. In the Overview tab, navigate to the **Timeline** section.
2. Select **+ New event**.
3. On the Add a new timeline event pop-up, fill the fields.

New Timeline event



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
Title	Enter the title for the timeline event.
Category	Select a category for the timeline event. The following categories are provided as a part of the base system, and you can choose one based on your requirements. ○ **Custom**. ○ **Response**. ○ **Threat**. To add or configure a Timeline event category, see Configure timeline categories for major security incidents.
Timestamp	Select the date and time of the timeline event using the Timestamp calendar. You can add events to the Timeline before and after the start date.
Description	Provide a brief description about the timeline event.
Linked to	Option to link the timeline event to a major security incident record.

4. Select **Create**.
5. You can use **Zoom in** and **Zoom out** icons to zoom in or out on the timeline progress bar, which includes displaying individual events when numbers are displayed to represent several events in close time proximity.

   You can also add the default zoom level to show all events.
6. Select the **Refresh** icon to display the latest timeline events.

View Major Security Incident trend charts

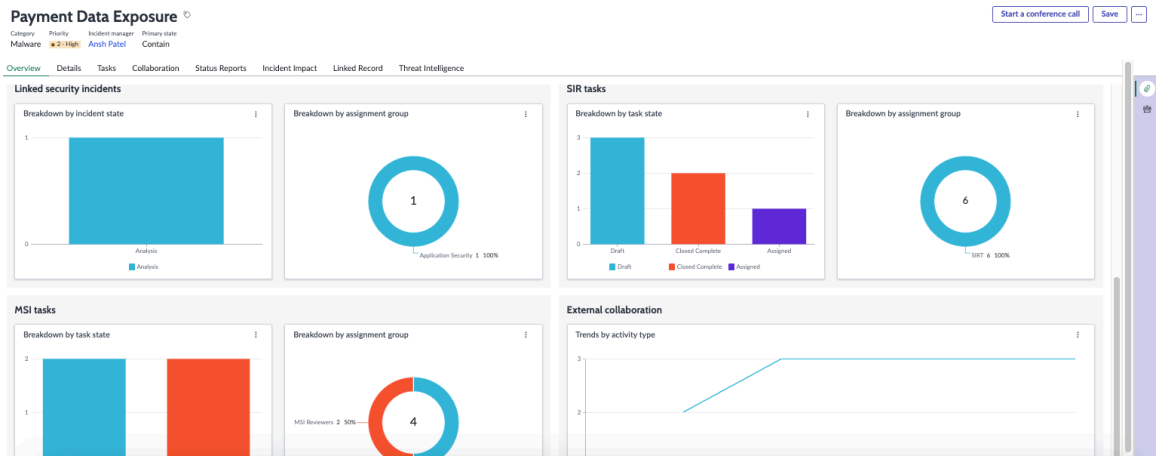
View the major security incident impact progress metrics visualized as bar graphs and charts.

In addition to the incident timeline and progress trend chart visualizations, the **Overview** tab provides relevant impact metrics to manage the changing scope of the incident, including rollup of affected assets, users, locations, and team resources.

The counts displayed in the visualization components are based on active tasks on linked Security Incident Response (SIR) incidents. As tasks are opened and closed, these counts change in terms of the nature and volume of remaining activity planned for the major security incident to represent the trends shown in the trend chart visualization components.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MSIM Overview tab impact metrics



Refer to the following table for the UI actions that you can perform from the **Overview** section:

Overview UI sections

Title	Description
Time	Displays the period in total number of days from when the major security incident is active. The time is calculated based on the **Detection Date** entered in the **Details** tab of the workspace. The Detection Date is often captured initially when the major security incident was first created or proposed. Whenever, this date is modified the time is automatically calculated, refreshed, and displayed in the format days: hours: minutes, for example 20D: 13H: 58M. **Estimated resolution date**: The date by when the incident resolution date is estimated to resolve. This date is often captured initially when the major security incident was first created or promoted. The date is updated and refreshed based on the estimated date provided in the **Details** tab of the workspace. If the estimated date is not provided in the Details section, then this section displays 'hyphen' without any date value.
Active Team	Displays the different response teams and team members from each team who are actively working on the major security incident and its related tasks. **Active Team** trend: Displays the trend chart of each team and its team members who are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview UI sections (continued)

Title	Description
	actively working on the major security incident and related tasks on regular interval. **Note:** View the assigned active groups from the **Details** tab of the workspace.
Linked SIR incidents	**By incident state**: View the distribution of linked security incidents based on a incident state such as Analysis, Contain, Eradicate, Recover, or Review. **Trends by incident state**: Further indicates the trend view of how the number of linked incidents are progressing based on incident state. Selecting each incident state link allows you to navigate and view the linked security incident details directly on the **Linked SI/VI** tab of the workspace. This section is updated and refreshed automatically whenever changes occur to the underlying incidents.
SIR Tasks	Displays active task totals that are linked to the MSI record via SIR incidents. • **By task state**: View the incident response tasks based on the incident state such as Draft, Assigned, Work in progress, Closed Complete. This distribution chart allows for a further distribution breakdown by assignment groups. Selecting each task state allows you to view a filtered list by incident task state on the **Tasks** tab of the workspace. The filtered view allows you to view and update individual task details. • **In progress tasks by incident state label**: Displays active tasks and groups based on incident state label that must be applied in the Task Organizer components. These default labels have values such as Analysis, Contain, Eradicate, Recover, or Review to indicate the nature of the task involved. • **Overdue**: Displays the security incident response tasks, which are active and had exceeded the due date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview UI sections (continued)

Title	Description
	You can view the details of all the overdue tasks by selecting the total Overdue count and having it auto navigate to the Tasks tab. • **Trends by task state**: View the progress trend of both work in progress and closed response tasks over the incident duration. **Note:** The trend chart graph retrieves the latest data based on the scheduled job. You can configure or modify the data retrieval time interval as required.
MSI Tasks	Displays active tasks in total, which were created directly on the MSI record (and these aren't linked response tasks): **By task state:** View the major security incident created tasks, assigned tasks and its related information. Selecting each task state allows you to view a filtered list by incident task state on the **Tasks** tab of the workspace. The filtered view will allow for viewing and updating individual task details.
External Collaboration	Displays collaboration activities in total for all the labelled collaboration activities from the Collaboration Activity Stream: • **By incident state label:**View the incident collaboration activities data that are coordinated with Microsoft Teams and Microsoft SharePoint files and folders and are labeled using incident state labels such as Analysis, Contain, Eradicate, or Recover from the **Collaboration** tab of the workspace. • **Trends by activity type**: View the trend chart for the number of Microsoft Teams and Microsoft SharePoint files and folders activities over the incident duration.

Update Major Security Incident details

View and update specific details related to the major security incident such as Incident Record Details, Active Team participants, and the corresponding activity log.

All the related details of the major security incident are displayed with various Form sections on the **Details** tab of the workspace. Displays the details such as Incident Record Details, Active Team participants, and the corresponding activity log. You can also view the linked SIR incidents,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Group record details, and an ability to broadcast an activity posting to all the linked incident records.

Primarily the Details tab contains:

1. Major Security Incident Form fields and incident-related UI sections.
2. Activity stream

The following table provides the details of the major security incident form fields:

Major Security Incident form sections

Field	Description
Incident	
Number	Major security incident record number.
Primary state	The primary state of the major security incident record.
Detection Date	The date when the major security incident was first created or proposed. Whenever you modify the Detection date on the Details tab, the date and time of the MSI is automatically calculated, refreshed, and displayed on the **Time** > **Time since the incident started** section on the **Overview** section of the workspace.
Title	Title of the Major security incident.
Code name	Code name for the major security incident. For example, Blue Tiger.
Next update on	The date and time of the next update for resolving the major security incident. For example, 5:00 pm EST on March 25, 2024.
Category	Category of the major security incident.
Sub category	Subcategory type of the major security incident.
Estimated resolution date	The estimated date by when the incident is expected to be resolved. The default value is 7 days from the time of the major security incident creation.
Priority	Priority of the major security incident.
Alert sensor	Alert sensor of the major security incident. For example, User Reported Phishing.
Source	Source of the major security incident.
Active Team	
Incident Manager	Name of the incident manager.
Assignment Groups	Indicates the different response teams and team members from each team who

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Major Security Incident form sections (continued)

Field	Description
	are actively working on the major security incident.
Candidate	
MSI candidate state	Indicates the major security incident candidate state such as proposed or promoted. If the incident is promoted, then the state is displayed as Accepted.
Promoted by	User who had promoted the major security incident.
Promoted	Date when the major security incident was promoted.
Justification	Justification of the major security incident. The justification should include the MSI number and the code name.
Potential impact	The potential impact and severity of the major security incident. The Potential impact should include the MSI number and the code name.
Restriction	
Enforce restriction	Select this option to enforce restrictions on certain major security incident restrictions. You can enforce restrictions to limit the view or modify access only to certain users or groups. For more information, see Restrict access to certain major security incidents.
Allowed members	List of users who can access the major security incident.
Allowed groups	List of groups who can access the major security incident.
Other actions	
Attachment	Any attachments related to the major security incident. Select **Select** option to add attachments to the incident.
Conference Call	Use conference calls with the third-party service providers as a communication channel to meet with the stakeholders to resolve the major security incidents. For more information, see Major Security Incident Management Conference Call Integration

Activity:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the Activity section to add your work notes and comments, and post your activity privately and also add additional comments as required using the Compose section. Save the activity after you post your work notes and comments to view the added activity or worknotes in the Activity section.

Note: Select the **Show more** details link to view the details of a specific security incident record, which are associated with that major security incident.

Set your preferences to view the related activities such as:

1. **Filters**: Select the **Filter sets** icon to set filters.

   Set filters to view the activity conversations such as activities added on the work notes, email, Timeline, and any additional comments.

2. **Flagged**: Select the **Flagged** icon to flag the activities.

   Flag any important activity conversations for you to keep them handy.

Restrict access to certain major security incidents

Manage who can view or modify major security incidents that contain sensitive information. You can enforce major security incident restrictions to determine who has access to view or modify certain major security incident records and related lists and limit the read or write access only to certain users or groups.

Before you begin

Role required: sn_msi.workspace_manager

About this task

Major security incident restrictions enable you to hide critical major security incidents from being accessed or modified by all users or groups in a particular organization. These restrictions enable you to provide a more granular way to control the major security incidents a user or group can view or modify. You can enforce a major security incident restriction by selecting the **Enforce restriction** check box and selecting the users or groups allowed to view or modify the particular major security incident.

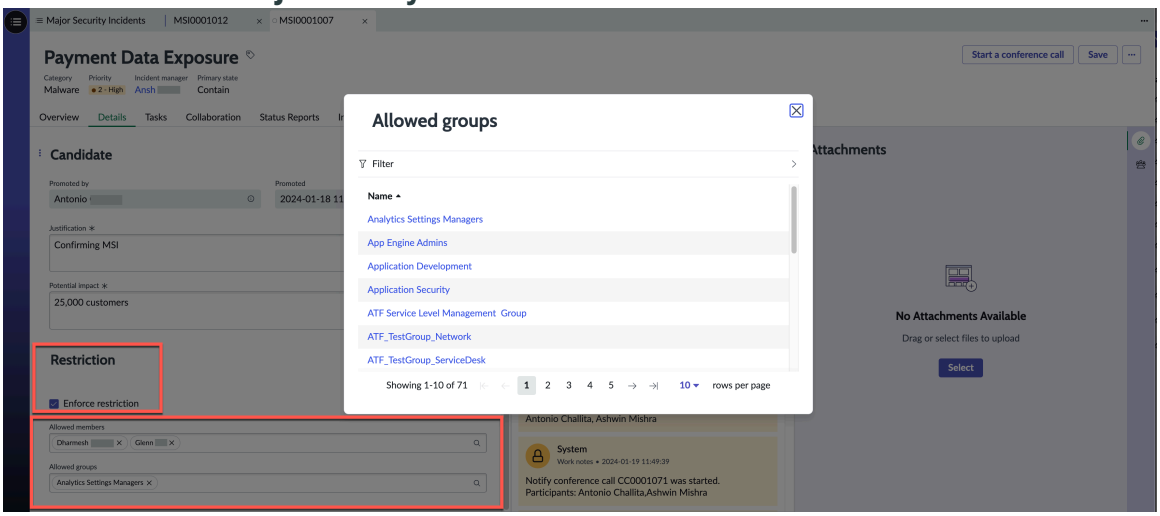
After you enforce the restriction on major security incidents or related lists to certain users or groups, all the remaining users or groups in your organization won't be able to view or modify these major security incidents or related lists.

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Details** tab.
5. Scroll down and select the **Restriction** section.
6. Select the **Enforce restriction** check box to enable the restriction of the major security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Restrict access to major security incidents



7. In the Allowed members field, select the users who can view or modify the major security incident using the Search option.
8. In the Allowed groups field, select the groups who can view or modify the major security incident using the Search option.

   Note: After the **Enforce restriction** check box is enabled for the major security incident, only the sn_msi.workspace_manager and allowed members or groups will have access to view or modify the major security incident.

9. Select **Save**.

Link additional records to Major Security Incident

In the workspace, use the linking records functionality to link any related Security Incident records and its child security incidents, Remediation Tasks from Vulnerability Response, and Security Cases from Threat Intelligence to a Major Security Incident (MSI) record.

Before you begin

Role required: sn_msi.workspace_manager and sn_msi.workspace_responder

Procedure

1. Navigate to **Major Security Incident Response** > **MSIM Workspace**.
2. Navigate to the **Lists** view, which is displayed in the left pane of the workspace.
3. Click **Accepted** to select the promoted major security incident records.
4. Select the incident record that is required to be linked which is not in the Closed state from the list of promoted records.
5. Click **Linked Records** tab.
   A drop-down list is provided to select other linked record tables.
   The Linked Records section displays the linked records and its related records, which were linked to the Major Security Incident.
6. Select the desired table view such as Security Incidents, Remediation Tasks (vulnerable items), or Security Case from the list.
   Based on your selection type records table view, the linked records that linked to the major security incident records are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Link a record that is not linked to any MSI record and is in the **Open** state by selecting the record and clicking **Link Record** in the top right of the page.

   Note: You can't link an incident record to an MSI record if it's in the **Closed** state.

8. Select the record to be linked and click **Link**.
   A confirmation message displays that the record is linked successfully and the rollup of related records will be processed in the background.

   Note: After a record is linked, the list view is refreshed automatically and lists the updated list of incident records.

Related topics

Unlink records from Major Security Incident

Unlink records from Major Security Incident

Using the Major Security Incident Management workspace, unlink the major security incident records from the Linked Records section.

Before you begin

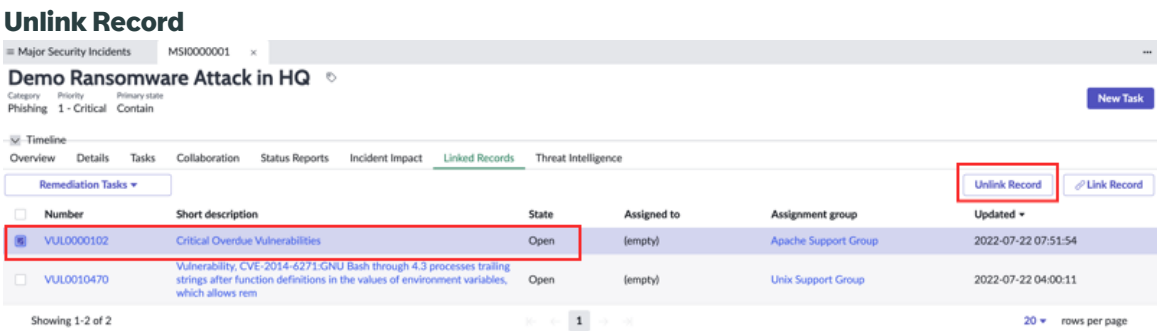
Role required: sn_msi.workspace_manager and sn_msi.workspace_responder

Note: You can only unlink a single record at a time. After you unlink a record, the related rolled up information will be removed from the Incident Impact and Threat Intelligence sections on the workspace and the action can't be undone.

For more information on roll up records, see Rollup Framework for MSIM.

Procedure

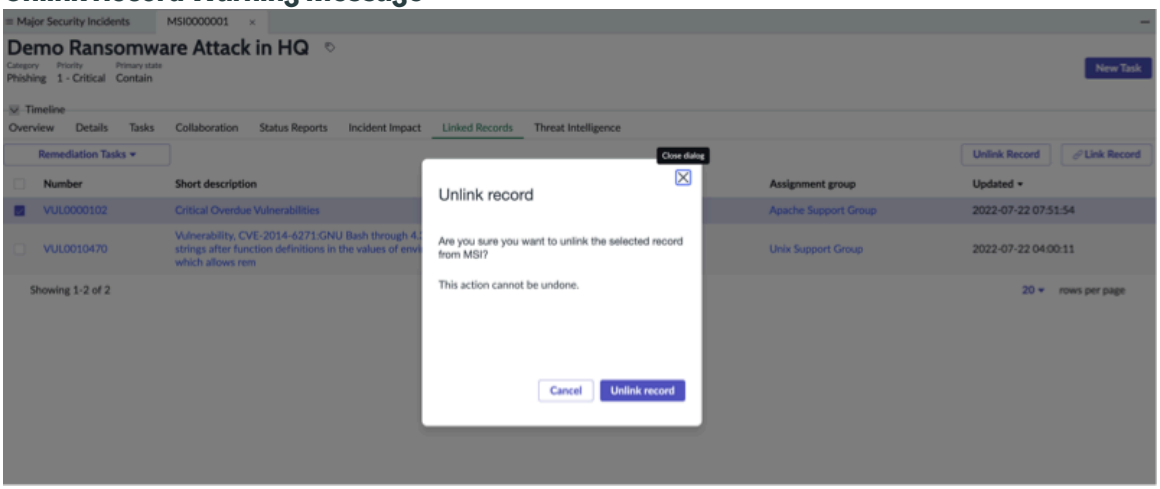
1. Navigate to **Major Security Incident Response** > **MSIM Workspace**.
2. Navigate to **Lists** view, which is displayed in the left pane of the workspace.
3. Click **Accepted** to select the promoted major security incident records.
4. Click the **Linked Records** tab.
   This section displays the linked records and its related records, which are linked to the Major Security Incident.
5. Select the desired table view such as Security Incidents, Remediation Tasks (vulnerable items), or Security Case.
6. Select the record to unlink from the list view of records.
7. Click **Unlink Record**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. A warning message is displayed asking if you want to unlink the selected record from MSI.

Unlink Record Warning Message



9. Click **Unlink Record**.
   The record is unlinked and once unlinked, the changes can't be reverted. The list view of Linked Records will be refreshed after unlinking.

Related topics

Configure Linked Records in Major Security Incident Management

Configure Rollup Records in Major Security Incident Management

Manage tasks in a Major Security Incident

The Task tab enables you to track and manage all the tasks associated with a major security incident from the MSIM workspace. You can view the various tasks using the default Visual Task Board (Kanban view) or the List view.

The sn_msi.workspace_manager can do the following on the Tasks tab:

- Create a task
- Modify tasks
- View and assign tasks to self or others
- Delete tasks

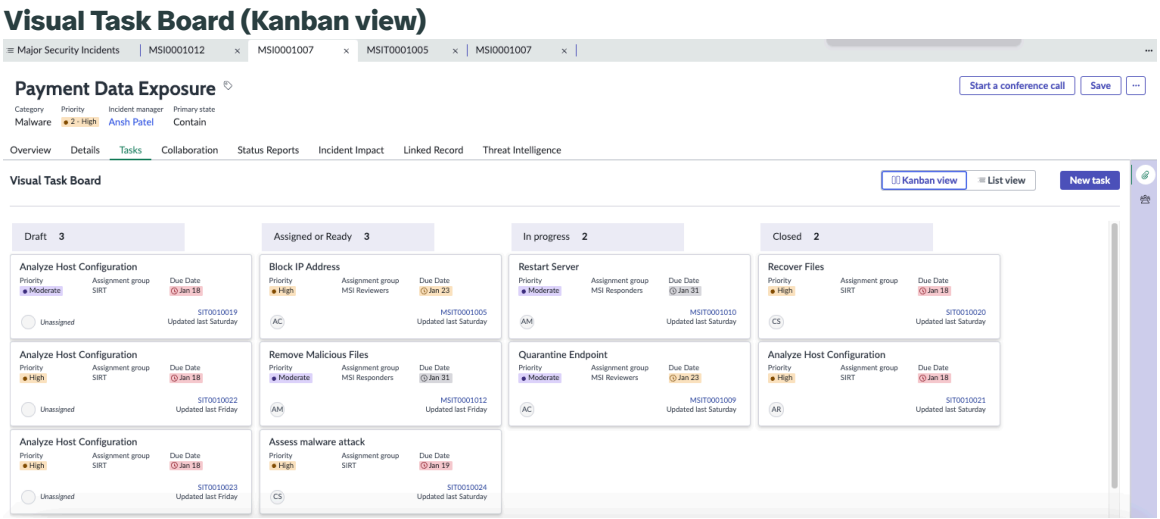
Note: Make sure you have installed the **MSIM VTB Task Card: 1.0.1v** app separately after installing the MSIM app.

The Tasks tab displays the details of all the tasks associated with a major security incident. The Task tab supports two views:

- **Visual Task Board (Kanban view)**:

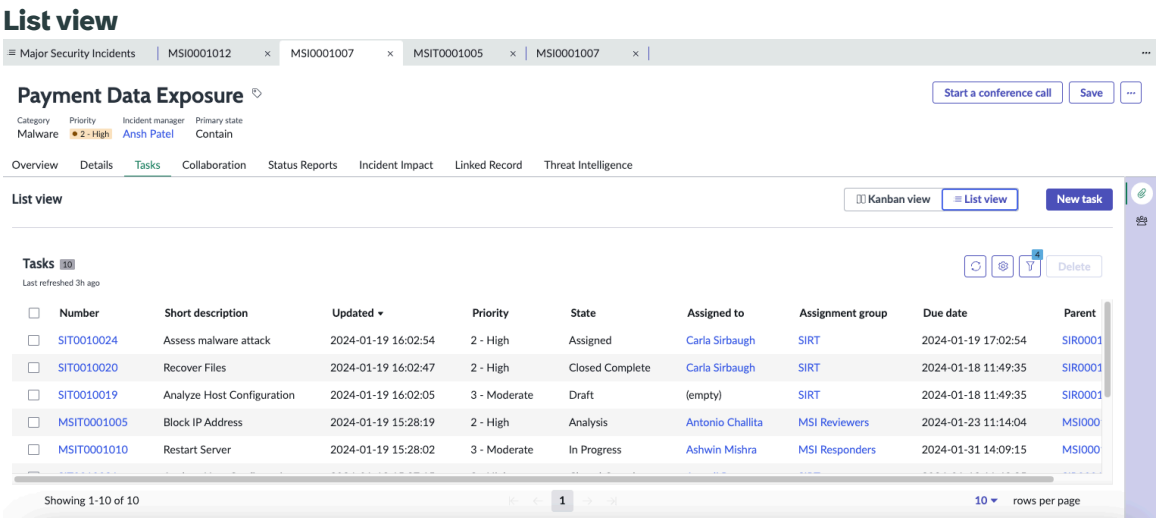
  View and update multiple task records, which appear as cards on the Visual Task Board that can be moved between lanes based on the status of the tasks in the major security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **List view**:

  View and update multiple task records using in the form of lists. Using these list categories and filters, you can quickly find and track the tasks you need to work on in a major security incident.



The labeled activities are summarized and displayed in the Overview section of the major security incident. A trend chart graph is available on the Overview section to view the consolidated task activities state.

Manage tasks using the Visual Task Board

Track and manage all the tasks associated with a major security incident using the Visual Task Board (Kanban view).

You can use the Visual Task Board to move the cards in a step-by-step manner between lanes like Draft, Assigned or Ready, In progress, and Closed depending on the status of the tasks. An activity stream on the board displays recent activity to track task changes easily. You can add task cards from any table that extends Task to quickly track updates and edit major security incidents directly from the board.

Create a task using the Visual Task Board

Role required: sn_msi.workspace_manager.

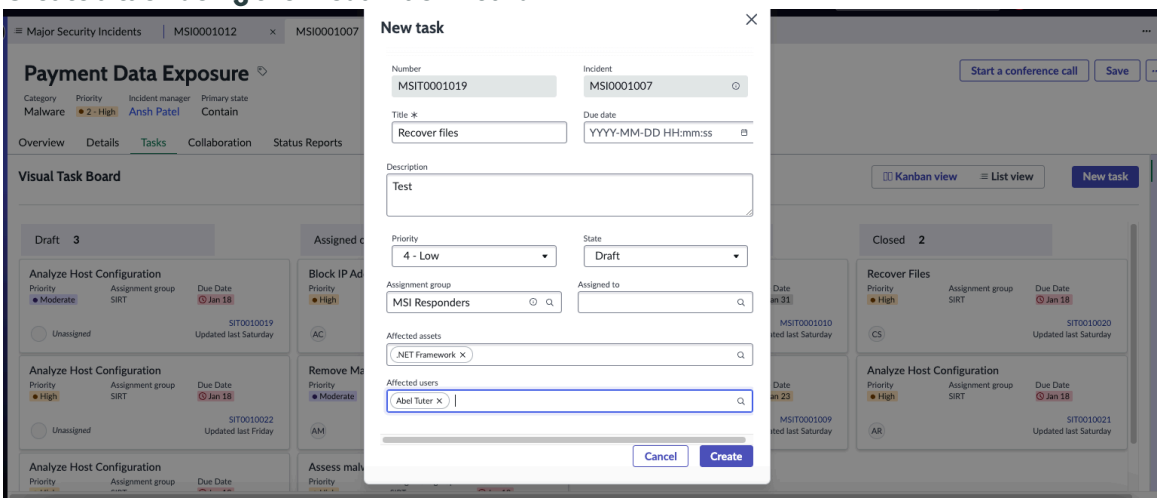
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Make sure you have installed the **MSIM VTB Task Card: 1.0.1v** app separately after installing the MSIM app.

MSI Managers can create a task in the Visual Task Board using the following steps:

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab.

Create a task using the Visual Task Board



5. Select **Kanban view**, and choose **New task**.
6. On the form, fill in the fields.

Field	Description
Number	A unique number that is automatically generated for the selected task. This field isn't editable.
Incident	Major security incident number. This field isn't editable.
Title	Provide a name for the task.
Due date	Select a due date and time for the task to be completed. Select a date using the **Calendar** option and specify the time on the **Select Time** section.
Description	Provide a unique description for the task.
Priority	Select the priority of the task to determine when the task is performed. The priority can be one of the following values: ○ **None** ○ **1-Critical** ○ **2 - High** ○ **3 - Moderate** ○ **4 - Low** ○ **5- Planning**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
State	Select the current state of the task. The state can be one of the following: ○ **Draft** ○ **Analysis** ○ **In Progress** ○ **Closed** The default state is **Draft**.
Assignment group	Select an assignment group of the user to assign the task using the search option.
Assigned to	Select the user to assign the task using the search option.
Affected assets	Select the affected assets by the task using the search option.
Affected users	Select the affected users by the task using the search option.

7. Select **Create** to create the task.

View and modify a task using the Visual Task Board

Role required: sn_msi.workspace_manager.

Note: Make sure you have installed the **MSIM VTB Task Card: 1.0.1v** app separately after installing the MSIM app.

MSI Managers can view the details of a task and activity information from the MSI Responders, and modify a task in the Visual Task Board using the following steps:

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab, and choose **Kanban view**.
5. Choose the desired Task card in one of the lanes to view the details of the task.

   The Task card can be in one of the lanes: Draft, Assigned or Ready, In progress, or Closed.
6. On the Task info section, you can modify the following details:

Field	Description
Number	A unique number that is automatically generated for the selected task. This field isn't editable.
Incident	Major security incident number. This field isn't editable.
Title	Provide a name for the task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

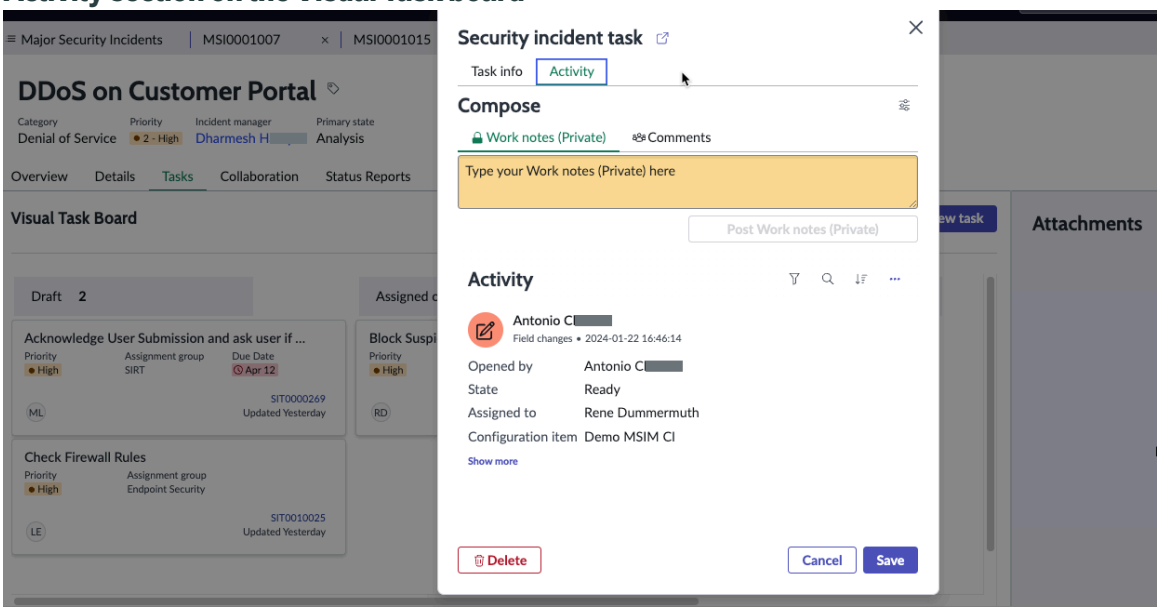
Field	Description
Due date	Select a due date and time for the task to be completed. Select a date using the **Calendar** option and specify the time on the **Select Time** section.
Description	Provide a unique description for the task.
Priority	Select the priority of the task to determine when the task is performed. The priority can be one of the following values: ○ **None** ○ **1-Critical** ○ **2 - High** ○ **3 - Moderate** ○ **4 - Low** ○ **5- Planning**
State	Select the current state of the task. The state can be one of the following: ○ **Draft** ○ **Analysis** ○ **In Progress** ○ **Closed** The default state is **Draft**.
Assignment group	Select an assignment group of the user to assign the task using the search option.
Assigned to	Select the user to assign the task using the search option.
Affected assets	Select the affected assets by the task using the search option.
Affected users	Select the affected users by the task using the search option.

7. Select the **Activity** section to view the activity details from the MSI Responders.

   Use the Activity section to add your work notes and comments, and post your activity privately and also add additional comments as required using the Compose section. Save the activity after you post your work notes and comments to view the added activity or worknotes in the Activity section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activity section on the Visual Task board



Note: Select the **Show more** details link to view the details of a specific security incident record, which is associated with that major security incident.

8. Select **Save** to update the task information.

   The task information gets updated instantly.

Delete a task using the Visual Task Board

Role required: sn_msi.workspace_manager.

Note: Make sure you have installed the **MSIM VTB Task Card: 1.0.1v** app separately after installing the MSIM app.

MSI Manager can delete a task in the Visual Task Board using following steps:

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab, and choose **Kanban view**
5. Choose the Task card that you want to delete.
6. In the Major security incident task pop-up, select the **Delete** option.

   The Delete task pop-up appears requesting you to confirm the deletion of the task.

7. Select **Delete**.

Manage tasks using the List view

Track and manage all the tasks associated with a major security incident using the List view.

The List view displays the details of all the tasks associated with the major security incident like Task number, priority, current state, assigned to, assigned group. Using these list categories and filters, you can quickly find and track the required tasks that you need to work on in a major security incident.

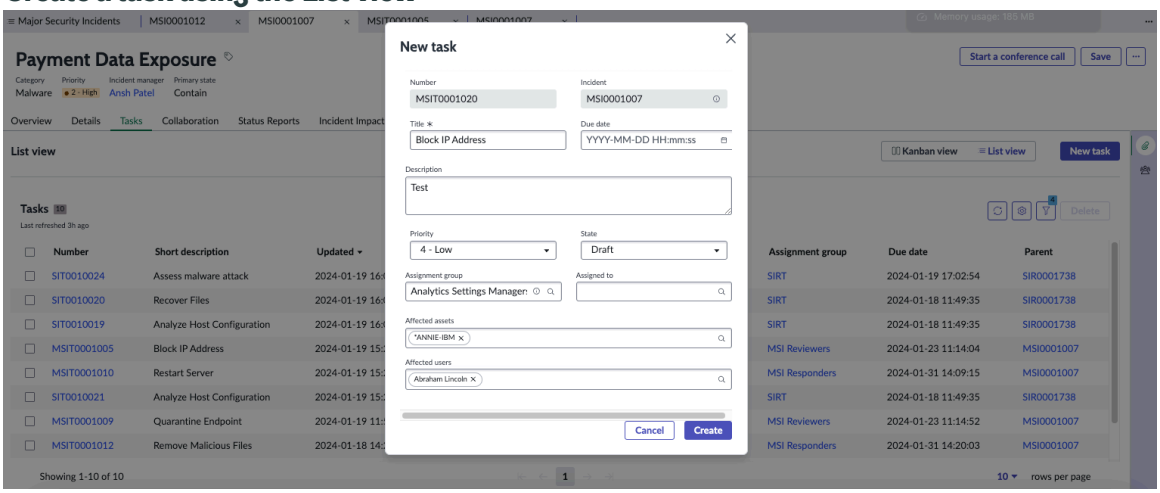
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a task using the List view

Role required: sn_msi.workspace_manager.

MSI Managers can create a task in the List view using the following steps:

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab.



5. Select **List view**, and choose **New task**.
6. On the form, fill in the fields.

Field	Description
Number	A unique number that is automatically generated for the selected task. This field isn't editable.
Incident	Major security incident number. This field isn't editable.
Title	Provide a name for the task.
Due date	Select a due date and time for the task to be completed. Select a date using the **Calendar** option and specify the time on the **Select Time** section.
Description	Provide a unique description for the task.
Priority	Select the priority of the task to determine when the task is performed. The priority can be one of the following values: ○ **None** ○ **1-Critical** ○ **2 - High** ○ **3 - Moderate**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **4 - Low** ○ **5- Planning**
State	Select the current state of the task. The state can be one of the following: ○ **Draft** ○ **Analysis** ○ **In Progress** ○ **Closed** The default state is **Draft**.
Assignment group	Select an assignment group of the user to assign the task using the search option.
Assigned to	Select the user to assign the task using the search option.
Affected assets	Select the affected assets by the task using the search option.
Affected users	Select the affected users by the task using the search option.

7. Select **Create** to create the task.

View and modify a task using the List view

Role required: sn_msi.workspace_manager.

MSI Managers can view the details of a task and activity information from the MSI Responders, and modify a task in the List view using the following steps

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab, and choose **List view**.
5. Choose the desired Task on the list view to view the details of the task.
6. On the Task Info section, you can modify the following details:

Field	Description
Number	A unique number that is automatically generated for the selected task. This field isn't editable.
Incident	Major security incident number. This field isn't editable.
Title	Provide a name for the task.
Due date	Select a due date and time for the task to be completed. Select a date using the **Calendar** option and specify the time on the **Select Time** section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

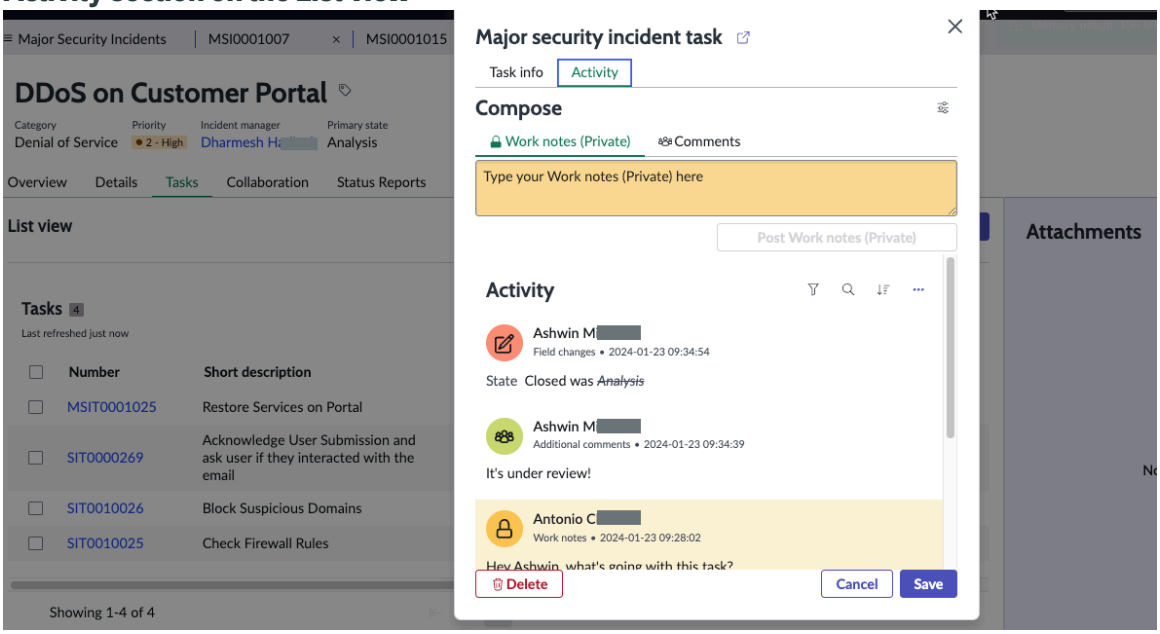
Field	Description
Description	Provide a unique description for the task.
Priority	Select the priority of the task to determine when the task is performed. The priority can be one of the following values: ○ **None** ○ **1-Critical** ○ **2 - High** ○ **3 - Moderate** ○ **4 - Low** ○ **5- Planning**
State	Select the current state of the task. The state can be one of the following: ○ **Draft** ○ **Analysis** ○ **In Progress** ○ **Closed** The default state is **Draft**.
Assignment group	Select an assignment group of the user to assign the task using the search option.
Assigned to	Select the user to assign the task using the search option.
Affected assets	Select the affected assets by the task using the search option.
Affected users	Select the affected users by the task using the search option.

7. Select the **Activity** section to view the activity details from the MSI Responders.

   Use the Activity section to add your work notes and comments, and post your activity privately and also add additional comments as required using the Compose section. Save the activity after you post your work notes and comments to view the added activity or worknotes in the Activity section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activity section on the List view



Note: Select the **Show more** details link to view the details of a specific security incident record, which is associated with that major security incident.

8. Select **Save** to update the task information.

   The task information gets updated instantly.

9. You can also perform the following actions on the List view:
   a. Select the **Refresh** icon to refresh the list of tasks on the List view.
   b. Select the **Settings** icon, and use the **Edit columns** option to modify the list of columns that appear on the List view. Use the **Reset widths** option to reset the widths of the columns.

Delete a task using the List view

Role required: sn_msi.workspace_manager.

MSI Manager can delete a task in the List view using following steps:

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Choose the required major security incident record.
4. Select the **Tasks** tab.
5. Select **List view**.
6. Choose a Task that you want to delete from the list.
7. In the Major security incident task pop-up, select the **Delete** option.

   The Delete task pop-up appears requesting you to confirm the deletion of the task.

8. Select **Delete**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Track collaboration activity via MSIM workspace

Track chat and file activities related to resolving major security incidents through the MSIM Workspace.

Activities are coordinated using Microsoft Teams chat and Microsoft SharePoint files and folders and then posted back to the Major Security Incident via integrations.

Once Microsoft Teams and Microsoft SharePoint are integrated with Major Security Incident Management, you can use the MSIM Workspace to track collaboration between incident response users and other groups who are contributing to the resolution of a major security incident. Any updates to collaboration folders and files in Microsoft SharePoint are synchronized with the MSIM Workspace File Explorer and also reflected in the Activity stream components.

When a security incident is promoted as major security incident:

1. A folder structure will be created in Microsoft SharePoint based on the folder template configuration. The same folder structure will be reflected on the File Explorer component of the workspace.
2. A team with multiple channels is created under Microsoft Teams application and the same will be reflected on the Chat Management component of the workspace.

Role required: sn_msi.workspace_manager.

Interact with files and folders

The File Explorer displays the file system so you can view and interact with files and folders related to resolving the incident.

Displays the file and folders which are captured at Microsoft SharePoint for a specific security incident. These folders will be automatically created on Microsoft SharePoint for that major security incident. You can use this default created folders to upload any supporting files, if required. You can rename, move, or delete these files and folders as required.

Also, whenever you upload a file to any of the folders, the activity corresponding to those folders will be automatically associated to the File Explorer folders in the Collaboration tab and the activity will be recorded and displayed in the Activity section of the Major Security Incident Management Workspace.

Note: On the **Collaboration** tab, the incident record is appended to the parent file on the sharepoint with a unique incident number and incident category.

1. **Repository view**: Lists the files and folders which are listed in the Microsoft SharePoint for that specific security incident. For each file or folder the repository view displays the Name, Modified by, Last modified, and Size will be displayed.

Repository view

Field	Description
Open in SharePoint	Select this option available next to your major security incident. Click on the link to select and view the folder structure in Microsoft SharePoint.
New Folder	Select this option to create a new folder as required. After you create a new folder, the same new folder is created and associated in your Microsoft SharePoint, by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. **Recents**: Displays all the recent activity logs. These logs include both your SharePoint and File Explorer activities. The recent activities are usually your supporting files which are inclusive of the parent folder.

   Following is the procedure to **Locate Log file:**

   a. Select the respective file to view the details.

   b. Click **Locate File**.

   > **Note:** The navigation and details of the parent file and the parent folders are displayed under the **Recents** list view section. You can open the same file in your SharePoint. Whenever you upload the related log files or any activities, all those files and activities are displayed both in SharePoint and File Explorer.

Manage Chat Channels communications using Microsoft Teams

The Chat Channel Manager displays Microsoft Teams with multiple channels created in the Microsoft Teams application based on a configuration template setup.

These configured channels are reflected in the Chat Management component along with the users and user groups assigned to them. The Chat Channel Manager enables you to perform the following:

- **Manage Chat channels**
- **Rename team**
- **Manage team members**

The team and channels are created based on the Chat Channel configuration in Microsoft Teams.

Manage Chat Channels

The Chat Channel Manager enables you to create, edit, or delete Chat Channels. To manage a Chat Channel in Microsoft Teams, perform the following steps:

1. Select the **Collaboration** tab.
2. Navigate to **Chat Channel Manager** > **Create New Channel**.
3. Add a new **Channel Name**, **Description**, and select the **Members** for the channel.
4. Select **Create**.

   > **Note:** A new channel record is created in the Microsoft Teams Channels section of the Microsoft Teams application and the same record will be reflected in MSIM.

5. To edit a Chat Channel, select a Chat Channel in the Chat Channel Manager list.
6. You can modify the Channel name, Members list, Group Members list based on your requirements.
7. Select **Save**.
8. To delete a Chat Channel, select a Chat Channel in the Chat Channel Manager list.
9. Select **Delete Channel**.

Rename Team

To rename a team in Microsoft Teams, perform the following steps:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Select the **Collaboration** tab.
2. Navigate to **Chat Channel Manager** > **Rename team**.
3. In the Team name field, rename the team according to your requirements.
4. Select **Save**.

> **Note:** Renaming the team name will also rename the team name in Microsoft Teams.

Manage team members

The Chat Channel Manager enables you to add or remove team members in Microsoft Teams. You can also add members through groups. To manage team members in Microsoft Teams, perform the following steps:

1. Select the **Collaboration** tab.
2. Navigate to **Chat Channel Manager** > **Manage team members**.
3. In the Members field, add or remove team members according to your requirements.
4. In the Add members via Groups field, select the groups that you want to add in Microsoft Teams.

   > **Note:** If the group members are already on the team, then those members won't be added.

5. Select **Save**.

   The Chat Channel Manager displays the details of the total team members and the number of new members who will be added.

Manage Chat Channels communications using Slack

The Chat Channel Manager displays Slack with multiple channels created in the Slack application based on a configuration template setup.

These configured channels are reflected in the Chat Management component along with the users and user groups assigned to them. The Chat Channel Manager enables you to **Manage Chat channels**. The team and channels are created based on the Chat Channel configuration in Slack.

Manage Chat Channels

The Chat Channel Manager enables you to create, edit, or delete Chat Channels in Slack. To manage a Chat Channel, perform the following steps:

1. Select the **Collaboration** tab.
2. Navigate to **Chat Channel Manager** > **Create New Channel**.
3. Add a new **Channel Name**, **Description**, and select the **Members** for the channel.
4. Select **Create**.

> **Note:** A new channel record is created in the Slack Channels section of the Slack application and the same record will be reflected in MSIM.

5. To edit a Chat Channel, select a Chat Channel in the Chat Channel Manager list.
6. You can modify the Channel name, Members list, Group Members list based on your requirements.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select **Save**.
8. To delete a Chat Channel, select a Chat Channel in the Chat Channel Manager list.
9. Select **Delete Channel**.

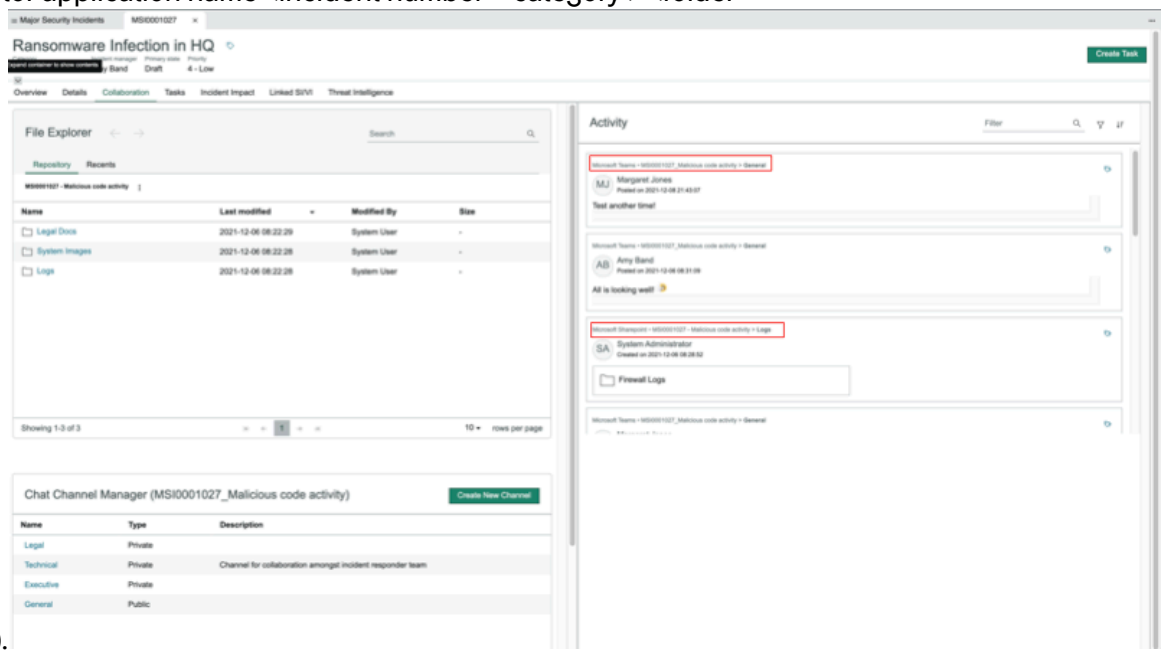
Manage activity stream conversations

Displays all the activities, logs, status that were performed on Microsoft SharePoint, File explorer, and Microsoft Teams.

If you want to view any specific activity or search the collaboration activity details which were interacted between various file and folders and also on Microsoft Teams, then you can use the filter capability which is displayed on top right of the Activity Stream section and locate the desired activity details.

Folders and chat conversations shared with Major Security Incident Management reflect as breadcrumbs with the structure:

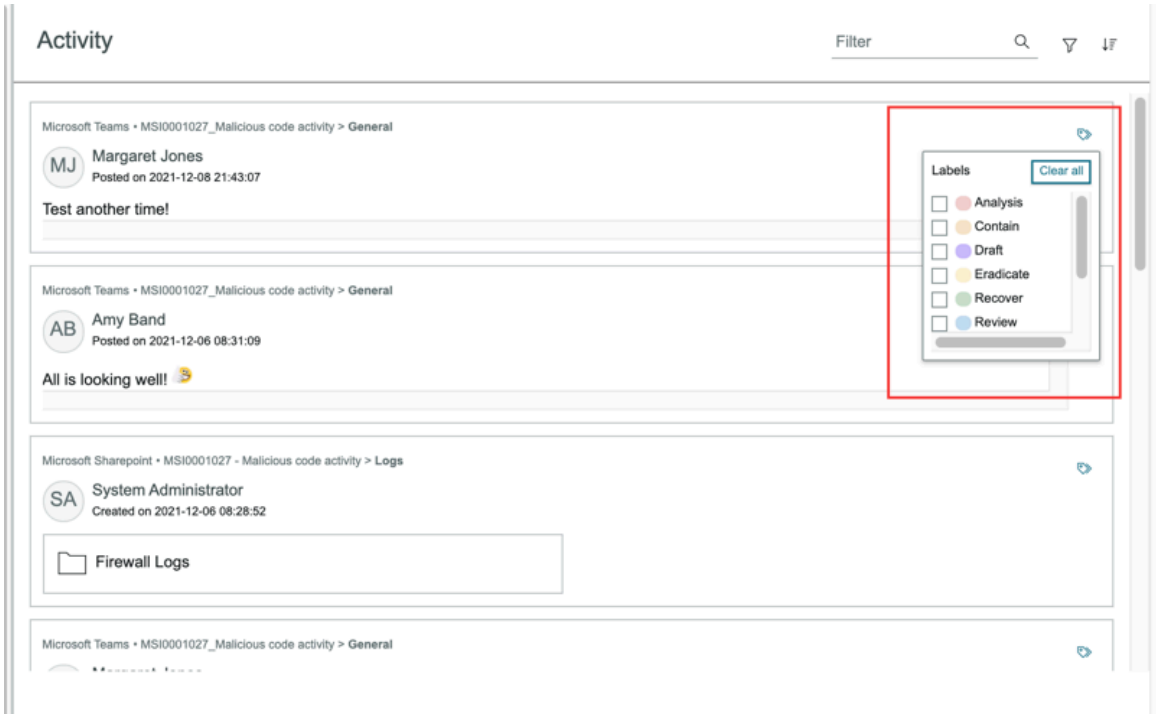
connector application name <incident number – category > <folder name>).



Label the activities:

1. Click on the **Label** icon.
2. Select the respective incident activity label check box as shown in the below screen shot.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. The labelled activities are color coded and depicted as progress trend graph on the **External Collaboration** section of the workspace.

Create and distribute MSIM Status Reports

As a Major Security Incident manager, you can create and distribute the different status reports to different stakeholders at various intervals based on the configured report template or a previous status report throughout the course of the major security incident resolution.

Before you begin

Role required: sn_msi.workspace_manager

You can preview the previously configured summary report data elements, add additional text or summary, remove individual report components as needed, and verify the accuracy and completeness of the report before distributing it to different stakeholders.

Create the status reports by selecting the desired report template that was initially configured on the MSI Report Templates Setup page.

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select the **Lists** view.
3. Select the respective promoted MSI record.
4. Select the **Status Reports** tab.
   The Status Reports tab contains three different types of subsections such as below.

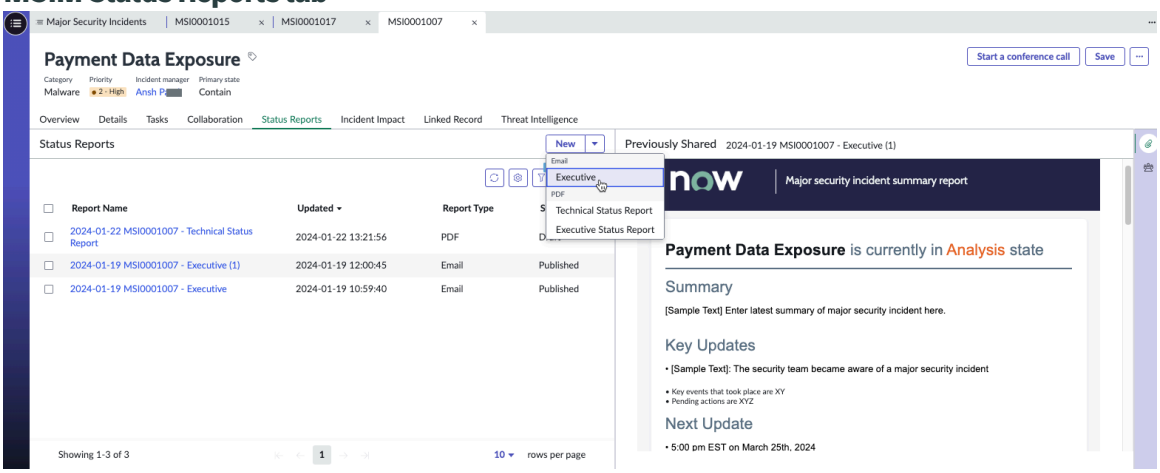
Field	Description
Report Name	Name of the status report template.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The Status Reports view lists the existing predefined report templates that are available as a part of the base system for the concerned persona. For example, Executive Status Reports through email (Mobile-friendly), Technical Status Reports and Executive Status Reports as PDFs.
Updated	The date when the report template was last updated.
Report Type	Type of status report. The status report can be in one of the following types: ○ PDF ○ Email
State	State of the status reports. The status reports can be in one of the following states: ○ Draft ○ Queued ○ Published

5. Select the type of the status report that you would want to view or select **New** to create a status report.

MSIM Status Reports tab



6. Choose one of the following status report types from the list.
   - **Executive** Email Status Reports that are mobile-friendly.
   - **Technical Status Report** PDF
   - **Executive Status Report** PDF

   Note: When you select any desired report template, the preview of the selected report is immediately generated in the right-pane. You can view the selected status report of the MSI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

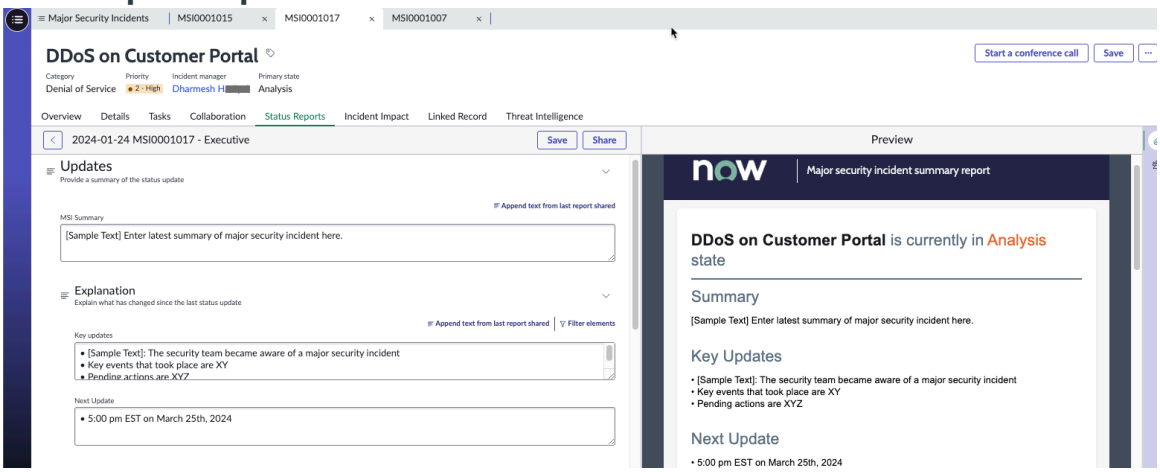
7. On the Executive Email Status Report template, fill the sections with the details of the status report.

Report section	Description
Updates	Provide a summary of the status update. This sec tion contains the following: ○ **MSI Summary**: Provide a brief summary of the ma jor security incident. ○ **Append text from last report shared**: Select this option to append the text from the last report shared.
Explanation	Add an explanation on what has changed since the last status update was done. This section contains the following: ○ **Key updates**: Provide key updates like what the se curity team should know about the major security incident, name the key events that took place, and list any pending actions. ○ **Next Update**: Provide the date and time of the next update for resolving the major security inci dent. For example, 5:00 pm EST on March 25th, 2024. ○ **Append text from last report shared**: Select this option to append the text from the last report shared. ○ **Filter elements**: Select the report elements to be included in the report. For example, Key Updates or Next Updates.
Additional Information	Provide specific details relevant to the status up date.
Visualizations	Select the visualizations that best help communi cate the status update. ○ **Incident Impact**: Select the Incident Impact met rics like Affected Assets, Affected Location, Affect ed Users that are related to the status update. ○ **Filter elements**: Select the report elements to be included in the report. For example, Incident Im pact.
Lists	Select lists of records that provide context to the sta tus update. ○ **Linked records**: Select the records that are linked to the major security incident status update. For example, Linked Security Incident. ○ **Filter elements**: Select the report elements to be included in the report. For example, Linked records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The options that you've selected from the Status Reports section are the same options that are rendered in the Preview report.

Status Report Template



8. Select **Save** to save the updates you made to the status report.
9. Select **Share** to share the status report with internal and external stakeholders.
   The Share dialog box appears.

   a. In the Subject field, enter the subject for the email report.

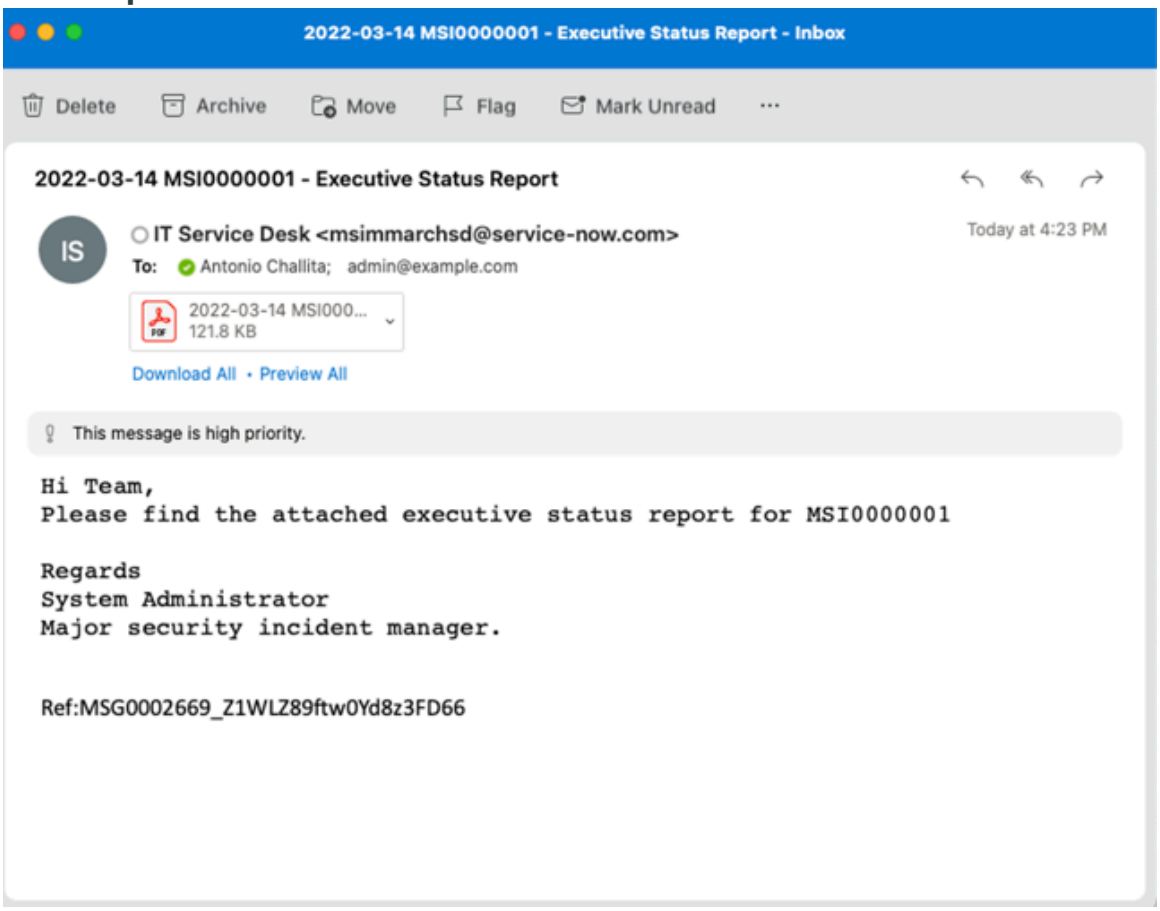
   b. In the Add internal recipients field, type and select the recipients for the email report.

   c. In the Add external recipients field, type the recipients' email or DL for the email report.
   You can add multiple email IDs using a comma or semi-colon.

10. Select **Email Report**.
    An email with the attached PDF Status Report is successfully sent to the concerned recipient for them to verify.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Status Report - email



11. You can also perform the following actions on the Status Reports tab:
    a. Use the **Refresh** action on the Status Reports view to refresh the status reports list.
    b. Use the **List Actions** action on the Status Reports view to edit columns or reset the widths of the status reports list.
    c. Use the **Filter** action on the Status Reports view to filter the status reports based on certain conditions.

Related topics

Configure Major Security Incident status reports

Managing MSIM status reports

Status Reports provide preconfigured trend charts with actionable data visualizations to improve security operations processes, measure and analyze the resolution timeline, overdue count, and status of each assigned task.

Configure Major Security Incident status reports

Configure major security incident reports to set up and download the reports according to your business needs throughout the life cycle of the major security incident record remediation process.

You can build the report templates with a specific format and layout, and customize these reports according to your specific requirements using the Status Reports feature of the Major Security Incident Management workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A user with the sn_msi.workspace_manager role can create and configure the report templates that outline the type of report information that can be used to generate all the status reports, which can be shared with specific users such as executive stakeholders, legal departments and map those templates to the major security incident records.

To customize your MSI status reports, you must first set up the report templates using **Report Templates**. With the help of Report Templates, you can build the report template types, define the report components for those report templates, add additional information, create visualized data to track the scope and progress metrics, add related list data, and generate the status reports.

The following describes the default fields provided in all the report template types. You can configure and format the report template based on your requirements using sections, subsections, and its elements:

Status Report components

Component Type	Description
Report Title	Title of the report type. For example, the default format of the report type is: {MSI Number} - {Executive Stakeholder Report} depicted as MSI0001001: Executive Stakeholder Report.
Name	Displays the name of the user who generated the report using the Status Reports section of the Major Security Incident Management workspace.
Summary	Displays a brief summary of the report.
Date	Displays the date on which the report is shared with the concerned recipient.
Progress	Displays the Scope and Progress Metrics such as the linked SIR Incidents, Response Tasks, Supplementary Tasks, External Collaboration, Timeline components, and Recent Timeline Events.
Challenges	This section displays a brief description on the challenges involved throughout the major security incident remediation process.
Next Steps	This section displays a brief description on the next steps involved in resolving the major security incident. For example, the active team subsection in the executive stakeholder report provides you with the information with the next step on the team assignment who is involved in further analysis of the major security incident record.
Other customizations	The report template also provides you with the capability to upload the logo and customize the headers and footers on the report.

Following are the types of report categories that can be set up and viewed:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Executive** Email
- **Technical Status Report** PDF
- **Executive Status Report** PDF

The above reports are configured and available for the user to select, view, and generate the report from the Major Security Incident Management workspace.

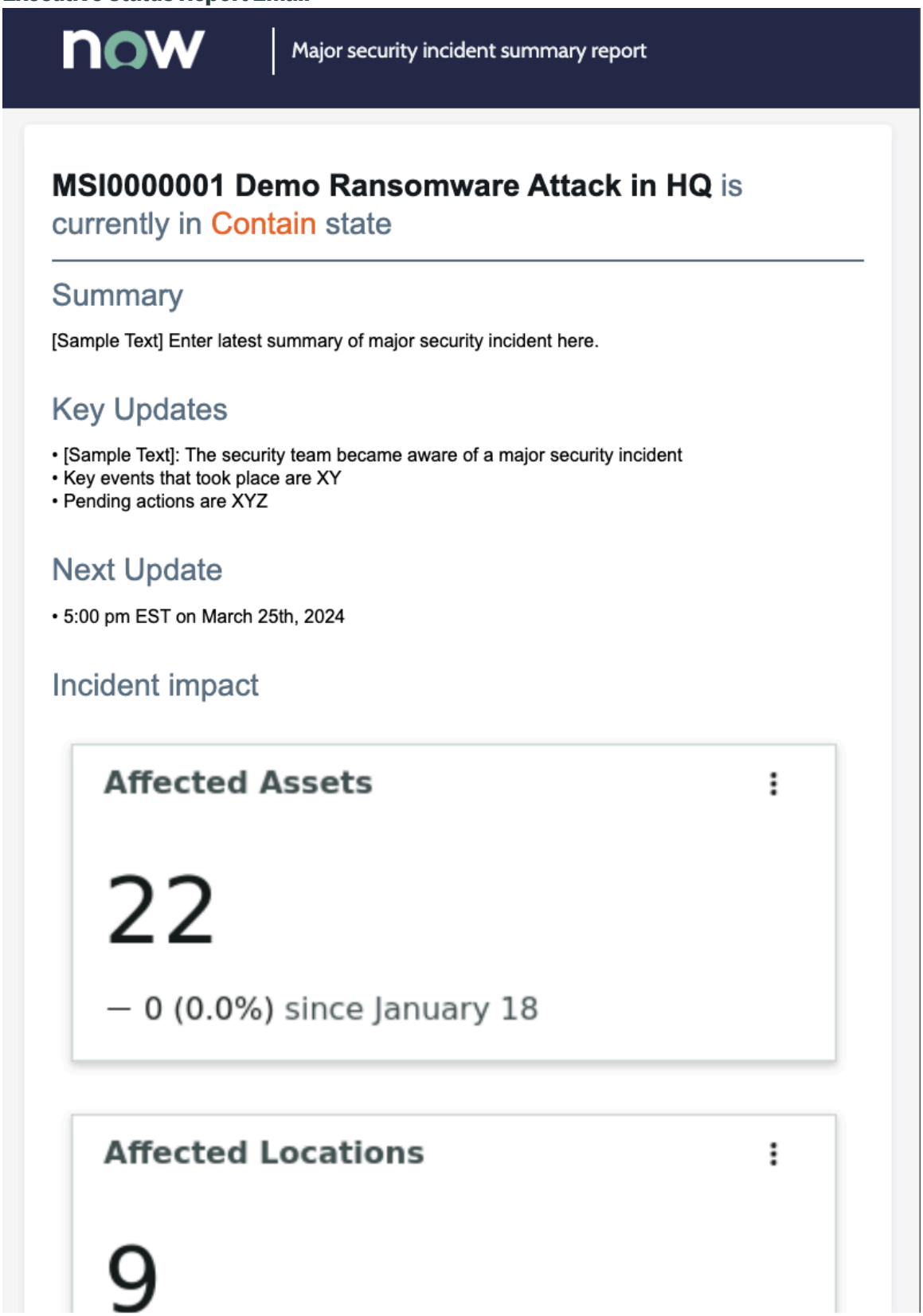
Mobile-friendly Executive Status Reports - Email

The Executive Status Reports - Email are mobile-friendly status reports that are generated in email format. The report section includes a summary of the report, MSI duration column, incident scope/impact, active team metrics, progress metrics, and Timeline components such as the recent timeline events for that specific major security incident record.

Customize and configure the following report template features to add additional information to the report. A sample executive email status report is shown below for your reference.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Executive Status Report Email



Executive Status Reports - PDF

The Executive Status Reports - PDF are status reports that are generated in PDF format. The report section includes a summary of the report, MSI duration column, incident scope/impact,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

active team metrics, progress metrics, and Timeline components such as the recent timeline events for that specific major security incident record.

Customize and configure the following report template features to add additional information to the report. A sample executive report is shown below for your reference.

Executive Status Report PDF



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22 — 0 (0.0%) since January 18
Affected Locations 9 — 0 (0.0%) since January 18
Affected users 45 — 0 (0.0%) since January 18

Figure 1. Incident Impact

Progress

By incident state — Analysis, Contain, Recover
Trends by incident state — Analysis, Contain, Recover, Eradicate, Review

Figure 2. Linked Security Incidents

In progress tasks by incident state label — Eradicate 1 17%, Analysis 2 33%, Contain 1 17%, Recover 2 33%, 6

Figure 3. Response Tasks

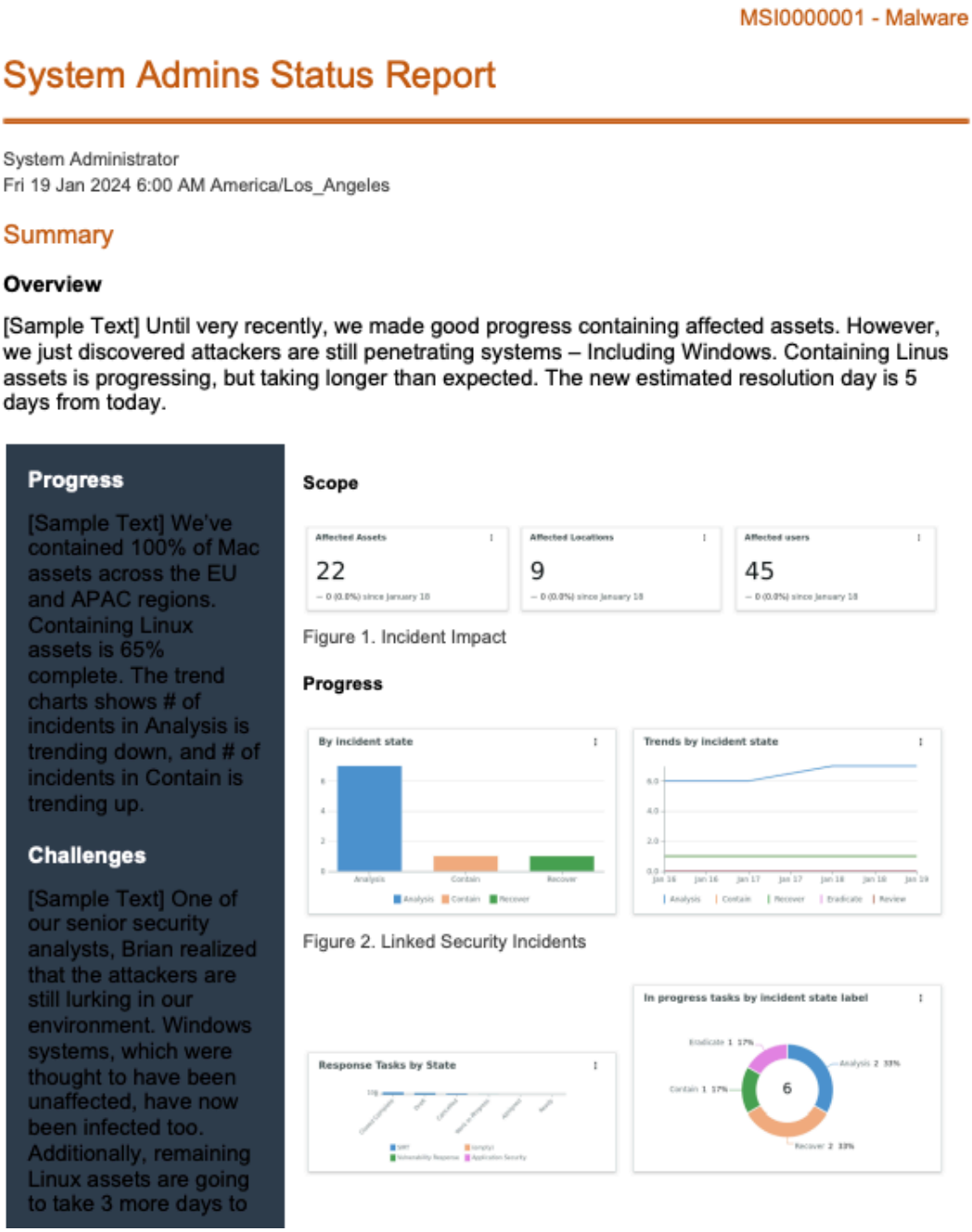
Technical Status Reports - PDF

The Technical Status Reports - PDF are status reports that are generated in PDF format. The report section includes a summary of the report, MSI duration column, incident scope/impact, active team metrics, progress metrics, and Timeline components such as the recent timeline events for that specific major security incident record, labeled Task updates and labeled activities, based on the assignment group and selected tag label since when the last status report is generated, and additional information such as incident impact and linked incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Customize and configure the report template to add additional information to the report. A sample technical report that shows the additional information, such as the incident impact, is illustrated below for your reference, and the remaining part of the report information is similar to the executive reports.

Technical Status Report - PDF



MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22 — 0 (0.0%) since January 18
Affected Locations 9 — 0 (0.0%) since January 18
Affected users 45 — 0 (0.0%) since January 18

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

The report template sections contain various subsections, which describe how you can construct the report subsections and its elements such as:

1. Branding: Add Branding to your Report Templates
2. Template Scripts: Use Template Scripts in your Report Templates
3. Use Visualizations in Report Templates
4. Use Reports Lists in Report Templates

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a Report Template

Create various report templates, which can be applied to the major security incidents and generate a status report. You can add standard and custom Major Security Incident Response form fields to the report template that are dot-walkable. In addition, you can format and configure the report based on your requirements using sections, subsections, and its elements.

Before you begin

Role required: sn_msi.workspace_manager

About this task

You can define report components to your report templates and provide additional information. Create visualized data to track the scope and progress metrics, add related list data, preview, and generate or share the status reports.

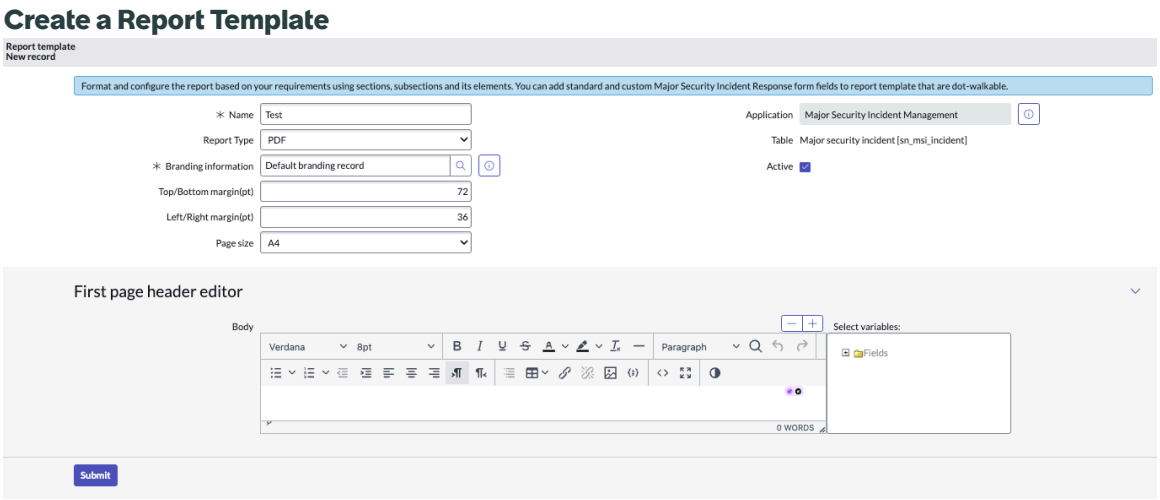
Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Select **New** to create a report template.
4. On the Report template form, fill the fields.

Field	Description
Name	Name of the report template.
Branding information	Select the branding information of your report template such as logo, header, and footer text. For example, Default branding record.
Report Type	Type of status report. The status report can be in one of the following types: ○ PDF ○ Email
Table	Name of the report template table.
Top/Bottom Margin	Define the top and bottom margin indenta tions required while generating the report.
Left/Right Margin	Define the left and right margin indentations required while generating the report.
Page Size	The page size of your report template. For ex ample, the default size is A4.
Active	Select the check box for the MSI Manager to generate a report from the template that was created from the **Reports Template** section. **Note:** If the check box is cleared, then the MSI Manager can't create a report for that specific report template type in the MSIM workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
First page header editor	Allows you to define the template body. Select the required variables to add to the template editor section.



5. **Submit** the new report template record.
   A new report template is created under the Reports Templates page.

Related topics

Create and distribute MSIM Status Reports

Add Branding to your Report Templates

Add branding to your reports. You can add header and footer image, header and footer text. You can include this branding information in any of the report template types that you want to create other than the two predefined reports.

Before you begin

Role required: sn_msi.workspace_manager

About this task

The key considerations while adding branding to your report templates are as follows:

- Upload the header and footer image and align the image position.
- The maximum size limit for the header and footer image is 5 MB. If the size exceeds more than the specified limit, then an error message, 'Image format can't be recognized' is displayed in the major security incident.
- Adjust the header and footer image height.
- The footer text length is limited to 100 characters.

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
2. Drill down to **Report Template** > **Branding**.
3. Select **Configure**.
4. Select **New** to add a branding to your report template.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. On the Branding template form, fill the fields.

Field	Description
Name	Name of the branding template.
Header image	Add a Header image for the branding tem plate by performing the following steps: **a.** Select **Click to add**. **b.** Select **Choose File** **c.** Choose an image from your system and se lect **OK**.
Footer image	Add a Footer image for the branding template by performing the following steps: **a.** Select **Click to add**. **b.** Select **Choose File** **c.** Choose an image from your system and se lect **OK**.
Header image position	Select a header image position for the brand ing template. You can choose **Left**, **Center**, or **Right**.
Footer image position	Select a header image position for the brand ing template. You can choose **Top left**, **Top center**, **Top Right**, **Bottom left**, **Bottom cen ter**, or **Bottom Right**.
Header image height	Provide a height value (in pt) for the Header image of the branding template.
Footer image height	Provide a height value (in pt) for the Footer im age of the branding template.
Footer text	Provide a footer text for the branding tem plate. You can include classification or confi dentiality information. For example, this email is classified as Confidential, Internal Only or Client Attorney Privileged.
Footer text position	Select a footer text position for the branding template. You can choose **Top left**, **Top cen ter**, **Top Right**, **Bottom left**, **Bottom center**, or **Bottom Right**.

6. Select **Submit**.
   A new branding template is created under the Branding Templates page.

Use Visualizations in Report Templates

Use report widgets to define and include User Interface Builder (UIB) elements such as data visualizations in the MSIM status reports.

Before you begin

Role required: sn_msi.workspace_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. Drill down to **Report Template** > **Visualizations**.
3. Select **Configure**.
   The following are the predefined UIB Visualizations as a part of the base system, which you can use to configure and modify your status reports.

Widget name	Description
Active Team	Displays the list of active teams involved in re solving the MSI.
Affected Assets	Displays the list of affected assets.
Affected Locations	Displays the list of affected locations.
Affected Users	Displays the list of affected users.
Collaboration Pie Graph	Includes the collaboration activities in the Pie graph.
Collaboration Trend Graph	Displays the collaboration activities as a trend graph.
Estimated resolution date	Displays the estimated resolution date by when the MSI is estimated to be resolved.
Linked Incidents Bar Graph	Displays the linked incidents bar graph.
Linked Incidents Trend Graph	Displays the linked incidents trend graph.
MSI Response Tasks Bar Graph	Displays the MSI Response tasks graph.
Response Tasks Bar Graph	Displays the Response tasks bar graph.
Response Tasks in Progress by Labels	Displays the response tasks in progress by la bels.
Response Tasks Overdue	Displays the total response tasks that are overdue for closure.
Response Tasks Trend Graph	Displays the response tasks trend graph.
Time elapsed since incident detection	Displays the time elapsed from the time the in cident is detected.
Timeline	Displays the timeline of key events and mile stones that have occurred as part of the ma jor security incident.

Related topics

Create a Visualization Type Element

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use Reports Lists in Report Templates

Use report lists to define and include the related list artifacts to generate lists in the PDF based on your configured MSI list records.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. Drill down to **Report Template** > **Lists**.
3. Select **Configure**.
   The MSI Status Reports Lists section describes how each specific related list is affected since the incident is created. The following are the predefined MSI Report Lists as a part of the base system, which you can use to configure and modify your status reports.

MSI Report Lists	Description
Affected Assets	The related list of affected assets view in the status report.
Affected Locations	The related list of affected locations view in the status report.
Affected Users	The related list of affected users view in the status report.
Indicators	The related list of indicators view in the status report.
Linked Security Incident	The related list of linked security incident view in the status report.
Observables	The related list of observables view in the sta tus report.

Related topics

Create a List Type Element

Use Template Scripts in your Report Templates

Create a script to include the related lists data, date operations, and any other data that aren't directly dot-walkable.

Before you begin

Role required: sn_msi.workspace_manager

About this task

You can use this predefined template script in your report templates to include any related data after the report templates are configured and customized.

Construct a template script to display the related list data on the report template. If you want to utilize and populate any template script, then you must add the tag template script tag as: `${template_script:script name}`.

Example: `${template_script:msi_collab_cards}`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can't delete the predefined template scripts. An error message is displayed if a user with an admin role attempts to delete a template script record if it's mapped with any report template.

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. Drill down to **Report Template** > **Template Scripts**.
3. Select **Configure**.
   The following are the predefined Template Scripts as a part of the base system, which you can use to configure and modify your status reports.

Template Script name	Description
formatted_current_date	Returns the current local date and time in the DDMMYYYY 00.00 AM or p.m. format. For ex ample, 21 Jan 2021 3:51 p.m. PST.
msi_active_team	Generate HTML for active team cards.
msi_collab_cards	Generate HTML for collaboration activity cards.
msi_task_activities	Generate HTML for task cards.
msi_timeline_events	Generate HTML for timeline event cards.
si_affected_users	Returns the affected users from the related list in a tabular form.
si_assessments	Returns the post incident assessment results in a tabular form.
si_associated_phish_emails	Returns the associated phishing emails from the related list in a tabular form.
si_associated_phish_headers	Returns the associated phishing headers from the related list in a tabular form.
si_business_criticality	Returns color-coded business criticality val ue.
si_malicious_observables	Returns the malicious observables from the related list in a tabular form.
si_observables	Returns the observables from the related list in a tabular form.
si_priority	Returns a color-coded priority value.
si_response_tasks	Returns the response tasks from the related list in a tabular form.
si_time_to_identify	Returns the duration spent in the Draft and Analysis state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Template Script name	Description
si_time_to_resolve	Returns the time to resolve the incident.

Note: You can also create your own template script to include the related lists data, date operations, and any other data that aren't directly dot-walkable, in addition to the listed template scripts.

Preview the Report Template

Use the Preview functionality to preview your design-time report template to generate and share the report with other stakeholders during run time from the Major Security Incident Management workspace.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Select the desired Report Template.
4. Select the Report Type as **Email** or **PDF** based on your requirement.
5. Select the **Save and Preview Report** action.

   The Preview Report dialogue box displays.
6. Select a major security incident using the Search option to preview a report with the selected template.
7. Select **Preview Report**.
   The report generates a preview according to the selected template configuration. If you selected the Report Type as **Email**, then the preview is in email template format. The status reports in email format are mobile-friendly.

Create a Report Section Template

A report can further be divided into various sections. Use the Report section to break down the report into multiple sections and reorganize them in order.

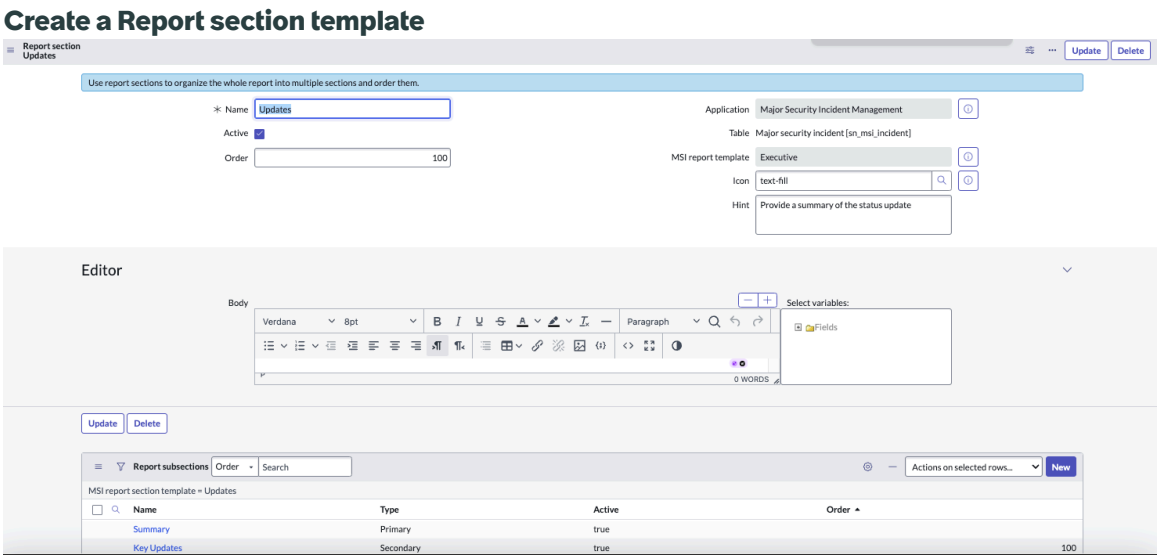
Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template.
4. Navigate to **Report sections** > **New**.
   The new report section page displays.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. On the Report section template form, fill in the fields.

Field	Description
Name	Name of the Report template section. For ex ample, Summary.
Table	Name of the report template table.
Active	Select the check box to create a report sec tion for the selected template in the MSIM workspace. **Note:** If the check box is unselected, the MSI Manager can't create a report section for this template in the MSIM workspace.
MSI report template	The MSI Report Template name for which the report is divided into sections.
Order	The order in which the report sections will be rendered.
Icon	Use the icon to display system icons in the re port.
Hint	Use the hint text to guide the report creation. Within the report, the hint text is displayed un der the section title.
Editor - Body	Define the template section body. You can de fine the section body by selecting the custom tokens or variables from the editor.

6. Save and **Submit** the new report template section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a Report Subsection Template

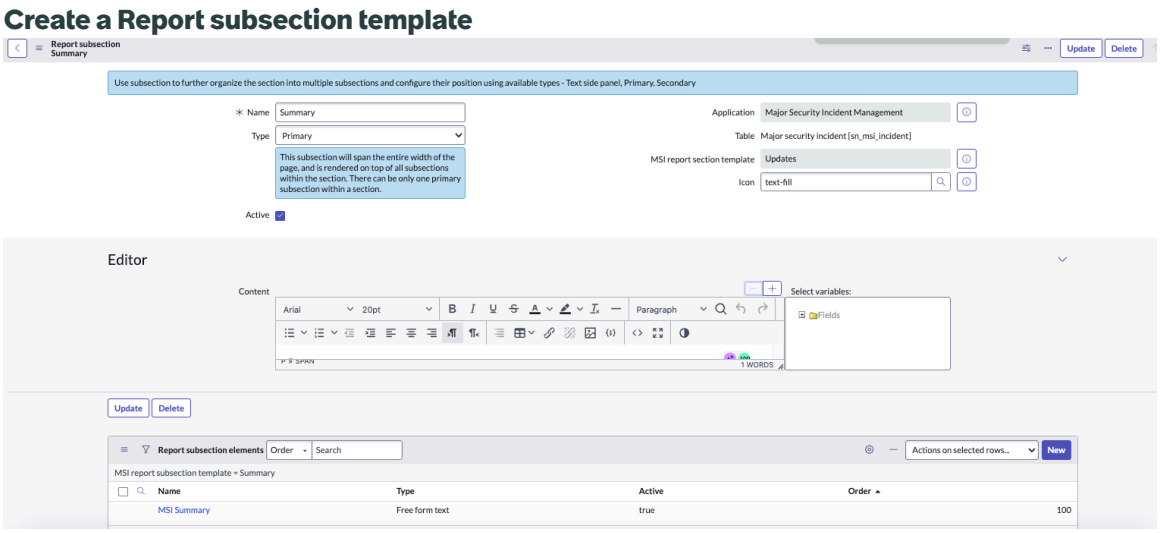
Use the report subsection to further organize the section into multiple subsections and configure their alignment and position using the available types such as Text side panel, Primary, and Secondary.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. Navigate to **Report subsections** > **New**.



6. On the Report subsection form, fill in the fields.

Field	Description
Name	Name of the Report template subsection. For example, Scope.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The existing subsections for the predefined reports are: Overview, Scope, Progress, Explanation. ○ **Overview**: Displays the overview as a subsection within the report. ○ **Scope**: Displays the visualization ele ments within the report such as the duration counters, incident impact, ac tive teams, and active teams trend. ○ **Progress**: Displays the visualization el ements within the report such as the Linked Security Incidents Graphs, Re sponse Tasks Graph, and Collabora tion Graphs.
Type	The report subsection type. The available types are: ○ **Primary**: This subsection spans the entire width of the page, and is rendered on top of all subsections within the section. There can be only one primary subsection within a section. ○ **Secondary**: This subsection spans the en tire width of the page unless used with the text side panel. ○ **Text side panel**: This subsection accom panies the secondary panel and only sup ports the text.
Table	Name of the report template table.
MSI report section template	The MSI Report Template name for which you're dividing the report into sections.
Order	The order in which the report subsections will be rendered.
Icon	Use the icon to indicate or highlight the sec tion container on the report runtime configura tion form.
Active	Select the check box to create a report sub section for the selected template in the MSIM workspace. **Note:** If the check box is unselected, the MSI Manager can't create a report subsection for this template in the MSIM workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Editor - Content	Define the template subsection content.

7. Save and **Submit** the new report template section.

Create Report Subsection Element template

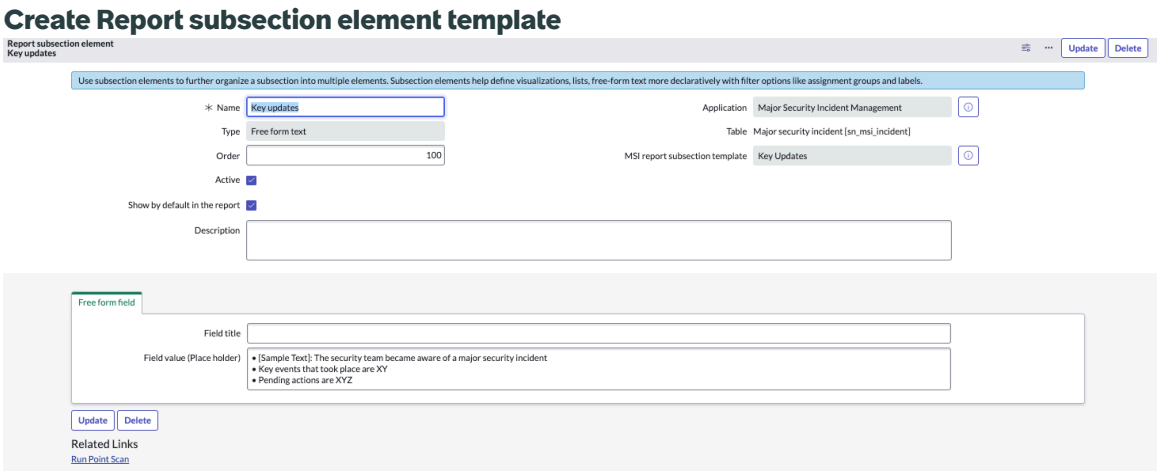
Use subsection elements to further organize a subsection into multiple elements. Subsection elements help define visualizations, lists, free-form text more declaratively with filter options such as assignment groups and labels.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. In the Report section template list, open an existing Report subsection template.
6. Navigate to **Report subsection elements** > **New**.



7. On the Report subsection elements form, fill in the fields.

Field	Description
Name	Name of the Report template subsection ele ment. For example, Scope.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The existing subsections for the predefined reports are: Duration counters, Incident impact, Active Team, Active Team Trend. ○ **Duration Counters**: Displays the duration counter as a subsection element such as estimated time to resolve the incident within the status report. ○ **Incident impact**: Displays the visualization elements within the report such as the impacted assets, impacted locations, and impacted users. ○ **Active Team**: Displays the visualization elements within the report such as the number of active teams involved in closing the major security incident. ○ **Active Team Trend:** Depicts the active teams trend in a graphical representation.
Type	The report subsection element type. The available types are: ○ Free Form Text ○ Visualization ○ Custom ○ List
Table	Name of the report template table.
Active	Select the check box to create a report section for the selected template in the MSIM workspace. **Note:** If the check box is unselected, the MSI Manager can't create a report section for this template in the MSIM workspace.
Show by default in the report	Select this check box if you want to include the section within the report to quickly render the elements.
MSI Report Template	The MSI Report Template name for which you're dividing the report into sections.
Order	The order in which the report sections will be rendered.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Provide a description to the subsection ele ment type.

8. Save and **Update** the new report template section.

Create a Free Form Type Element

Create a free form element type to define the free form text more declaratively with filter options such as assignment groups and labels.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. In the Report section template list, open an existing Report subsection template.
6. Navigate to **Report subsection elements** > **New**.
7. Fill in the report subsection elements form with the required details as explained in Create Report Subsection Element template.
8. Navigate to the Report Subsection element Type field, and select the **Free Form field** option. This displays the **Free form field** section.
9. On the Free Form tab, fill in the fields.

Field	Description
Field title	Name of the field title. For example, Overview.
Field value (Placeholder)	Enter the description of the field value. For ex ample, Here's a sample Overview text. `We made good progress contain ing affected assets. However, we just discovered attackers are still penetrating systems - Including Windows. Containing Linus assets is progressing, but taking longer than expect ed. The new estimated resolu tion day is 5 days from today.`

Create a Visualization Type Element

Create a visualization element type to define the visualization elements more declaratively with filter options such as assignment groups and labels.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

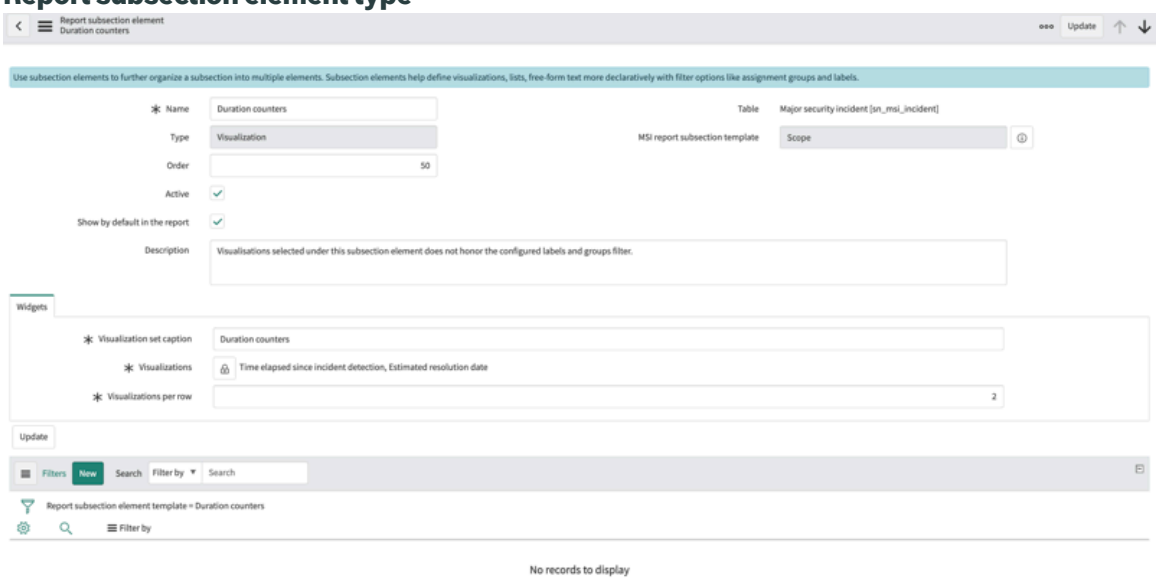
1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page is displayed.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. In the Report section template list, open an existing Report subsection template.
6. Navigate to **Report subsection elements** > **New**.
7. Fill in the report subsection elements form with the required details as explained in Create Report Subsection Element template.
8. Navigate to the Report Subsection element Type field, and select the **Visualization** option.
   This displays the **Visualization** section.
9. On the Visualization form, fill in the fields.

Field	Description
Visualizations set caption	Enter the Visualizations set caption name. For example, Duration Counters.
Visualizations	Select the type of Visualizations. For example, select Time elapsed since incident detection, Estimated resolution date for the subsection type: Duration Counters.
Visualizations per row	Select the number of Visualizations displayed according to each row.

10. Select **Submit**.

Example: Report template subsection element type for a Technical Status Report

Report subsection element type



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a List Type Element

Create a list type element, which defines the related list elements more declaratively with filter options such as assignment groups and labels.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. In the Report section template list, open an existing Report subsection template.
6. Navigate to **Report subsection elements** > **New**.
7. Fill in the report subsection elements form with the required details as explained in Create Report Subsection Element template.
8. Navigate to the Report Subsection element Type field, and select the **List** option.
   This displays the **Lists** section.
9. On the List form, fill in the fields.

Field	Description
Lists	Name of the related lists associated with the MSI. For example, Observables, Indicators. Select a list using the search option.

Create a Custom Type Element

Create a list type element, which defines the related list elements more declaratively with filter options such as assignment groups and labels.

Before you begin

Role required: sn_msi.workspace_manager

Procedure

1. Navigate to **Major Security Incident Management** > **MSI Administration** > **Status Report Setup**.
   The MSI Status Report Setup page displays.
2. In the Report Template section, select **Configure**.
3. Open an existing report template and navigate to the respective Report sections list.
4. In the Report sections list, open an existing Report section template.
5. In the Report section template list, open an existing Report subsection template.
6. Navigate to **Report subsection elements** > **New**.
7. Fill in the report subsection elements form with the required details as explained in Create Report Subsection Element template.
8. Navigate to the Report Subsection element Type field, and select the **Custom** option.
   This displays the **Custom content** section.

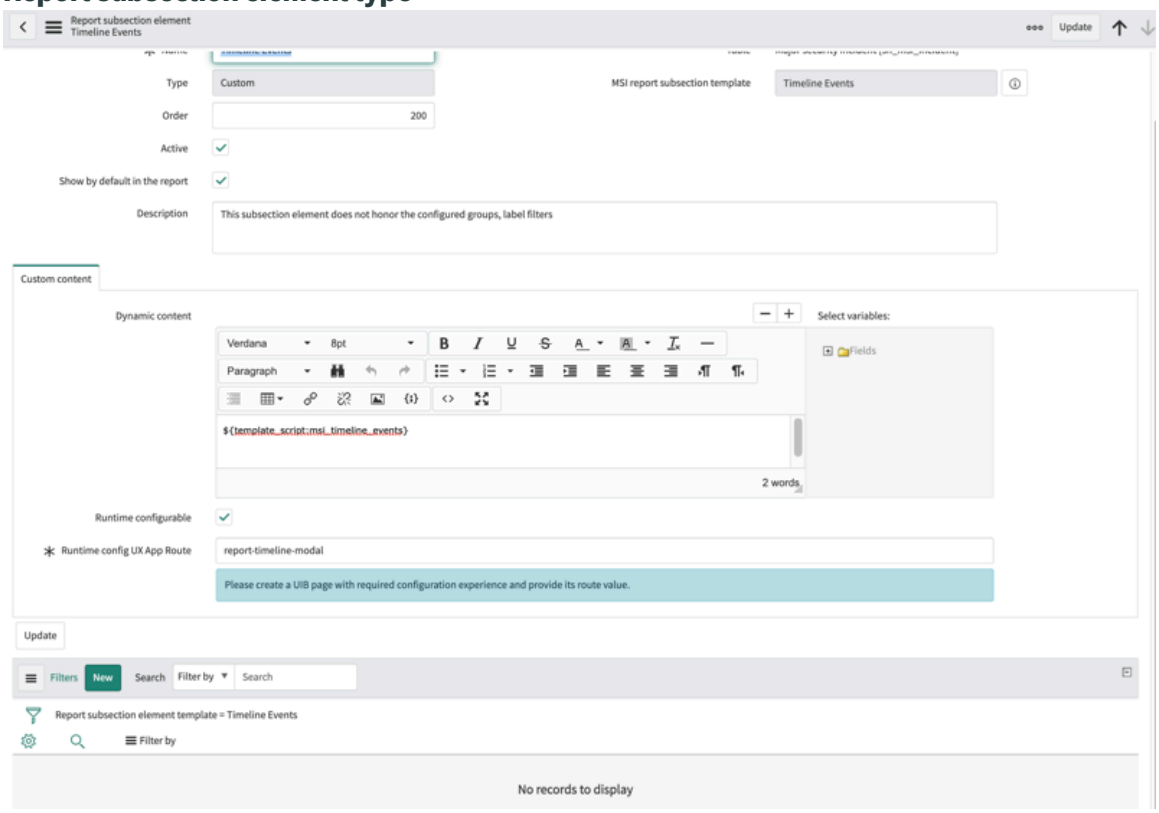
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. On the Custom content form, fill in the fields.

Field	Description
Dynamic content	Enter the dynamic content such as the tem plate scripts.
Run time configurable	Select this check box if the custom element type is run time configurable.
Runtime config UX App Route	Enter the Runtime configuration UX App Route value when a UIB page is created with the required configuration experience. **Note:** This field appears only when the **Run time configurable** option is select ed.

Example: The following is an example of the report template subsection element type for a Technical Status Report

Report subsection element type



Add system properties

Add system properties to control MSIM application behavior. Following are the default system properties that are introduced as part of the Major Security Incident Management status reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System Properties

Property Name	Description
sn_msi.export_img	Use this property to control the exporting of images. The default value is set to ON.
sn_msi.export_img_log	Use this property to enable logging in to the browser console. The default value is set to OFF.
sn_msi.export_img_parallel_threshold	Use this property to control the maximum number of parallel requests to generate the images from report widget configurations. The default value is set to 14.
sn_msi.img_export_log	Use this property to enable the console logs in the browser.
sn_msi.img_export_poll_interval	Use this property to control the time gap between polls that checks if the image is generated or not. The default poll interval time is set to 3000 milliseconds.
sn_msi.export_poll_request_timeout	Use this property to control the maximum time the system can poll for exported image. The default value is 120000 milliseconds.
sn_msi.msi_report_uib_element_js_path	Use this property to control the generic path to capture the image out of the UIB page portion.
sn_msi.report_default_style_objects	Use this property to change the CSS of the generated PDFs such as font size, font color, or field value. For example, if sn_msi.workspace_manager would prefer to change the font color of the left panel of the generated PDF status report then the workspace manager can modify the system property font color and render the PDF in a desired view.

Major Security Incident Management Playbooks

You can invoke the Major Security Incident Management playbook flow automatically or manually.

A Playbook is visible only if at least one playbook is associated with a security incident. The playbook component is supported only for the Process Automation Designer (PAD) built. Major Security Incident Management provides the Legal Request playbook with the base system.

Create processes for MSIM playbook

Use these steps to create processes for Legal MSIM playbook in the Process Automation Designer (PAD).

Before you begin

Role required: sn_msi.workspace_manager.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Click **ALL** > **Process Automation Designer** > > **Create a new process**.

   For example, Legal MSIM Playbook.

2. Enter a name for the process, the description, and the application for which the process is being created.
3. Click **Select a trigger**.
4. Select **Define your own conditions for when your process runs**, and select the trigger condition for when your process must run.
5. Click **Set your trigger conditions**.
6. Choose the conditions to define when your process must run by selecting a table and filling in the conditions.
7. Click **Go to Designer**.
   The Process Automation Designer page opens.
8. To start designing your automated process, click **Add a new lane**.
   The Lane properties pane opens on the right side of the UI.
9. In the Lane properties pane, enter the following details: **Name**, **Description**, **Run condition**, and **Indicate when to start**.
   The **Run condition** and **Indicate when to start** fields imply when the lane would run.
10. Click **Save and close**.
11. To add another lane, click **Add another lane**.
    Similarly, you can create as many lanes as you want. In this example, you can create a lane for Analysis, Contain, Eradicate, and Review respectively. In the following example, **Analysis** lane starts immediately and has no run condition. **Contain** lane start after the previous lane is completed and has a run condition that is based on the outcome of an activity in the previous lane.
    After adding the lanes, you need to add process activities for each lane.
12. Click **Add another process activity** under a particular lane (For example, Analysis lane).
    The Add activity pop-up opens.

    a. In the Add activity pop-up, select the required activity definition.

13. Click **Create a new activity**.
    After an activity definition is added, it can be further configured similar to lanes. Similarly, you can create other process activities under each lane.
14. In the Activity properties pane, add a run condition and indicate when to start the process activity.
15. Add a run condition and indicate when to start.
    All the input required for this activity (Includes inputs in the automation plan that are configured) will be shown. You can override the values or use the preconfigured values.
16. Click **View all properties** and enable the **Advanced properties** toggle to display all the activity experience fields from the activity definition.

Using the MSIM playbook

Use these steps to learn how you can use the Legal MSIM playbook in the MSIM Workspace and its capabilities.

Before you begin

Role required: sn_msi.workspace_manager.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the MSIM workspace, open a major security incident.
2. Select the **Playbook** tab.

   You can view the playbooks that have been enabled for the major security incident.

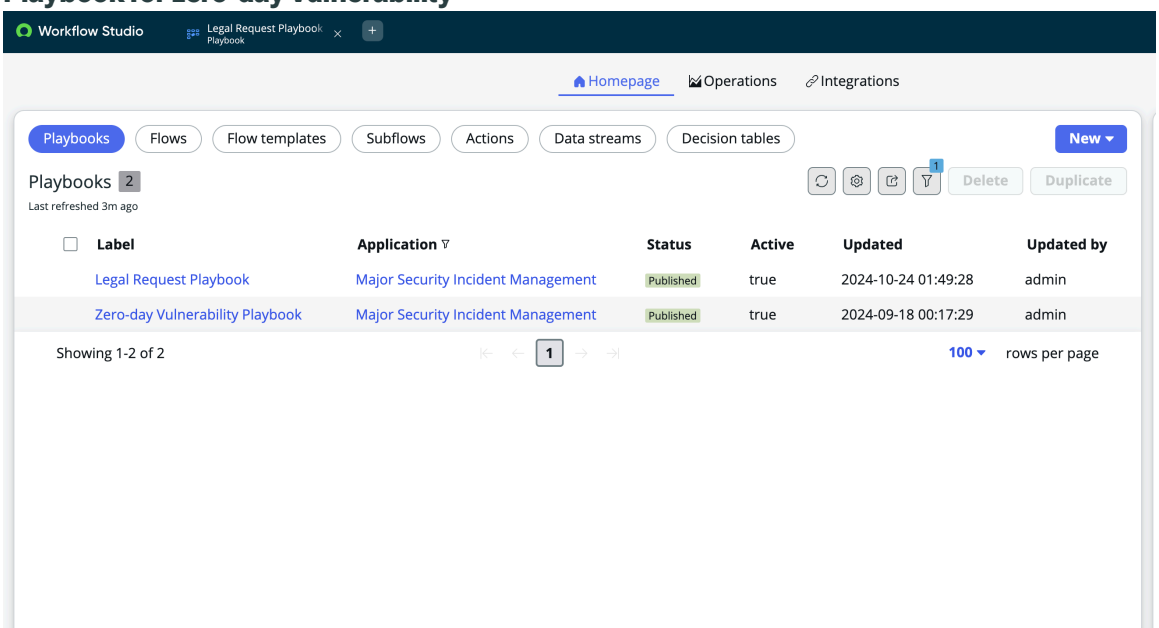
   Note: If you don't see the playbooks listed, then you need to go to PAD and enable them to see it in the **Playbook** tab.

3. Select the **Legal MSIM Playbook**.
4. Click each lane to know what tasks have been performed by this playbook.
5. Click **Analysis** to see the list of activities performed in the Analysis phase.
   You have the option to change it as per your requirements.
6. Similarly, you can click Contain, Eradicate, and Review to view the list of activities that have been performed in the respective phase.
   You have the option to change them as per your requirements. If there's any remaining activity or user action that you need to perform, it's displayed in the respective phase.
7. If there's any remaining activity or user action required in any of the phases, click the respective phase and perform the action to complete the activity.

Playbook for zero-day vulnerability

A Zero-Day Vulnerability Playbook is a step-by-step guide for addressing and mitigating zero-day threats—vulnerabilities in software that are unknown to the vendor, leaving systems exposed to attacks.

Playbook for zero-day vulnerability



Using the Zero-day Vulnerability Playbook

Use these steps to learn how you can use the Zero-day Vulnerability Playbook in the MSIM Workspace and its capabilities.

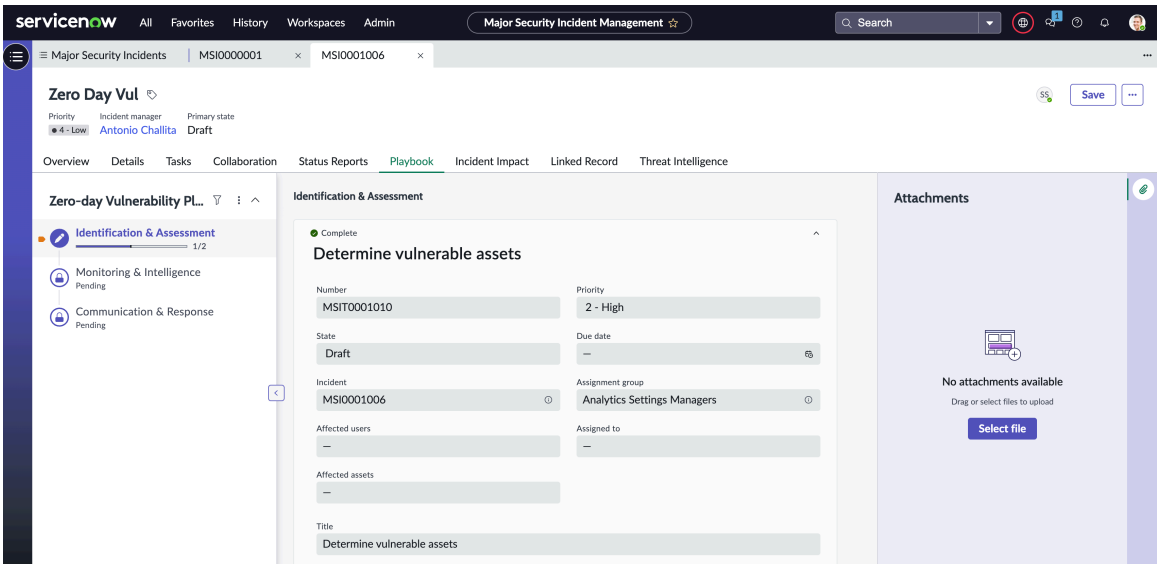
Before you begin

Role required: sn_msi.workspace_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Major Security Incident Management** > **Major Security Incidents**.
2. Select **MSI number**
   It takes you to the playbook page.



3. Go to the **Ellipsis** menu.
4. Select **Add Playbook**.
   It opens the playbook selection menu.
5. Select the **Zero- day Vulnerability Playbook**.
6. Select **Add Playbook**.
7. Select each lane to explore the tasks this playbook performs.
8. Select the first lane **Identification & Assessment**.
9. It has two activities **Determine vulnerable assets** and **Determine impacted customers** which creates an MSI task.

   Note: All the tasks can be customized according to your needs.

10. Open **Determine vulnerable assets**.
    It's used to identify the assets that are exposed to risks or vulnerabilities.
11. Enter the title and provide a detailed description of the task to clarify the objective.
12. Set the priority to confirm the incident is addressed with the appropriate urgency.
13. Select the appropriate **Assignment Group** from the menu.

    Note: Selecting an assignment group is required.

14. Set the due date based on the urgency of the incident.
15. Select **Mark Complete** to complete the task.
    This activity creates an MSI task and assigns it to that particular assignment group.
16. Move to the next activity **Determine impacted customers**.
    It's used to identify customers affected by vulnerabilities or security incidents.
17. Enter the title and provide a detailed description of the task to clarify the objective.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

18. Select **Mark Complete** to complete the task.

    Note: All the lanes are sequential. Complete one lane to unlock and move on to the next.

19. Move to second lane **Monitoring and Intelligence**.
20. It has one activity **Monitor threat intel for additional info on Vulnerability**.
    It's used to track and analyze threat intelligence to gather more information on vulnerabilities.
21. Enter the title and provide a detailed description of the task.
22. Select**Mark Complete** to complete the task.
23. Move to the third lane **Communication and Response**.
24. It has two activities **Draft communication about vulnerability** and **Prepare mitigation plan**.
25. Open **Draft communication about vulnerability**.
    It's used to prepare and draft communication to inform stakeholders about the vulnerability.
26. Enter the title and provide a detailed description of the task.
27. Select the appropriate **Assignment Group** from the menu to assign the vulnerability to a specific team.

    Note: Selecting an assignment group is required.

28. Select **Mark Complete** to complete the task.
29. Move to the next activity **Prepare mitigation plan**.
    It's used to develop a detailed plan to mitigate the impact of the vulnerability and reduce associated risks.
30. Enter the title and provide a detailed description of the task to clarify the objective.
31. Select the appropriate **Assignment Group** from the menu.

    Note: Selecting an assignment group is required.

32. Select **Mark Complete** to complete the task.

Playbook for Legal Request

The Legal Request playbook provides step-by-step guidance on how you can inform legal about the latest summary of an MSI so that they can notify the SEC in the 4-day time frame that is required for material breaches.

Overview

As an Incident Manager, you can use the Legal Request playbook to inform the legal team about the latest summary of an MSI so that they can notify the SEC for material breaches. You can use the Process Automation Designer (PAD) templates to perform the steps in the Legal Request playbook and inform the Legal team accordingly.

This playbook can be used if a major security incident is created or updated. You need to activate the Legal Request playbook on PAD and then perform all the tasks, such as analysis, contain, eradicate, and review.

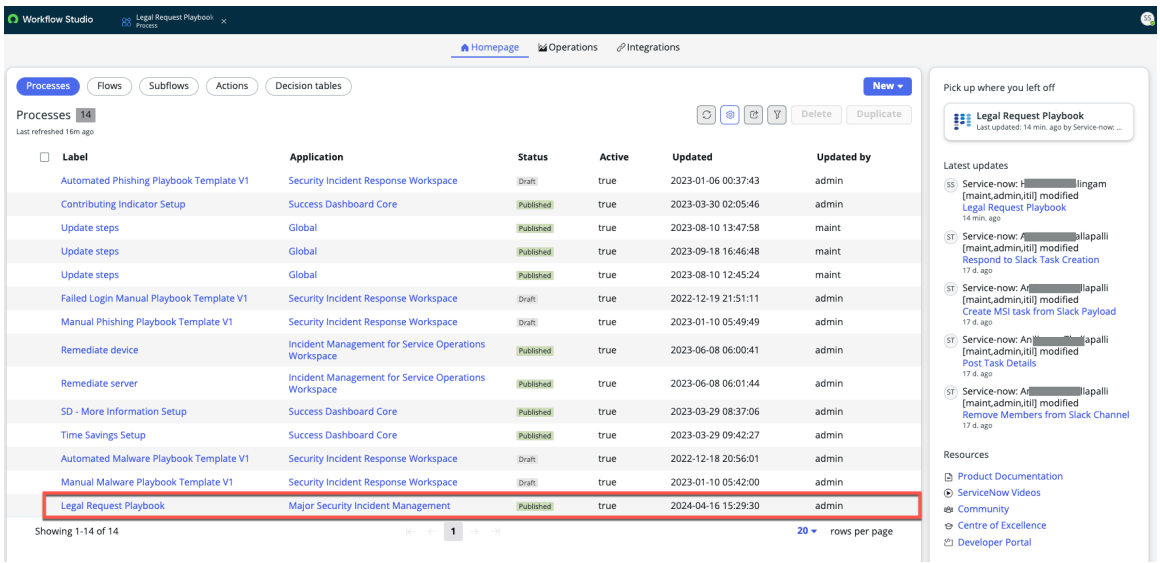
The following are the lanes of the process definition and correspond to the major security incident state:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Analysis
- Contain
- Eradicate
- Review

Each lane has certain activities within it.

Playbook for Legal Request



Once you mark a task complete in a lane, you can move to the next task. You can save a task at any point in time and return to the playbook at a later date and time. After you complete all the tasks in a lane, you can move to the next lane. The status is reflected in the left-hand panel as you keep completing tasks and lanes. An Activity Log on the right-hand side of the playbook shows all the data that you have entered for each task.

After you complete all the tasks, you're asked to review the details you entered in all the lanes. You can choose to edit any field or select **Finish** to complete the process of creating the entitlement.

Rollup Framework for MSIM

Extends the capability of linking the source records from Major Security Incident Management workspace.

Overview

Rollup Framework makes the rollup flow configurable and extendable. Use this framework model to configure the information, which can be rolled up to a Major Security Incident.

Earlier, sn_msi.workspace_manager was able to link the security incidents and vulnerable items which were proposed or promoted as MSI. After linking the security incident or vulnerable item, the information was then rolled up to a major security incident. The type of information needed to be rolled up was hard-coded in the scripts.

You can use the framework model to configure the rollup flow, which supports the following features and also addresses the existing issues in the application:

The rollup framework model enables the sn_msi.workspace_manager with the following benefits to:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Add or remove the linking, propose, or promote MSI record capabilities on any table, which extends the task table.
- Control the type of information to be rolled up to MSI while performing actions such as link/propose/promote on the incident records.
- Support linking, propose, or promote for Security Incidents, Remediation tasks, and Security Cases Out of the box (OOTB) both from the classic environment and Major Security Incident Management workspace.

Rollup framework exhibit the configurations as explained in the following table.

Rollup Framework configurations

Name	Description
Linked Record Configuration	Stores the information of task tables which can be used to link/promote/propose to Major Security Incident.
Rollup Record Configuration	Captures the information which can be rolled up from task table when link/promote/propose actions are performed.
List Layout Configuration	Controls the labels and list layout for various tables as shown in the Major Security Incident Management workspace tabs such as Incident Impact, Linked Records, and Threat Intelligence.

Configure Linked Records in Major Security Incident Management

Use Linked Records Configuration to store the information of task tables that can be used to link/promote/propose to Major Security Incident.

Role required: admin and sn_msi.workspace_admin.

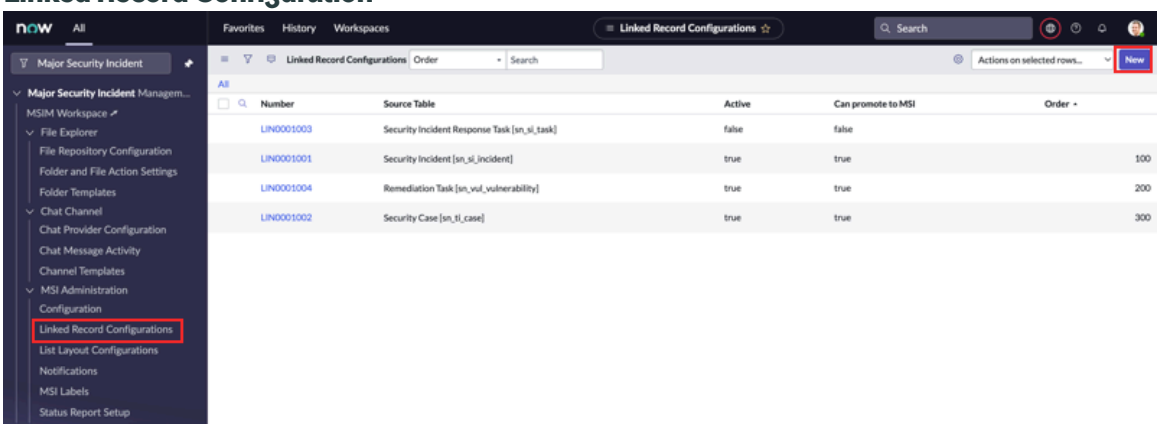
Note: Admin can create the record and MSIM workspace admin can update the record.

Procedure

1. Navigate to **Major Security Incident Management** > **Linked Record Configurations**.

   The Linked Record Configuration page displays.

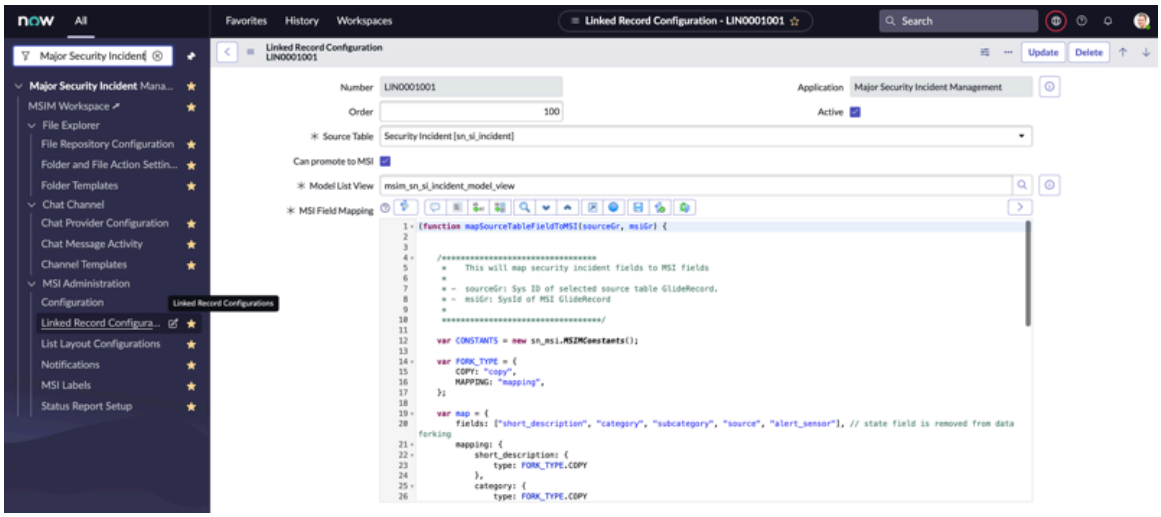
Linked Record Configuration



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. On the Linked Record Configuration page, click **New**

Note: Ensure that the application is in Major Security Incident Management scope.



3. On the record configuration form, fill in the fields.

Linked Records Field Descriptions

Field	Description
Source Table	Indicates the task table that must be linked and rolled up to Major Security Incident.
Order	Allows you to control the order of the current source table in MSIM workspace drop-down. Below is an example of the **order**. Refer to image 1 below, which is provided after this table.
Model ListView	Select a view which can control the list layout that is shown in the Linked Record Modal List.
Can Promote to MSI	Select this check box to confirm whether the record is a primary record. Below is an example of **Can Promote to MSI** option selection. Refer to the following image 2, which is provided after this table. If this check box is selected and the value is true, then: ○ you can directly propose and promote a source record to Major Security Incident using the classic environment actions with additional configurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ you can link source records to major security incidents both from the classic environment and MSIM workspace. ○ Major Security Incident Management workspace linked record page displays the linked source table records. **Note:** If a record can be directly proposed/promoted as a Major Security Incident, then that record is a primary record. For example, in the Security Response task table configuration, the value of **Can Promote to MSI** is false as you can't directly promote Security Response task to Major Security Incident. Hence, it does not show up in the MSIM workspace linked record tab drop-down list.
MSI Field Mapping	Write a script to map the source record fields to a newly created major security incident when the source tables record is in the process of being proposed or promoted. This script executes only when **Can Promote to MSI** value is true.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Image 1: Linked Records list view order

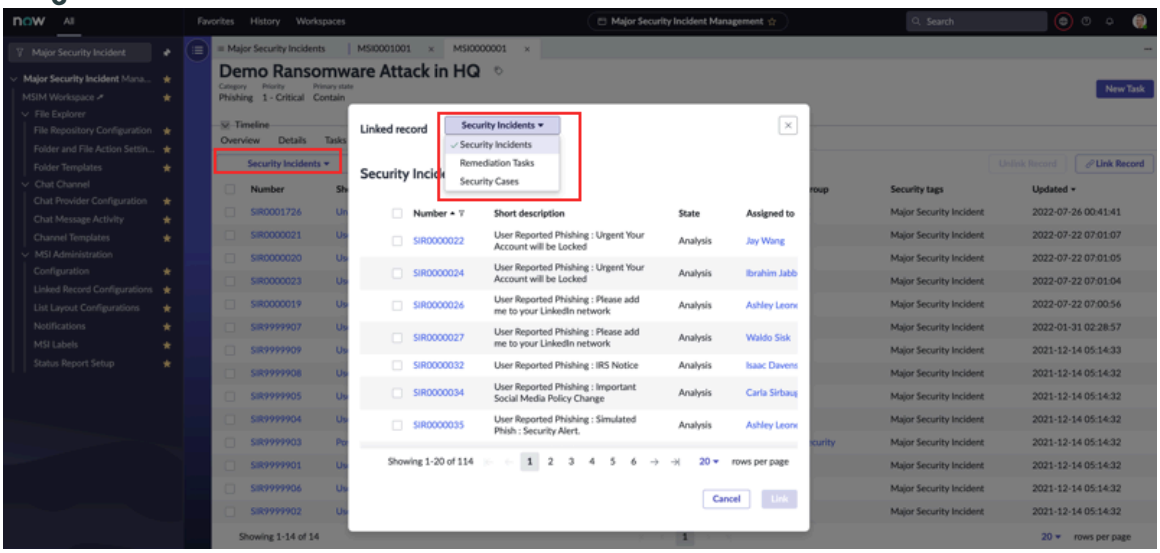
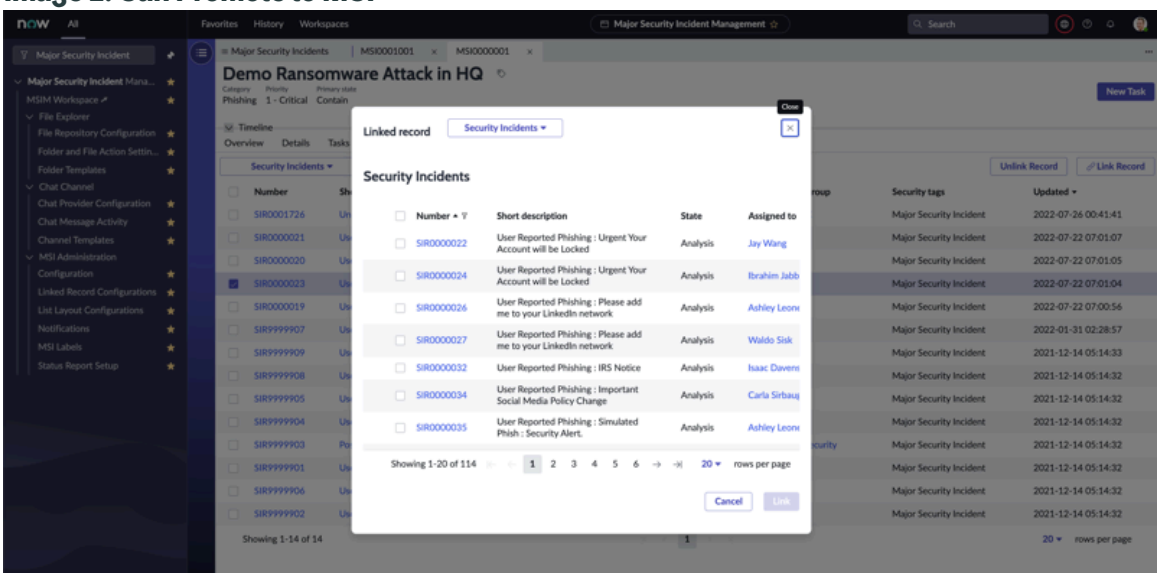


Image 2: Can Promote to MSI



Configure Rollup Records in Major Security Incident Management

Configure Roll up records in Major Security Incident Management to control the information, which will be rolled up when the source record is linked/proposed/promoted as Major Security Incidents.

Role required: admin and sn_msi.workspace_admin.

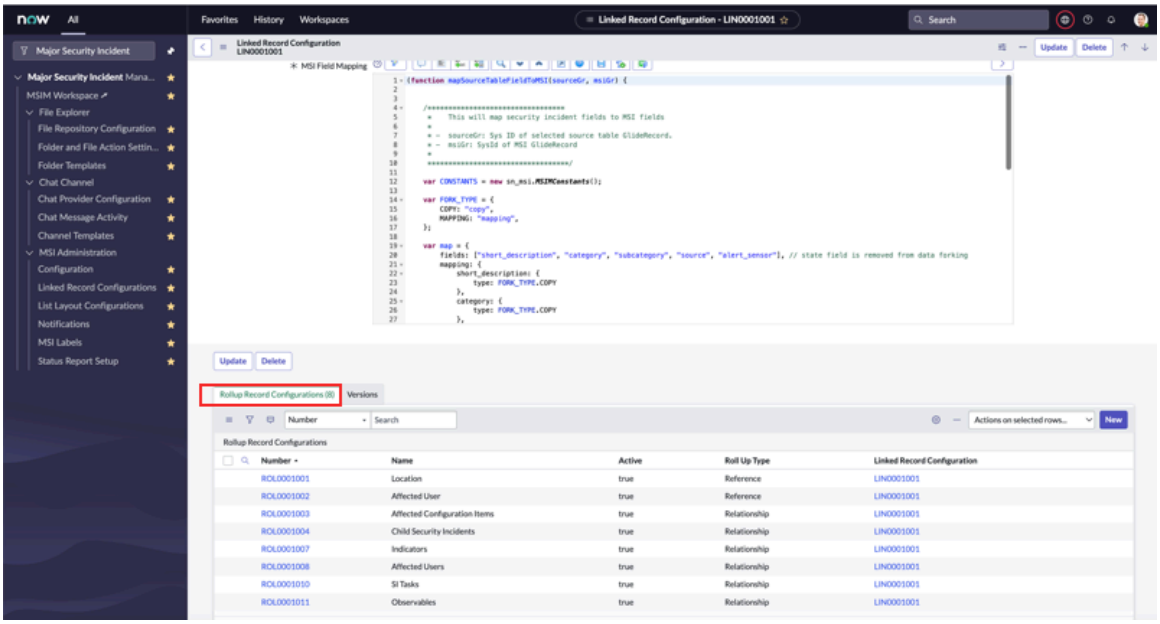
Note: The system admin can create the record and MSI workspace admin can update it.

Procedure

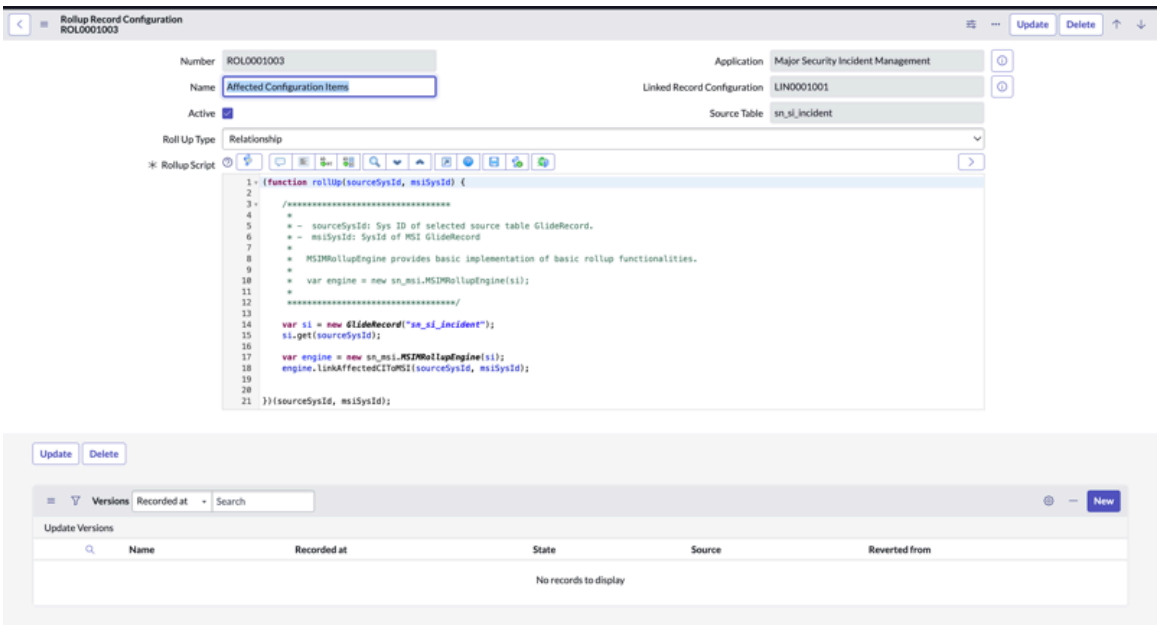
1. Navigate to **Major Security Incident Response** > **Linked Records Configuration**. The Linked Record Configurations page displays.
2. Select or create a new linked record and navigate to the **Roll up Record Configuration** section from the same page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rollup Record Configuration section



3. Click **New**.



4. On the configuration page, fill the details.

Rollup Record Configuration

Field Name	Field Description
Name	Indicates the name of the rolling up record.
Active	Select this check box to implement the current configuration when rollup of source record happens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Field Description
Linked Record Configuration	Indicates a unique number, which refers to your parent linked records configuration and read-only.
Source Table	The source table name used in the Linked Record configuration, which is read-only.
Rollup Type	Describes the type of information which should be rolled up. ○ **Relationship**: Select this option if the data need to be present as a related list. ○ **Reference**: Select this option if the data is present as a reference field on the source table form.
Rollup Script	If the rollup type is: **Relationship**, then the **Rollup Script** field is enabled, which allows you to write script and can be used to rollup information. Here the script will receive the inputs which contains information of the source record and major security incident. The script should be able to find the information from the relationship tables and rollup to Linked Record (sn_msi_m2m_child) table.
Source Field	If the rollup type is: **Reference**, then the **Source Field** is available. This enables you to select the Source Table reference field which contains the information that needed to be rolled up.
Target Field	If the rollup type is: **Reference**, then the **Target Field** is available. This enables you to reference field from the Linked Record(sn_msi_m2m_child) table and will store the data which is present in the selected Source Field and in the Source Table record.

Writing script for rollup

Name	Description
Inputs	• sourceSysId: Sys ID of source table record which is either getting linked / proposed / promoted. • msiSysId: Sys ID of major security incident to which source record is getting linked / proposed / promoted.
Output	No output return value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

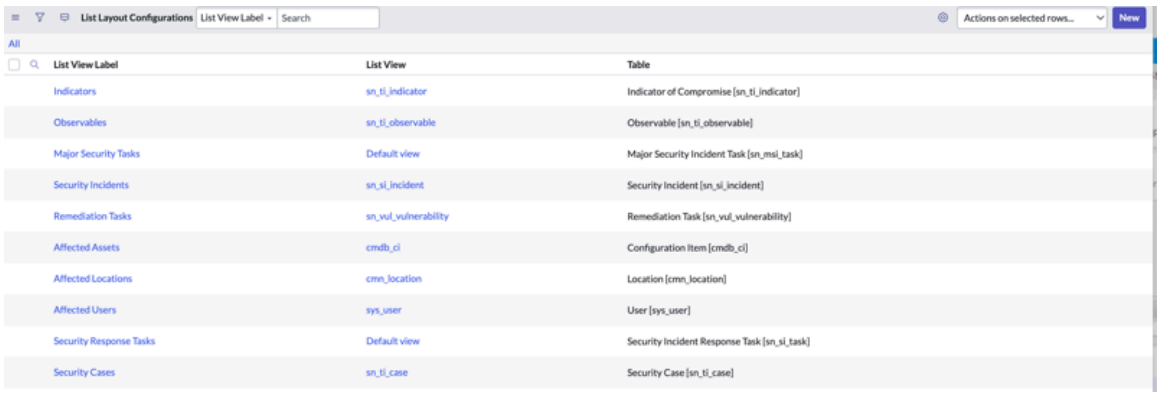
Name	Description
Responsibility	Script should rollup information to Linked Record(sn_msi_m2m_child) table. • Use sourceSysID to query data from ServiceNow relationship tables. • After the data is fetched, roll up the data to a Linked Record (sn_msi_m2m_child) using MSIRollupEngine utility to roll up data.

Configure List Layout in Major Security Incident Management

Configure list layout to customize the layout and labels used in Major Security Incident Management workspace such as Incident Impact, Linked Records, and Threat Intelligence tabs.

Role required: admin and sn_msi.workspace_admin.

Note: The system admin can create the record and MSI workspace admin can update it.

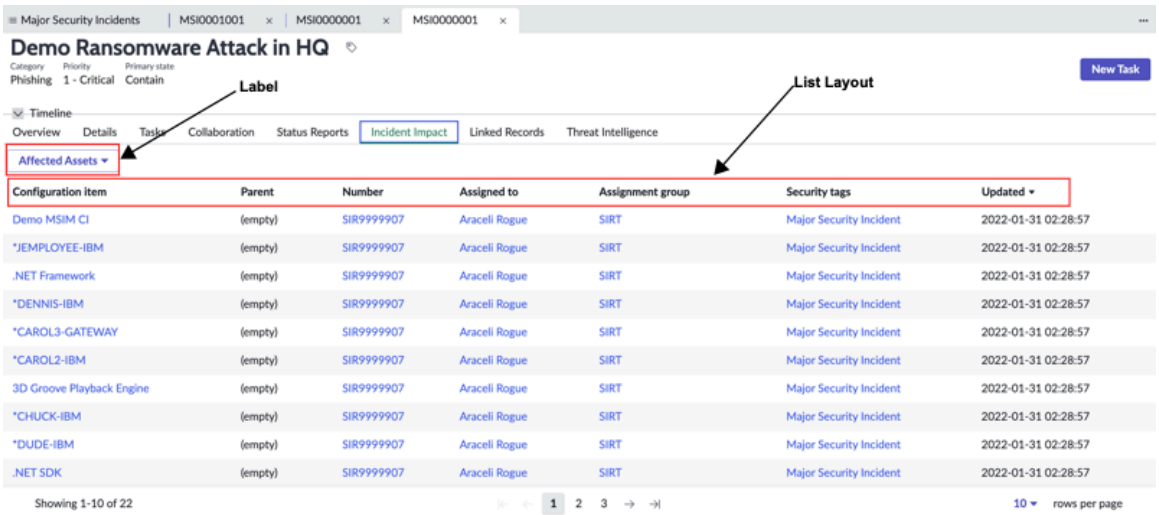


The list layout configurations were already shipped for existing known tables shown in Major Security Incident Management workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- If you want to render the custom view for the existing tables, you can update respective table record in list layout configuration with custom list view.
- For new task tables, you can create a new List Layout configuration to render the custom list view and labels. For more detailed procedure, see on how to Step 4. Create a view for a new Linked Record Tab for a Security Case



Rollup example use case implementation for a Security Case

The following steps explain an example use case on how to add support to link/propose/promote to Major Security Incident for a Security Case table.

- Step 1. Create linked record configuration for a Security Case
- Step 2. Create a view for modal window for a Security Case
- Step 3. Create UI actions for the Source Table for a Security Case
- Step 4. Create a view for a new Linked Record Tab for a Security Case
- Step 5. Add Access Control Lists (ACLs) for Major Security Incident Management workspace users
- Step 6. Create business rules for a Security Case
- Step 7. Create rollup record configurations

Step 1. Create linked record configuration for a Security Case

Create a Linked Record configuration for a Security Case.

Before you begin

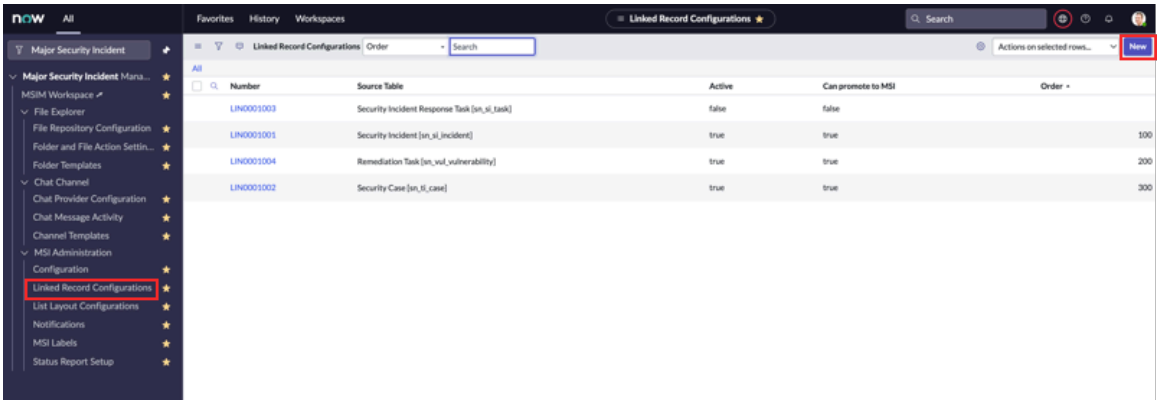
Role required: admin and sn_msi.workspace_admin

Note: The system admin can create the record and MSI workspace admin can update it.

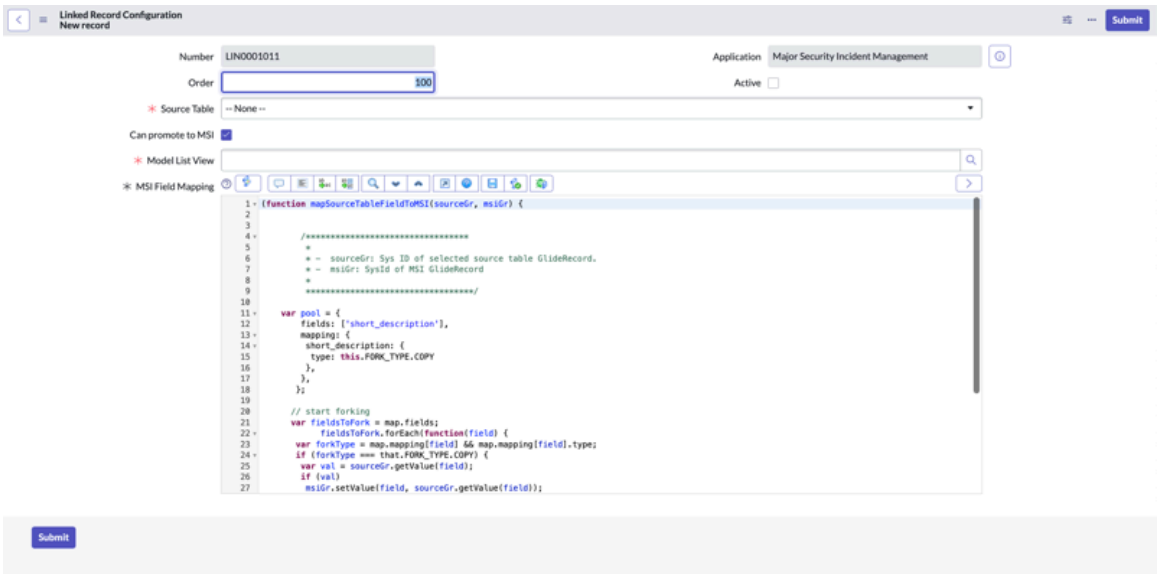
Procedure

1. Search for the Linked Record Configuration from the left navigation.
2. Click **New**.

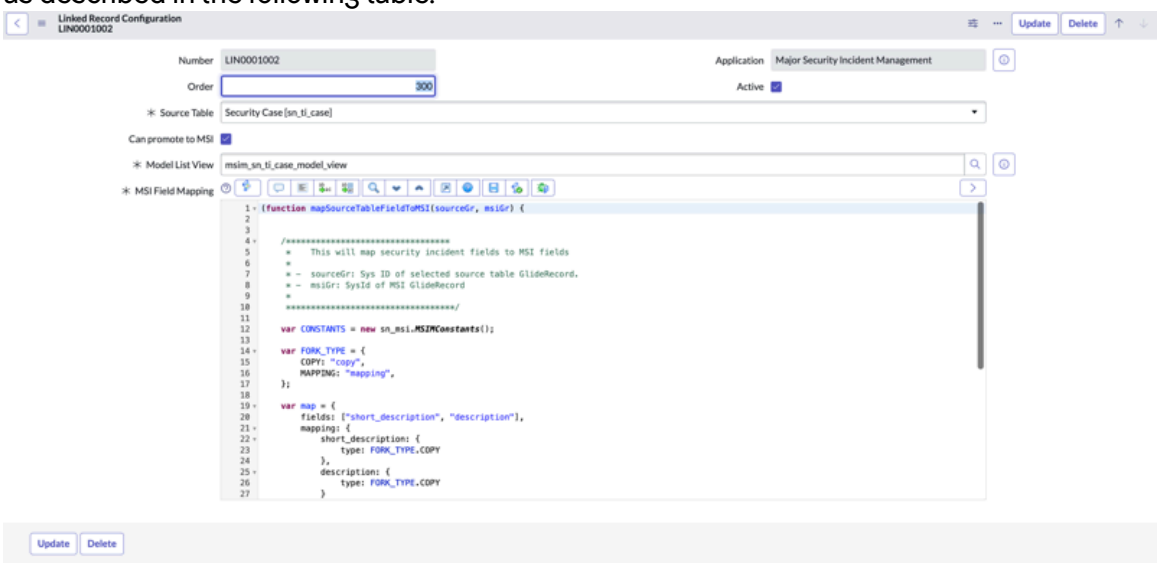
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Fill the form with the required columns and write a field mapping script.



4. You have now created a linked record configuration for the Security Case by adding the values as described in the following table.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
Source Table	Security Case (sn_ti_case). Here in this example, link/promote/propose a security case as MSI.
Order	Input value: 300 **Note:** Lower the order takes precedence over higher orders. As a Security Case have a higher order than the Security Incident and Remediation Task, it will appear in the last sequence.
Can promote to MSI	True, select this check box to promote the security case to MSI. **Note:** ○ Link and Unlink security case records to major security incidents both from Major Security Incident Management workspace. Also, Unlink record functionality is visible only for the linked records. ▪ This will enable the link, promote, and propose to Security Case to Major Security Incident using classic environment actions, but those UI actions will not be available out of the box. Each UI action needs to be created manually. For more information, see Step 3. Create UI actions for the Source Table for a Security Case. ▪ Link/Promote/Propose UI action are available for Security Incident, Remediation Task, and Security Case out of the box. ○ MSIM workspace linked record page will show the linked Security Case records. Refer to the below image 1 to view the options available after selecting this check box.
Modal List View	msim_sn_ti_case_model_view **Note:** This view contains fields and fields order shown in list view on the Link Record Modal in MSIM workspace. For more information, see Step 2. Create a view for modal window for a Security Case

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	Refer to the below image 2 to view from the **Linked Records** page.
Field Mapping Script	This script describes the fields from source tables record will mapped to newly created major security incident when source tables record is getting proposed or promoted. which will receive inputs: ○ sourceGr: security case glide record object ○ msiGr: major security incident glide record object Script will read from the short description of the security case and copy it over as title to major security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Image 1: Can Promote to MSI

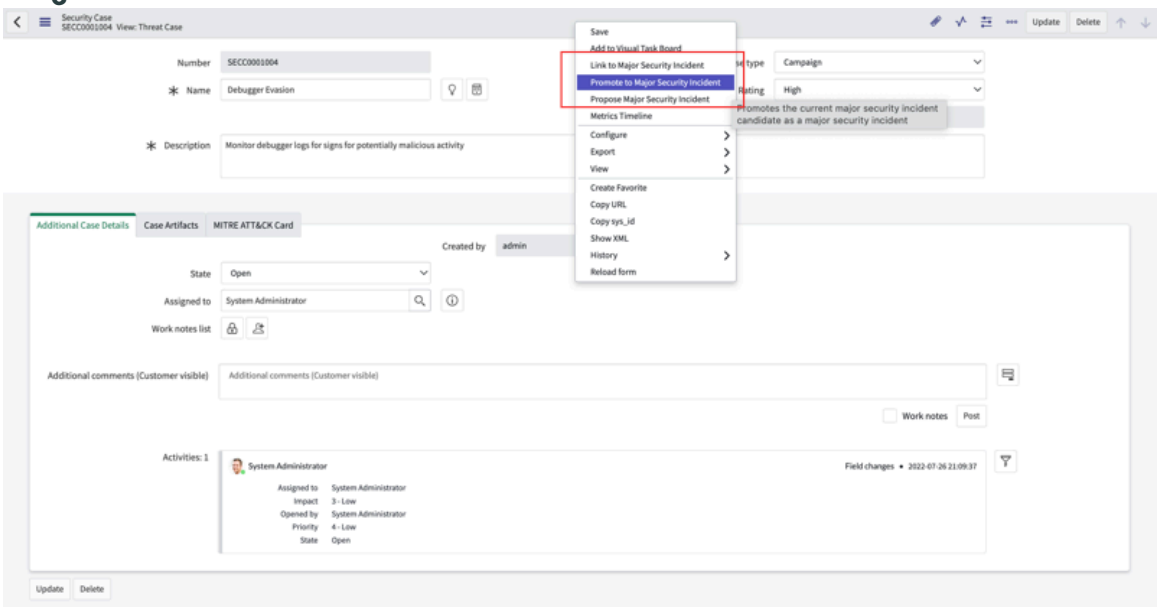
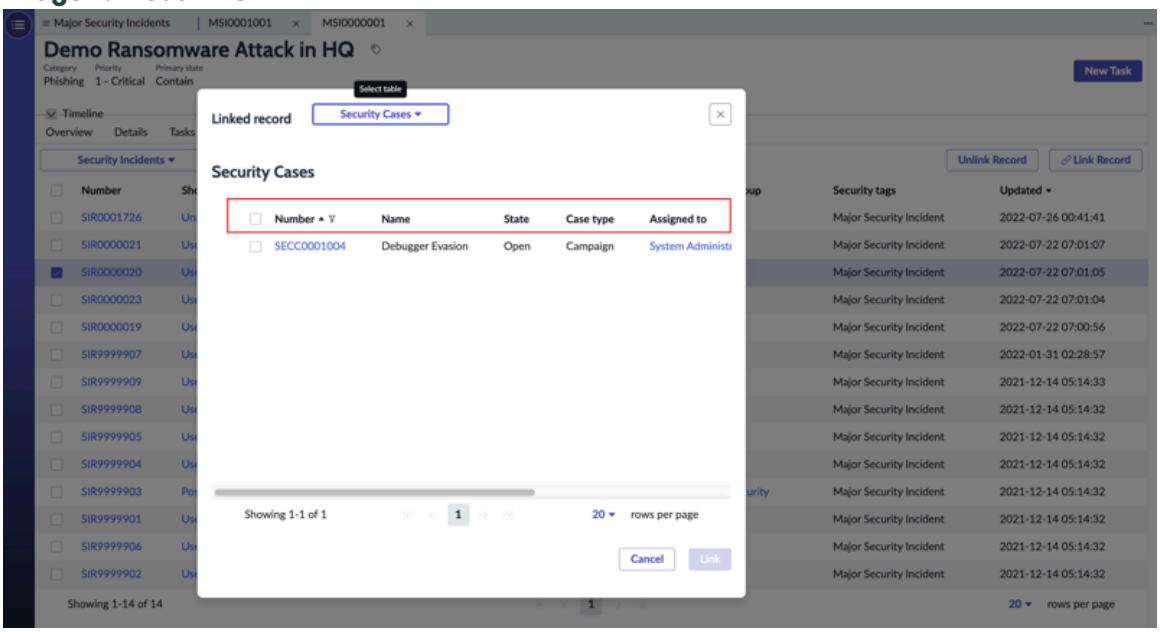


Image 2. Modal View



Step 2. Create a view for modal window for a Security Case

Create a view for modal window for a Security Case.

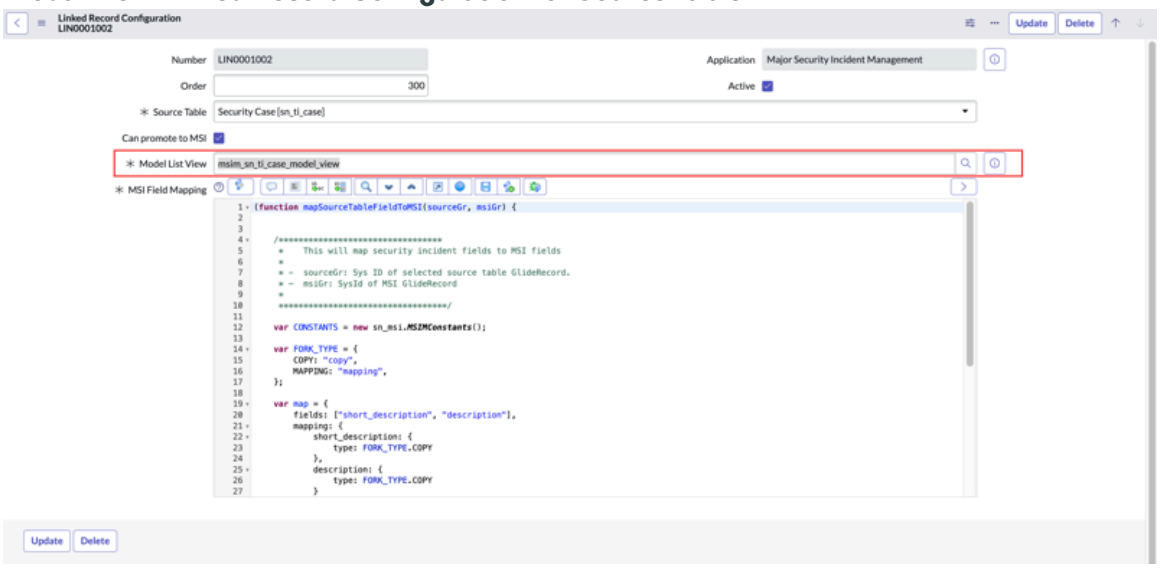
Before you begin

Key Consideration:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- By default, the linked record modal list will only be showing the **Default** list layout. If you want to customize the list layout, you can do so using **Custom View** on the Source Table.
- If you want to render the custom view, the custom view should also be selected in the Linked Record Configuration for Source Table.

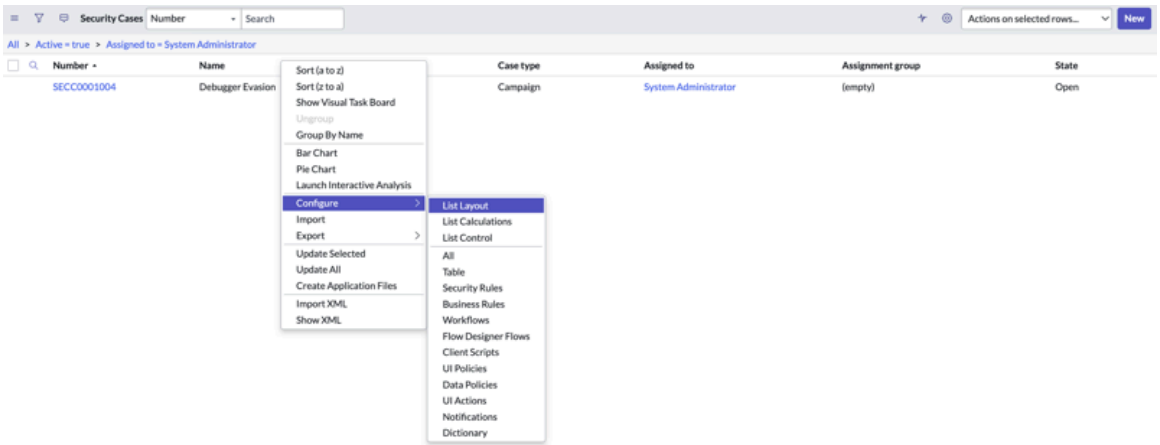
Modal view Linked Record Configuration for Source Table



Role required: admin

Procedure

1. Go to the source table and click **Configure** > **List Layout**.



2. Go to **List view** > **View name**.
3. Click **New** in the View name drop-down list and create a new view, for example, msim_sn_ti_case_modal_view.
4. Select the newly created view.
   Once selected, you can choose the required fields from the Available list.
5. Click **Save**.
6. Navigate to **Menu** > **Views** to verify if the view has rendered properly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Step 3. Create UI actions for the Source Table for a Security Case

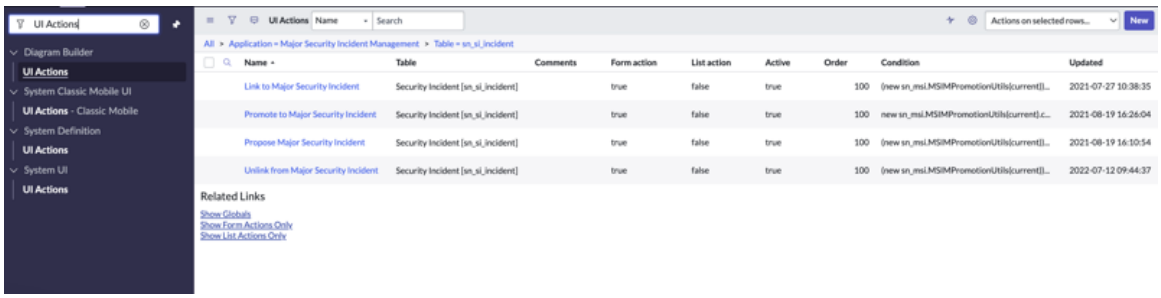
Create UI actions for the source table for a Security Case.

Before you begin

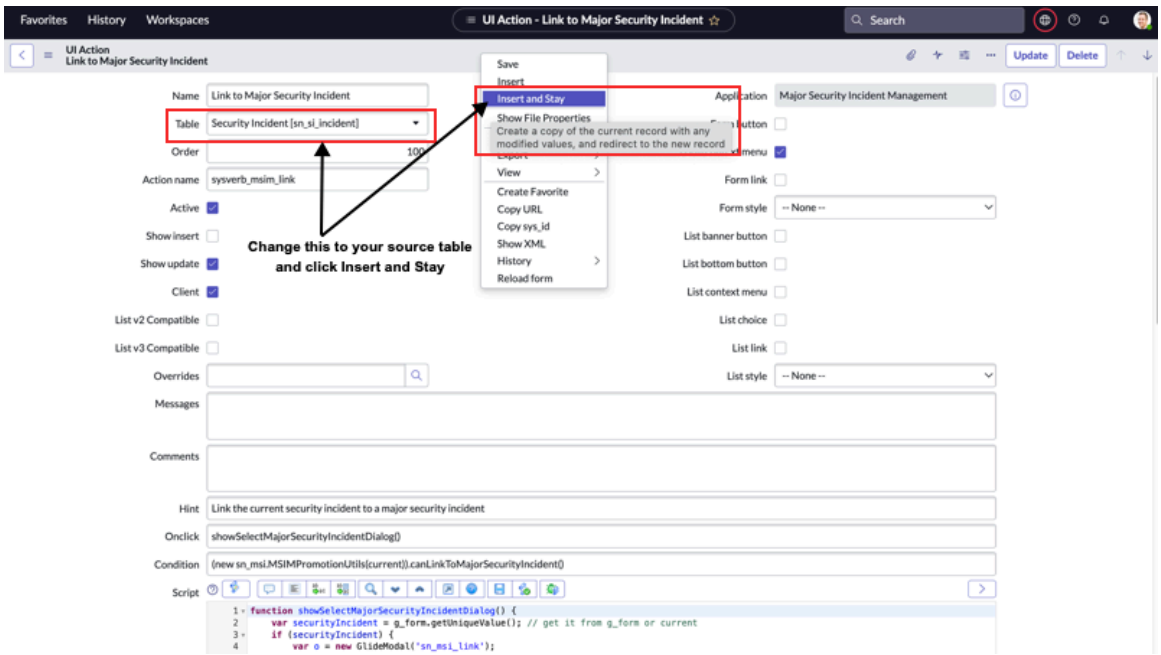
Role required: admin

Procedure

1. Navigate to **System Definition** > **UI actions**.
2. Run the Filter option to filter out the list by **Application**: Major Security Incident Management and **Table**: sn_si_incident.



3. Select each UI action one by one and save the details for the source table.



4. Repeat the same steps as above for the following UI actions:
   - Link to Major Security incident
   - Proposed Major Security Incident
   - Unlink from Major Security Incident
   - Promote to Major Security Incident

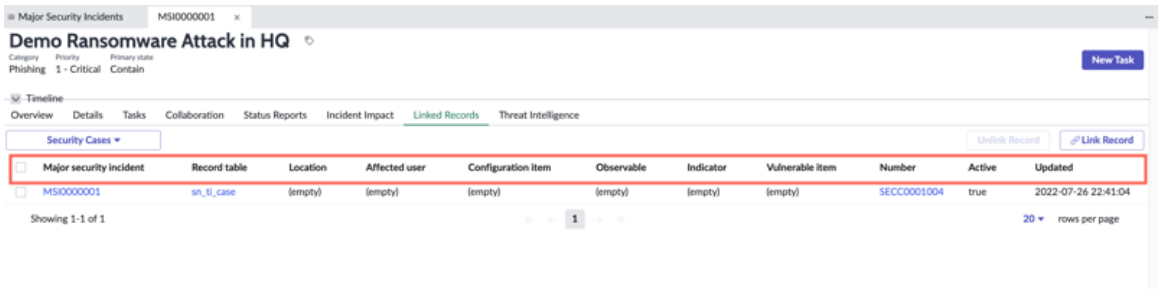
Step 4. Create a view for a new Linked Record Tab for a Security Case

Customize the List layout for a Security Case table when it is displayed on the Link Records page with the Major Security Incident Management workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Prerequisites:

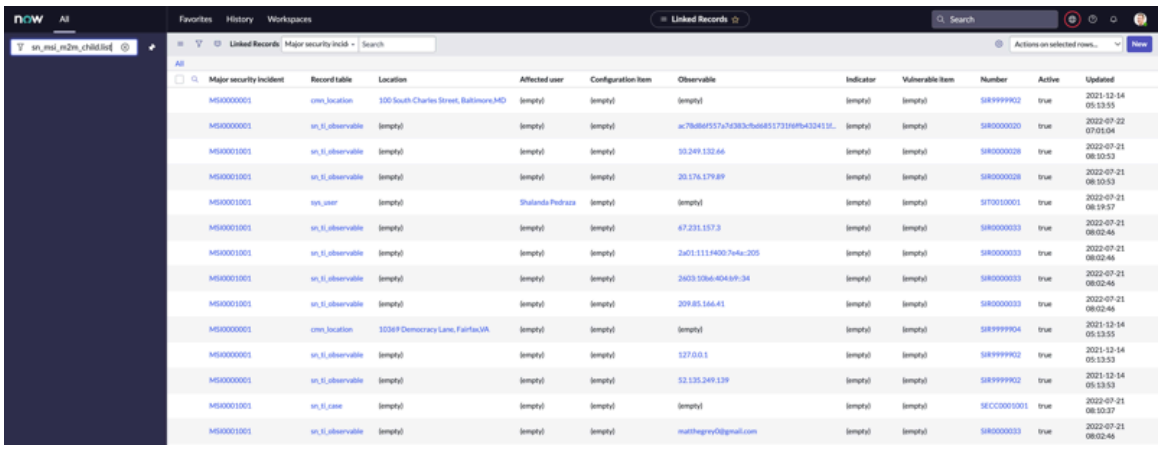
- Choose the column that should be visible when a list is rendered for a Security Case table.
- Choose the order of the fields to be displayed in the drop-down list.



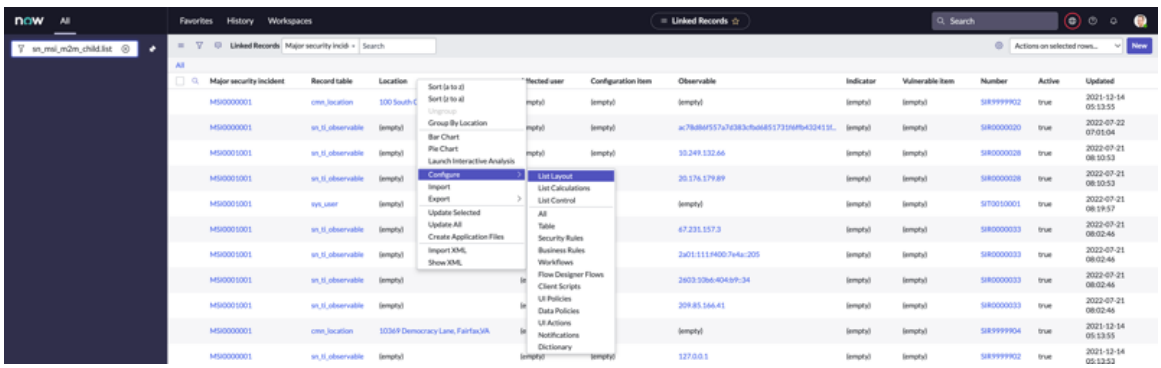
Role required: admin

Procedure

1. Search for **sn_msi_m2m_child.list** using the left navigation.
   The Linked Records table is displayed.

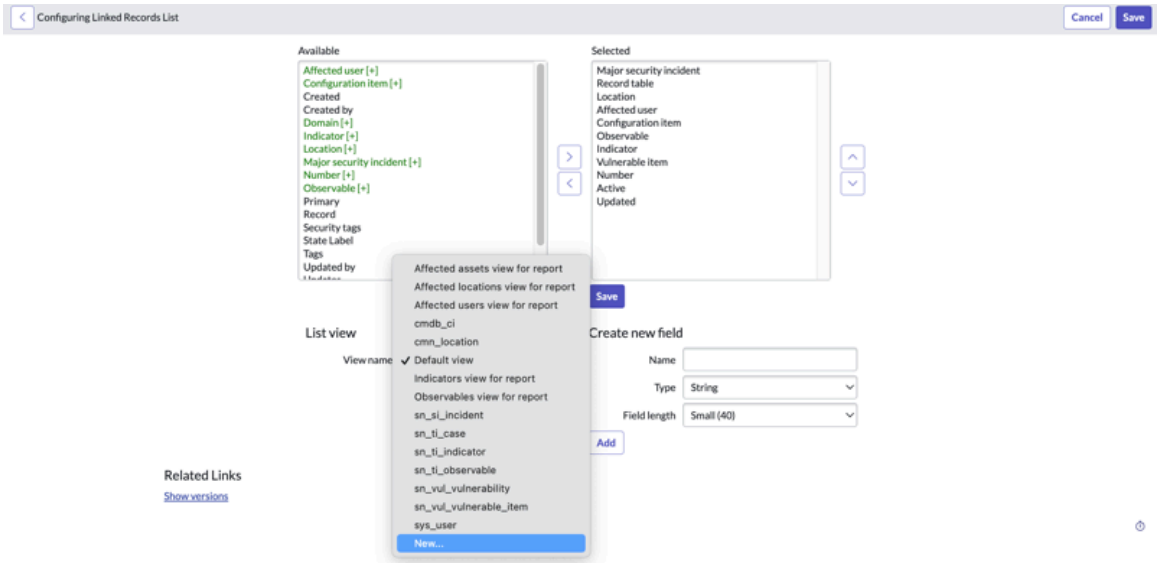


2. Right-click the header and select **Configure** > **List Layout**.
   The Configuring Linked Records List page is displayed.

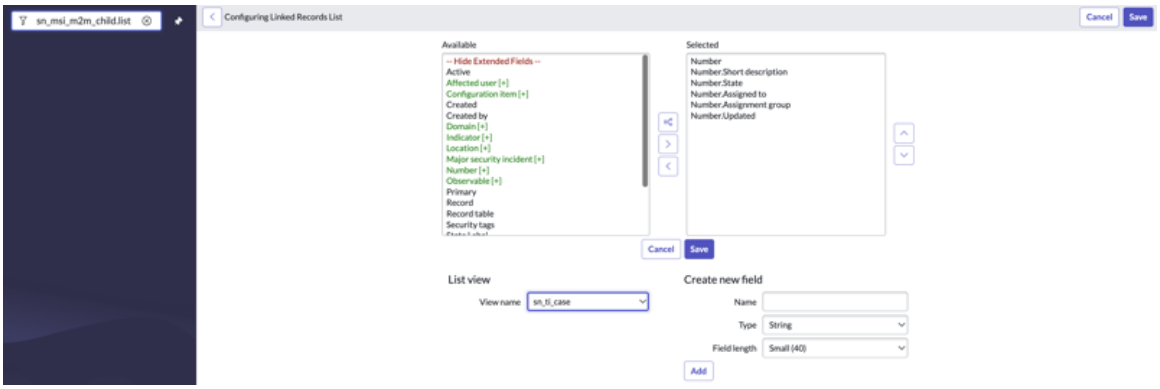


3. Go to **List View** > **View name**.
4. Select **New** from the View name drop-down list.

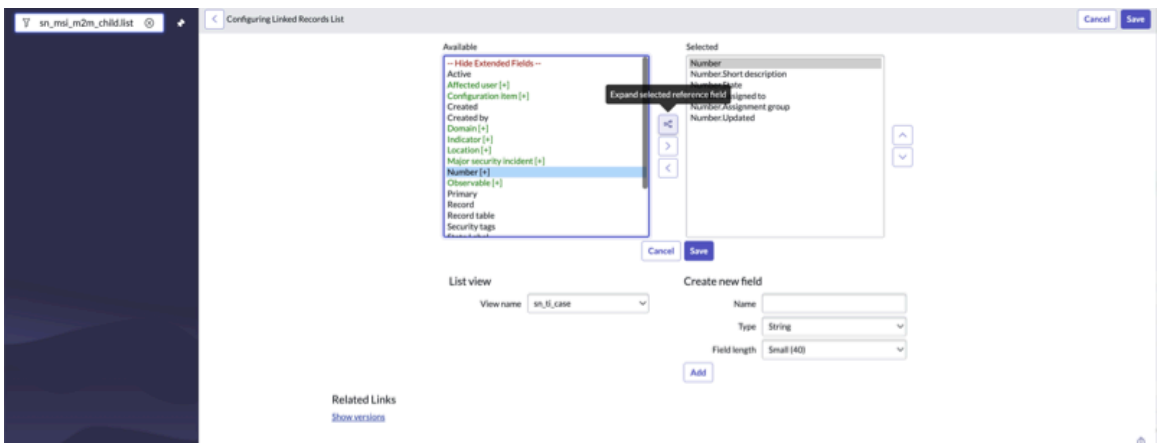
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Select the columns that will render on the workspace list view.
   The security case record is stored in the **Number** column. To render information from a security case, you must dot walk on the **Number** column.

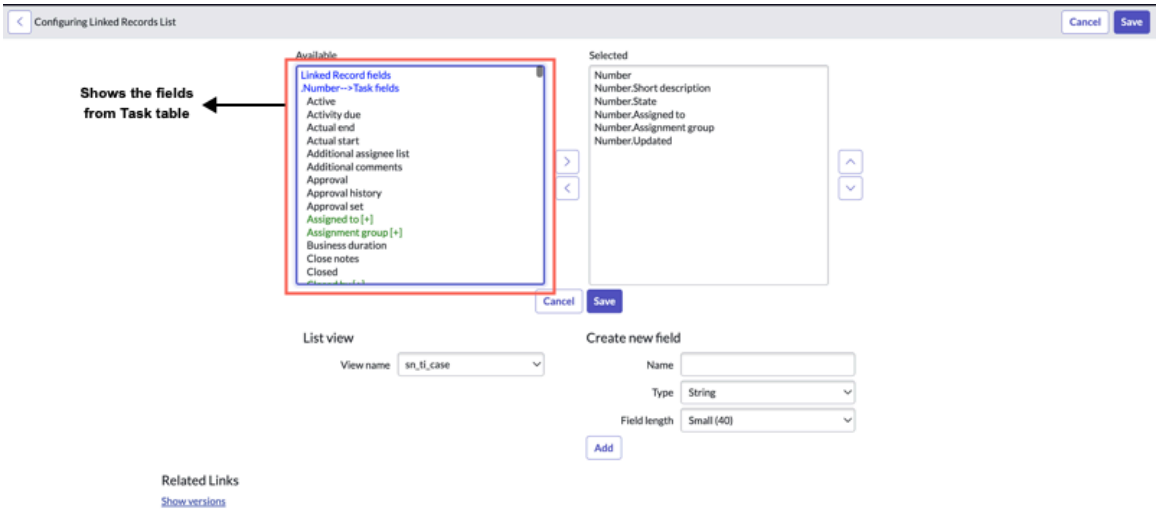


   a. To dot walk, first select the **Number** column from the Available list and then click **Expand Selected Reference Field**.



   b. Expand the columns from **Number** to select and move them to the Selected list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. Click **Save** to save and create a view.

6. The next step is to render the created view within the Major Security Incident Management workspace, you need to create a **List Layout Configuration**.

   a. Search for the **List Layout Configuration** using the left navigation.

   b. Click **MSI Administration** > **List Layout configurations**.

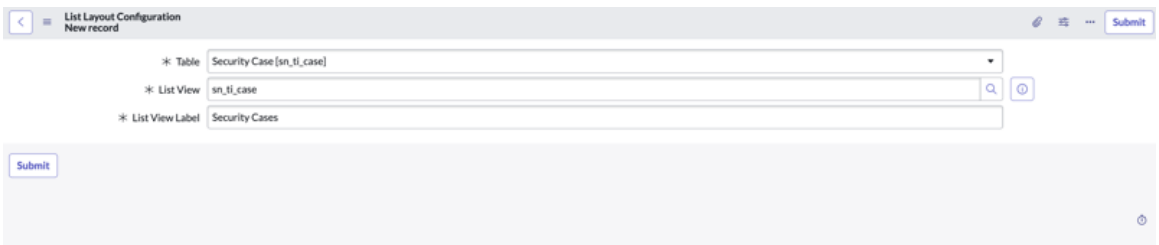
   c. Click **New** to create a new configuration.

   d. Select the source table from the Table column and select the newly created view from the List View field.

   e. The **List View** label enables you to control labels when the same source table is rendered in the Major Security Incident Management workspace.

   f. **Save** the record.

   Note: After the record is saved, navigate to Major Security Incident Management workspace to view the rendered list view and label within the workspace.



Step 5. Add Access Control Lists (ACLs) for Major Security Incident Management workspace users

Add Access Control Lists (ACLs) for Major Security Incident Management workspace users.

Before you begin
Role required: admin

Note: The permissions required to linking and unlinking capabilities are controlled by the sn_msi.linkedsivi_read role.

Major Security Incident Management persona contains sn_msi.linkedsivi_read role.

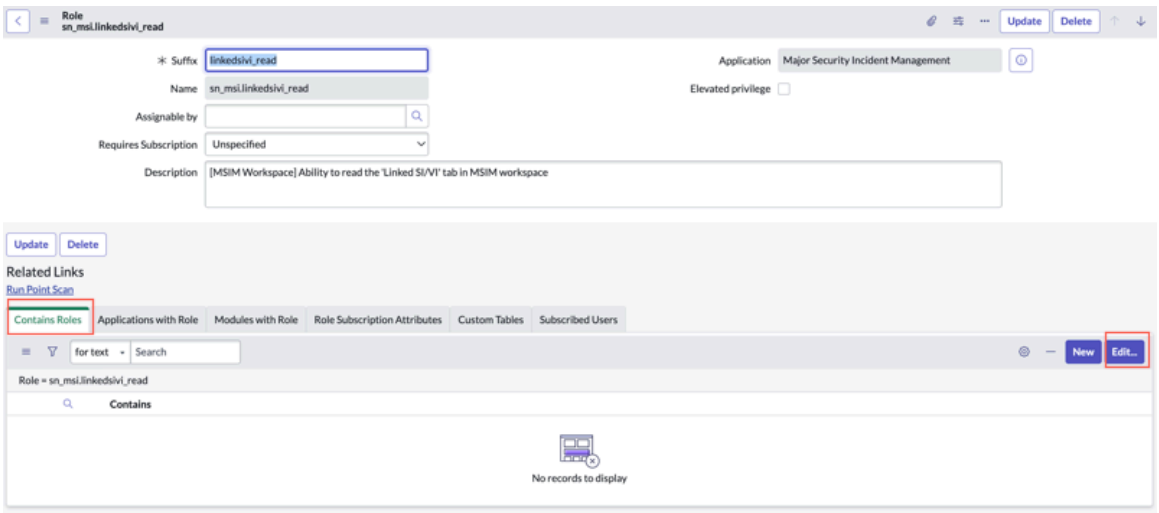
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. sn_msi.workspace_admin (MSIM Workspace admin)
2. sn_msi.workspace_manager (MSIM Workspace manager)
3. sn_msi.workspace_responder (MSIM Workspace responder)

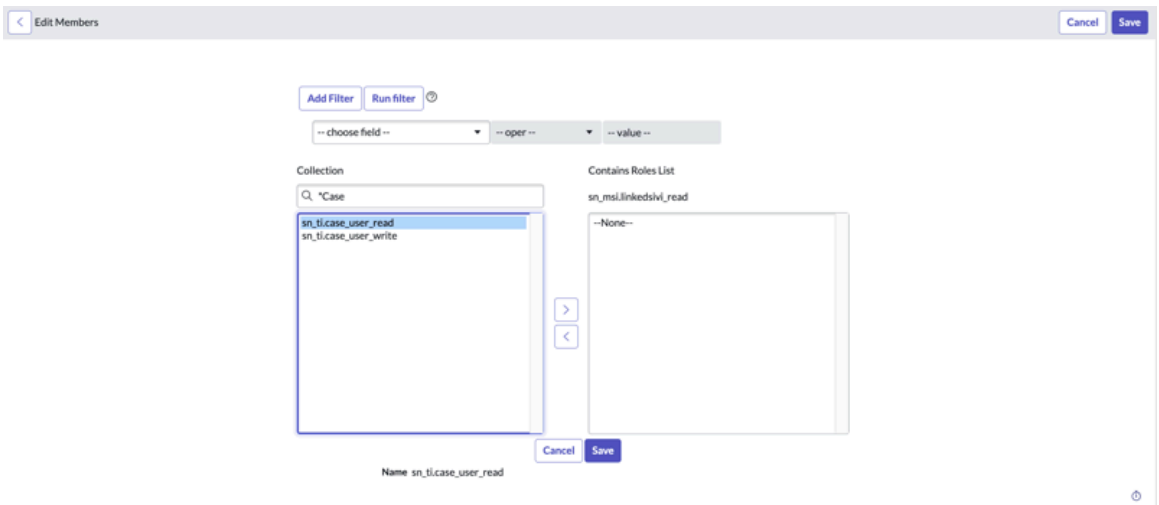
Note: For any source table, you must make sure that the required roles are added to the sn_msi.linkedsivi_read role.

Procedure

1. Navigate to **User Administration** > **Roles** and search for **sn_msi.linkedsivi_read** role.
2. Click **Edit** in the Contains Roles related list section.



3. Make sure that your source table roles are added under the Contains Roles section.
   The Edit Members page is displayed to configure the roles required for a security case.



4. Search for the source table roles, in the Collections section.
   Select the required roles that allow read and write access on the source table for a security case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- For a Security case, two separate roles for read and write are needed.
- Write access on tables for the ability to select source record from Major Security Incident Management workspace linked Record modal.

5. Click **Save** to add roles.
6. Verify that the roles are added successfully to the **Contains Roles** related list section.

Step 6. Create business rules for a Security Case

Create required business rules for a Security Case.

Before you begin
Role required: admin

Create the three following business rules for the new source table Security Case (sn_ti_case). These business rules are required to maintain the consistency in behavior with out of the box provided source table such as Security incident (sn_si_incident).

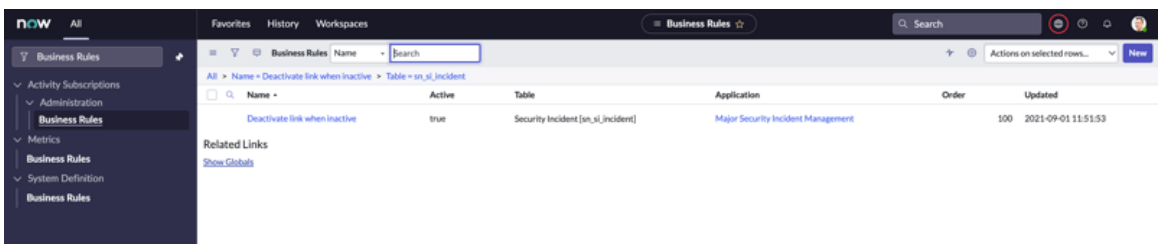
Business rules for the new source table:

1. **Deactivate link when inactive**: Once the security case is closed, related information will no longer be shown in Major Security Incident Management workspace page.
2. **Sync up team info on update**: Major Security Incident details tab shows the information about the all the active teams and users working on different tasks. Once we update assigned to user or assignment group is changed in the security case, we need to update security case team information in the Major Security Incident active team section. These business rules will update new assigned to user and assignment group in the active team section.
3. **Sync up team info on delete**: Major Security Incident details tab shows the information about the all the active teams and users working on different tasks. Once we close the security case, we no longer need to show security case team information in the Major Security Incident active team section. These business rules will remove the assigned to user and assignment group from the active team.

Create business rules for new source table:

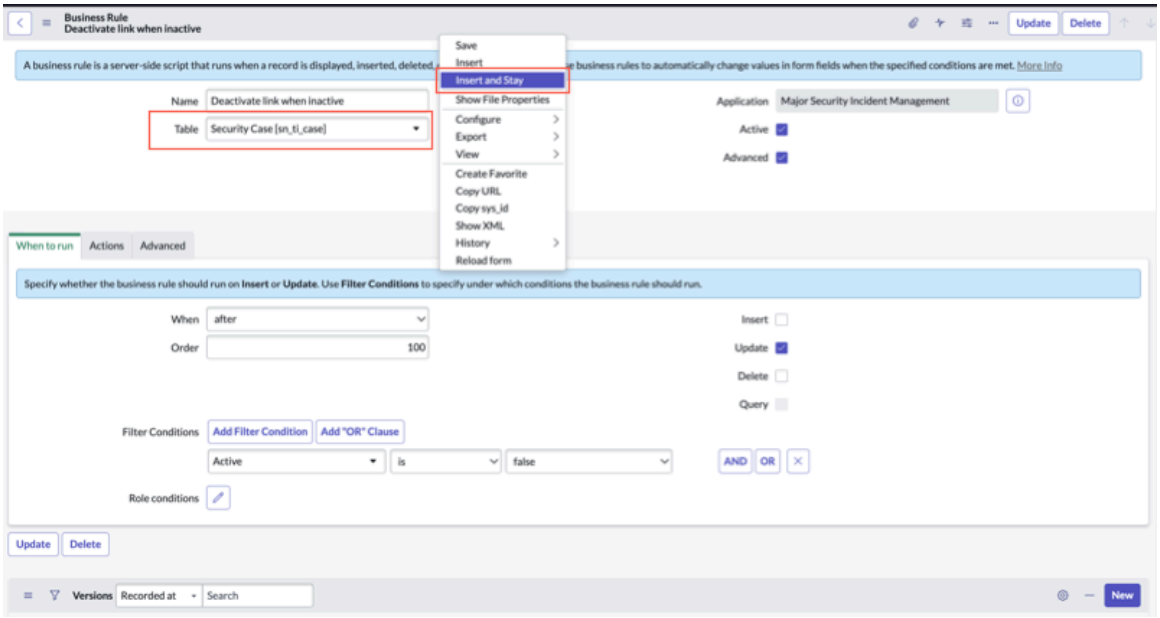
Procedure

1. Navigate to **System definition** > **Business Rules**.
2. Run the filter option to filter business rules criteria with below information:
   - **Name**: Deactivate link when inactive
   - **Table**: sn_si_incident



3. Open record and change the table name to a new source table: sn_ti_case.
4. Right-click the menu on the page and click **Insert and Stay** to create the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Repeat the procedure for another two business rules as well.
   - Sync up team info on delete
   - Sync up team info on update

Step 7. Create rollup record configurations

Create rollup record configuration to link and unlink additional records to MSI.

Before you begin

Role required: admin and sn_msi.workspace_admin

Note: The system admin can create the record and MSI workspace admin can update it.

To rollup information such as configuration items, observables, and indicator of compromise related to a Security case, create a rollup record configuration.

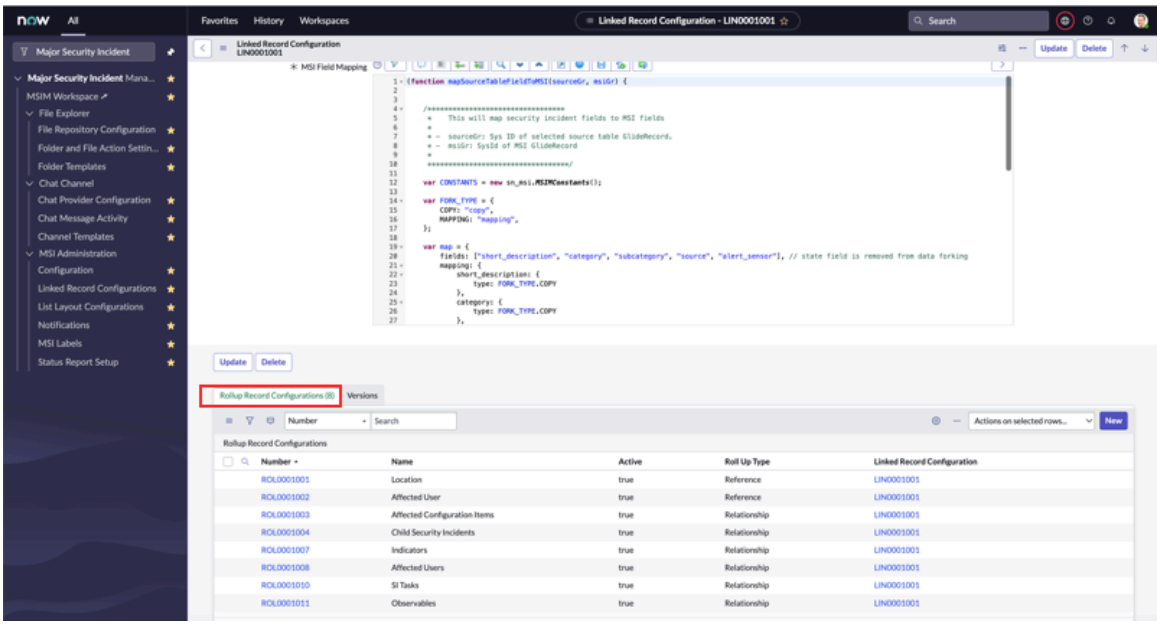
Procedure

1. Navigate to **Major Security Incident Response** > **Linked Records Configuration**.
   The Linked Record Configurations page displays.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Select or create a new linked record and navigate to the **Rollup Record Configuration** section from the same page.

Rollup Record Configuration section



What to do next

- For more detailed information, see Configure Rollup Records in Major Security Incident Management
- For a security case example information, seeWriting script for a Security Case

Writing script for a Security Case

Writing a script for a Security Case to roll up record configuration.

Before you begin

Role required: admin and sn_msi.workspace_admin

Note: The system admin can create the record and MSI workspace admin can update it.

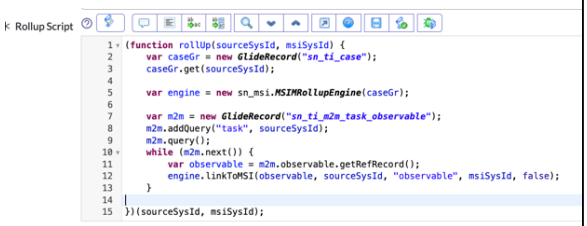
Procedure

1. Search for the Linked Record configurations using the left navigation.
2. Navigate to **MSI Administration** > **Linked Record Configuration**.
3. Open the configuration record which was created for a security case.
4. The Rollup Record configuration will be displayed in the Related List section.
5. Click **New** to create a new roll up record configuration.

   Below is an example record created to Rollup Observables data related to Security Case we are trying to Rollup with the field values as:

Name	Description
Roll up Type	Relationship

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	Note: The observable information is available in a related list format.
Rollup Script	Input sourceSysId contains security case sys id and msiSysId contains major security incident sys id.  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: *MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")*

Perform on demand atomic rollup

Rollup framework cannot handle updates to the existing linked records. In such cases, on demand atomic rollup should happen for linked records, which can be achieved via business rules.

To capture updates to the linked records, business rules must be created on the source table.

These business rules work on insert, update, and delete operations. When you perform insert or update, you need to add or update rolled up information to MSI. If you delete then the rolled up information will be removed from MSI.

For example, once a security incident is linked to MSI, the related information will be rolled up automatically MSI. But later, if you add a new observable to an MSI, then the newly added observable also will be rolled up to MSI. Here, **Sync rolled up observable** business rule captures

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the update and rollup the updated record to MSI. Similarly, the same business rule also handles the removal of the existing rolled up observables, if it gets removed from the security incident.

Predefined business rules

Following are a few predefined business rules that helps you understand on how to handle atomic rollups

Rule	Description
Sync rolled up indicator (sn_ti_m2m_task_indicator)	Use this business rule to handle the rollup and removal of indicator of compromise from Security Incident, Security Case, and Remediation task.
Sync rolled up observable (sn_ti_m2m_task_observable)	Use this business rule handles the rollup and removal of linked observables from Security Incident, Security Case, and Remediation task.
Sync rolled up affected user (sn_si_m2m_task_affected_user)	Use this business rule handles the rollup and removal of linked affected users from Security Incident, Security Case and Remediation task.
Sync rolled up affected CI (task_ci)	Use this business rule handles the rollup and removal of associated configuration items from Security Incident, Security Case and Remediation task.

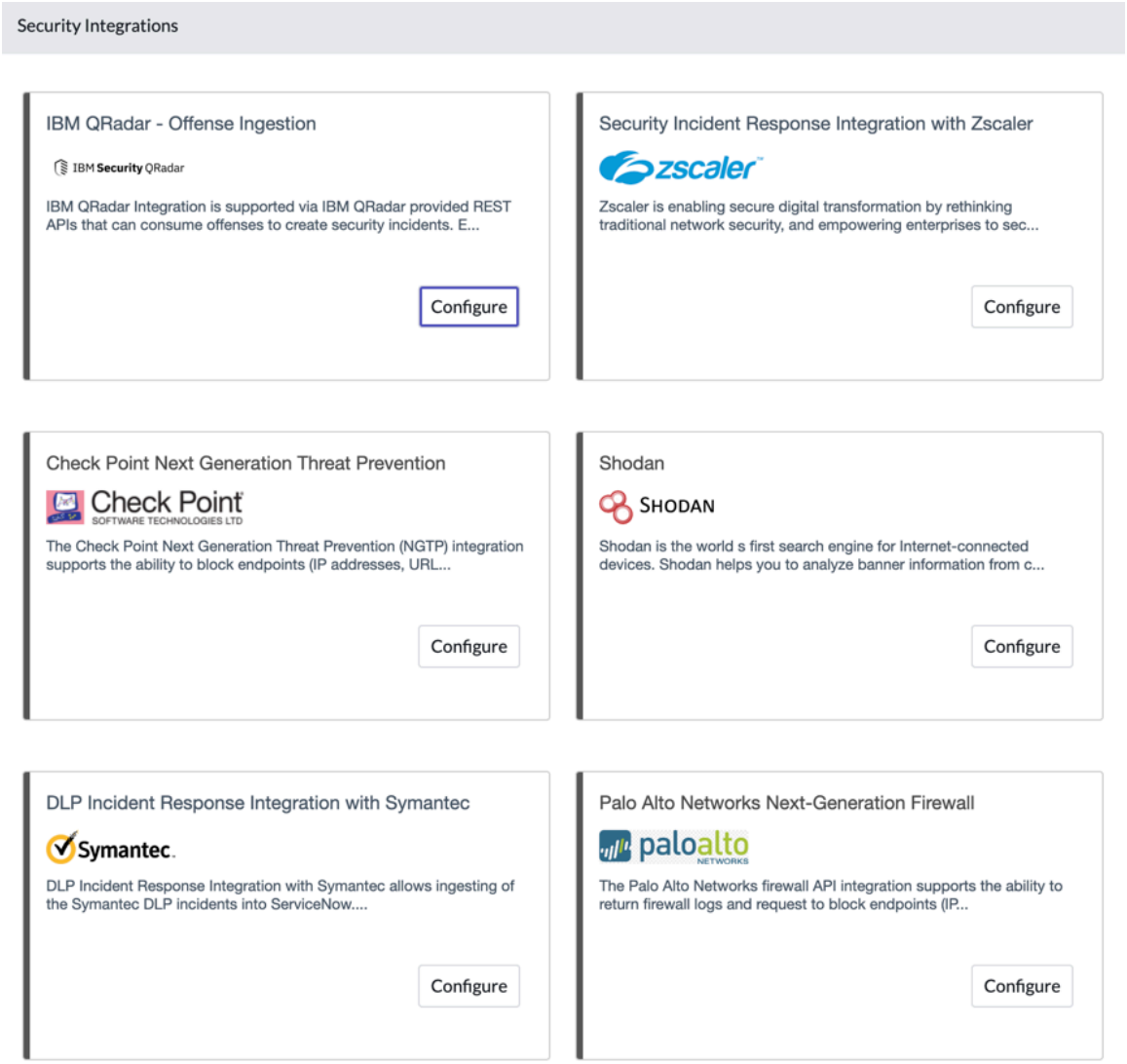
Security Incident Response integrations

All the Security Operations core applications and non-core third-party integrations are available from the ServiceNow Store. This section provides instructions for activating the integrations and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.

Integration Configurations

The base system includes a series of "cards" for each of the integration implementations you can activate and use. Also, cards are displayed for any integrations posted on the ServiceNow Store that have dependencies on Security Operations plugins. The integration cards can be viewed by selecting **Security Operations** > **Integration Configurations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can filter the visible integrations using the **Category** drop-down menu. The **Show Configurations** drop-down menu lets you see multiple instances of implementations that allow their creation.

Buttons on integration cards

Integration cards display different buttons depending on the current state of the integration and the source of the card.

Button	Description
Install Plugin	Click this button to install the applicable plugin to activate the integration. After the plugin is installed, the button changes to **Configure**.
Configure	Click this button to enter information for configuring the integration. For some integrations, you may need to enter API keys or URLs acquired from the website of the third-party integration.
New	Certain integrations, such as Carbon Black and IBM QRadar, allow you to define multiple implementations of the same integration. For those integrations, click **New** after the plugin is activated. The cards allow you to install plugins (where applicable) and configure the implementations for use.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Button	Description
Open Page	In the base system, your instance performs a query to the ServiceNow Store for any applications that have dependencies on Security Operations plugins. When those applications are found, and the associated application plugins are activated, integration cards for them are displayed with the other security integration cards. Click **Open Page** to access the website of the third-party application to configure the integration. After you have completed the configuration, the **Open Page** button changes to **Configure**.

ArcSight ESM Event Ingestion for Security Operations integration

The ArcSight ESM event ingestion integration with the Security Incident Response product allows security incident analysts to collect correlated events and automate creation of security incidents with the ServiceNow platform. Data is ingested continually based on a configured polling schedule, and it is used by analysts to identify and respond to potential cyber security threats.

With this integration, correlated events that are candidates for security incidents can be ingested on a periodic basis. You can map fields in correlated events to security incident fields, preview the setup of an event as a security incident, and setup scheduled ingestion of events to automatically create security incidents on an ongoing basis.

Overview

This integration provides a security operations center (SOC) analyst with visibility to correlation events in ArcSight ESM. This data can be integrated into ServiceNow AI Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles are created in your ServiceNow AI Platform instance to handle different correlation event types that are created and made available via correlation query viewers in ArcSight ESM. These profiles customize how different ArcSight ESM correlated event fields are displayed on SIR security incidents.

Key features

This integration includes the following key features:

- Create multiple event ingestion profiles to create SIR security incidents for specific types of threats such as malware and unauthorized access attempts.
- Drag-and-drop mapping of ArcSight ESM correlation event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample correlation events to validate event mapping details.
- Ingest historical correlation events as well as new notable events on configurable intervals.
- Filter out correlation events that do not meet SIR incident generation criteria, e.g. low priority events
- Aggregate events to existing SIR security incidents based on matching field values to avoid duplicate security incidents.
- Update correlation events based on SIR incident creation and/or closure conditionals via a bi-directional interface.

Supported ServiceNow AI Platform versions

This integration supports the New York Patch 6 and Orlando ServiceNow AI Platform releases.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response
4. Event and Alert Ingestion for Security Operations
5. Integration Hub Plugins
   a. ServiceNow Integration Hub Runtime
   b. ServiceNow Integration Hub Action Step - REST

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

ArcSight ESM supported versions

This integration has been tested with Version 7.0.0.2436 of the ArcSight ESM Manager. The integration supports both ArcSight ESM on-premises and Cloud/Hosted service environments.

MID Server

This integration requires an installed and configured MID Server in your ServiceNow AI Platform® instance to connect to the ArcSight ESM service when the ArcSight ESM server is deployed within your corporate network. If you are using the ArcSight ESM cloud service, a MID Server is not required. See the ServiceNow Product Documentation website for more information about MID Servers.

References

Reference	Document Identifier	Document Title
1	ArcSight ESM product documentation	ArcSight product documentation.
2	ServiceNow Product documentation website	ServiceNow Product Documentation website

Set up your ServiceNow AI Platform® instance for the ArcSight ESM event ingestion integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the application from the ServiceNow Store.

Before you begin

Role required: admin

About this task

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description

Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.	The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform® instance.
	• A user with the ServiceNow AI Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.
	• A user with the sn_si.admin role oversees the following tasks in the ServiceNow AI Platform®:
	  ○ Names, creates, and edits event profiles.
	  ○ Selects and maps values from ArcSight ESM correlation events to security incidents.
	  ○ Previews security incident details for accuracy prior to finalizing the configuration.
	  ○ Schedules on-going correlated event ingestion.
	  ○ Enables correlated event updates when a SIR incident is created and closed.
	  ○ Assigns the security incident analyst (sn_si.analyst) role.
	  ○ Users with the sn_si.analyst work with security incidents.
	For more information about roles and assigning roles to users, see Roles on the Servicenow Product Documentation website.

Verify that you are using version 7.0.0.2436 or later of the ArcSight ESM Manager. Earlier versions are not supported.	If you have access to the ArcSight ESM Query Viewer, you have access to the API that is required for this integration. There is no other special setup required for the API.
Set up the Query Viewer in ArcSight ESM.	Before you can ingest correlation events, you must configure the Query Viewer in the ArcSight ESM console. See Set up the ArcSight ESM Query Viewer for details.
Optional Create custom stages in ArcSight ESM for correlation event updates.	A correlation event goes through many stages in its life cycle before it is closed. ArcSight ESM provides default stages like Initial, Monitoring, Queued, and Closed. Some of these stages require user inputs but other stages are automatically applied to the event without any user intervention (the **User Required** field is unchecked in the ArcSight ESM console. You can create custom stages that do not require any user intervention and use them in your ServiceNow AI Platform® instance. See Additional options: Automate correlated event updates and closure based on SIR incident status for details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
Verify that you have installed and configured a MID Server Application.	Configured MID Server Application A MID Server in your ServiceNow AI Platform® instance is required to connect to the ArcSight ESM service if the ArcSight ESM server is deployed within your corporate network. See Install and configure the ServiceNow application for the ArcSight ESM Event Ingestion integration for instructions on how to configure a MID Server Application. See the MID Server for information about MID Servers. If you are using a hosted or cloud service, that is Internet accessible, a MID Server is not required.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Event and Alert Ingestion for Security Operations: This application requires: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST **5.** Threat Core For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

What to do next

You have successfully set up your ServiceNow AI Platform® instance for the integration. The next step is to install the ArcSight ESM Security Event Ingestion for Security Operations application from the ServiceNow Store for the integration.

Set up the ArcSight ESM Query Viewer

Create a query viewer and define filters that will include recently created correlation events that will be ingested ServiceNow.

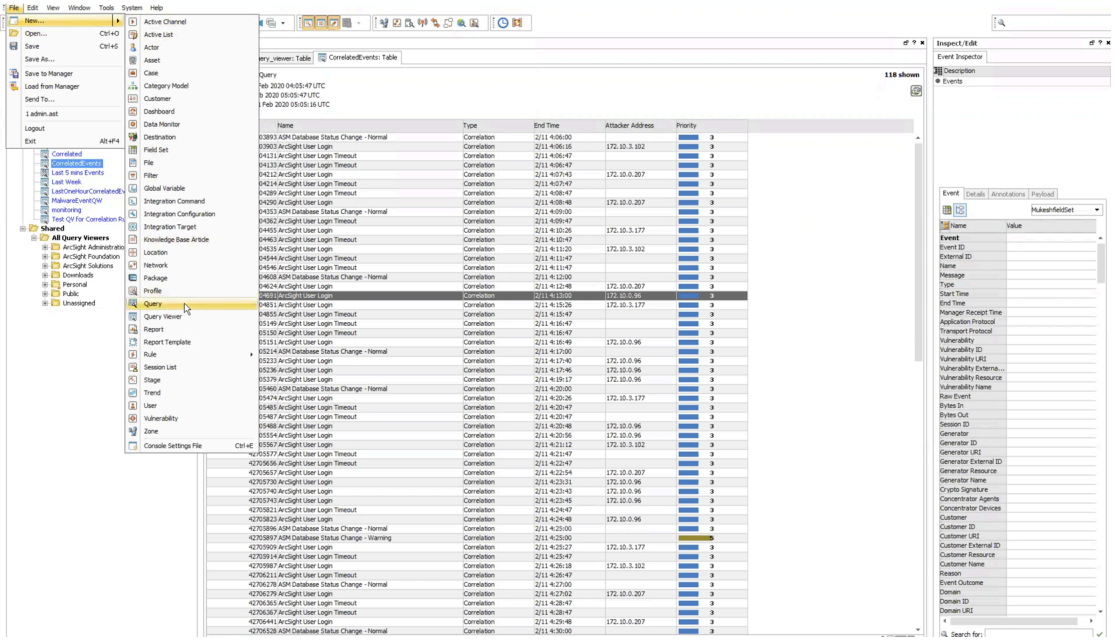
Before you begin

Role required: ArcSight Administrator

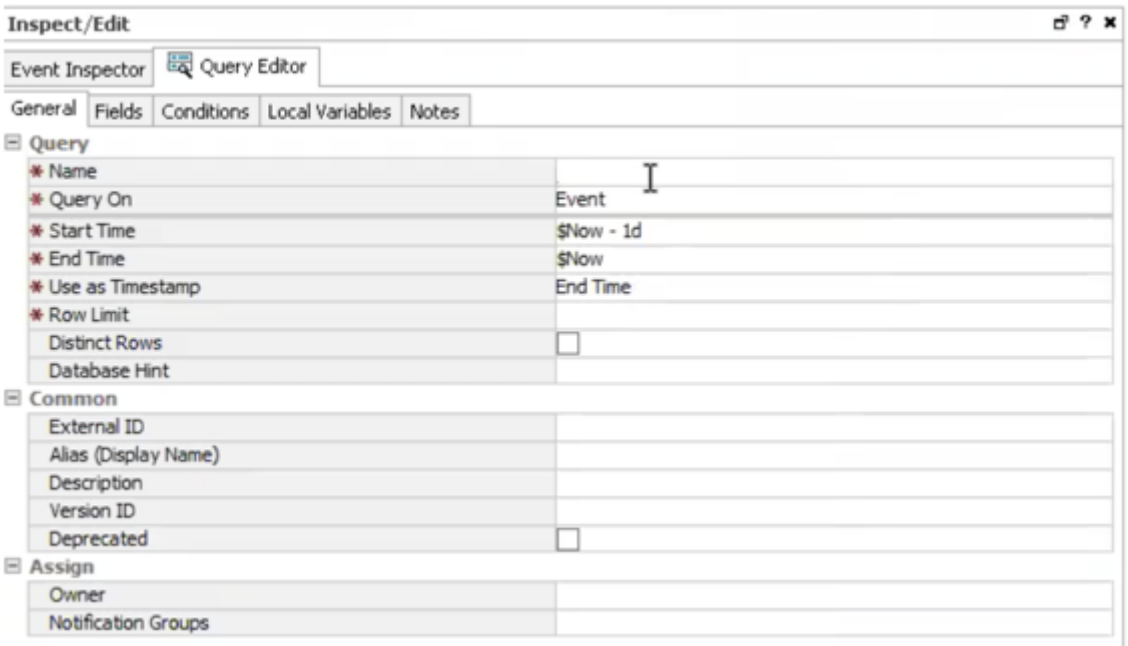
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Log into the ArcSight ESM console to create a query viewer.
2. To create a new query, navigate to **File** > **New** > **Query**.



3. Define conditions for the Query Viewer in the **Inspect/Edit** panel.



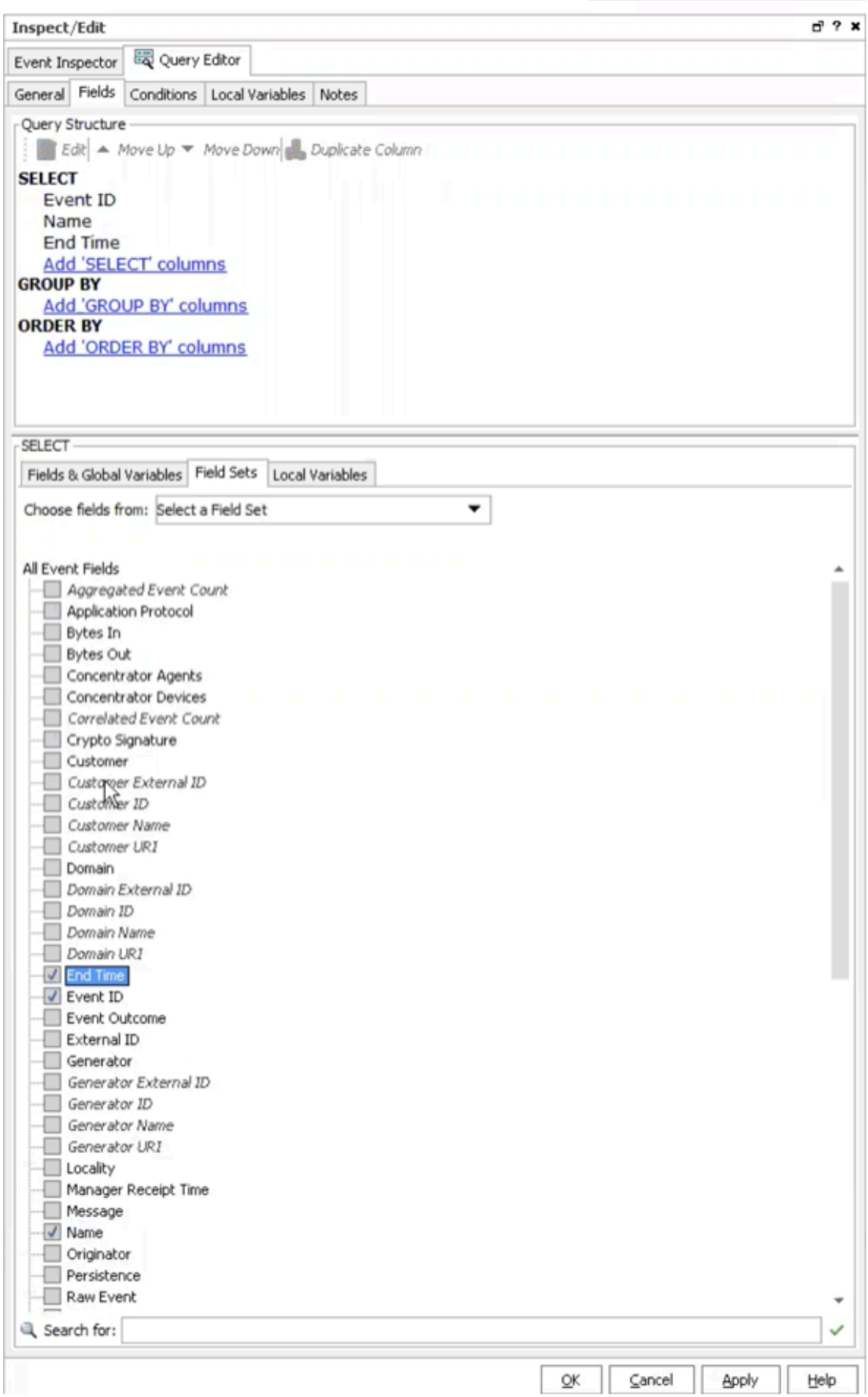
Field Name	Description
Name	Enter a name for the query.
Query On	Select **Event** from the drop down list.
Start Time	To ingest the most recent data, select the date from the events are to be ingested. Specify a date that is a day or a few days earlier than the current date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
	Note: You cannot specify a date that is more than 7 days older than the current date. If you are ingesting a large num ber of events, you must specify a date that is 1 or 2 days old er than the current date.
End Time	This is the current date.
Row Limit	The maximum number of events that can be ingested at a time. Specify a value that is less than 5000 here.

4. Click on the **Fields** tab.

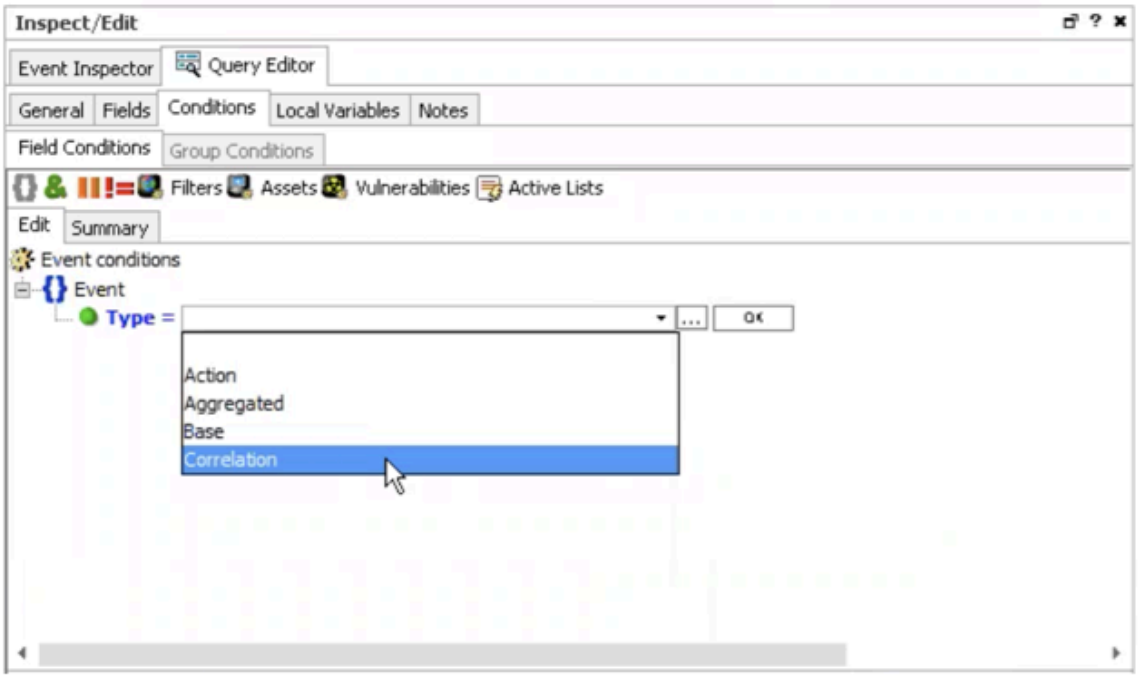
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

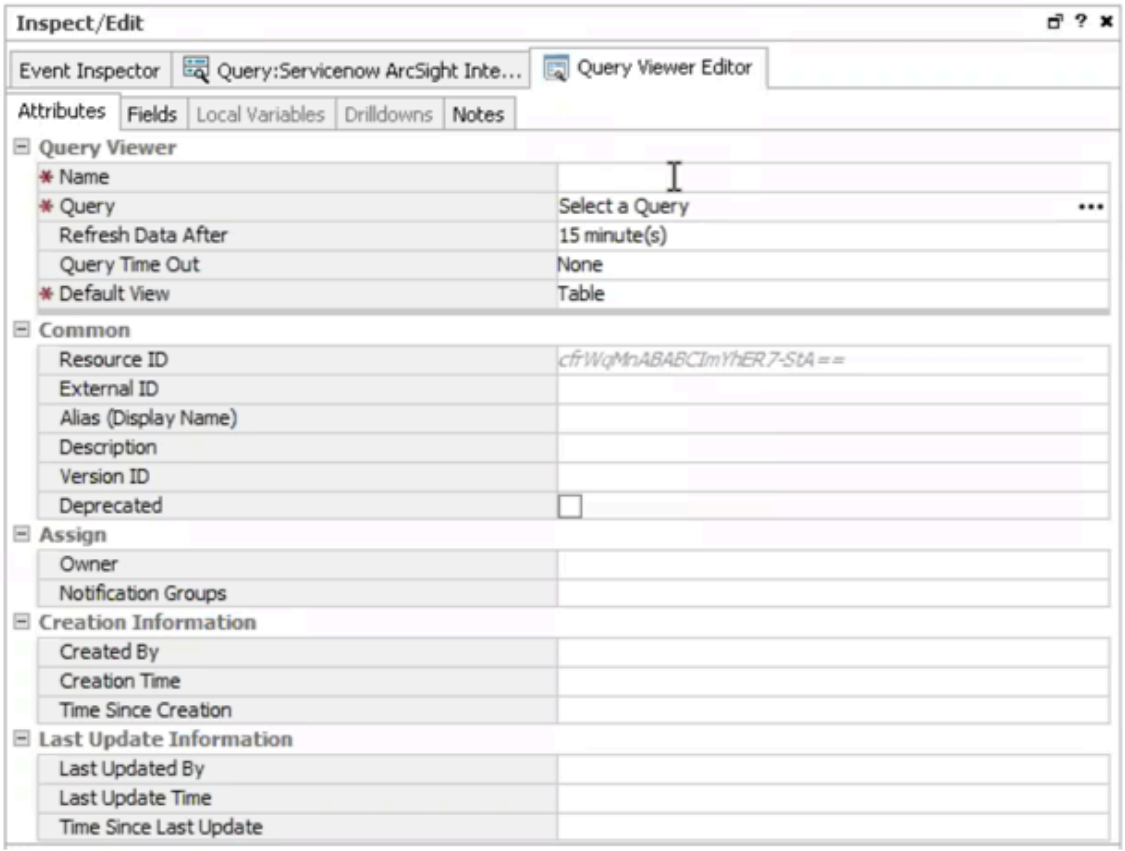
5. Select the fields that must be included during ingestion.
   You must select the *Event ID*, *Name*, and *End Time* fields for ingestion to be successful.
6. Click the **Add 'ORDER BY' columns** link and select **Event ID** field and specify the sort order as **Descending** to ensure that the latest events are ingested.
7. Click the **Conditions** tab.
8. Right click **Event** under **Event Conditions** under the **Summary** section.
9. Click **New Condition** > **Root** > **Type** and select the Event Type as **Correlation**.

> **Important:** Only correlation events will be retrieved; base events for correlations will not be retrieved.



10. Click **OK** to save the query.
    The next step is to create a Query Viewer for this query.
11. Navigate to **File** > **New** > **Query Viewer**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

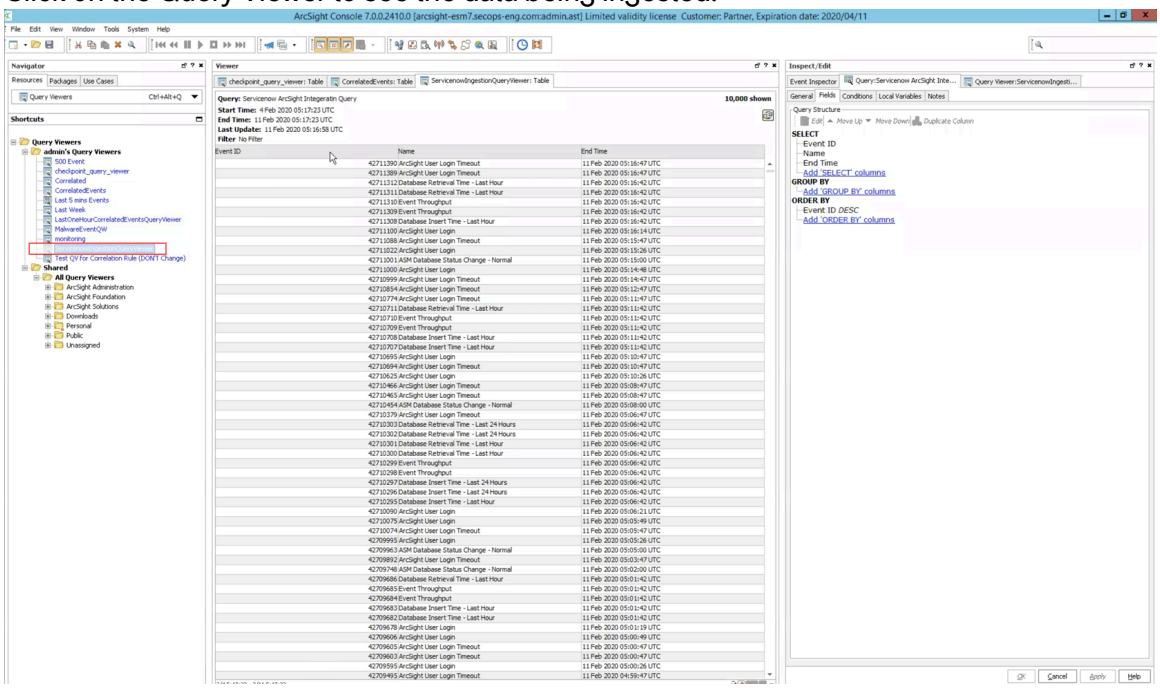


Field Name	Description
Name	Enter a name for the Query Viewer.
Query	Select the query you have just created.
Refresh Data After	Specify the frequency at which the data is to be refreshed.

12. Click the **Fields** tab and ensure that the mandatory fields (*`Event ID, Name, End Time`*) you have specified in your query are selected.
13. Click **Apply** to save the Query Viewer.
    The new Query Viewer that you have created is listed in the Query Viewers section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

14. Click on the Query Viewer to see the data being ingested.



Install and configure the ServiceNow application for the ArcSight ESM Event Ingestion integration

Before you run the integration on your ServiceNow AI Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.admin

Procedure

1. If you have not installed the ArcSight ESM application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **Integrations** > **Integrations Configurations** and locate the ArcSight ESM tile.
3. To configure the application, click **New**.
4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.
5. On the form, fill in the fields.

Field	Description
Name	Unique name for the ArcSight ESM Manager that will be used in the integration profile con figuration to distinguish amongnst multiple Ar cSight ESM Manager sources if required. Spaces are supported for names, but paren theses are not supported.
ArcSight API Endpoint URL	URL for your ArcSight ESM Manager serv er. Note that the URL should include the API

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

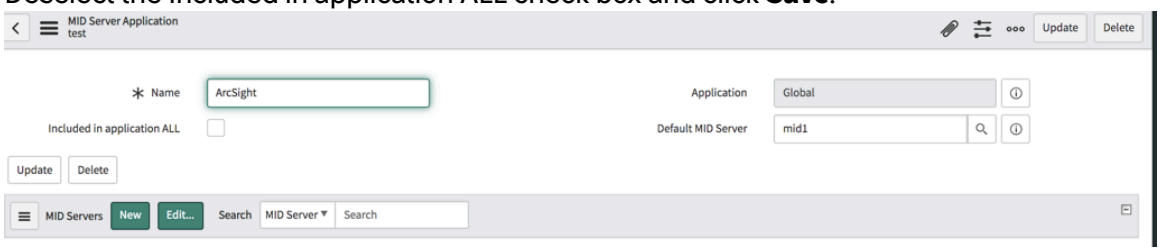
Field	Description
	port, for example: `https://arcsight-esm.com:8443`
API Account User Name	User name that you created for your API user account in the ArcSight ESM Manager con sole.
API Password	Password that you created for your API user account in the ArcSight ESM Manager con sole.
On Premises Deployment	Default is unchecked. If you are using the cloud-based version of Ar cSight ESM that has direct Internet access, verify that the check box is cleared. For an on-premises deployment, select this check box and specify the MID Server Appli cation.
MID Server Application	Specify a MID Server Application name here. This MID Server Application can point to any of the MID Servers that have been config ured and any MID Server that is available will be used. If you do not have a Mid Server Application configured, you must create a new MID Serv er Application for this integration. **Note:** The MID Server Application can be configured only by users with sys tem administrator role.

To create a new MID Server Application, follow these steps:

a. Navigate to **Mid Server** > **Applications** and click **New**.

b. Enter a name for the MID Server Application and select a MID Server to be used as the default.

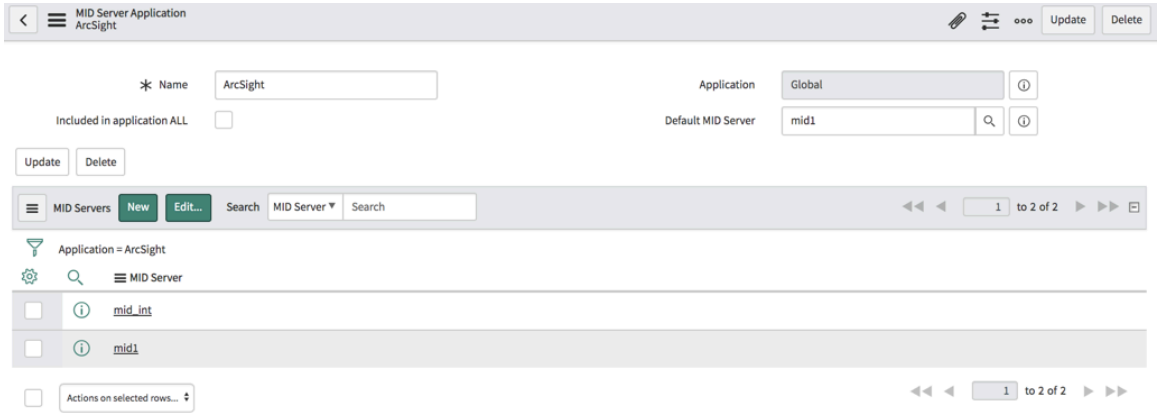
c. Deselect the Included in application ALL check box and click **Save**.



d. Click **Edit**. In the **Edit Members** page, select all available MID Servers, move them to the MID Servers List, and click **Save**.

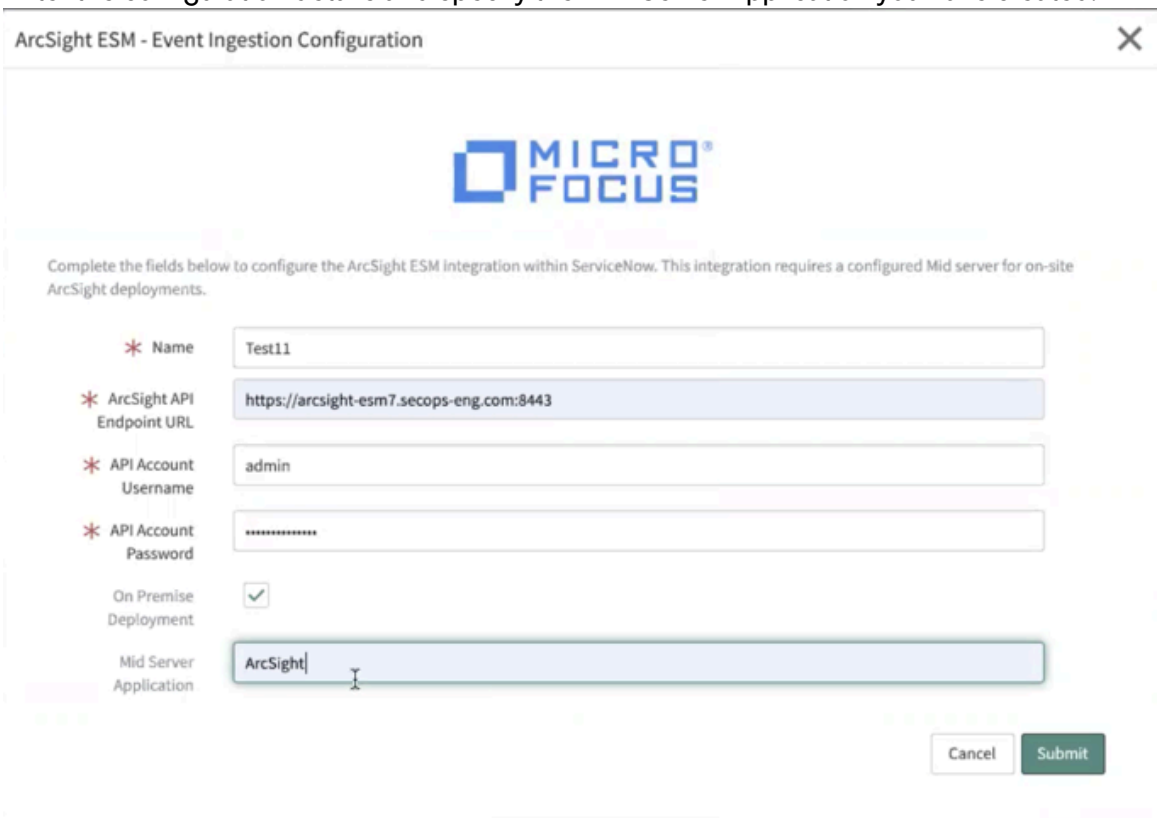
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. The selected MID Servers will be listed as shown below.



Depending on the availability, one of the MID Servers configured with the MID Server Application will be used.

6. Enter the configuration details and specify the MID Server Application you have created.



Each correlation event that you ingest from your ArcSight ESM Manager console requires a unique event profile in your instance. However, the ArcSight ESM source that you configure on the Event Ingestion Configuration form can be reused for multiple profiles as long as each profile ingests unique correlation event types.

7. Click **Submit**.
After it is successfully validated and submitted, each ArcSight ESM server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
You have successfully installed and configured the application. The next step is to create an event profile.

Create a profile for ArcSight ESM correlation event ingestion integration

As a user with the sn_si.admin role, you create a profile in your ServiceNow AI Platform instance and determine which correlation events create security incidents. Before ServiceNow AI Platform Security Incident Response (SIR) security incidents are created from correlation events, the field values from events are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident will be created.

Before you begin
Role required: sn_si.admin

About this task
Correlation events are automatically ingested into the Security Operations environment of your ServiceNow AI Platform instance depending on the profile type defined. A profile is an encapsulation of one type of correlation event like unauthorized access attempts or malware.

After a correlation event has been ingested, you can map individual correlation event fields to corresponding fields in the security incident. You can filter correlation events to specify which events create security incidents. For example, you may prefer filters that create security incidents only for correlation events identified as high-risk. You can also define additional event aggregation criteria so that incoming duplicate correlation events are aggregated to an open security incident. Finally, you can define an ingestion schedule and activate the profile.

Names for the event profiles in your ServiceNow AI Platform instance must be unique and can only be mapped to one active event profile at any given time.

Create and name the profile for ArcSight ESM event ingestion integration

You can set up a profile to ingest correlation events.

Before you begin
Role required: sn_si.admin

Procedure
1. To create an event profile for a correlation event in your ServiceNow AI Platform instance, navigate to **ArcSight ESM Integration** > **ArcSight ESM Event Profile**.
2. Click **New**.
3. Fill in the fields.

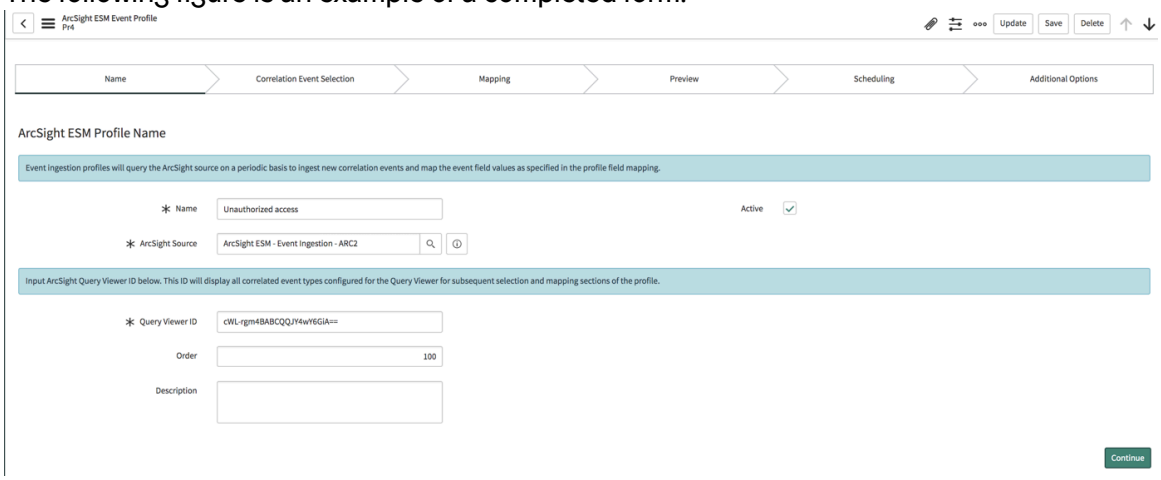
   An example of a completed form follows the table.

Field	Description
Name	Unique name for the profile. If names are not unique, an error will be displayed and dupli cate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Active	heck box is cleared by default. If this option is disabled, the profile is not active and inges tion will not take place.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: You should complete all sec tions in the profile before making it ac tive.
ArcSight Source	The ArcSight ESM server configured during the initial authentication step. If you have mul tiple ArcSight ESM servers configured, se lect the appropriate server for the correlation event types that will be ingested for the pro file. You are required to select a value.
Query Viewer ID	Enter the Resource ID of the configured Query Viewer in the ArcSight ESM Console. The Resource ID is a unique identifier for any Query Viewer configured in the ArcSight ESM server. Once the Resource ID is submit ted, the name of the Query View will be re turned to ensure that the right Query Viewer has been selected. See the section below for screen shot view of how to determine the Re source ID for the selected Query Viewer in Ar cSight ESM.
Order	Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same trig gering conditions. The workflow in the profile with the lowest number has the highest priori ty.
(Optional) Description	Additional text to help you distinguish this pro file from other profiles.

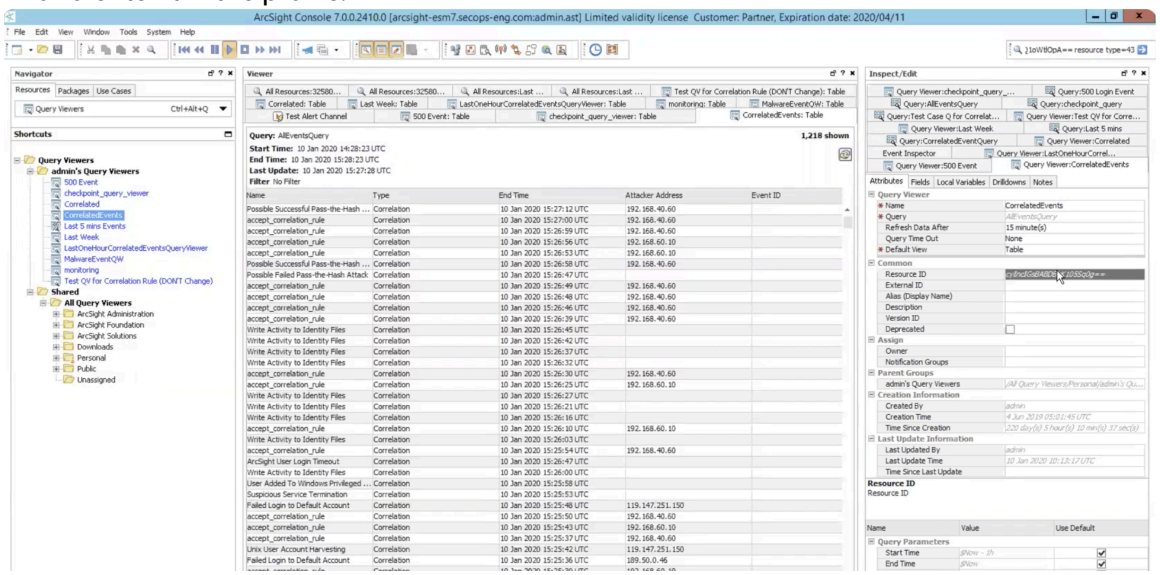
The following figure is an example of a completed form.



After you have entered the profile details, click **Continue**. The Query Viewer ID is validated and if a corresponding Resource ID is present in the ArcSight ESM Query Viewer, the name of the Query Viewer will be returned as shown below. If the validation fails, check if the Resource ID

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

exists in the ArcSight ESM console. If the Resource ID is not found, find the correct Resource ID and enter it in the profile.



What to do next

The next step is to select the correlation event types for ingestion from the Query Viewer that was selected in the prior step.

Select correlation events for ArcSight ESM event ingestion integration

Based on the ArcSight ESM source and the Query Viewer configured, select a correlation event rule for the profile.

Before you begin

Role required: sn_si.admin

About this task

View the available correlation events listed in the Correlation Event Selection in your ServiceNow AI Platform instance so you can determine which correlation events you want to ingest and create security incidents. You can only select one correlation rule type from the list for each profile.

The Query Viewer ID and the Query Viewer Name as specified in the Query Viewer form is displayed. Select a correlation event from the list that you can use to create a configuration mapping for the ingested correlated event.

Click on the drop down list in the Correlation Events List field. A list of correlation events that are present in the ArcSight ESM Query Viewer Console is displayed.

Click **Continue** to proceed to the next step in the wizard.

Mapping correlation event fields for the ArcSight ESM event ingestion integration

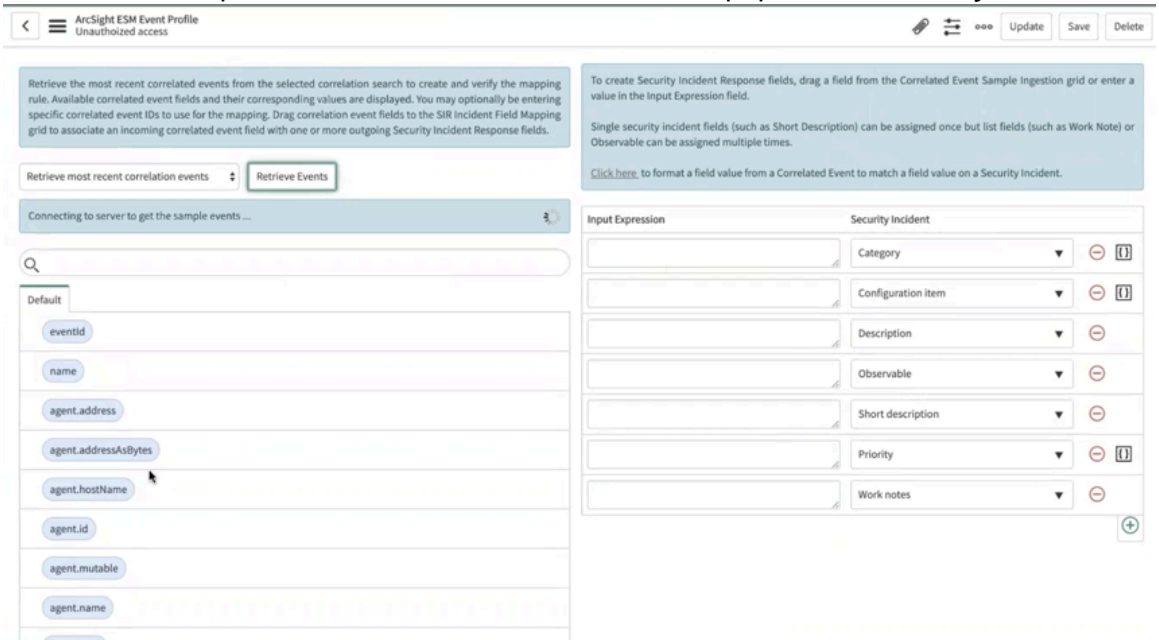
After you identify the specific correlation event rule from the list, the next step is to map correlation event fields to the fields in the security incident form.

Overview

For the mapping step, you can ingest sample correlation events for the selected correlation rule. During this mapping phase, you can ensure all relevant correlation event field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure shows the default mapping configuration that is provided for creating the correlation event profile. You can customize the fields that populate the security incident.



When you click **Retrieve Events**, the correlation event field names and the corresponding values are populated on the left side of the form. These are the ArcSight ESM correlation event fields that are available to map to the security incident fields.

You may prefer to review a few sample correlation events on your console to ingest for the field mapping configuration step. This step is labeled Mapping on the progress bar. If this page is not displayed, click **Mapping** on the progress bar. You can ingest up to five sample correlation events from the ArcSight ESM Manager for the selected correlation rule to assist with the field mapping process. There are options to either ingest the five most recent correlation events for the selected Correlation Event or ingest up to five specific correlation events based on the event IDs.

Below is a summary of the steps required to map correlation events:

- Field Mapping: Edit the mapping configuration by dragging correlation event fields from the left side and dropping them on the SIR incident mapping section on the right. The mapping on the right associates the incoming correlation event field with an outgoing security incident field.
- Mapping Experience: Customize the mapping grid by adding or removing fields using the + icon at the bottom of the SIR incident field mapping section. Track overlooked or previously mapped fields with the color coding that is provided (mapped fields are greyed out, blue fields are unmapped).
- Incident Generation Conditions: Once the mapping section is complete, you can define filter conditions so that you can filter which correlation events should create security incidents versus correlation events that should be filtered out, for example, low priority correlation events. This is done in the Incident Generation Conditions section located below the Correlation Event Sample Ingestion section.
- Event Aggregation Criteria: Define additional event aggregation criteria that aggregates an incoming correlation event to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related security notable event data on a single security incident.
- Format Field Translation: In certain cases, event field values in the ArcSight ESM correlation event may not translate directly to the fields on the SIR security incident. For these values, you

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

The next step is to ingest sample correlation events and map values to the SIR security incident fields.

Create mappings for ArcSight ESM event ingestion integration

In this step, you ingest sample correlation events and map values to the SIR security incident fields.

Before you begin

Role required: admin, sn_si.admin

About this task

As a user with the sn_si.admin role, you can review up to five sample correlation events from the Correlation Event Sample Ingestion column on the left of the form to assist with mapping and translating event field values to the security incident fields in the SIR Incident Field Mapping column on the right.
Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Fields displayed by default are typically important fields to populate on the security incident response form. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map ArcSight ESM fields that are not displayed on the default mapping grid on the security incident.

Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. You can either pull the most recent sample correlation events for the selected correlation rule or provide the unique correlation event IDs for the specific correlation events that you want to use for your correlation event mapping experience.
3. From the drop down list, select one of the following:
   - Retrieve most recent correlation events
   - Select correlation events based on event ID

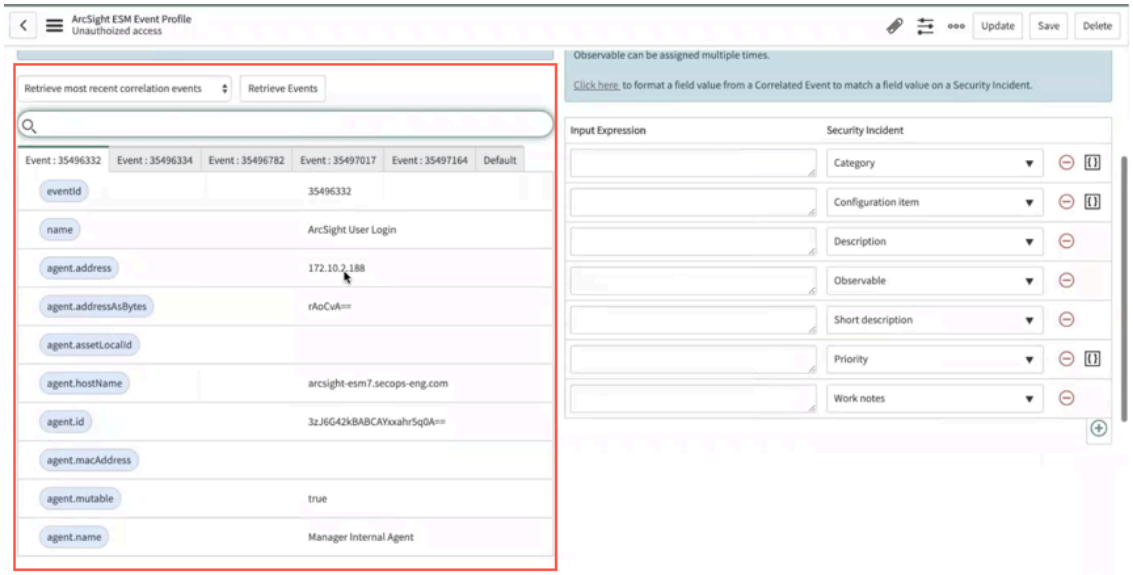
   Click **Retrieve Events** to pull the latest sample correlation events from the ArcSight ESM console for the selected correlation search rule.

   The correlation event fields and values results are displayed as individual tabs.

   The pull for sample correlation events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

   In the following figure, the field-name value pairs for the ingested correlation event, or the imported sample events, are displayed on the left side of this form after the ingestion pull is completed. These values are the values that you map to the security incident fields on the SIR Incident Field Mapping side of the form.

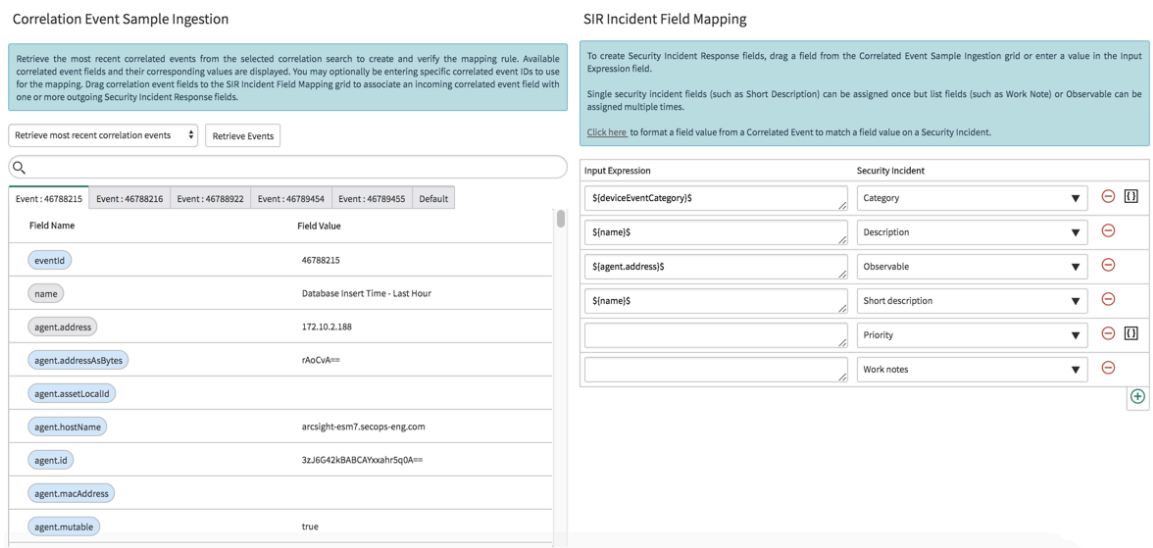
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
5. Drag the field name, for example, `agent.hostname`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

   To help you ensure that no event fields are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a correlation event field is not yet selected and mapped on the security incident. You may prefer to associate an incoming correlation field with more than one field on a security incident.

   A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track which event fields have already been utilized for future security incident field mappings.



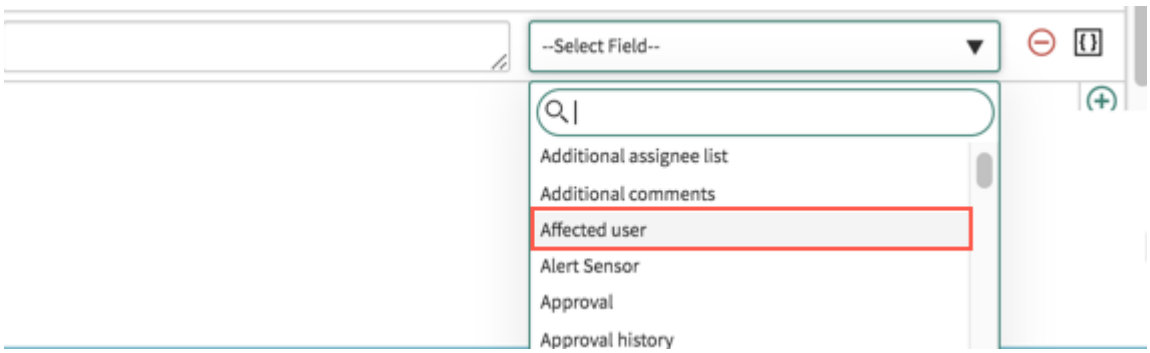
6. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.

   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon.
   A new field is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. In the Security Incident column, expand the choice list that is displayed, and select a field.

In the expanded choice list for the new field, some fields are shaded. In the following figure, `Affected User` has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the correlation events fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.



Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the **Event ID** that you want in the **Input Expression** field.
With the drag-and-drop feature, map it next to your new field.

7. **Optional:** Open the script editor and continue editing.

(Optional) For more information about the script editor, see Use the script editor to format correlation event values for ArcSight ESM integration.**Incident generation filtering conditions**

8. **Optional:** After you have completed the preceding field mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming correlation event must satisfy to create a SIR security incident.
To set incident generation conditions, follow these steps.

a. Scroll to the Incident Generation Conditions section on the form and select the **Filter based on conditions** check box to enable the option.

(Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the Correlation Event Sample Ingestion section for the events you ingested. These fields are dynamic and change depending on the correlation events that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the ArcSight ESM correlation event.

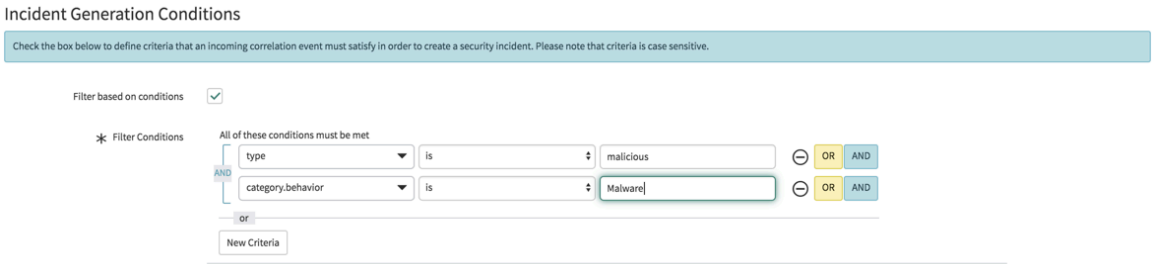
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the choice lists and fields of the condition builder, set filters for the first row.

b. To add more conditions, to the right of the fields, click **AND** or **OR**.
If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

c. Optional: In the second row, set a second filter condition.

(Optional) The following image is an example with two conditions that must be matched before security incidents are created.



(Optional) You have set the incident generation conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of incident generation condition filtering helps you narrow down the security events, and limit the number of unnecessary security incidents that you create without modifying the underlying correlation search or filter out events in ArcSight ESM. If additional filtering criteria are set, only correlation events that match all criteria are mapped to incidents.

Note: If any of the event field names have special characters such as quotes (“),hyphens (’), underscores (-), or ampersands (@), these characters may need to be replaced for mapping translation purposes and possibly create a duplicate event name. The mapping can be done appropriately but a numerical suffix is appended to differentiate fields with duplicate event names. For example, if the first event field is `events.event` and the second event field is `events.event`, these fields cannot be uniquely identified as the remaining standard text characters are the same. In this case, a suffix is added to the second event field and the field is renamed to `events@event(1)`.

Event Aggregation Criteria to Handle Similar Correlation Events and Prevent Duplicate Incidents

9. Optional: To avoid creating duplicate security incidents, define additional event aggregation criteria so that incoming correlation events are aggregated to an open security incident.
To set the criteria, follow these steps below:

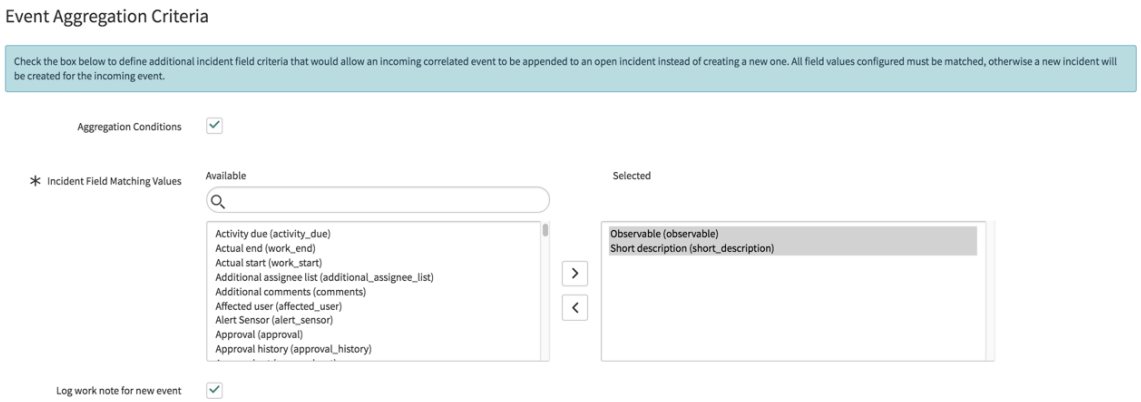
a. Scroll to the **Event Aggregation Criteria** section on the form and select the Aggregation conditions check box to enable this option.

(Optional) The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

b. From the Available list, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform and move them to the Selected list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

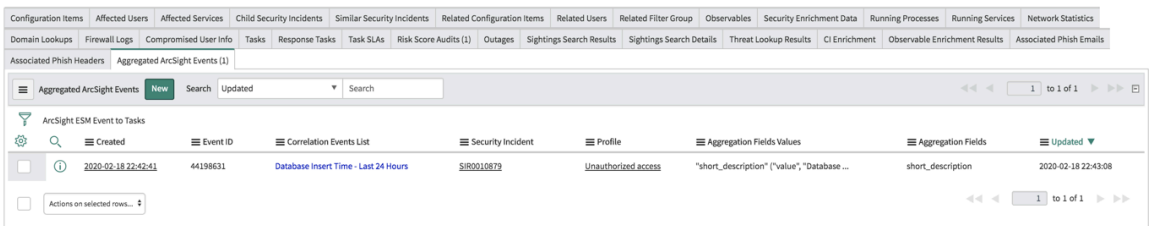
(Optional) All the field values that you select must be matched to append this incoming correlation event to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple correlation event field values mapped to them. All values must match. If only a subset of the values are matched, the event aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.



If a new correlation event matches all the values that are selected in the aggregation field conditions in the mapping step, the new correlation event is automatically added to the most recently opened security incident with the same field values. As a SOC analyst working with security incidents, you can view all the added aggregated correlation events on a related list on a security incident. All of the aggregated correlation events on a security incident are displayed on the **Aggregated ArcSight Events** related list. This list details associated time stamps and aggregated field values. This information helps you understand why these correlation events are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under **Related Links** and click the **Show All Related Lists** link.

Note: If you do not see this related list, follow these steps:

- Right click the Security Incident form header and click **Configure** > **Related Lists**.
- Select **Aggregated ArcSight Events** in the Available list, move it to the Selected list and click **Save**.
- Click **Show Related Lists**. You will now see the **Aggregated ArcSight Events** tab in the Related List section.



c. **Optional:** To log a work note for each time an event is aggregated on the security incident, select the check box to enable this option.
The work note logs that a new correlated event has been added along with a link to the correlated event details.

You have successfully mapped values from a correlation event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also aggregated correlation events

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

to existing SIR security incidents when event field values match the configured aggregation criteria.

10. Choose one to continue with the profile configuration.

Option	Description
Continue	The Mapping form is displayed. **Preview** is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.
Update	Your data is saved and the ArcSight ESM Event Profiles list is displayed.
Previous	The Correlation Event Selection form is dis played.
Delete	Delete this event profile and the Event Pro files list is displayed.

Preview the security incident for the ArcSight ESM event ingestion Integration

After you complete the mapping step, preview the values that you mapped in a ServiceNow AI Platform Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the correlation fields that you want displayed on the security incident.

Before you begin

Role required: sn_si.admin.

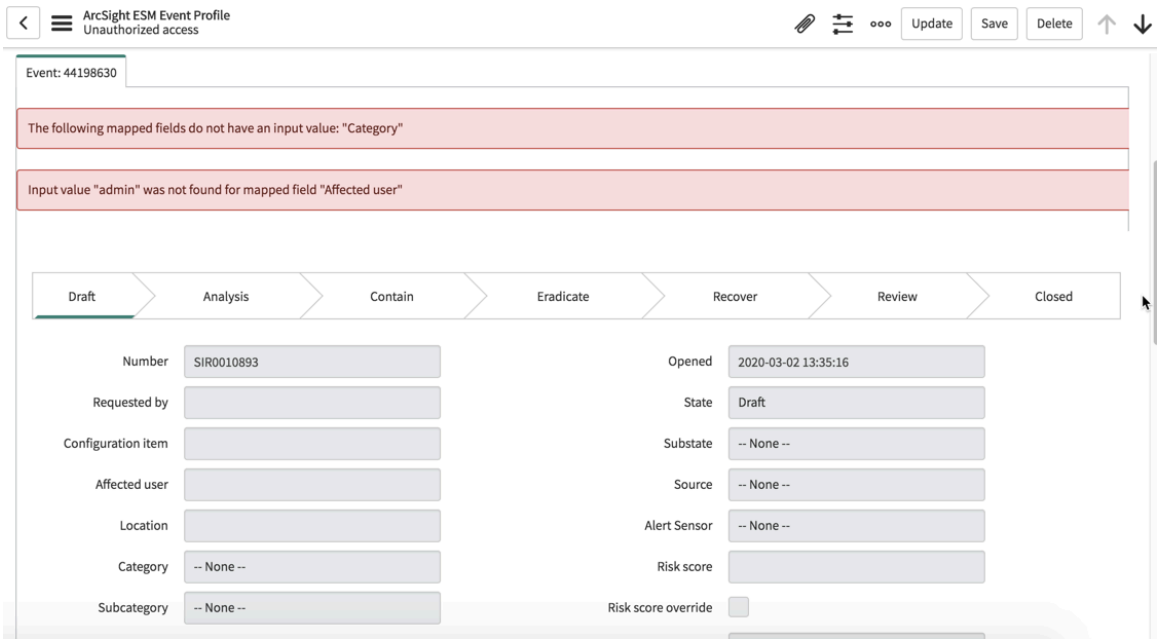
About this task

As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of security incidents are not saved as actual incidents in the Security Incident Response product.

Procedure

1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. From the Sample Event IDs choice list, select an item.
   The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the correlation event values on the security incident.

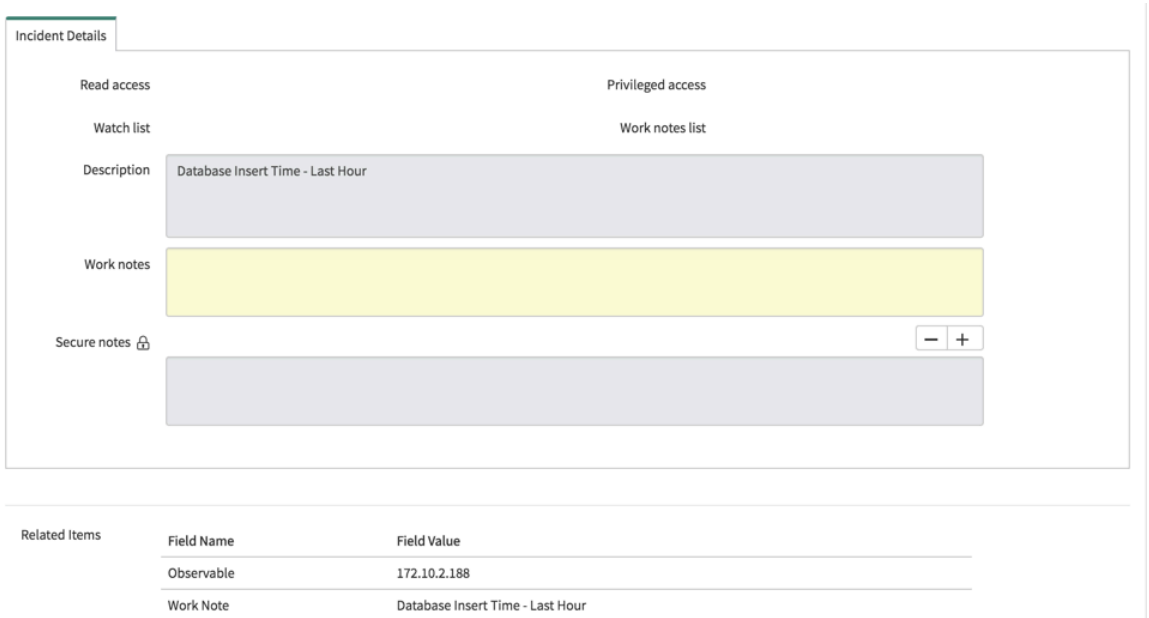
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The preceding image is an example of a preview with a mapping error. In this example, a field value from the correlation event does not have an acceptable value for the reference field on the SIR incident form. An error message is displayed that indicates an input value was not found for the `Category` field which is a reference field with a specific set of values. As a result, this mapped field value will not appear on the SIR security incident form without further modification.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

   The following figure is an example of the Incident Details tab on the bottom half of a security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the ArcSight ESM correlation event samples.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Create a schedule for ArcSight ESM event ingestion ingestion

You can define the polling or pull schedule for new correlated events. During this step, you can verify the existing settings for correlation event retrieval or modify the scheduling as needed. This step also permits you to retrieve historical correlation events using a date range.

Before you begin
Role required: sn_si.admin.

About this task
You can choose whether you want to ingest any historical correlation events during the Scheduling step. You also choose how often you will poll for future new correlation events that match the profile configuration.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the ArcSight ESM correlation event ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the ArcSight ESM server against a desire to be notified as soon as possible when an event is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

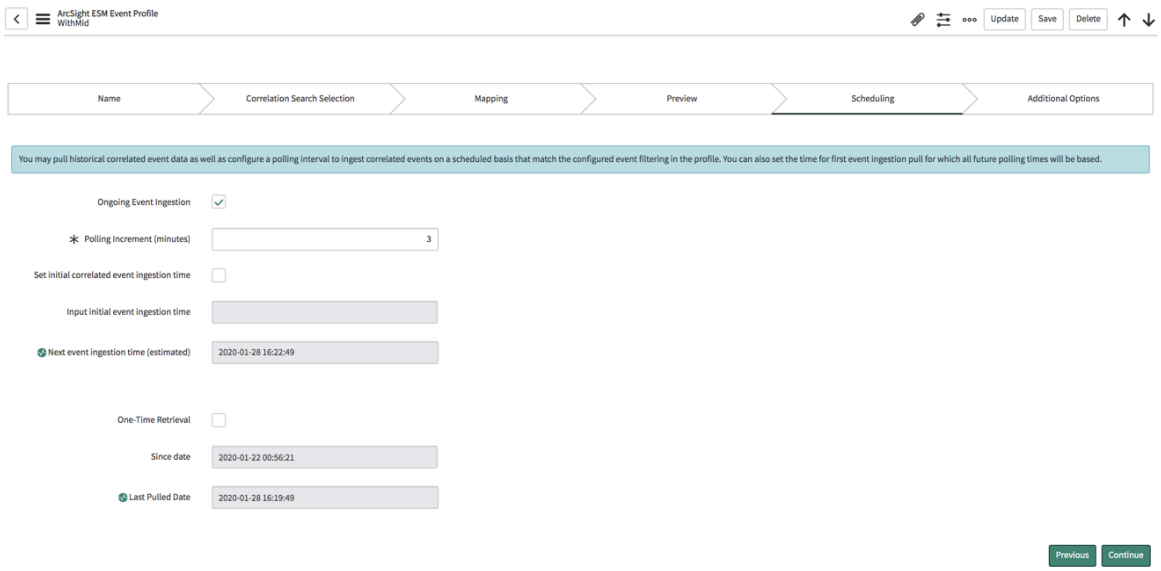
Pulling new and updated correlation events

Procedure
1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when correlation events are pulled from the <ArcSight> console.

Option	Description
○ **Ongoing Event Ingestion field selected** ○ **One-Time Retrieval field cleared**	On-going Event Based on the default setting, the ServiceNow AI Platform instance pulls from the ArcSight ESM server for new correlation events every five minutes. Security incidents are created if correlation events are found and incident gen eration filtering criteria are matched. To bal ance ingestion polling overhead desire to get the most current data, five minutes is the de fault setting. However, this value can be modi fied to as low as one minute if needed.
○ **Ongoing Event Ingestion field cleared** ○ **One-Time Retrieval field selected**	One-Time Retrieval Use this configuration if you want a one-time pull to ingest historical correlation events. When this setting is configured, a profile is used once to retrieve correlation events from historical events that are based on a date range. To the right of the Since date field, click the calendar icon. In the calendar that is dis played, select the date that you want to start

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	pulling alerts. Starting with the Since date value, correlation events are retrieved up through the current date. Note that you can retrieve events as far back as seven days from the current date. This functionality is not intended to retrieve signifi cant amounts of historical events for archival reasons but rather a minimal amount of in-flight events that are being actively worked at the time of profile activation. After the correlation events are pulled, this setting will not retrieve more correlation events for this profile going forward from the current date. This setting populates the securi ty incident with all the correlation events that are found for the range you enter.



As an example for scheduling an initial correlation event ingestion time, if you have a daily ArcSight ESM security check that runs once a day at 4 AM local time, you can set up the corresponding correlation event profile in your ServiceNow AI Platform instance to run at 4:05 AM local time to capture the security failure event right away and create a security incident. Enter `04 05 00` in the Initial event ingestion field. In the Increment (Minutes) field, enter `1440` (24 hours) to schedule the next event ingestion for 24 hours from the initial event ingestion. Both the initial event ingestion time and next event ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

   a. With the Scheduling page displayed, select the **Ongoing event ingestion** check box to enable this option.

   b. In the Increment (Minutes) field, enter `1440` (24 hours).

   c. Click the **Set initial correlated event ingestion time** check box to enable editing for the Initial event ingestion and Next event ingestion fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. In the Initial event ingestion time field, enter `04 05 00`.
In the Next event ingestion time (estimated) field, the time of the next event ingestion is displayed.

4. Click **Continue** to navigate to the Additional Options page.

> **Note:** The default number of security incidents that can be created and aggregated in a day, and the flow time period are defined in the ArcSight ESM Integration Settings. You can modify these settings if required. See ArcSight ESM Integration Settings for event ingestion integration for details.

Additional options: Automate correlated event updates and closure based on SIR incident status

The ArcSight ESM integration has a bi-directional interface that allows for both correlation events to create security incidents, as well as an ability to update the correlation events once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, SIR incident URL, and so on.

Before you begin

Role required: sn_si.admin

Procedure

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.
2. Follow the instructions below to complete the configuration for updating correlated events when the security incident is created.

Option or Field	Description
Update Correlated Events upon SIR Incident Creation	Select this option if you want to update the correlation event stage in ArcSight ESM and update the event with additional comments when a security incident is created from the correlation event. This can occur for correlation events that could either create a new security incident, as well as aggregate existing security incidents. **Note:** If this option is not selected, the event stage will not be updated when the security incident is created.
Correlated Event Stage Update	Select a stage option from the Correlated Event Stage Update choice list that displays all available stages retrieved from the ArcSight ESM server.

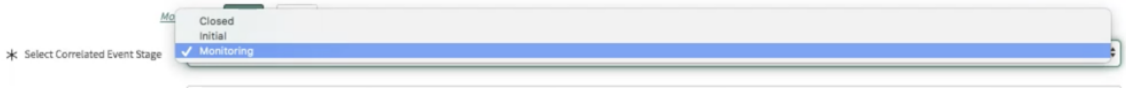
Correlated event stage not configured: If you have not configured any correlated event stages in your ServiceNow AI Platform instance, you will only see the **Assign Stage - Initial Setup** in the Correlated Event Stage Update choice list. To configure the stage, follow these steps:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Enter a resource ID in the Enter Stage Resource ID field and click **Submit**. The resource ID is validated in the ArcSight ESM console and the following screen is displayed.



- Click **Save** to save the new stage (**Monitoring**).
- Click the Select Correlated Event Stage drop down list.



- You can select the newly created stage from the list.

Correlated event stage already configured: If you have already configured the correlated event stage, follow these steps:

- Select **Use Previously Assigned Stage** in the Correlated Event Stage Update choice list.
- Select an existing stage from the Select Correlated Event Stage choice list as shown below.



- Initial Comments posted back to Correlated Event: In addition to updating the correlation event stage value, you can also post comments to the correlation stage annotations. As indicated in the instructions, you may edit the default text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response incident form.

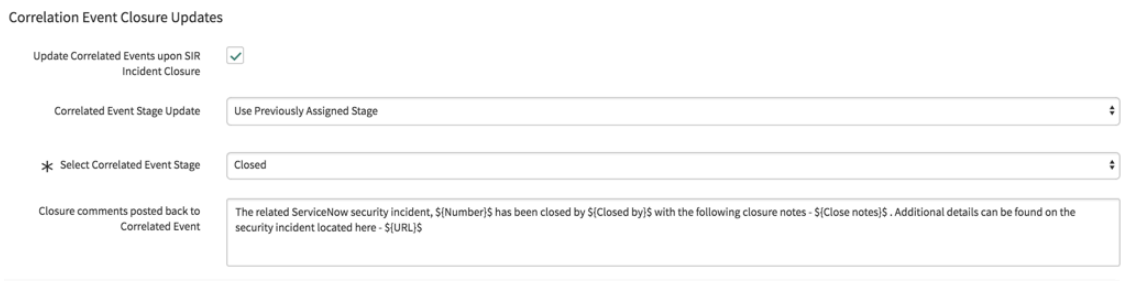
Note: You can either use the default stages defined in the ArcSight ESM console or create your own custom stages. To create a new stage, follow these steps:

- In the ArcSight ESM console, select **File** > **New** > **Stage**. The Inspect/Edit tab is displayed.
- Define the new stage and do not select the **User Required** check box. Ensure that the stage is defined correctly and is in the correct position in the event life cycle.

3. In the Automating Correlated Event Closure section, you can define how to update the security incident when it is closed.
4. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or Field	Description
Update Correlated Events upon SIR Incident Closure	Select this option if you want to update the correlation event status and add additional comments when a security incident is closed from the correlated event. This will occur for both the initial triggering notable events that create the security incident, as well as aggregated events. **Note:** If this option is not selected, the event stage will not be updated when the security incident is closed.
Correlated Event Stage Update	Select a stage option from the menu that displays all available stages retrieved from the ArcSight ESM server. Select the stage value to be set for all correlation events when a security incident is to be closed. **Note:** The stages displayed here are based on the stages configured in the Correlation Event Initial Updates section.
Select Correlated Event Stage	Select an appropriate status here.
Closure Comments Posted back to Correlated Event	In addition to updating the correlation event status value, you can also post closure comments to the correlation event annotations. As indicated in the instructions, you may edit the default text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response incident form.



5. Click **Finish** to complete the configuration.
   A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull correlation events from the ArcSight ESM console based on your scheduling.

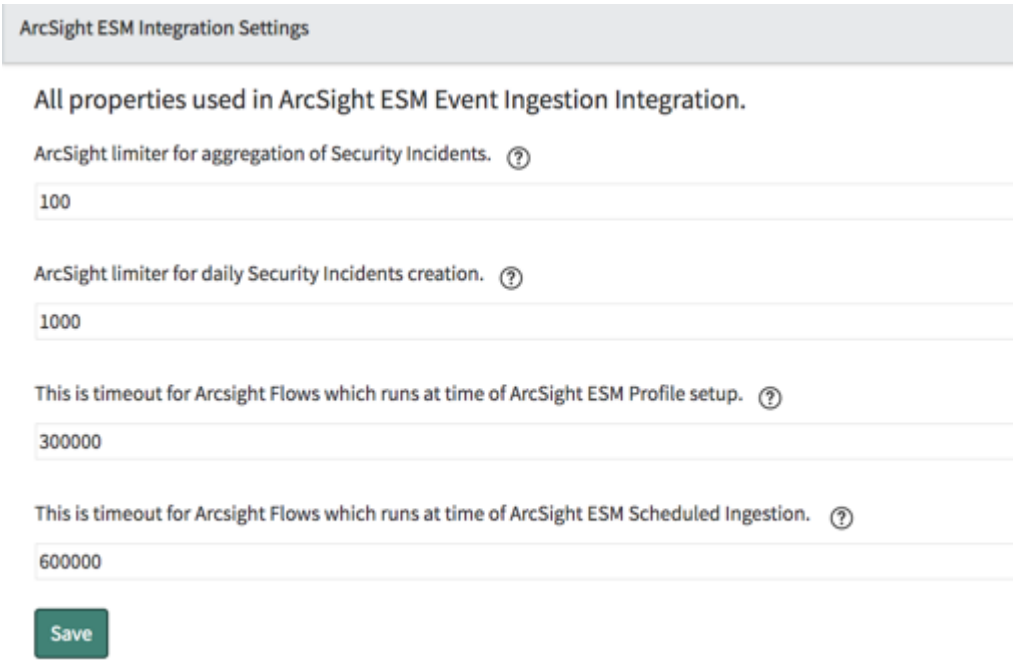
ArcSight ESM Integration Settings for event ingestion integration

Use this option to modify the ArcSight ESM default ingestion settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To modify the system properties, log in as a user with the *sn_si.admin* role and navigate to **ArcSight ESM Integration** > **ArcSight ESM Integration Settings**.

The default configuration settings are displayed. You can modify these settings if required.

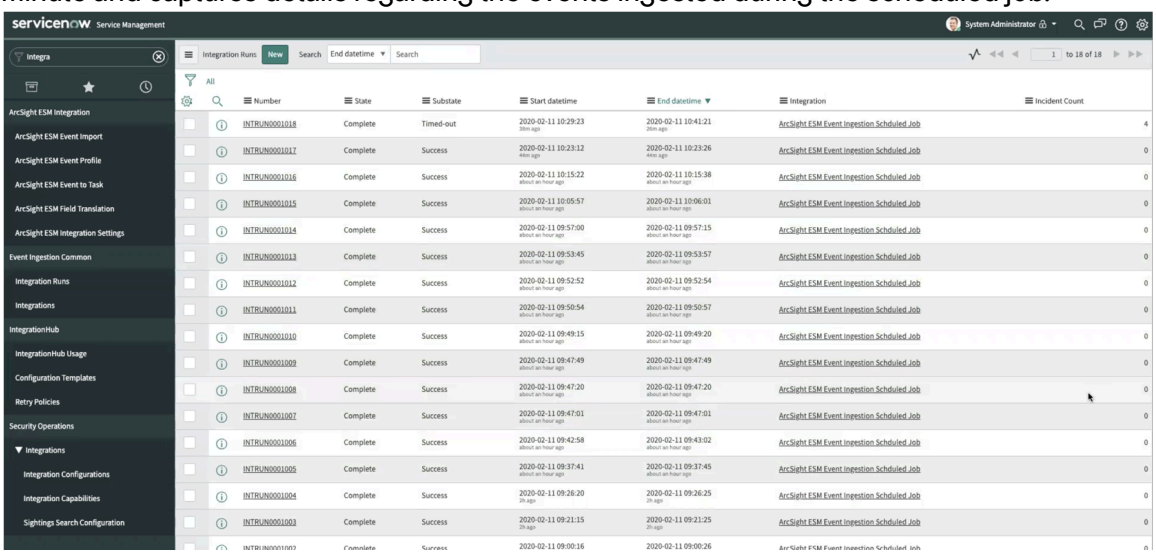


Troubleshooting ArcSight ESM event ingestion integration

This section provides information on how to troubleshoot any errors that may occur during event ingestion.

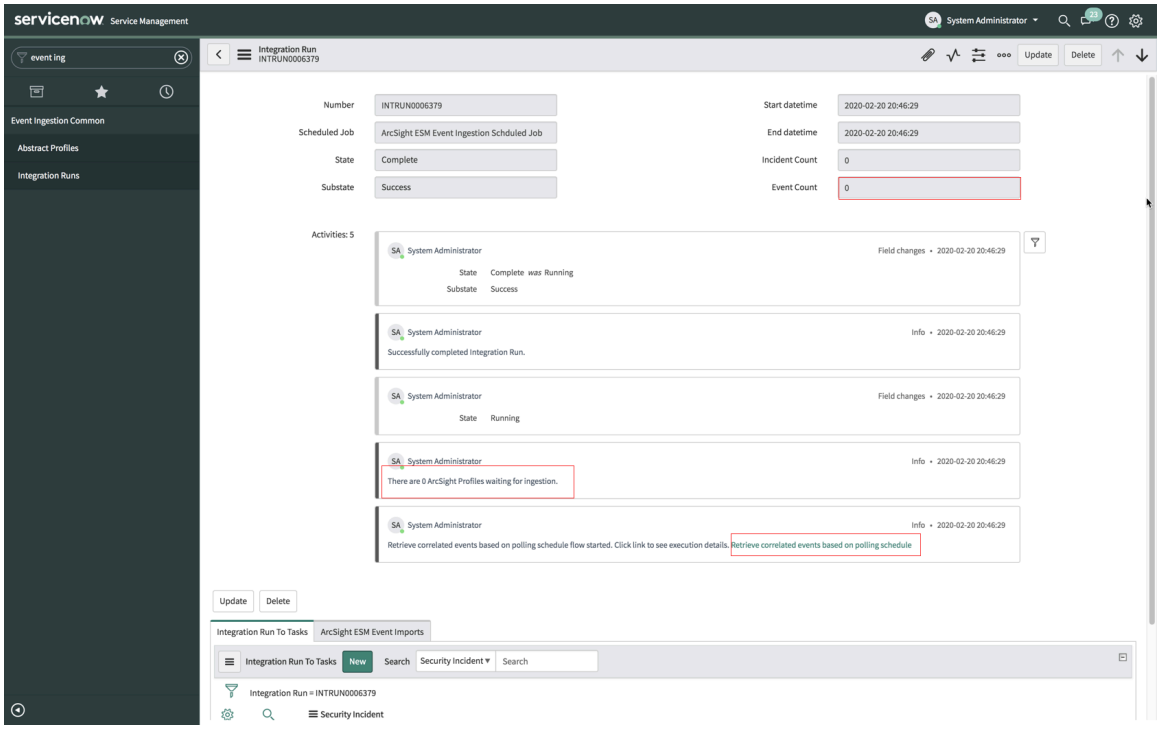
Integration runs

Navigate to **Event Ingestion Common** > **Integration Runs**. An integration run takes place every minute and captures details regarding the events ingested during the scheduled job.



You can see the list of integration runs and status of each run (Success, Timed-out, Waiting) and the number of security incidents that were created. Click on the Number link to drill down to the detailed Integration Run page.

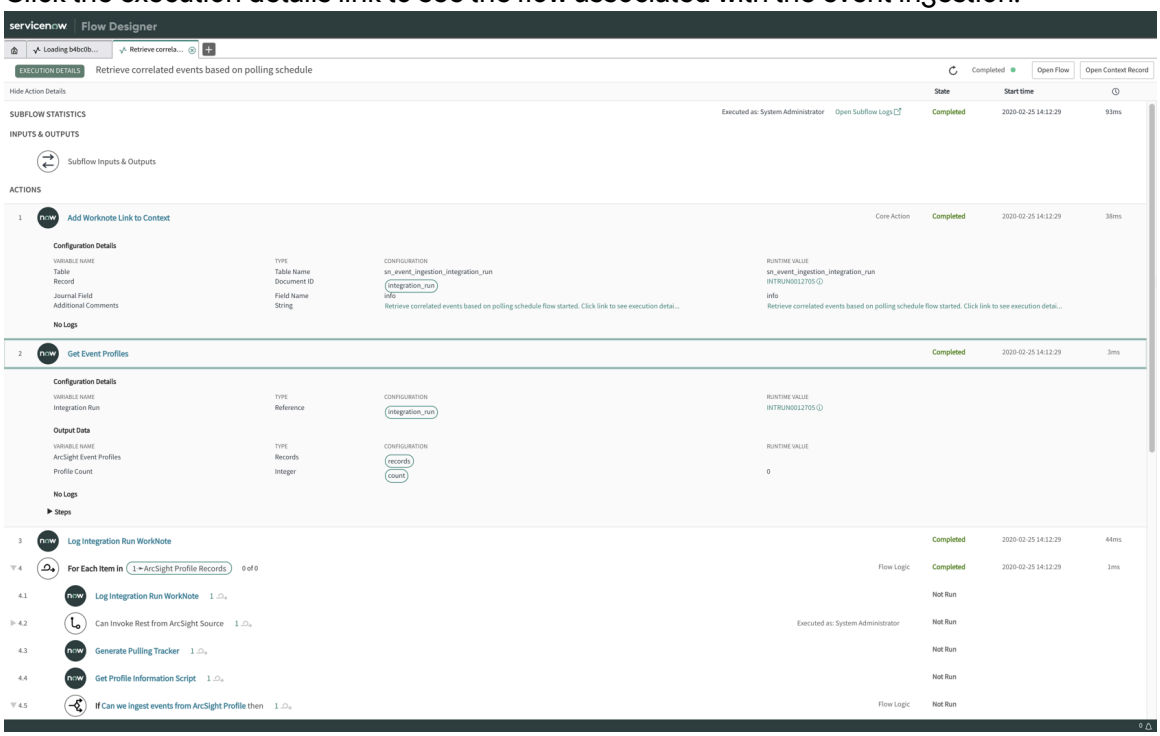
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can view details like the number of events that were ingested, the status, which event that was transformed into a security incident, and the different tasks there were performed during the ingestion. Additionally, you can click the link to view the flow execution details.

Flow execution details

Click the execution details link to see the flow associated with the event ingestion.



You can view a step by step execution of the flow detailing the various actions and subflows that were executed as part of the flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Copy ArcSight ESM profile for event ingestion integration

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

Before you begin

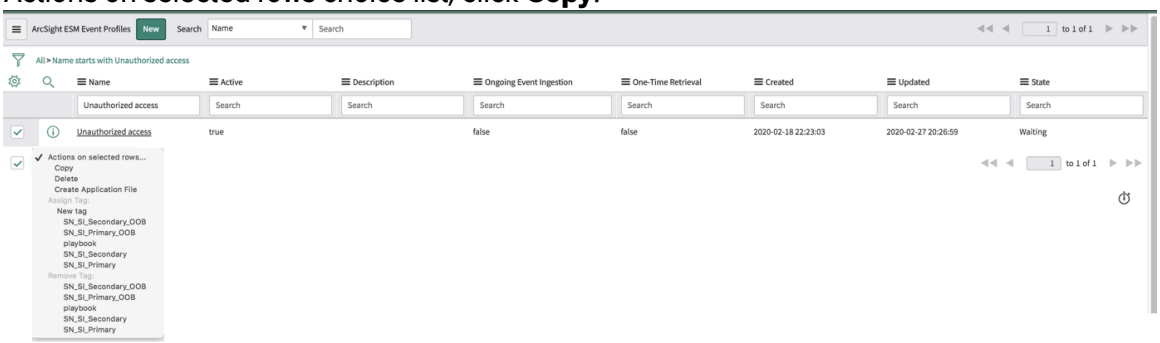
Role required: sn_si.admin

About this task

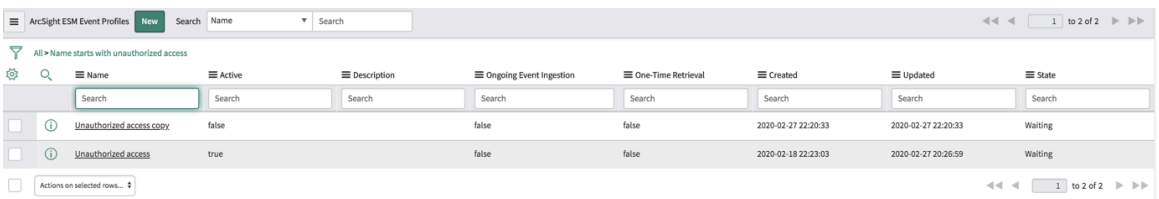
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure

1. Navigate to **All** > **ArcSight ESM Integration** > **ArcSight ESM Event Profile**.
2. In the ArcSight Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.



The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.



You have successfully copied the settings from an existing profile to a new profile. Note that the **Active** column status is set to false as the profile needs to be activated.

Use the script editor to format correlation event values for ArcSight ESM integration

In addition to the directly mapped fields from the ingested correlation event values, use the script editor to format field values on the security incident during the mapping step.

Before you begin

Role required: sn_si.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The script editor changes the values of a ArcSight ESM correlation event field so that values that are supported by the ServiceNow AI Platform SIR security incident are mapped to the Category, Configuration item (CI), Observable, and other security incident fields.

In certain cases, ArcSight ESM correlation event values are mapped to reference fields such as, Category, Configuration item (CI), and Observable fields on the security incident. As a user with the sn_si.admin role, you may prefer to edit the mapped event field values to translate format or data values to conform with incident field formats and values expected. If you want to translate the value of a ArcSight ESM correlation event to a value that is supported by these fields on the SIR security incident, use the script editor.

Procedure

1. With the mapping form displayed, click the link to open the script editor.
2. From the choice list, select a destination field for the value that you want to edit.
3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon [{ }] next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For a correlation event, for example, a value for the Configuration item may not be matched.

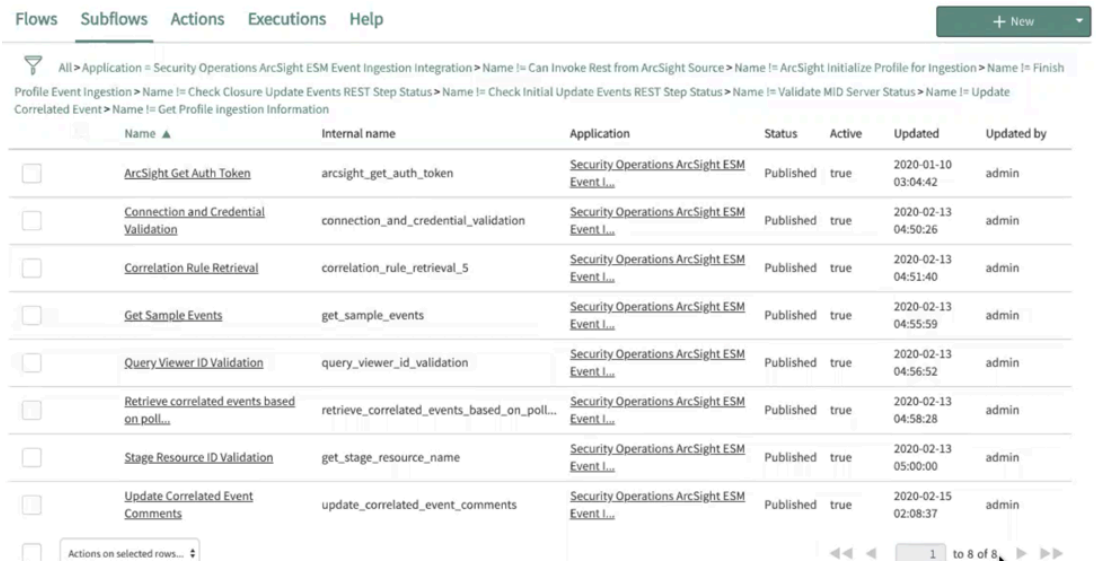
   As shown in the following figure, if a match for a host name cannot be found in the ServiceNow AI Platform CMDB for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field.

   The editor opens with the field displayed in Destination Field.
4. Enter any changes to then script, and click **Update** to save your changes.
   The ArcSight ESM Field Translations table is displayed.
5. Close the table to return to the Mapping form.

Flow Designer usage with ArcSight ESM event ingestion integration

Using the Integration Hub and Flow Designer, several flows, subflows, and actions are available with the ArcSight ESM integration.

To view these subflows, navigate to **Flow Designer** > **Designer** and click on the **SubFlows** tab. The figure below shows the important subflows used during profile creation and the scheduled ingestion job.

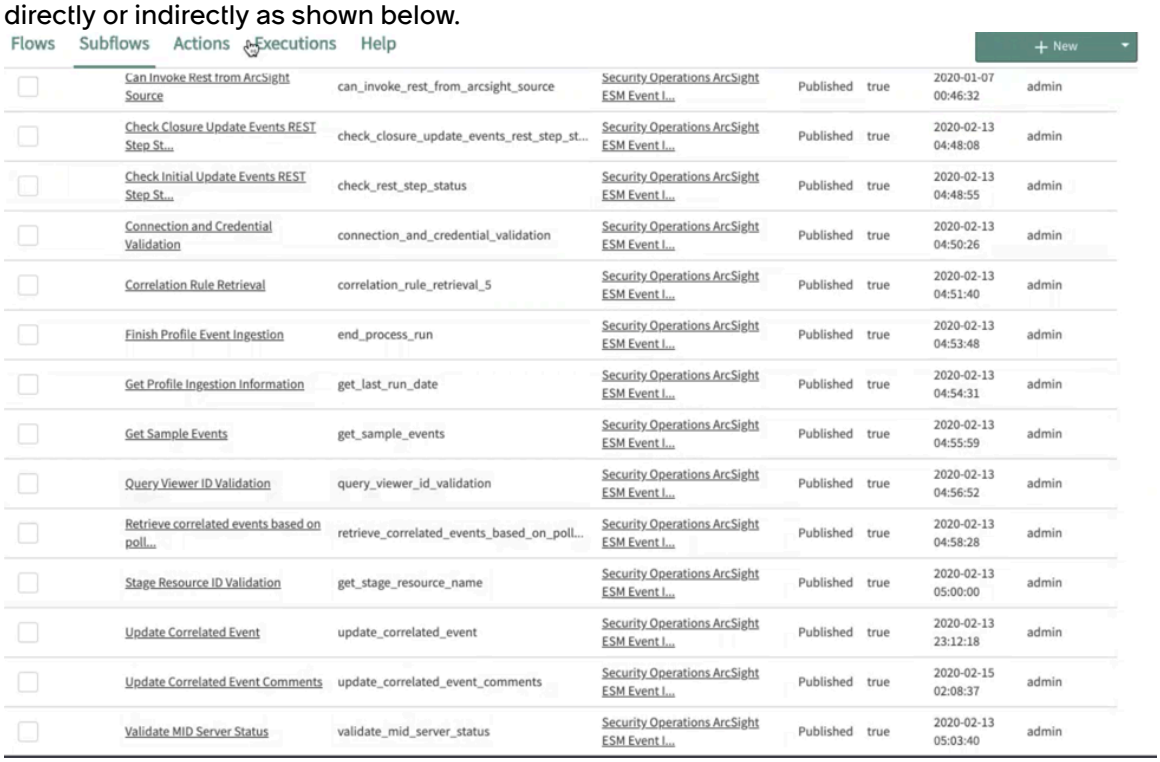


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These subflows are listed in the sequence in which they are executed below:

- **Connection and credential validation**: This subflow validates ServiceNow connectivity with the ArcSight ESM server and the specified credentials. This subflow is used when you click the **Configure** button in the **ArcSight ESM - Event Ingestion**tile in the **Security Operations** > **Integrations** > **Integrations Configuration** page.
- **ArcSight Get Auth Token**: This subflow generates the ArcSight ESM Authentication token from the Username and Password using the ArcSight ESM Login Service. The Login Service provides the authentication token that can be used to call any other ArcSight ESM endpoint. This subflow is used in all other subflows.
- **Query Viewer ID Validation**: This subflow verifies if the Query Viewer ID specified during profile creation is present in the ArcSight ESM server.
- **Correlation Rule Retrieval**: This subflow retrieves the correlation rules based on the Query Viewer ID.
- **Get Sample Event**: This subflow fetches the sample correlation events from the ArcSight ESM server. These sample events are then mapped to the security incident fields in the Mapping section of the profile.
- **Stage Resource ID Validation**: This subflow validates the specified Stage Resource ID in the ArcSight ESM console and fetches the Resource Name.
- **Update Correlated Event Comments**: This subflow updates the Correlated Event comments in the Initial and Closure of Incident sections in the Additional Options page of the profile.
- **Retrieve Correlated Events Based on Polling Schedule**: This subflow runs the scheduled job that fetches the correlated events based on the polling interval.

During execution, the above subflows also trigger several other subflows and actions either directly or indirectly as shown below.



Amazon Web Services (AWS) Security Hub integration

AWS Security Hub is a cloud security posture management (CSPM) service that provides automated and continuous security checks and best practice checks against your AWS resources.

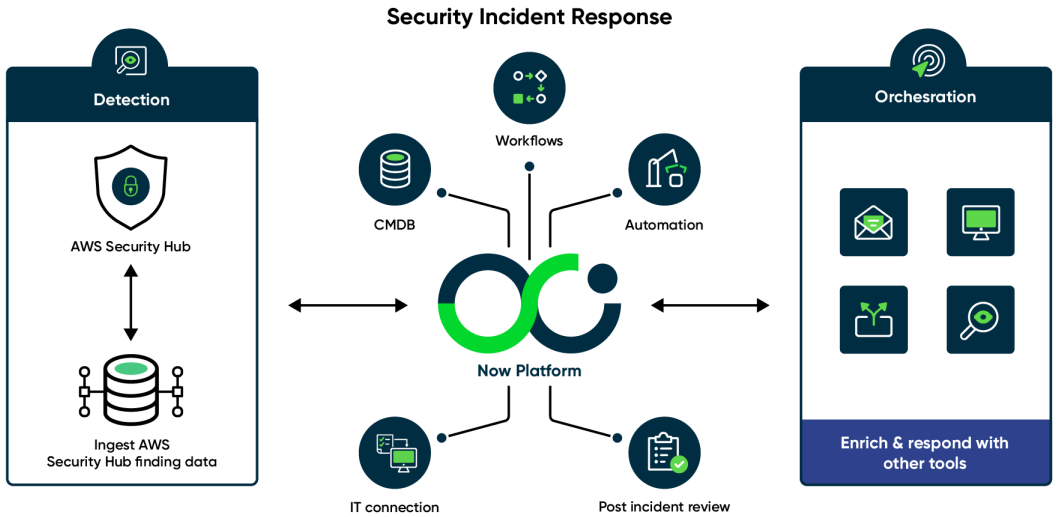
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview of the AWS Security Hub integration

AWS Security Hub enables you to identify issues in your configurations. Security Hub aggregates your security alerts, which are referred as findings. AWS Security Hub generates these findings in a standardized format and prioritizes them so that you can more easily enrich, investigate, and remediate them. You can use the AWS Security Hub integration to ingest Security Hub findings and automatically create security incidents in Security Incident Response.

AWS Security Hub integration in SIR follows a bidirectional architecture. SIR ingests Security Hub findings data to create a security incident and simultaneously updates a Security Hub finding with any updates in the corresponding security incident.

See the following diagram to learn how AWS Security Hub integrates with the ServiceNow AI Platform Security Operations applications.



Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Key features

Use the key features of this integration to do the following actions:

- Discover AWS Security Hub findings that are candidates for security incidents and automate the creation of these security incidents.
- Map AWS Security Hub findings and entity fields to SIR security incident fields.
- Filter AWS Security Hub findings.
- Aggregate findings to existing open security incidents so that you don't have to create duplicate security incidents.
- Automate AWS Security Hub findings status updates for Security Incident Response so that you can create and close security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: ServiceNow also updates the status of AWS Security Hub findings based on the creation, progress, or closure of the security incident. This update also includes comments of aggregated and new findings.

- Schedule findings ingestion to create security incidents periodically.
- Synchronize AWS Security Hub finding comments with SIR Work notes.

Learn about this integration

Document identifier	Document title
AWS Security Hub product documentation website	AWS Security Hub Documentation website
ServiceNow product documentation website	ServiceNow Product Documentation website

Get started with AWS Security Hub integration

Activate and set up the AWS Security Hub findings integration for Security Operation plug-in to interface with your ServiceNow® instance and Security Incident Response product.

Before you begin

Role required: sn_si.admin

Before you can use the AWS Security Hub integration, you must download it from the ServiceNow Store.

About this task

Review the following setup checklist and verify that you've completed all the tasks for a smooth integration.

Checklist

Assign and verify the required ServiceNow® platform and Security Incident Response roles.	The following roles are required for configuration and verification of the expected results:
	• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.admin role.
	• The sn_si.admin role performs the following tasks:
	  ○ Configures the integration.
	  ○ Creates incident profiles.
	  ○ Maps the AWS Security Hub finding data fields to the security incident fields.
	  ○ Schedules on-going incident ingestion.
	  ○ Enables incident updates when a Security Incident Response incident is created or closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Assign the AWS Security Hub required roles.	The following roles are required in AWS Security Hub to register and configure your application: • SecurityHubReadOnlyAccess • SecurityHubFullAccess
Review the AWS Security Hub integration settings	Navigate to **All** > **AWS Security Hub findings integration** > **AWS Security Hub Findings Integration Settings**. Review or modify the properties settings according to your requirement.
Configure your application in the AWS portal.	Register your application in the AWS portal and grant your users with read and write access to the application. Refer to the following topics for more information: • Setting Up AWS Config with the Console • Security Hub integrations.

Register and configure the AWS Security Hub portal

Register your application in the AWS Security Hub portal and grant your users with read and write access to the application.

Registering a ServiceNow® user profile on AWS portal

Before you begin

Role required: AWSSecurityHubFullAccess

Procedure

1. Log in to the AWS portal.
2. Navigate to **Identity and Access Management (IAM)** > **Users** > **Create New User**.
3. The following table describes the fields that you must configure to create a user profile:

Create a user profile

Field	Description
Specify user details > **User name**	Name for the user profile.
Set permissions > **Add user to group**	Add the user profile to a group with predefined permission policies. You can create a group according to your preference and assign permission policies to the group. Later, you can add user profiles to the group and the permission policies

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	assigned to the group is automatically assigned to the user profiles.
Copy permissions	Copy permissions from a user profile and assign the same to the new user profile.
Attach policies directly	Add AWSSecurityHubFullAccess as the permission policy for your user profile. Assign a new permission policy to the user profile according to your preference.
Review and create	Review all the details that you added in the user profile.

4. Select **Create user**.
5. Select **View user** from the displayed pop-up window.
6. Create an access key and a secret access key for the user profile.
   You require these keys to access the AWS Security Hub integration from your ServiceNow® instance.
7. Navigate to **AWS Services** > **Search** > **AWS Security Hub** > **.**
8. Select **Go to** *Security Hub*.
9. In the Enable AWS Security Hub page, select **Download** to enable AWS Config.
   Download the files and run them in your account. This grants you permission to gather all the information from various AWS reporting services and aggregate into AWS Security Hub.
10. Select **Enable** *AWS Security Hub*at the bottom of the page.
    It takes a few moments for the *AWS Security Hub* Dashboard to display all the details.
11. Change Region from **Global** to **US East (Ohio)**.
    The code for **US East (Ohio)** is **us-east-2**. All ServiceNow® resources are assigned to this region code.

Install and configure the AWS Security Hub integration

Install and configure the AWS Security Hub integration from the ServiceNow Store on your ServiceNow AI Platform instance to start ingesting AWS Security Hub findings.

Before you begin

Role required: sn_si.admin

Procedure

1. Download the AWS Security Hub integration from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the AWS Security Hub tile and click **Configure**.
4. On the form, fill in the fields.

AWS Security Hub Configuration form

Field	Description
Name	Name for the AWS Security Hub instance configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Region name	Region you assigned in the ServiceNow® user profile on AWS Security Hub portal.
Secret Key	Secret key you created for the ServiceNow® user profile on AWS Security Hub portal.
Access Key	Access key you created for the ServiceNow® user profile on AWS Security Hub portal.

5. Click **Submit**.

Result
After you successfully validate and submit the configuration, each Security Hub findings ingestion server configuration is saved on the Security Integrations page as a tile.

Create a profile for AWS Security Hub finding integration

Create an AWS Security Hub profile in your ServiceNow AI Platform instance which you are going to use to ingest data from AWS Security Hub and create a corresponding security incident in Security Incident Response Workspace.

Before you begin
Role required: admin

About this task
The integration enables you to create security incidents for different types of findings on the AWS Security Hub platform, such as unauthorized access attempts and malware. These incidents are created based on the profiles that you configure in the ServiceNow AI Platform instance. All incidents are initially created for a configured finding type in a profile. You can further filter the findings you have created to specify which findings create security incidents.

All findings that meet the selection criteria in your AWS Security Hub tenant, and are available over the AWS Security Hub API, are initially ingested into your ServiceNow AI Platform instance.

Procedure
1. Navigate to **All** > **AWS Security Hub Findings Integration** > **AWS Security Hub Findings Profile**.
2. Click **New**.
3. On the form, fill in the fields.

AWS Security Hub - Findings Ingestion Configuration form

Field	Description
Name	Name for the profile. This name helps you to identify the profile type and is also the default name for the security tag that is associated with this profile.
Active	Select to activate the profile. When the profile is active, it implies that the ServiceNow AI Platform actively ingests AWS

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Security Hub findings data and corresponding security incidents are created in SIR when the filtering conditions are matched.
Source	The AWS Security Hub Integration tenant that you have configured to ingest findings. If you have multiple tenants configured, select the appropriate tenant for the finding types that you are planning to ingest for the profile.
Order	Enter a value for this field which indicates the order that flows are executed when two or more profiles share triggering conditions. The flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400. The default is 100.
Description	Extra text to help you distinguish this profile from other profiles.

Map the AWS Security Hub finding fields

Map the individual AWS Security Hub finding fields to the fields on the SIR security incident so that you can create incidents with the mapped data.

Before you begin

Role required: sn_si.admin

Procedure

1. On the mapping page, in the AWS Security Hub Mapping section, select one of the Sample Ingestion Methods.

Sample Ingestion Methods

Field	Description
All default finding fields	Use this ingestion method to view the static list of all the findings fields. This method contains only default field names without any values. You can use this information to map with the SIR fields.
Retrieve Recent AWS Security Hub findings	Use this ingestion method to import the most recent findings data. You can ingest 5 sample findings by default and a maximum of 20 sample findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The sample finding field values populate when the profile ingests the sample findings. You can map these findings to the **SIR Incident Target Fields**. The finding fields and values appear as individual tabs.
Import Sample Data	Select **Import Sample Data** to import sample findings from AWS Security Hub. This button appears when you select the Retrieve Recent AWS Security Hub findings ingestion method. Retrieving sample findings from AWS Security Hub server takes some moments. Map these findings to the **SIR Incident Target Fields**. The finding fields and values appear as individual tabs.

2. To add fields to the default fields that are displayed on the security incident, do the following actions:

   On the SIR Incident Target Fields section, select the ⊕ Map another field button. It shows a list of SIR fields, from which you can select to display a new field.

   a. In the Security Incident column, expand the list that is displayed and then select a field.

      Note: Multiple observables can be displayed on the same security incident. For example, the **Observable** field can be mapped multiple times with different values. Similarly, the **Configuration Item** and **Work notes fields** support multiple values. If you try to map two values to a field that can't support multiple values, you see an error message that this field doesn't support multiple values. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field doesn't populate on the security incident.

   b. From the AWS Security Hub Source Fields section, drag your field to map it to your new field.

   c. When you select the check box that corresponds to a field, any new or updated changes made in AWS Security Hub are automatically updated in the respective SIR with new incident data.

      Note: In the base system, the system property sn_sec_security.finding_updates is by default set to True to receive the AWS Security Hub updates related to new alerts that are linked to SIR.

      - By default, the Affected Users, Configuration items, and Observables fields are checked. This means that whenever there are new observables or associated configuration items, or affected users that get added to the incident then that information is automatically

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

extracted and populated in the respective related lists in the Security Incident Response (SIR) during that polling interval.

- For any other fields, you must select the check box that corresponds to a field for any new or updated changes made in the finding in AWS Security Hub. This automatically updates the respective SIR incident data with the new incident data.

> **Important:** Due diligence is required to be done before selecting this functionality as overriding the existing data may result in unstable data for the analyst to work with and any other automation that is set even by the field values of security incident may also get affected. So, it is important to do the due diligence before you select any override functionality.

3. To remove a field, use the ⊖, (**Remove item**) button next to the input expression field in the SIR Incident Target Fields section.
4. To map a field value from the AWS Security Hub Source Fields section to a field on the SIR Incident Target Fields section, use one of the following actions:

   a. Drag the field name (for example, id) and drop it next to a field name in the SIR Incident Target Fields column.

   You can match any value from the AWS Security Hub Source Fields section to a field on the SIR Incident Target Fields section. Fields are color-coded so that you don't overlook or duplicate finding fields in the mapping process. Light blue fields indicate that a finding field isn't yet selected and mapped on the security incident. You may prefer to associate an incoming finding field with more than one field on a security incident. A gray field indicates that a finding field has been selected and mapped to a field on the security incident. This way, you can visualize which field values have been added to the security incident and if any remaining important finding information remains unmapped. However, there are some fields in the AWS Security Hub Source Fields section that aren't compatible with fields on the SIR Incident Target Fields section. If you map such values, it isn't displayed when the SIR is created.

   b. You can add a combination of text and field.
   For example, `Finding name is ${name}$`. Here, `Finding name is` can be manually entered while `${name}$` is mapped from the AWS Security Hub Source Fields section.

   c. You can manually enter and map a source finding field to a target field.
   Use the ${field name}$ format to manually map a source finding field. For example, to map a finding field Severity, the format is`${properties(severity)}$`.

   This integration classifies certain observable sub-types. When you map an AWS Security Hub finding field with the SIR observable field, the ServiceNow AI Platform auto-classifies the observable. If you want to generically map the incoming AWS Security Hub observable to the observable type in SIR, then drag and drop the AWS Security Hub field in the Observable field. However, if you are aware of the observable type for the incoming AWS Security Hub observable in SIR, then map specifically to the SIR Observable type field. Some examples of specific observable types in SIR include Observable(Domain name), Observable(Email address), Observable(IP address (V4)), and Observable(Host name).

   Sometimes, finding field values in AWS Security Hub may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. To format a field translation for a new field from an AWS Security Hub finding to match a field value on a Security Incident, click the **Click here** link in the **SIR Incident Target Fields** header.

6. To modify the fields which support field translation, click the  script format field translation icon.
   The fields that support field translation are **Category**, **Configuration Item**, and **Priority**.

   For example, click on  icon next to the Category. The AWS Security Hub findings Field Translation script editor opens.

7. Enter any changes to the script and click **Update** to save the changes and return to the Mapping page.
   For example, for Category define the following in the script editor:

   ```
   "<Incoming Security Hub finding Field Value>" : "<Category to
    assign to the Security Incident>".
   ```

   This mapping ensures that a profile uses only configured categories.

8. Continue your mapping by adding or removing field values.
   You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming finding must satisfy to create a security incident.

9. To move to the Filtering and Aggregation section, click **Continue**.

What to do next

Define and set filter conditions so that you can specify which findings create security incidents. You can use the same field values (defined in the Mapping section) in the Incident Generation Conditions builder (in the Filtering and Aggregation section) to define additional criteria that an incoming finding must satisfy to create a security incident.

Define filter and aggregation criteria for AWS Security Hub findings ingestion

You can define and set filter conditions so that you can specify which incoming findings should create security incidents. You can also define additional incident field criteria that allows an incoming finding to be appended to an open security incident instead of creating an another security incident for the same finding.

Set the filtering conditions for AWS Security Hub findings to create security incidents

Set the filtering conditions so that security incidents are created only when the filtering conditions match.

Before you begin

Role required: sn_si.admin

About this task

This type of filtering helps you to isolate security incidents and limits the number of security incidents that you create. If you set additional filtering criteria, only the required findings are ingested without having to change the query or the triggered incident configuration.

Perform the following steps to define the criteria that an incoming AWS Security Hub finding must satisfy so that a security incident is created:

Procedure

1. Select **Apply Pre-Filter** in the Pre-Filtering section.

   You can use this option to filter specific findings and reduce the load of findings ingestion.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the **API Filter** field, enter a JSON condition as per your requirement that filters out specific findings based on the condition. For example, enter the following value to filter out findings that have Workflow Status as Resolved in Security Hub:

```
{"Filters"{
  "WorkflowStatus":[{
  "Comparison":"NOT_EQUALS",
  "Value": "RESOLVED"}]
 }
}
```

Based on the provided condition, AWS Security Hub findings are ingested and displayed in the AWS Security Hub findings raw table.

Navigate to **All** > **AWS Security Hub Findings Integration** > **AWS Security Hub findings raw** to view the raw findings data.

2. In the Select Finding fields for filter conditions section, select **Display available finding fields** to display a list of all available fields in a AWS Security Hub finding.
From **All finding fields** list, select the finding fields which you want to be displayed in the Security incident generation conditions section.

   Note: An AWS Security Hub finding contains multiple fields and values. In the **All finding fields** list, you can search for a finding field as per your requirement and select it.

3. In the Security incident generation conditions section, select **Filter based on conditions** to define the criteria that an incoming AWS Security Hub finding must satisfy so that a security incident is created.

   The first field in the Filter Conditions contains a default list of two hundred fields that are available on a AWS Security Hub finding and the finding fields you selected in the Select Finding fields for filter conditions section.

   The second field in the Filter Conditions contain conditional operators. The option you choose determines the condition that must be fulfilled to ingest a finding.

   The third field in the Filter Conditions contain values supported by the available finding fields. Verify that the finding field that you enter matches the values of the findings.

   For example, use the filter condition *contains* for the following fields with multiple values:

   - Workflow(Status)
   - WorkflowState

4. Using the lists and fields of the conditions builder, set the filters for the first row.
5. To add more conditions, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
6. To set a second filter condition, click **New Criteria**.

Result

Based on the filtering conditions, AWS Security Hub findings are imported to SIR. Navigate to **All** > **AWS Security Hub Findings Integration** > **AWS Security Hub findings import** to view the imported findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define conditions to aggregate AWS Security Hub findings to a security incident

Define additional incident aggregation criteria that aggregates an incoming AWS Security Hub finding to an existing SIR security incident instead of creating similar, potentially duplicate incidents. When you use field matching value criteria for each profile, this additional aggregation can reduce the number of active, overlapping security incidents by placing all related incidents data on a single security incident.

Before you begin

Role required: sn_si.admin

About this task

If a new incident matches all the values that are selected in the aggregation field conditions in the mapping step, the incident is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate incidents on a related list on a security incident. All the aggregated AWS Security Hub findings on a security incident are displayed on the AWS Security Hub related list. This list details the associated timestamps and aggregated field values. This information helps you understand why AWS Security Hub findings are added to the existing security incidents.

Procedure

1. To define additional incident field criteria that allows an incoming AWS Security Hub finding to be appended to an open security incident instead of creating a new incident, select the **Aggregation Conditions** option.
2. In the **Incident fields with matching values** field, enter the field values that you want to match on existing security incidents in your ServiceNow AI Platform instance.
   All field values that you selected in the multi-selection input field must match so that the aggregation criteria is met and that this incoming incident can be appended to an existing security incident. This selection implies it is an *AND* condition where fields, such as Observables and Configuration Items that may have multiple field values, are mapped to them. If only a subset of the values is matched, the AWS Security Hub findings aggregation conditions are not met and a new security incident is created.
3. To add multiple field matching conditions, click **Add New Criteria**.
   The aggregation occurs if any one of the multi-selection field conditions that you define are met. This selection implies the *OR* condition.
4. To update the work note for a new finding when it is added to a security incident, select **Log work note for new finding**.

   The work note logs that a new finding is added and includes a link to the finding details. The log work note also updates more details that you add to the work note field in your mapping section.
5. To configure the schedule, click **Continue**.

Result

Based on the aggregation conditions, AWS Security Hub findings are are aggregated to create to create a SIR incident. Navigate to **All** > **AWS Security Hub Findings Integration** > **AWS Security Hub findings to task** to view the list of security incidents that have been created.

What to do next

Set a schedule to retrieve the finding data and finding incidents that match the criteria in the profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Schedule the AWS Security Hub finding retrieval

Set a schedule to retrieve the finding data and to ingest the AWS Security Hub findings that match the criteria in the profile.

Before you begin

Role required: sn_sni.admin

About this task

You can plan how often you want to poll for future AWS Security Hub findings that match the AWS Security Hub finding profile configuration.

The polling interval is configured for each profile individually. The different polling intervals may impact the performance of the AWS Security Hub findings integration. When scheduling, plan to balance the system load against the urgency of an incident. A one-minute default value is set for all profiles. You can modify this setting based on the urgency of the incident and the anticipated load on your system.

Any alerts that gets added to the incident in a particular polling interval is processed and then appended to the AWS Security Hub alerts related lists and comments.

Procedure

1. On the scheduling form, fill in the fields.

   Configure the schedule to define how and when you pull findings from the AWS Security Hub tenant.

   Scheduling form

Field	Description
Ongoing finding ingestion	Ongoing finding ingestion that the ServiceNow AI Platform instance pulls from the AWS Security Hub tenant for new incidents. Security incidents are created if triggered findings are found and the security incident generation filtering criteria matches.
Poll closed findings	Polling findings that have been resolved. These findings are ingested during ongoing incident ingestion.
Polling increment (minutes)	Polling frequency that is defined in minutes.
Set Initial finding ingestion time	Findings ingestion that is based on the configured date and time. You can use this option to define a specific date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.
Input Initial finding ingestion time	Date and time that you specify for the incident ingestion.
One-Time Retrieval	Select this checkbox to allow one-time retrieval of historical AWS Security Hub findings and then do the reconciliation of the data. When you select this checkbox, the application will pull all the open and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	closed AWS Security Hub findings for the period up to 90 days approximately. When processing the data both ongoing findings and historical data are pulled, but the processing of the ongoing findings takes precedence over historical pull. Otherwise, the historical pull may take some time based on the duration as well as the number of findings that are ingested. **Note:** The retrieved historical AWS Security Hub findings undergo de-duplication checks to prevent any duplicates within the Security Incident Response application.
Since date	The date since when the historical findings are ingested from AWS Security Hub. **Note:** The findings data is approximately pulled from the past 90 days.

The scheduling page enables you to define how and when findings are pulled from the AWS Security Hub tenant.

2. To navigate to the Additional Options page, click **Continue**.

Automate the AWS Security Hub finding updates and closures by the SIR incident status

Automate the updates and closures of findings on AWS Security Hub according to the SIR incident status. The AWS Security Hub integration has a bi-directional interface that enables findings ingestion to create security incidents and to update the findings' status according to the changes in the SIR incident.

Before you begin

Role required: sn_si.admin

Procedure

1. On the form, fill in the details.
   Follow the instructions to complete the configuration for updating AWS Security Hub findings when you create or close a security incident in SIR.

Automating Incident Updates form

Category	Field	Description
Update State	SIR Incident State	Displays a list of SIR incident states. Select an option from this list to map it to a Security Hub Finding State.
	Security Hub Finding State	Displays a list of Security Hub workflow statuses. The workflow status of a finding is updated on AWS Security Hub when

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Category	Field	Description
		the corresponding SIR state incident state changes.
Update Priority	SIR Incident Priority	Displays a list of SIR incident priority levels. Select an option from this list to map it to a Security Hub finding priority level.
	Security Hub Finding Priority	Select an option from the list of Security Hub severity levels. The severity of a finding is updated on AWS Security Hub when the corresponding security incident priority changes.
Update Work Notes	Select this option to update the notes section of aSecurity Hub when a work note is updated for the correspondingSIR incident. The work notes section on SIR has a limit of 512 characters as the notes section of a Security Hub finding supports the same.	
Update Additional Comments	Select to update the AWS Security Hub finding comments section with the additional comments you provided in SIR incident.	
Update Resolution Notes	Select to update the AWS Security Hub closing comments section with the resolution notes you provided when the SIR incident is resolved.	

Note: Each update from the work notes overrides the last update in the notes section of a Security Hub finding. We recommend you to add relevant work notes in a SIR incident.

2. Select **Finish**.

What to do next

The profile moves to the Waiting state. When the confirmation message shows that the setup and configuration is complete, you can activate the profile.

SIR form after an AWS Security Hub finding ingestion

After the ServiceNow AI Platform ingests the AWS Security Hub finding, a security incident is created and the updates are made to that security incident record.

Work notes

A work note is posted when an incident is aggregated and if you have configured the **Log work note for new finding** option in the Define filter and aggregation criteria for AWS Security Hub findings ingestion.

You can also view the internal finding import record that contains the raw incident data.

When you click the **Click here** link, you can view the record in the AWS Security Hub environment. The following example shows the record in the AWS Security Hub environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Aggregated AWS Security Hub findings

View Aggregated AWS Security Hub findings: View the incidents that are aggregated to the security incident. Navigate to **Show All Related Lists** > **Aggregated AWS Security Hub findings**.

Create security incident: Select an incident from the list, click the **Actions** menu, and then click **Create security incident**. This option creates a new security incident for the incident and this incident is de-aggregated from the parent security incident.

Carbon Black - Incident Enrichment integration

Use the Carbon Black integration to investigate and respond to security incidents using APIs to query and interact with endpoints associated with security incidents.

Find Carbon Black- Incident Enrichment integration resources

- Get started with the Carbon Black - Incident Enrichment integration
- Security Operations Carbon Black Integration - Get Running Processes Flow
- Security Operations Carbon Black Integration - Isolate Host Flow
- Security Operations Carbon Black Integration- Remove Host Isolation Flow

Understand integration concepts

- Types of ServiceNow integrations provided
- Security Operations workflow triggers

Get help from ServiceNow resources

- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support
- Upgrade to Madrid

Get started with the Carbon Black - Incident Enrichment integration

The Carbon Black incident enrichment facilitates the investigation of a security incident by querying logs for potentially malicious indicators. Before you can use the Carbon Black - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate Endpoint Base URL and MID server.

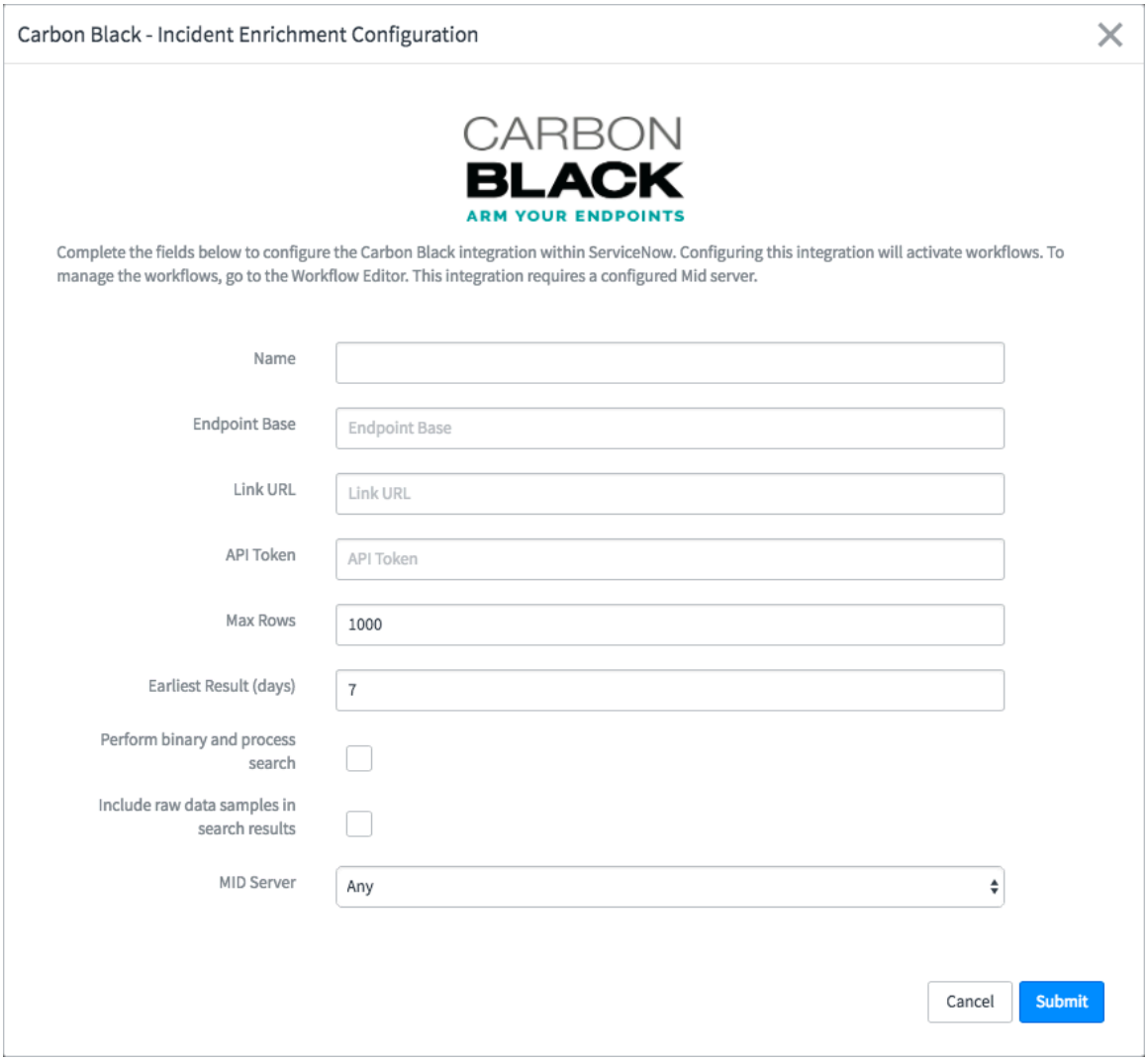
Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the download is complete, access the Carbon Black website and obtain the Endpoint Base URL and API Token under your profile.
3. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configuration**.
4. In the Carbon Black - Incident Enrichment card, click **Configure**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.
Endpoint Base	The endpoint URL you acquired from the Carbon Black site.
Link URL	The Link URL that links to a Carbon Black instance, when available.
API Token	The API token you acquired from the Carbon Black site.
Max Rows	The maximum number of rows you want to search. The default is 1000 rows.
Earliest Result (days)	The earliest results you want to see in number of days.
Perform binary and process search	Select this to perform binary searches to find binary files such as file hashes, and process searches for .exe processes that may have run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.
7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Carbon Black integration

The Carbon Black integration enables you to investigate and respond to security incidents using APIs to query and interact with endpoints associated with security incidents.

Explore

- Security Incident Response integrations
- Carbon Black - Incident Enrichment integration

Set up

Get started with the Carbon Black integration

Use

- Security Operations workflow triggers
- View affected items for a security incident
- Security Operations - Get Running Processes Flow
- Security Operations Carbon Black Integration - Get Running Processes Flow
- View affected items for a security incident
- Run Block Request
- Security Operations Integration - Block Request Flow
- Run Isolate Host
- Security Operations Carbon Black Integration - Isolate Host Flow
- Security Operations Carbon Black Integration- Remove Host Isolation Flow

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Get started with the Carbon Black integration

Carbon Black is an advanced security system easily integrating with Security Operations . Before you can use the Carbon Black integration, you must download the integration from the ServiceNow Store and add the appropriate Endpoint Base and API Token.

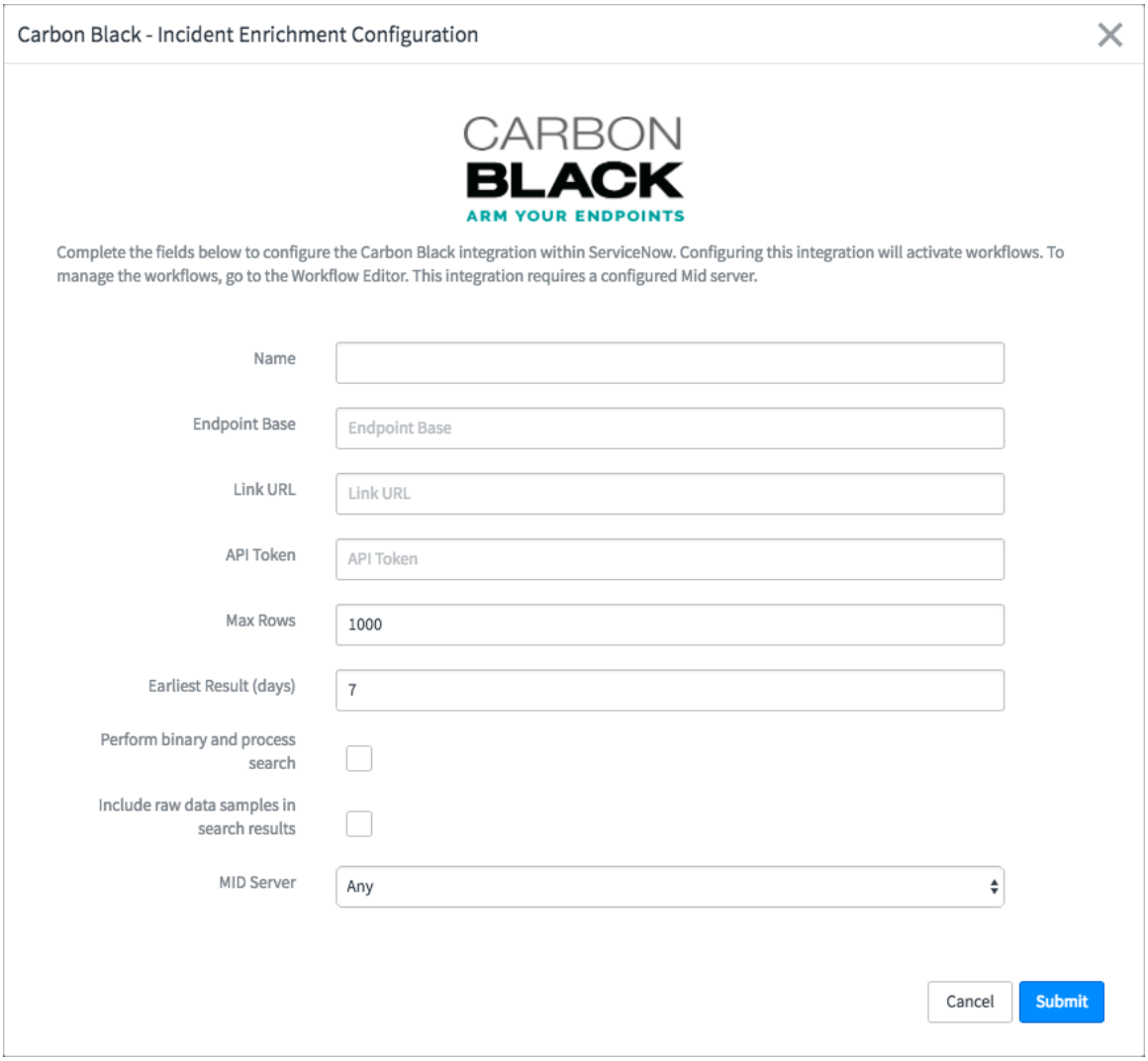
Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access the Carbon Black website and obtain the Endpoint Base URL and API Token under your profile.
3. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configurations**. The available security integrations appear as a series of cards.
4. In the Carbon Black card, click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.
Endpoint Base	The endpoint base you acquired from the Carbon Black site.
API Token	The API token you acquired from the Carbon Black site.
Use MID Server	Select this check box if it is not already checked.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.
Enable Isolate Host	Select this check box to allow selected configuration items to be isolated from the **Configuration Items** related list tab in a security incident.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Submit**.
   The integration configuration card displays.
7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Check Point Anti-bot - Email Parser integration

Check Point Anti-bot - Email Parser integration is supported using an email parser that consumes email notifications from Check Point Anti-bot to create security incidents and drive enrichment and response workflows.

Configure the Check Point Anti-bot - Email Parser integration

The Check Point Anti-bot - Email Parser integration uses email notifications to drive enrichment, and response workflows.

Before you begin

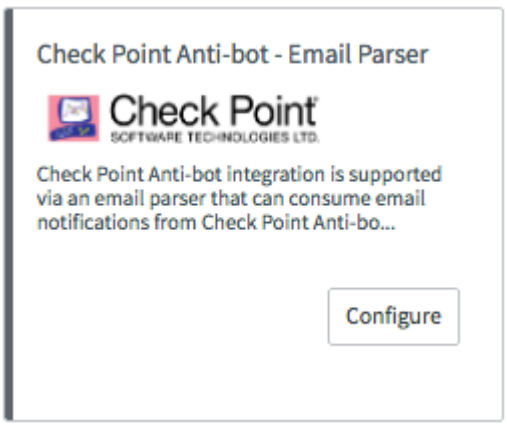
Role required: sn_si_admin

About this task

A Check Point Anti-bot email parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.

Procedure

1. Navigate to **All** > **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.



2. In the Check Point Anti-bot - Email Parser card, click **Configure**.
3. In the **Check Point Anti-bot - Email Parser Configuration** dialog box, click the **Configure Email Parser** link.
4. Click the **Check Point Anti-bot** link to edit the settings in the template email parser provided. At a minimum, fill in the `Email is from` field. To create an email parser, see Create email parsers in Security Operations.
5. Check the **Active** box.
6. Click **Update** in the **Email Parser** form.
   The email parser is active. You do not need to return to **Integration Configurations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Check Point Next Generation Threat Prevention integration

This document describes the steps required to integrate Check Point Next Generation Threat Prevention (NGTP) capabilities with ServiceNow® Security Incident Response (SIR) so that applications function properly together.

Once installed and configured, the security incident analyst uses this integration to block malicious IP addresses, URLs, and Domains using Block Request List capabilities with the ServiceNow Security Incident Response (SIR) products. This Block Request List is configured on Check Point Gateways as a Custom Intelligence Feed. The Custom Intelligence Feeds feature provides an ability to add custom cyber intelligence feeds into the Next Generation Threat Prevention engine. It allows fetching feeds from a third-party server, in this case the ServiceNow Security Incident Response application, directly to the Check Point Next Generation Gateway to be enforced by Anti-Virus and Anti-Bot blades. The security incident response analyst creates entries for Check Point Block List from observables determined to be malicious on ServiceNow SIR security incidents.

For most implementations, a Block Request List is a csv file that is hosted on an external web server. For this integration, this web server is your ServiceNow AI Platform instance, which permits the Check Point next-generation Threat Prevention Engine to fetch the list of IP Addresses, URLs and Domains to be blocked.

To enforce the blocking observables on Check Point Gateway, ensure that Threat Prevention Policy is configured with Anti-Bot and Anti-Virus Blades activated. As the Block List entries are modified, the Threat Prevention Engine dynamically imports the list at the configured interval and enforces policy without a configuration change or a commit on the firewall. For this integration, ServiceNow AI Platform has created a table containing Block List entries that are retrieved by authorized Check Point next-generation Gateway at the configured retrieval intervals.

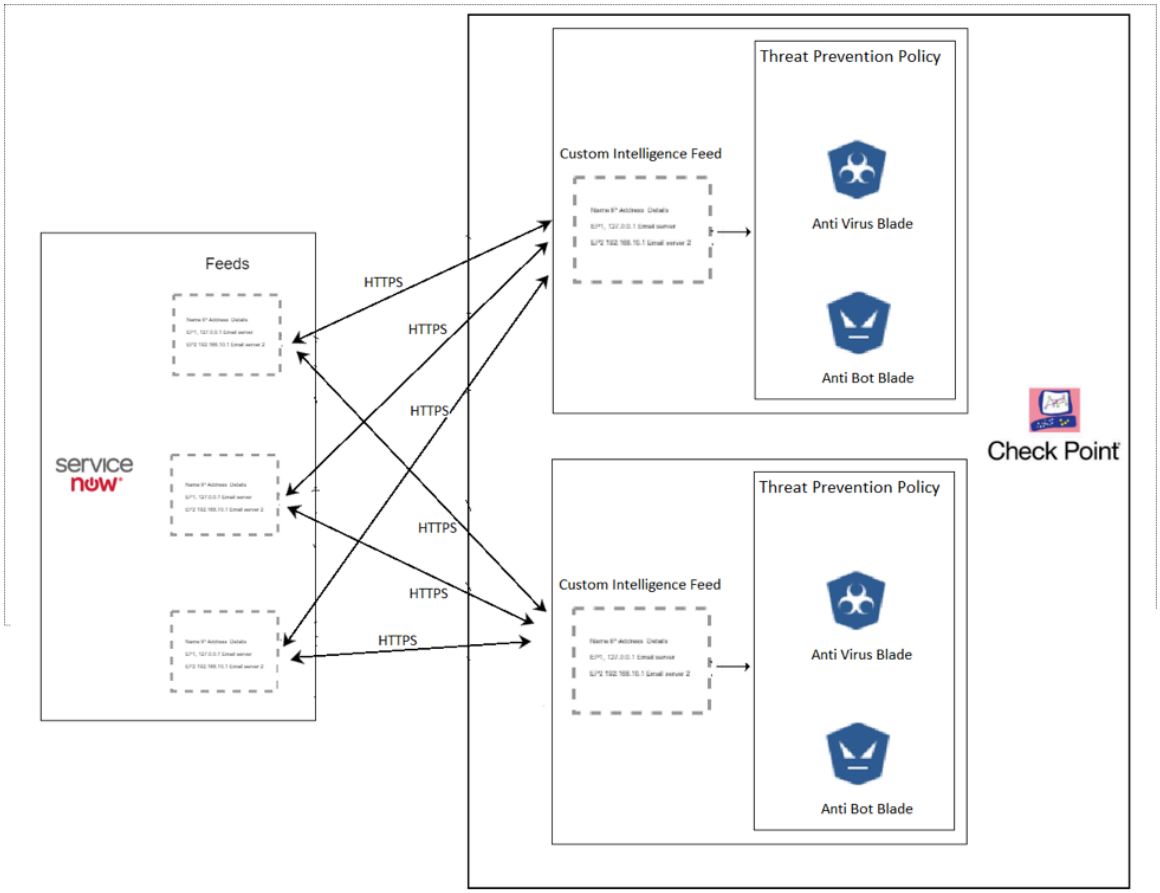
The integration includes the following features:

- Flexibility to create multiple Block Lists that apply to multiple Check Point Gateways.
- Detailed reporting on the types of sites being blocked (phishing, malware, and allow listed sites).
- Tagging of ServiceNow AI Platform security incidents with Block List entries by the observable type (URL, domain, IP address).
- Configuring Block List expiration periods to maintain Block List size by automatically expiring or removing older entries.
- Searching Block List entries between different Block Lists.
- Linking Block List entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

Integration architecture diagram

Below is the high-level architecture diagram depicting the components involved and integration points between ServiceNow AI Platform and Check Point Systems.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: The Check Point Systems logo, Anti-Virus Blade image, and Anti Bot Blade image are from Check Point Systems ©. They are the Property of Check Point Systems.

Plugins

The integration requires that the Security Incident Response (com.snc.security_incident) plugin be activated.

To install Security Incident Response plugins:

1. Log in to your instance with your HI credentials.
2. Verify you have the administrator (admin) role.
3. Navigate to System Definition>plugins in your instance.
4. Select and click Security Incident Response.

Once these plugins have been installed, you are able to upload the new Check Point integration plugin from the ServiceNow store and follow the following configuration instructions.

Supported Check Point OS versions

This integration requires the Custom Intelligence Feed of Check Point and Anti-Bot and Anti-Virus blades. These are supported from R80.20 and higher. Install the hot fix of Custom Intelligence Feature known as Check Point R80.10 Jumbo HF take 121 and above. Refer to the Check Point Custom Intelligence Feed Documentation's Installation section for more information on product compatibility matrix.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After installing the hot fix, ensure that below commands are accessible on Check Point Gateway. SSH to the Gateway and login to expert mode.

```
gw-93440b> expert
Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Supported ServiceNow versions

San Diego release version or later is supported.

References

Below are some of the Check Point references which are useful in setting up the Pre-requisites.

1. Custom Intelligence Feeds Feature - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. To set up Anti-Bot and Anti-Virus blades refer the Check Point User Guide. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. To set up HTTPS Inspection on Check Point follow the link below. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Permissions and roles

The following ServiceNow roles are required.

- Administrator (admin) for installation of the integration application plugin
- Security incident administrator (sn_si.admin) for creating Block Lists in ServiceNow and approving requests for adding and deactivating Blocklist Entries.
- Security analyst (also referred to here as a SOC Analyst, sn_si.analyst) for creating and maintaining Block List Entry records.

For more information on assigning the security analyst role, on the ServiceNow documentation website, navigate to Security operations>Security Incident Response> Assigning security analysts.

Check Point NGTP setup

Before you can use the Check Point NGTP integration, you must create an API account, set up policies, and activate the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create an API account for the Check Point NGTP integration

An API account role is required in your ServiceNow AI Platform instance for this integration. The Username and Password associated with this account are created in the ServiceNow AI Platform and entered in Check Point, so the Check Point authenticates with the ServiceNow AI Platform when retrieving Block List entries.

Before you begin

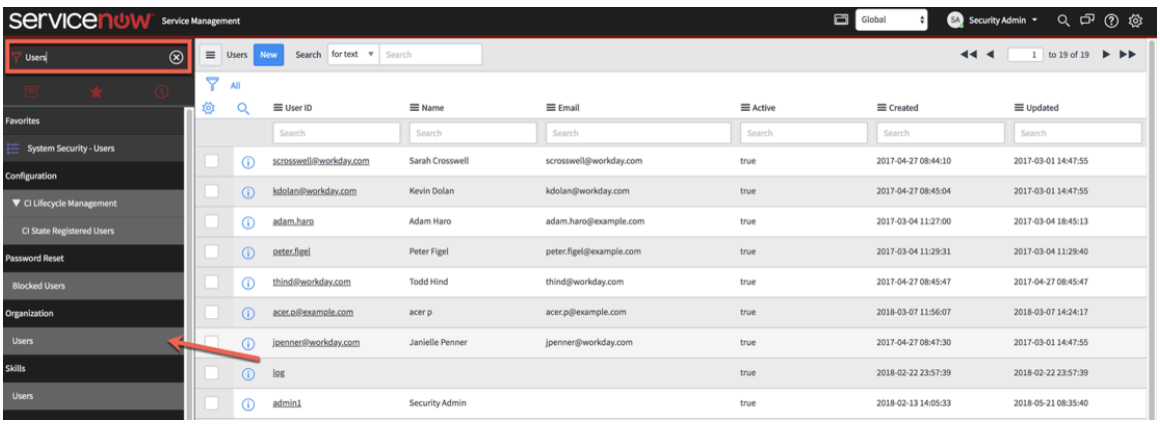
Role required: admin

About this task

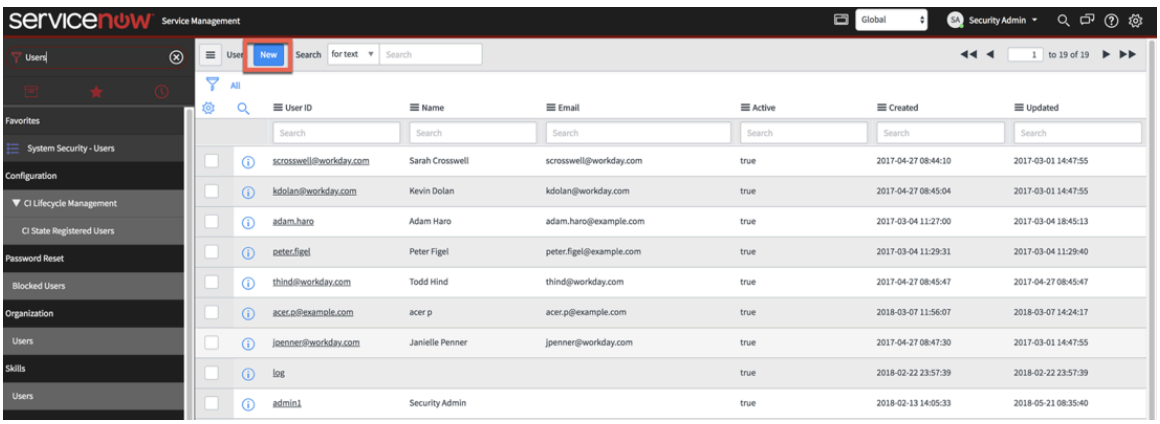
The ServiceNow AI Platform admin creates an API account role (sn_sec_checkpoint.api_account_access). This account is used exclusively for entering credentials required for authentication on Check Point, so the Gateway can retrieve Block Lists from the ServiceNow AI Platform. This account is a separate, unique API user account in the ServiceNow AI Platform instance, and assigned to the Check Point administrator.

Procedure

1. Navigate to **All** > **Organization** > **Users**.
2. Click the **Users** module.

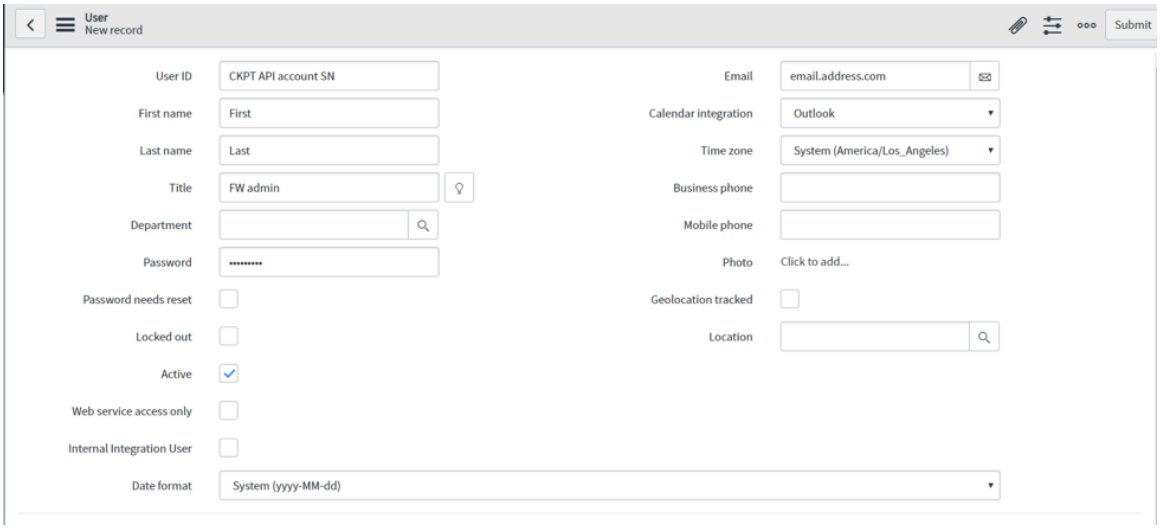


3. On the Users list that is displayed, click **New**.



A new form is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

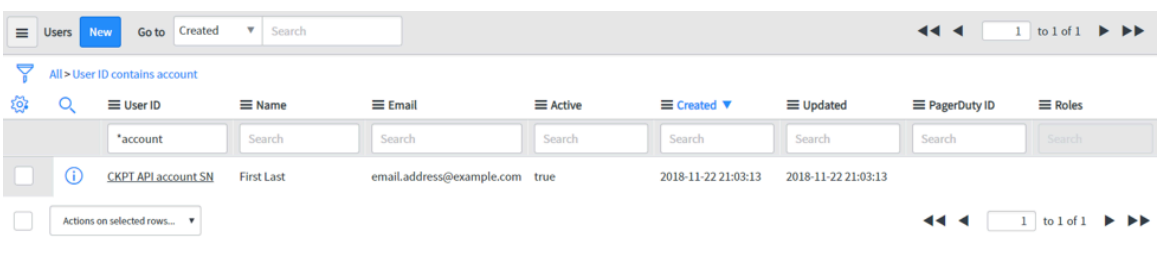


4. Fill in the form, as needed.

   Note: The values for User ID title, and email address shown in the following table and figure are example values.

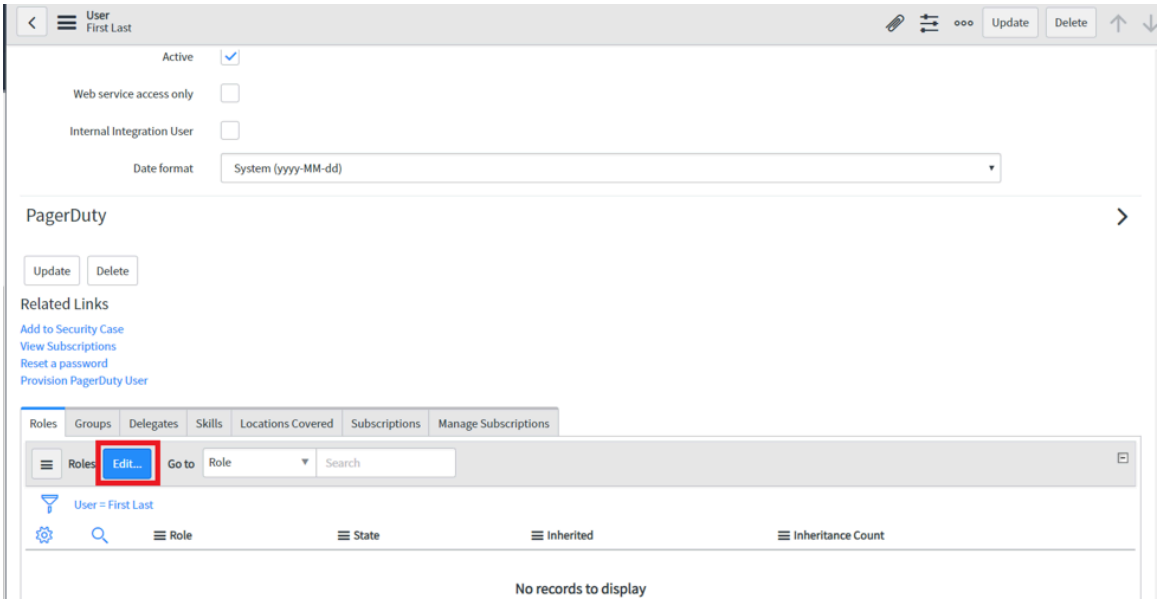
Field	Description
User ID	Unique User ID for the role in your ServiceNow AI Platform instance. This user ID is entered in the **Username** field in the **Client Authentication** section of the Block List Configuration Check Point gateway. An example is CKPT API account SN.
First Name	Person you are assigning
Last Name	Person you are assigning
Title	Job Title, for example FW admin.
Password	Unique password created for this role. This password is entered in the **Password** field in the **Client Authentication** section of the Block List Configuration on Check Point gateway.
Email	Unique email address

5. Click **Submit**.
   Once submitted, you can assign the role.
6. On the Users list in the User ID column, click the name of the user ID you entered, CKPTAPI account SN, for example.

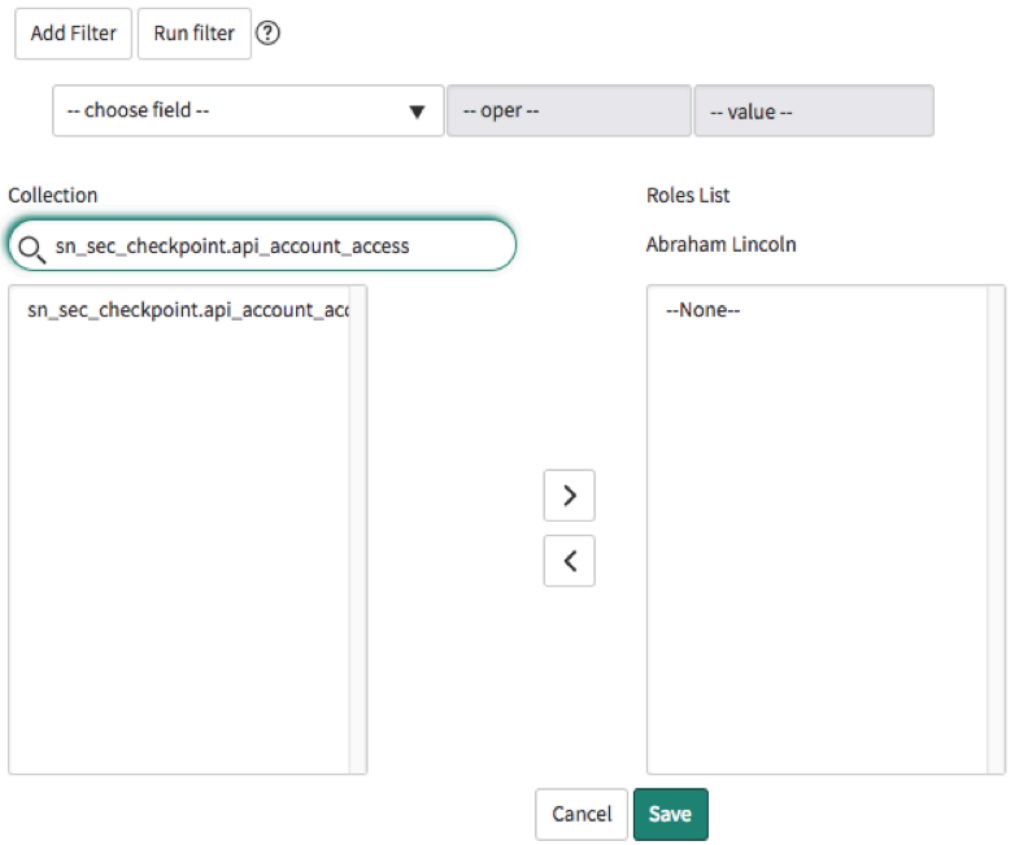


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. On the open record in the Roles section, click **Edit**.



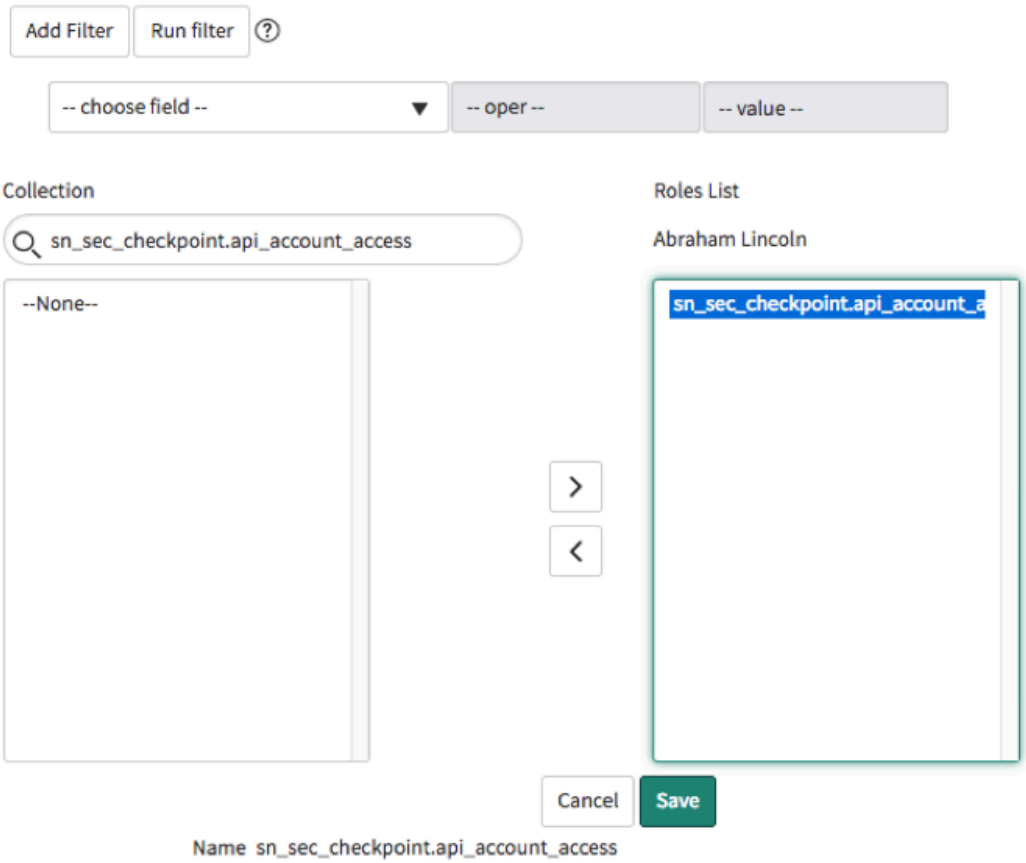
8. On the **Edit Members** form that is displayed, enter sn_sec_checkpoint.api_account_access in the **Collection** field.



9. In the **Collection** column, select then move sn_sec_checkpoint.api_account_access to the **Roles List**.
10. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

11. Navigate to **Users**, and in the **User** column on the list, click the ID name that you created for the role (CKPT API account SN).



12. 

The user record is displayed. This record verifies that the user account has been assigned.

Set up the Check Point NGTP integration

Complete the following steps to set up the Check Point Next Generation Threat Prevention integration. This would ensure that the pre-requisites for the integration to work are in place.

Before you begin

Role required: admin

Procedure

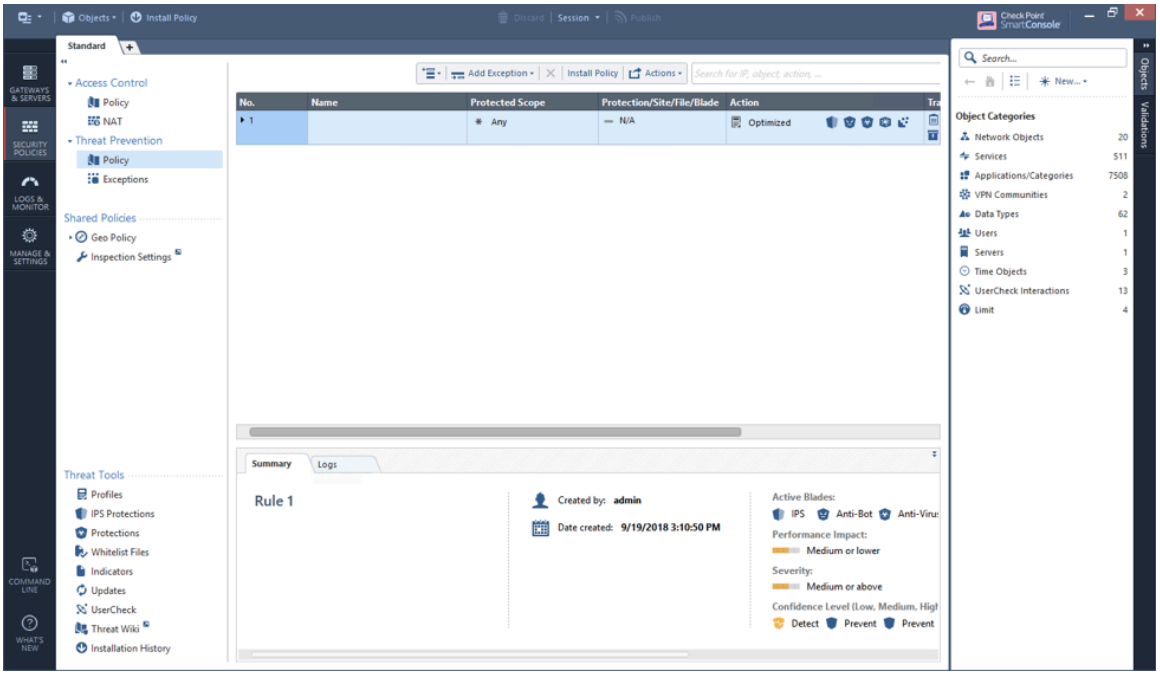
1. Verify that Threat Prevention Policy is configured with Anti-Bot and Anti-Virus Blades activated. Refer the Check Point User Guide mentioned in Reference section for detailed information on setting up Anti-Bot and Anti-Virus Blades.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

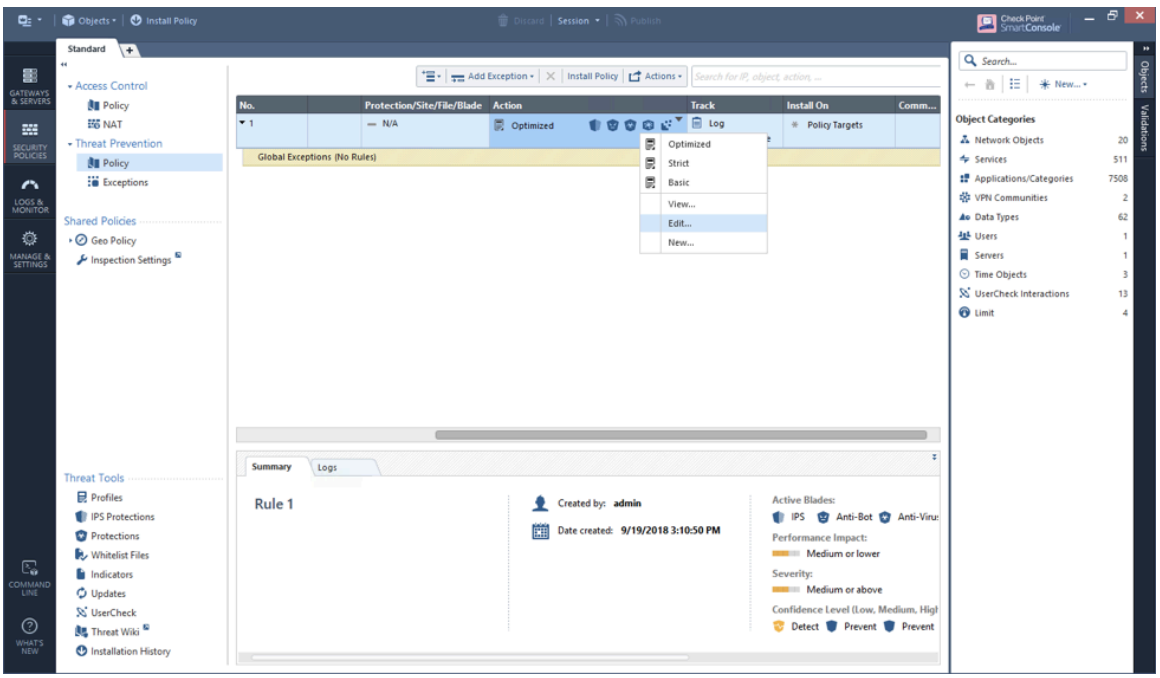
Note: The images in this topic are privileged and proprietary and are used with permission from Check Point Software Technologies, Ltd.

a. Login to **Smart Console**.

b. Navigate to **Security Policies** > **Threat Prevention** > **Policy**.



c. Open the Threat Prevention Policy in Edit Mode.

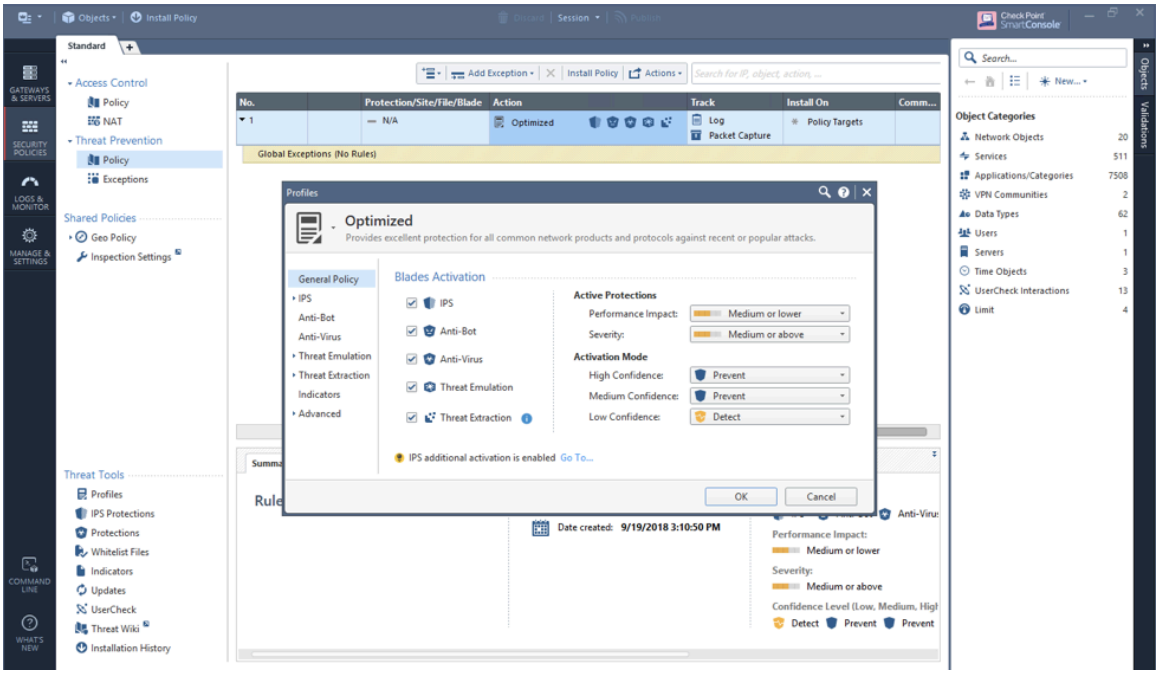


d. Active Protections → Severity should be “Medium or above”

e. Activation Mode → High Confidence should be “Prevent”

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

f. Blades Activation à Anti-Virus and Anti-Bot should be selected.



g. Publish the changes (if any) and Install the Policy.

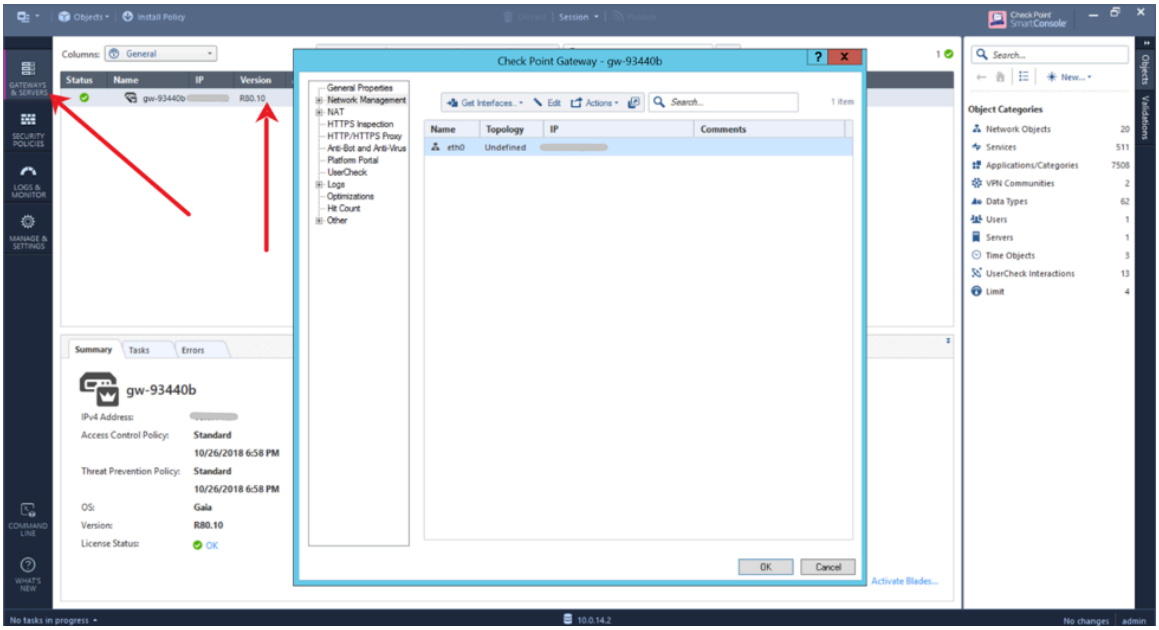
2. If not already configured, Custom Intelligence Feeds should be added after activating Anti-Bot and Anti-Virus Blades.
   Refer to the Installation section of Check Point Custom Intelligence Feed Feature documentation.https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
3. If not already configured, set up the Check Point Gateway to route all the internet traffic via HTTP Proxy (if configuring HTTPS Inspection).

> **Note:** For URL blocking on Check Point NGTP, there are certain settings that needs to be ensured. HTTPS internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy. However, HTTPS can hide malicious traffic which should have been blocked. For Check Point Gateway to get the visibility into HTTPS traffic, either route the traffic via HTTP Proxy or setup HTTPS Inspection(recommended). This section details the steps to follow to setup HTTP Proxy on Check Point Gateway.

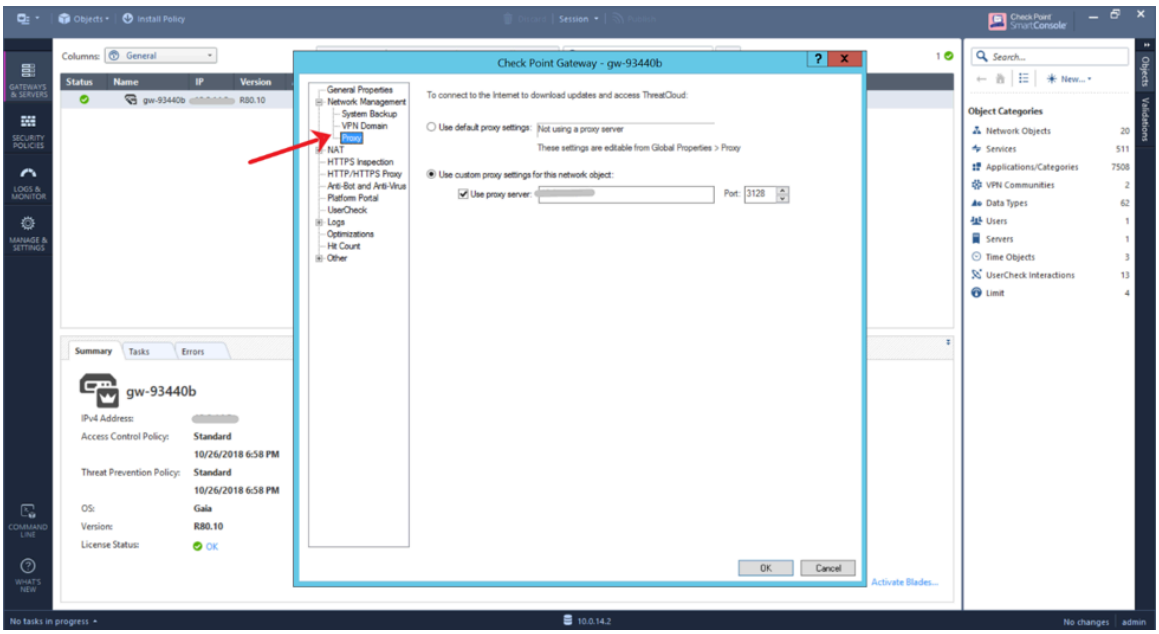
a. Login to **Smart Console**.

b. Navigate to **Servers and Gateways**, and double-click on the applicable server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. Navigate to **Network Management** > **Proxy**.



d. Provide the Proxy Details to be used for routing the HTTP traffic.

e. Ensure that HTTP requests from Client Endpoint are via the HTTP Proxy.

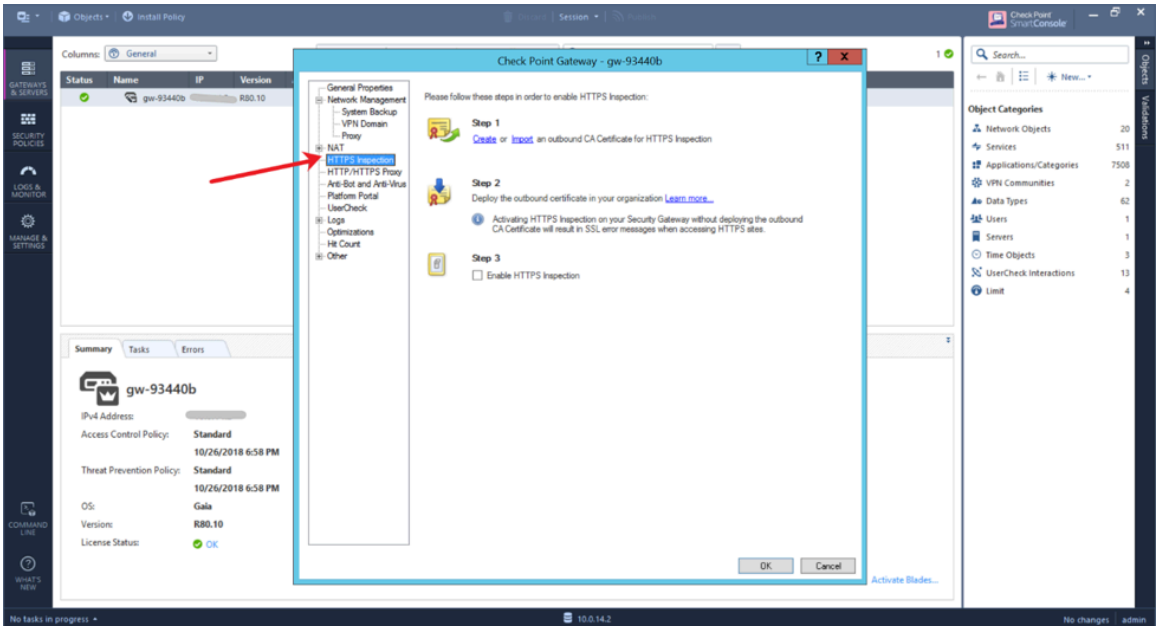
4. If not already configured, enable HTTPS inspection (if HTTP Proxy configured).
When most of the traffic is over SSL, it is recommended to use HTTPS Inspection Blade. This makes the traffic transparent to GW. Enable HTTPS Inspection on Check Point Gateway, as follows.

a. Login to **Smart Console**.

b. Navigate to **Servers and Gateways**, and double-click on the applicable server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Navigate to **HTTPS Inspection**.



d. Follow the steps to configure HTTPS Inspection in the Check Point User Guide.

Activate the Check Point NGTP integration

If you have not installed the application, follow the instructions to install it.

Before you begin

Role required: admin

Procedure

1. Log in to the instance you want to install the application on.
2. Navigate to **System Applications** > **Applications**.
3. Click the **Downloads** tab.
   A list of applications available for installation is displayed.
4. Locate the Check Point Next Generation Threat Prevention application, select it, and click **Install**.
   Your application is automatically installed onto your instance.

Working with block lists

The ServiceNow Check Point Next Generation Threat Prevention Integration supports Block Lists that accept IP, URL, and Domain observables.

ServiceNow configured block list is a csv file that is hosted on an external web server, which for this integration is the ServiceNow AI Platform instance. Custom Intelligence Feed is configured on the Check Point Gateway, which pulls the IP addresses, URLs, and domains from the ServiceNow AI Platform at pre-configured interval.

This integration supports three types of Block Lists:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- IP Address (This includes an individual IP Address (IPv4 only) for block list, and CIDR blocks (ranges) of addresses for allow list).
- URL
- Domain

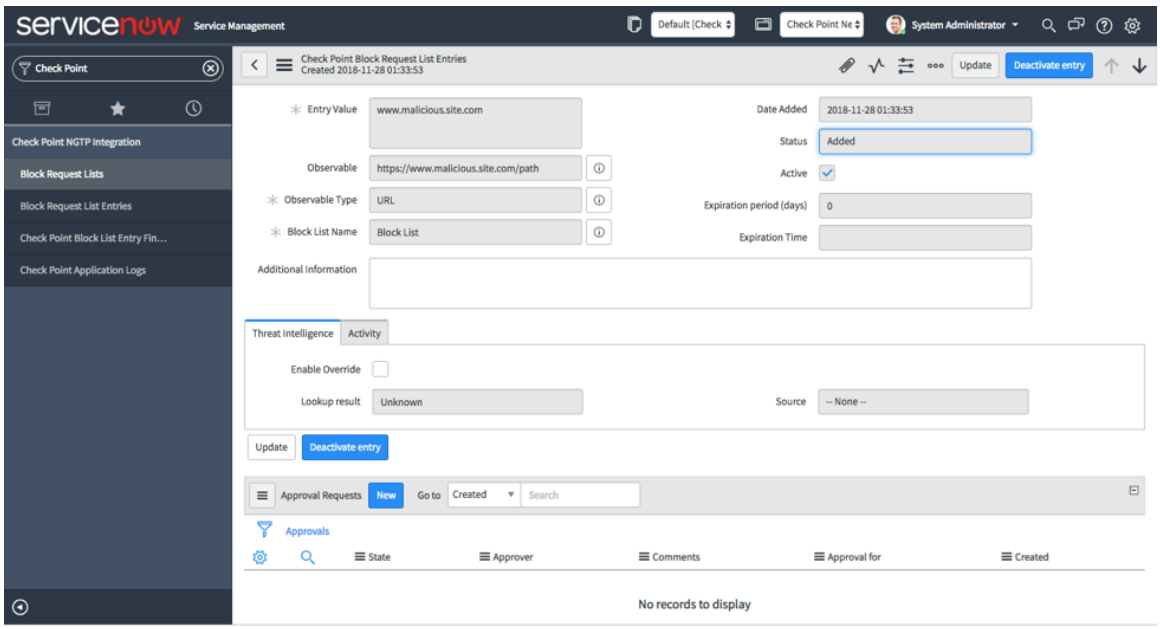
Observables supported by the Check Point NGTP integration

The section lists descriptions of the observables supported by this integration and example formats for each type.

Observable Type	Examples	Description
Domain	• example.com • mail.example.com	Wildcards are not supported.
IP Address	95.153.103.54 (IPv4)	Represents a single, distinct interface address. The integration supports only IPv4 and CIDR formats (CIDR format is only supported for allow listing purpose). For allow list purpose, integration has support for IP address observables includes CIDR (Classless Inter-Domain Routing) ranges, for example, 95.153.100.0/22. **Note:** An error message is displayed when you try to attach a single IP address to a Block List that you have already allowed listed as a part of a CIDR range. For example, the single address 95.153.103.54 is part of the CIDR range represented by 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Description - The HTTPS URL are formatted by the application to trim the path from the URL and retain the domain name only. Check Point NGTP relies on HTTP CONNECT request to evaluate the web traffic and enforce blocking. For HTTPS CONNECT request,

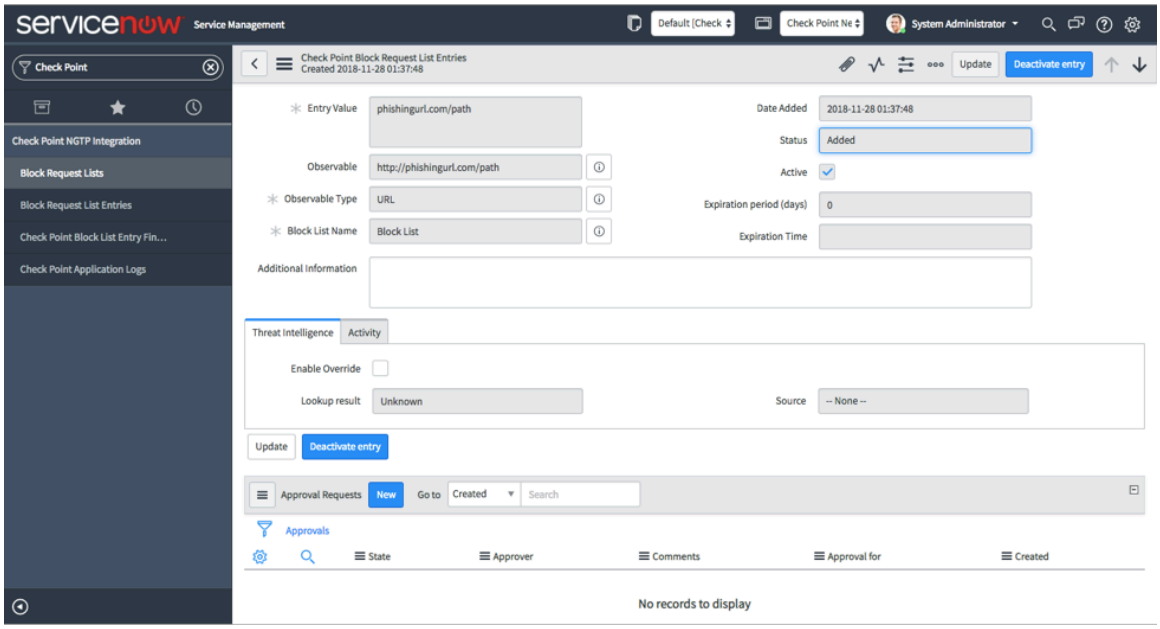
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Observable Type	Examples	Description
		the entire URL isn't visible in the request and only domain name is visible. When a user blocks any HTTPS URL with specific path (example; https://www.example.com/path), the application trims the path automatically (www.example.com). The application maintains the relationship between original observable and the formatted URL. Below is the screenshot of Block List Entry which shows the formatted URL and the original observable.



For HTTP URLs with a specific path (for example, http://www.example.com/path), Check Point would block the specified URL as the entire URL is visible in CONNECT request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Create a block list for the Check Point NGTP integration

Create a Block List in your ServiceNow AI Platform instance. Once approved and activated, you can create entries for these Block Lists from observables determined to be malicious on Now Platform Security Incident Response (SIR) incidents and request approval to block them.

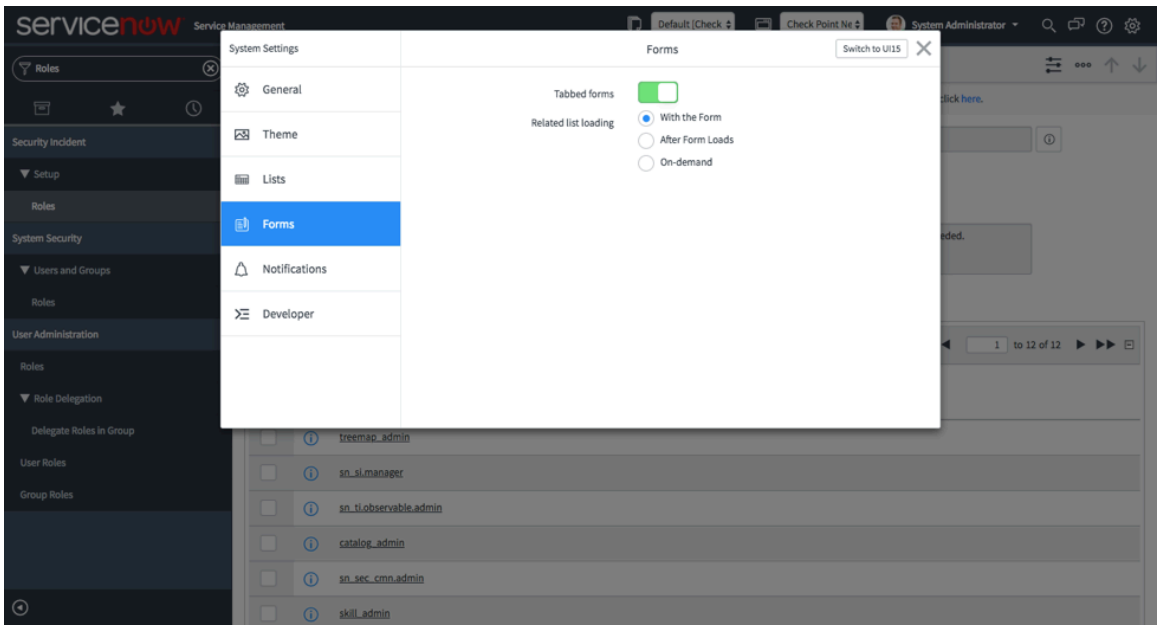
Before you begin

Role required: Security Incident Administrator (sn_si.admin)

About this task

Create the Block List on your ServiceNow AI Platform instance so that the Check Point can import objects — IP addresses, URLs, domains — included in the list. Custom Intelligence Feed is configured on Check Point Gateway which pulls the IP addresses, URLs, Domains from ServiceNow AI Platform at pre-configured interval. To ensure blocking the observables, the Threat Prevention Policy should be configured with Anti-Bot and Anti-Virus Blades activated.

Note: The figures in this topic are shown with **Tabbed forms** cleared in System Settings.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

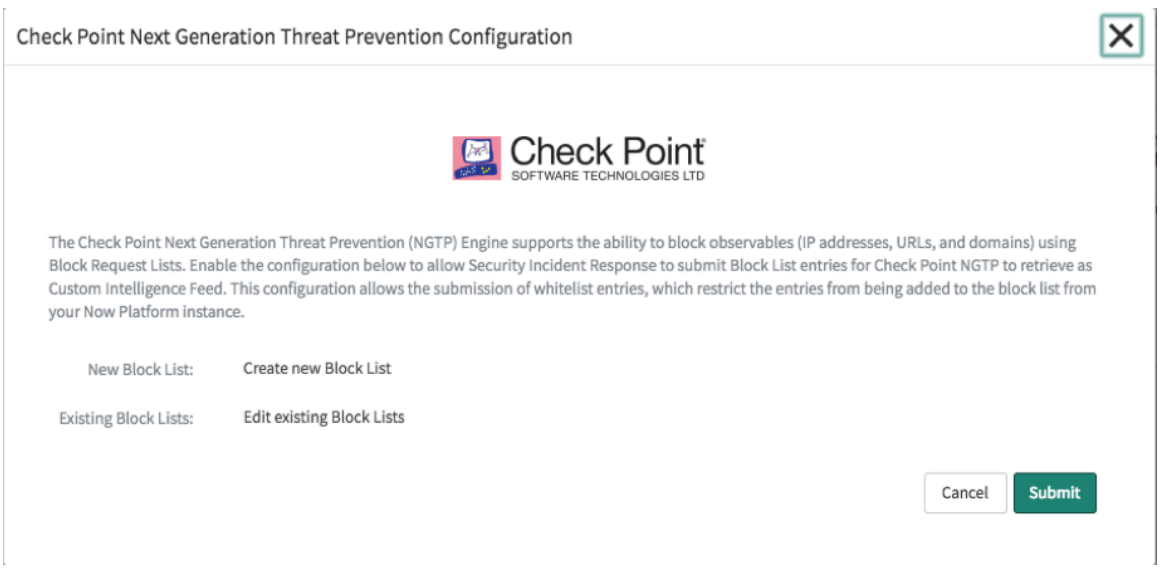
Procedure

1. After the application installation is complete, navigate to **Integrations** > **Integration Configurations**.
2. Locate the **Check Point Next Generation Threat Prevention** card and click **Configure**.



Note: Privileged and Proprietary content used with permission from Check Point Software Technologies, Ltd.

3. Click **Create new Block List**.



4. On the form, fill in the fields.

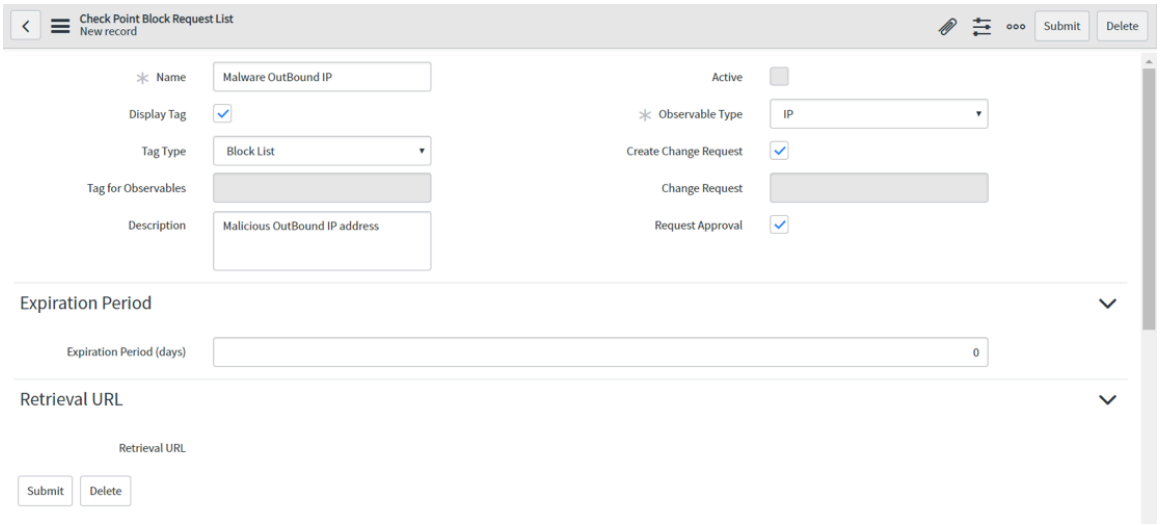
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Check Point Block Request List name. Include the observable type (URL, IP, domain) in this field so the security analyst can easily recognize the intention of the Block List by its name. The name should also clearly indicate what firewall policy these Block List objects are mapped to. Some examples of Block List names are, Outbound Malware IP, or Outbound Phishing URL.
Active	This check box is cleared by default to indicate that the Block List is inactive. When inactive, the Block List is unable to receive additional entries. When the check box is selected (When Change Request is closed or change request is not generated), the Block List is activated and available for Block List entries.
Display Tag	Check box is selected by default to automatically tag the observable and the associated security incident record if the observable is blocked on Block List. When selected, the "Tag for observables" field is available on the form. **Note:** A tag name is created by default from the value you enter in the Name field with a Check Point-prefix, for example, Check Point-Malware OutBound IP. You can change the tag name and color. The tag name is displayed in the field "Tag for observables", once the Block List is saved. When the check box is cleared, no tag is created, and the "Tag for observables" field is not available on the form.
Observable Type	Select an observable type this Block List accepts from the list: IP Address (including CIDR for allow list), URL, or domain.
Tag Type	Tags that are available from the list. A Block list is a list of observables that you want the Check Point Next Generation Threat Prevention to block. A allow list is a list of observables you do not want to block in Check Point Next Generation Threat Prevention in any case. By default, the Block list tag color is black, and the allow list tag color is Gray. You can change the color.
Create Change Request	This check box is selected by default to automatically create a change request and change tasks in your ServiceNow AI Platform instance, which are attached to the Block List record. The change request is used to configure the Block List retrieval URL in the Check Point Next Generation firewall gateway. This option is recommended if your firewall administrator is also using the ServiceNow AI Platform for firewall policy or rule changes. If you create a request, once it is closed, the Block List is automatically activated. Clear the check box to manually activate the Block List after receiving notice via email from the firewall administrator that the Custom Intelligence Feed has been configured on all the Check Point Gateways.

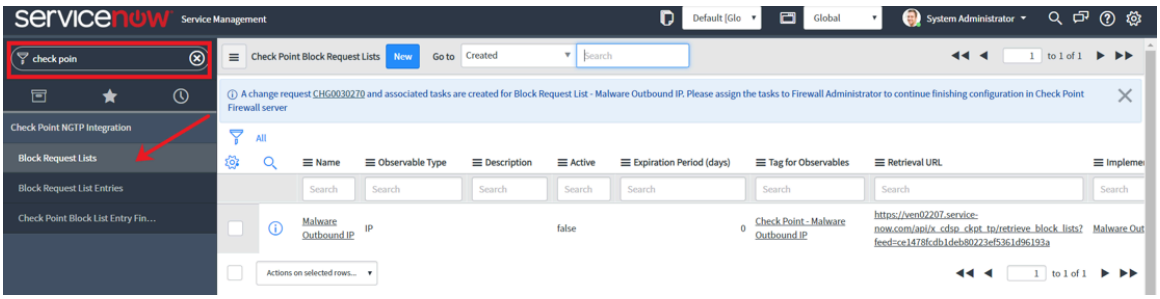
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	When the check box for Create change request is cleared, the Change request field is unavailable.
Request Approval	This check box is selected by default to request approvals for activating/removing Block List entries from Block Lists. Approval is requested from the users having role Security Incident Administrator(sn_si.admin). Approval request will be sent via email to the approvers. Once the approval is accepted, the entry will be activated on that Block List. When the check box is not selected, the entries for that Block List will not follow approval workflow and will be directly activated on block list.
Tag for Observable	This field is displayed only if the Display tag check box is selected. Field is automatically populated after the Block List is saved with a default value from the Name field. If Block List is created with name 'Malware URL', the tag name derived is 'Block List – Malware URL'
Change Request	When the Create change request check box is selected, the change request number is displayed on the Now Platform instance once the Block List is saved. When the check box for Create change request is cleared, this field is not displayed.
Description	Description of the Check Point Block List. The name generally contains the types of sites and observables you would expect to be on this Block List, and you can use this field for more details.
Expiration Period (days)	Expiration period of the Block List. 0 (the default) indicates that the Block List entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1 which is 24 hours, and there is no maximum value.
Retrieval URL	Retrieval URL will be generated automatically, once the Block List is saved. To configure this Block List on Check Point Gateways, you must use this URL. Once this URL is configured, Check Point fetches observables to be blocked in csv format.

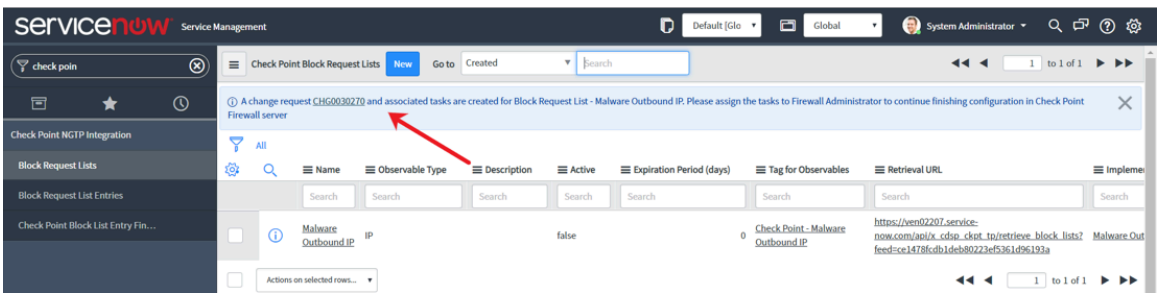
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.
6. If the Check Point Block Request List is not displayed, navigate to **Check Point NGTP Integration** > **Block Request Lists**.

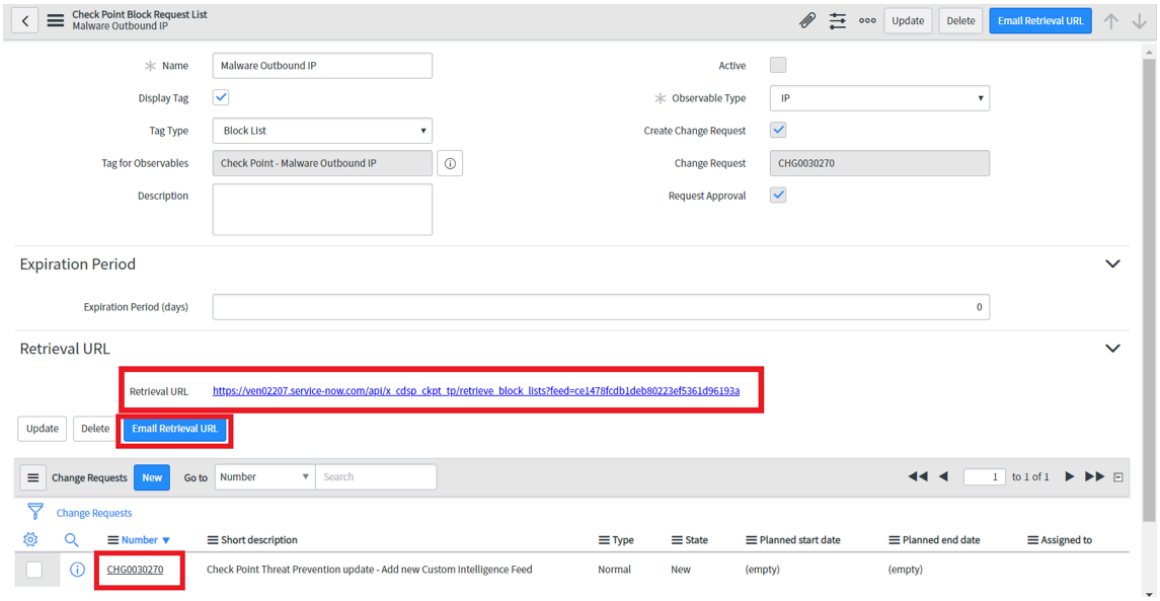


The new Block List is displayed. The Block List status is still inactive (false), which means the Block List is not available to accept entries. If Create change request was configured, a message is displayed indicating a change request and tasks have been created in your ServiceNow AI Platform instance.



7. In the **Name** column, click an item to open the record.
   The Block List record is displayed. This example shows a Malware Outbound IP Block List. The following fields, options, and links are displayed on the new record after submission and described in the following table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Field	Description
Email Retrieval URL	Emails a notice that the Block Link is available for configuration to the Check Point firewall administrator.
Retrieval URL	This URL is used to configure Custom Intelligence Feed on Check Point Gateways. **Note:** If you have your System Settings set to Tabbed forms, this link is displayed on the Block List Retrieval Info tab at the bottom of the record.
ServiceNow AI Platform change request	A link to the change request record is displayed in the Change Requests section when configured, and the request number is displayed in the Change request field.
Update	Modify data and update the editable fields.
Delete	Delete the record.

8. Create and add more Block Lists as required.
   The Block Lists are displayed on the Check Point Block Request Lists Page.

What to do next
Activate the Block Request List manually, or with a ServiceNow AI Platform change request.

Activate a block list for the Check Point NGTP integration

After the Block List has been created in your ServiceNow AI Platform and the URL is available, the Check Point administrator configures the Block List as Custom Intelligence Feed on all the Check Point Next Generation Gateways. Before it can accept Block List entries, the Block List must be configured in Check Point and activated in the ServiceNow AI Platform.

Before you begin
Role required: Security Incident Administrator (sn_si.admin)

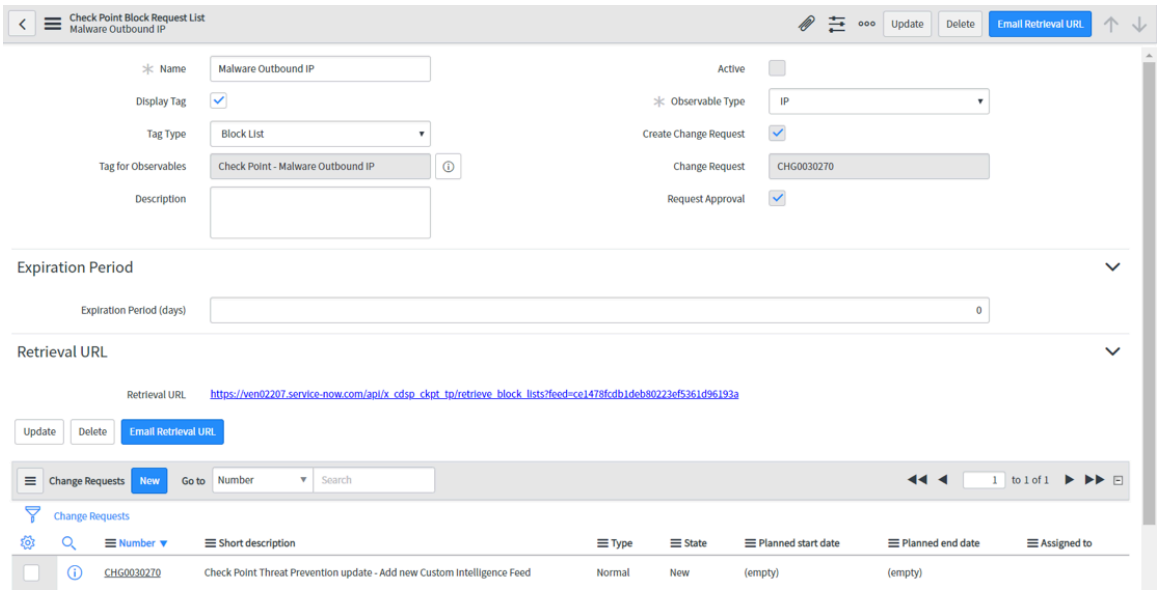
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

After the Block List is configured, as the security incident administrator, you can activate the Block List manually, or, the Block List is automatically activated upon completion of a ServiceNow AI Platform Change Request. The Change Request must be approved and moved from the inactive state to the active state before it can accept Block List entries.

Procedure

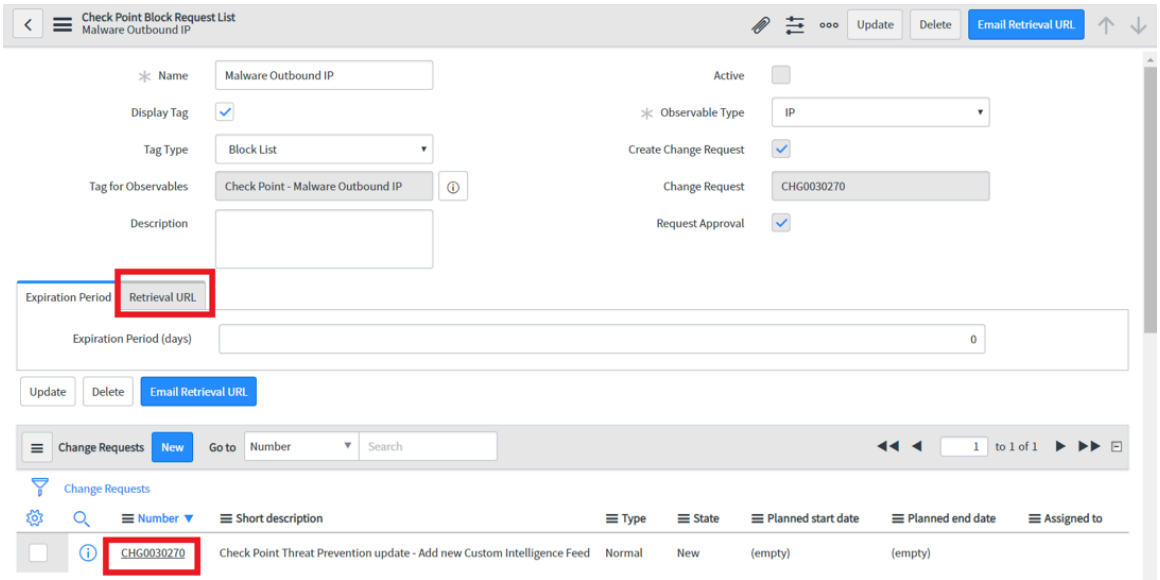
1. Navigate to **All** > **Check Point NGTP Integration** > **Block Request Lists**, and select the **Block Request Lists** module.
2. In the **Check Point Block Request Lists** list that is displayed, select your new Block List in the **Name** column.
3. On the record that is displayed, note the **Email Retrieval URL** button, the active Block List Retrieval URL link, and, if configured, the ServiceNow AI Platform change request in the Change Requests section.
   Also note that the Active check box is cleared.



Note: With Tabbed forms cleared in your system settings, the Block List Retrieval URL appears in Retrieval URL section.

4. Click the **Block List Retrieval URL** tab to display the retrieval URL.
   The following figure shows the Block List Retrieval URL displayed as a tab with Tabbed forms selected in your system settings. The link to the change request (CH0030270) is also displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. To complete the configuration and move the Block List from inactive to active, you must choose one of the following options to notify the firewall administrator that the retrieval URL is available.

Option	Description
Click Email Retrieval URL.	Email Block List Retrieval URL directly to the firewall administrator. This option permits the firewall administrator to finish the configuration on the Check Point platform. Choose this option if the firewall administrator is not using the ServiceNow AI Platform.
Complete the ServiceNow AI Platform change request and assign the configuration tasks to the firewall administrator.	This option is available only if the firewall administrator for Check Point is also using the Now Platform, and the ServiceNow AI Platform change management and approval processes are configured. **Note:** Users with the Security Incident Administrator (sn_si.admin) role can approve the ServiceNow AI Platform change request. Once the configuration tasks are completed and the change request has been closed, the Block List is activated automatically.

What to do next

After you notify the firewall administrator that the retrieval URL is available, and you confirm the Block List has been configured in Check Point, as the security incident administrator, your next step is to activate the Block List. You either activate the Block List manually or, if configured, use the ServiceNow AI Platform change request form to activate the Block List. The Block List is automatically activated when the change request is closed.

Configure a block list as a Custom Intelligence Feed on the Check Point NGTP integration

The firewall administrator must configure the Custom Intelligence Feed corresponding to the Block List created in ServiceNow AI Platform.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

This task needs to be performed on each of the Check Point NGTP Gateway. The firewall administrator would need the SSH access of the Gateway servers. If your organization has ServiceNow AI Platform change management and approval processes, verify that email send/receive capability is enabled.

The firewall administrator would need the retrieval URL of Block List and the ServiceNow user credentials with role Check Point API Account Access Role (sn_sec_checkpoint.api_account_access).

If Firewall administrator is not using ServiceNow AI Platform, the NOW Security Incident Administrator can provide the required information via an Email. Alternately, if firewall administrator is using ServiceNow AI Platform, the Change Request associated with Block List can be assigned to firewall administrator. This Change Request has the required information to configure Custom Intelligence Feed.

For more information on setting up Custom Intelligence Feed on Check Point Gateways, refer to: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Procedure

1. Verify that email send/receive capability is enabled in your ServiceNow AI Platform instance by navigating to **Email properties** > **Administration** > **Email Properties**.
2. Under Outbound Email Configuration, verify that **Email sending** and **Email receiving** are selected.
3. Modify SSH to Check Point Gateway with expert mode.
4. Execute the command to add Custom Intelligence Feed.
   The command execution is interactive and prompts for feed format and password.
   - When prompted for Feed Format, enter 'cp_csv'
   - When prompted for ServiceNow AI Platform user password with API Access.

   The command execution would warn about the server certificate (NOW platform) not being trusted by the machine and would prompt to add the server security certificate to machine's trusted store. Enter **Y**.

   "Status:Succeed" message would appear, confirming that the Feed is successfully added.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Submit block list entries from a security incident for the Check Point NGTP integration

Observables attached to a security incident record are submitted for approval as Block List entries to different Block Lists. An optional approval process for Block List entries is part of the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

preconfigured workflow. The Gateway imports Block List entries — IP addresses, URLs, domains — that are included in Block Lists.

Before you begin

Role required:

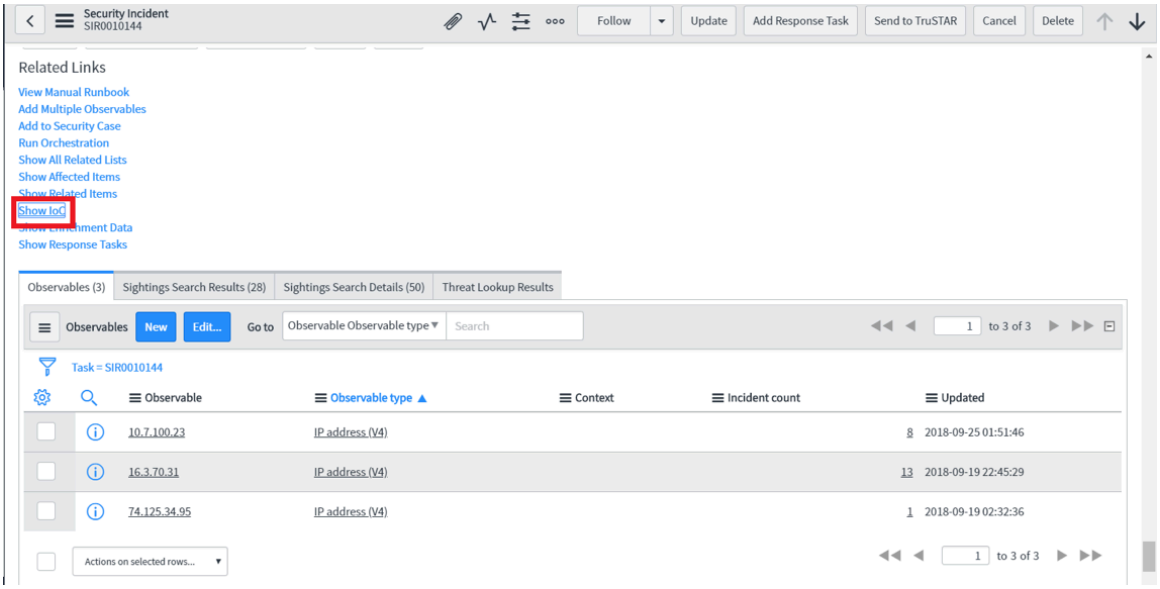
- Security Incident Analyst (sn_si.analyst) to submit block list entries.
- Security Incident Administrator (sn_si.admin) to approve block list entries. This authority can be assigned as required by your organization.

About this task

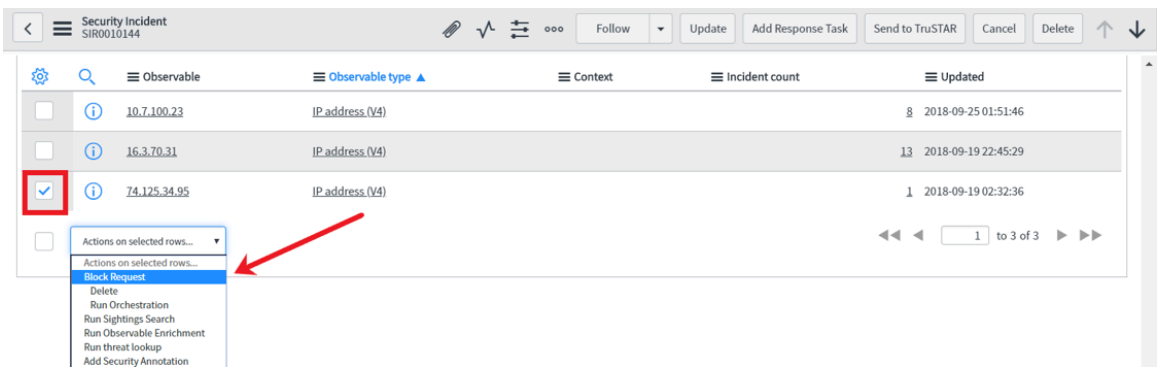
Users with the sn_si.analyst role submit Block entries by requesting a block on observables attached to a security incident record. Once submitted, a Block List entry with a status of Pending is generated and sent for approval. The following example shows a block request for a URL observable.

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**, and click a security incident record to open it.
2. Click the **Show IoC** related link.

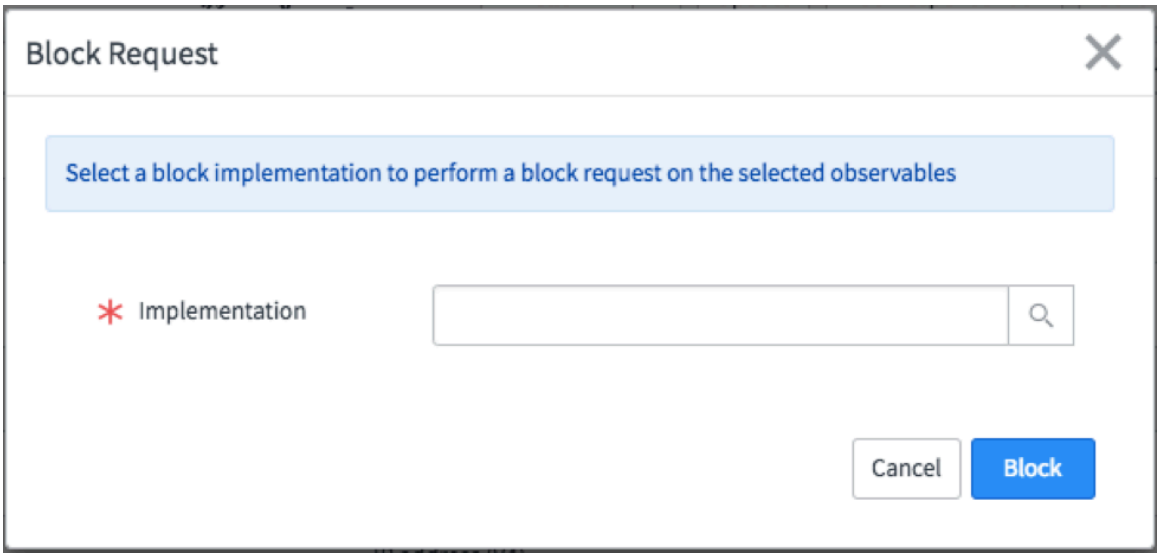


3. In the Observables related list, select the observables you want to block and, from the **Actions on selected rows** list, select **Block Request**.



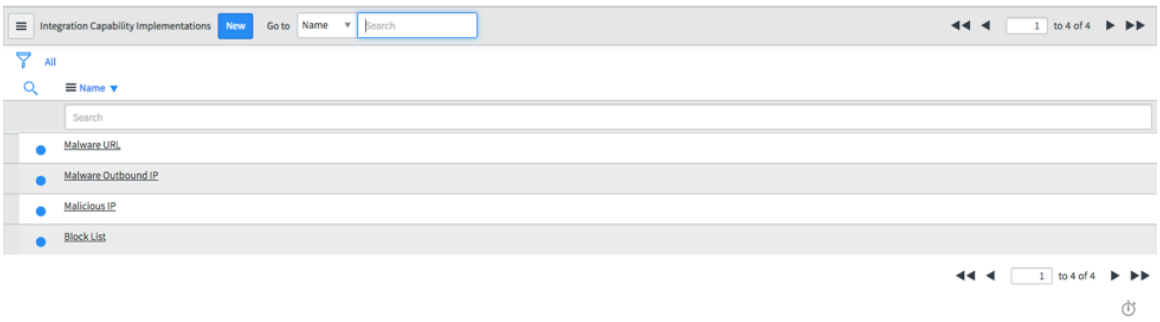
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the dialog box that is displayed, click the search icon ( )

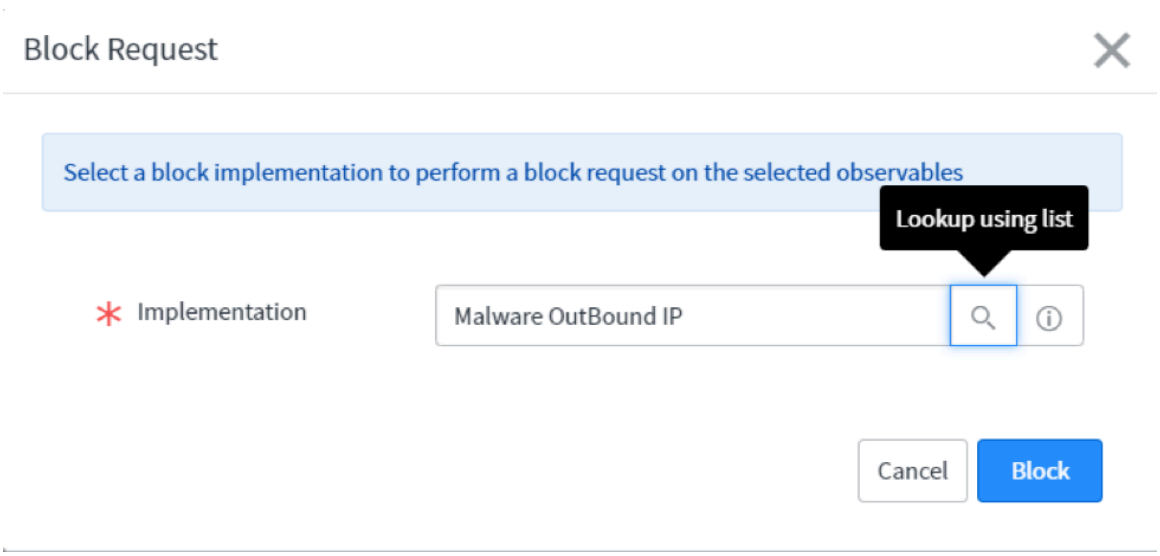


5. From the list, select the Block List you want to attach this entry to.

Note: For this example, the entry observable type (IP) should match the Block List observable type (IP).



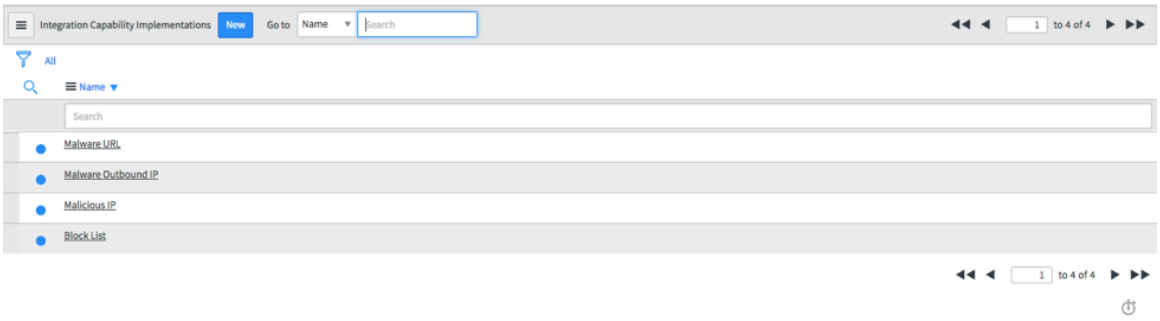
6. In the Block Request dialog box with the Block List name displayed in the Implementation field, click **Block**.



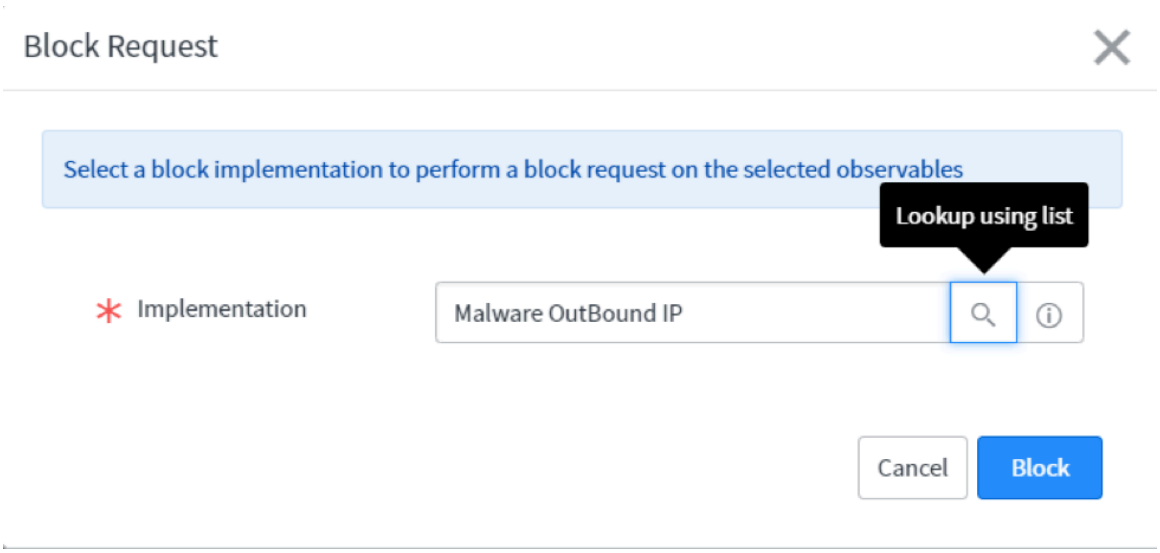
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. From the list that is displayed, select the Block List you want to attach this entry to.

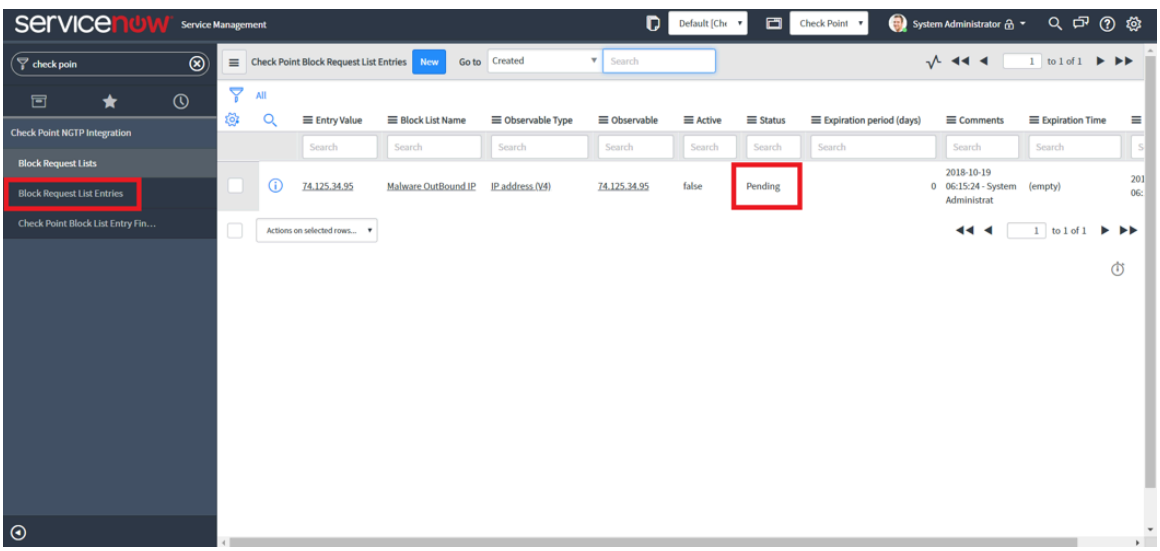
   Note: For this example, the entry observable type (IP) should match the Block List observable type (IP).



8. In the Block Request dialog box with the Block List name displayed in the **Implementation** field, click **Block**.

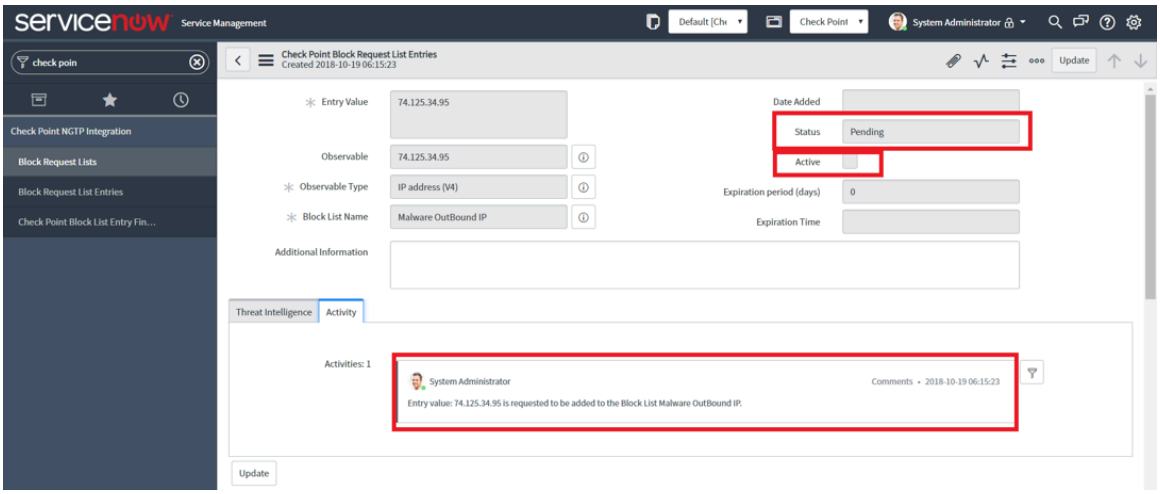


9. Navigate to **Check Point NGTP Integration** > **Block Request List Entries**, and click **Block Request List Entries**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. In the Check Point Block Request List Entries list, click your observable in the **Entry value** column to open the record.
    For this example, the record for **74.125.34.95** is displayed.



The status is Pending, the Active check box is cleared, and the work notes show that there is a request to add the observable. This Block List Entry request is ready for approval.

The icon next to the Observable field is a link to the ServiceNow AI Platform Observable table.

The value in the Observable field (74.125.34.95) links to the Observable table, and it matches the format that was brought over from the Security Incident Response incident-triggering event.

Submit block list entries directly from the Block List Entry Table

For observables determined to be malicious, and not associated with a specific Now Platform security incident, you submit Block List entries from the block list.

Before you begin

Role required: Security Incident Administrator (sn_si.analyst)

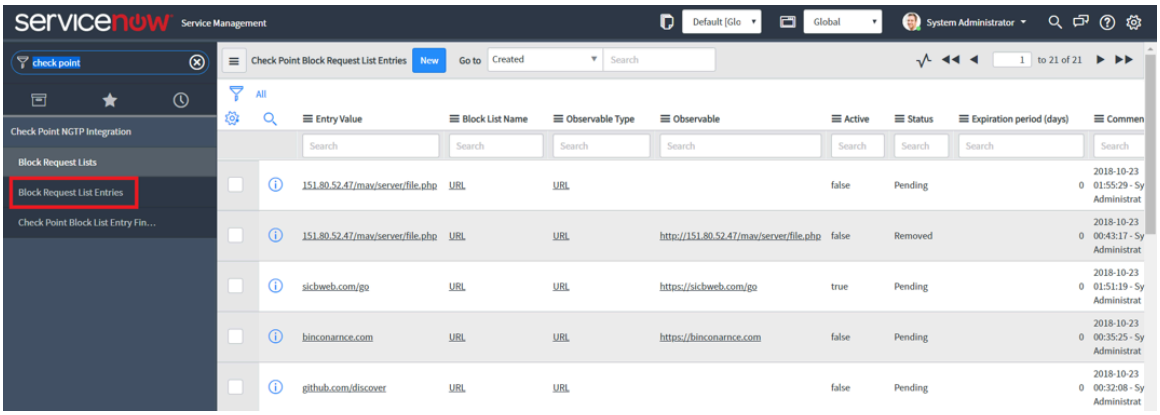
About this task

When you want to block an observable that you have determined is malicious or allow an observable you have determined is not malicious, and the observable is not associated with a specific ServiceNow AI Platform security incident record, you submit Block List entries directly from the block list. Examples of these types of Block List entries might be URLs or domains for specific sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

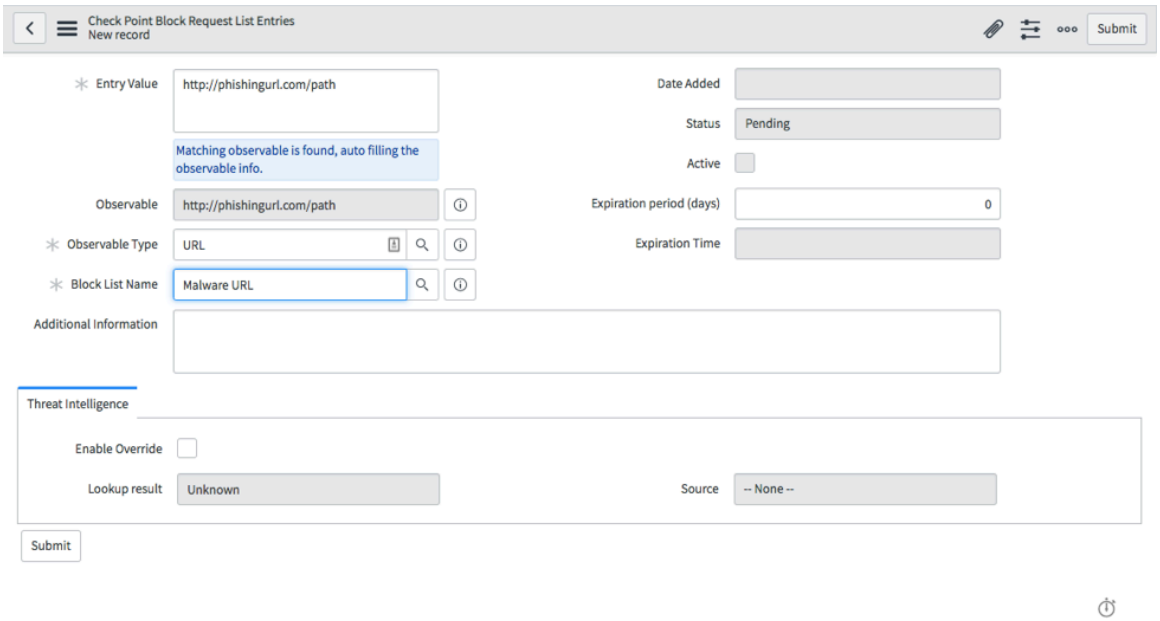
Procedure

1. Navigate to **All** > **Check Point NGTP Integration** > **Block Request Entries**.



2. Click the **Block Request Lists** module.
3. In Check Point Block Request List Entries list, click **New**.
4. In the **Entry value** field, enter a value for your observable.
   The two possible outcomes of this entry:
   - The remaining fields on the form are completed automatically.
   - A matching observable is found, and a message is displayed that a matching observable exists. Select the Block List you want to attach this entry to and click Submit. Select the Block List you want to attach this entry to prior to setting the Expiration period.

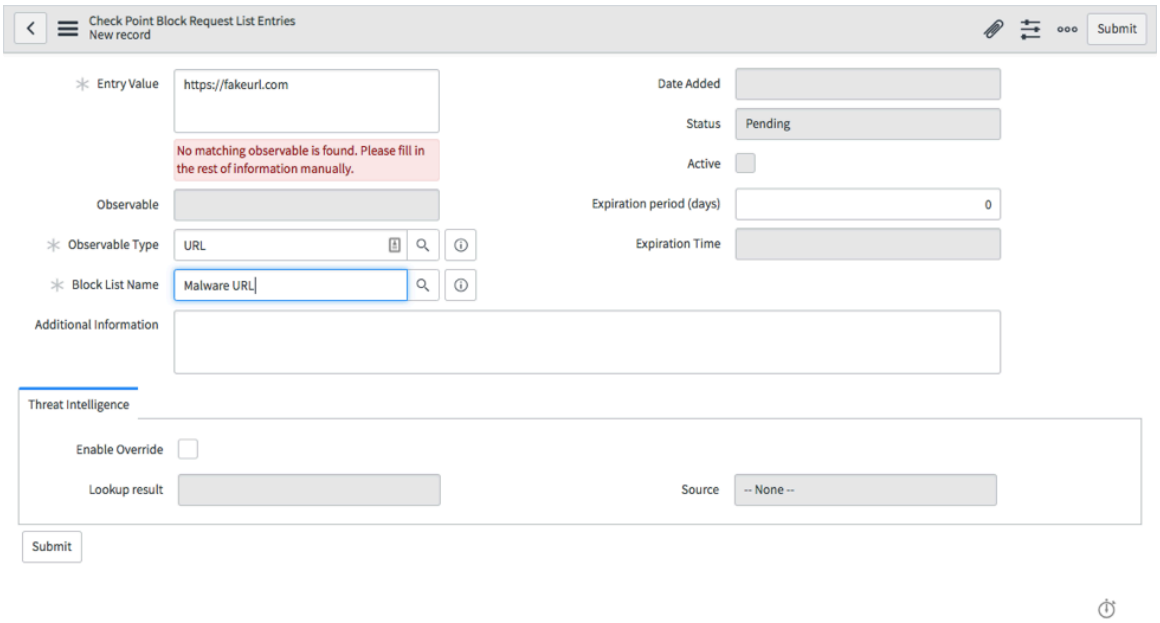
   A message is displayed that instructs you to complete the form. A matching observable has not been found, and you must complete the form. After you complete it, select the Block List you want to attach the observable to and click Submit. An observable record is created. The following figure shows an example of an existing domain observable and how the fields are completed automatically.



5. Click the search icon to select the Block List you want to attach the entry to.
6. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

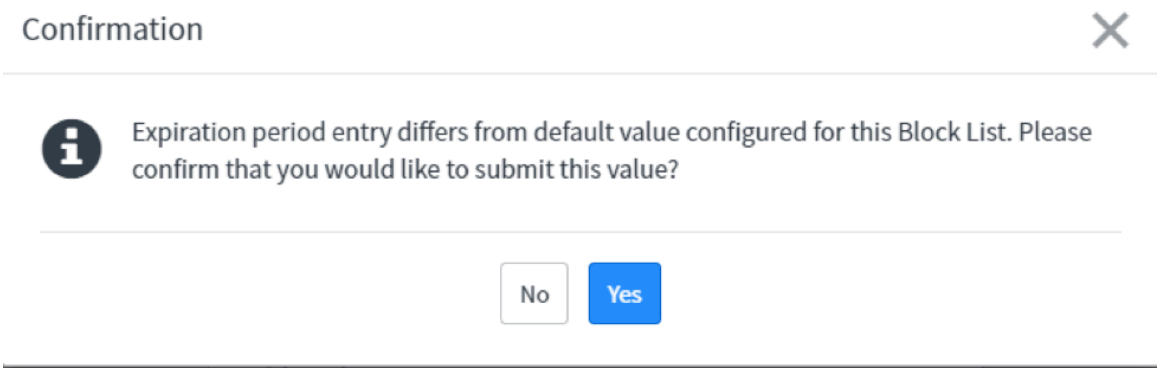
7. If you have email approval configured in your workflow, an approval email request is sent. If a message is displayed that requests you to fill in the rest of the information manually, fill in the fields.



Field	Description
Observable type	Observable type that is supported from the dialog.
Block List name	Block List you want to the entry to. **Note:** Select the Block List you want to attach the entry to prior to setting the Expiration period.
Enable override (default is selected)	Lookup result or source. When configured, permits you to enter a Lookup result and the source used to find the results. These fields are typically populated when a security incident record is created. In this case, there is no lookup result or source, and you fill in these fields in manually.
Lookup Result	Select **Unknown** or **Malicious**.
Source	Source that performs a threat lookup on the Block List entry, for example, ThreatCrowd, etc
Expiration period	The expiration period inherited from the Block List by default. You can override this value, but only during the creation of the entry. 0 indicates that the Block List entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the Block List entry will expire at 2:01 PM on May 31. However, scheduler checks for expired entries at 00:00 every day and changes the state of the entry to 'expired' at 00:00 June 1.

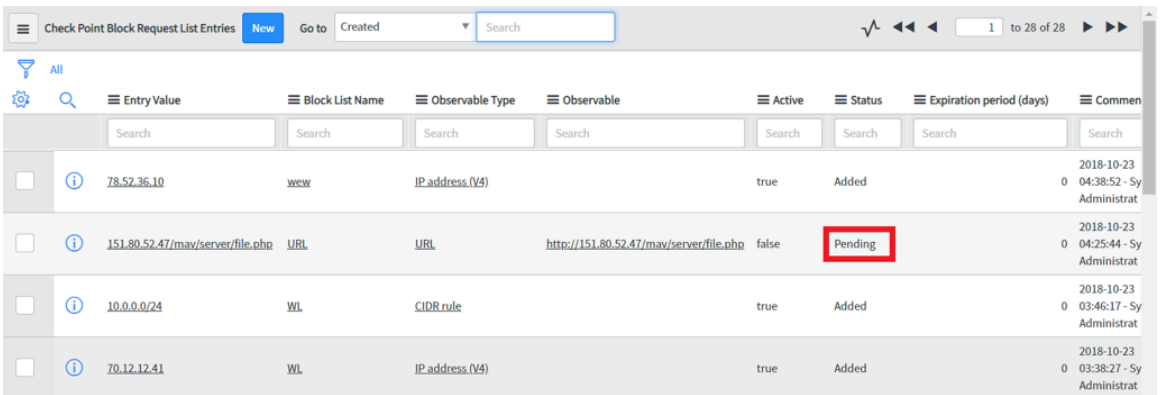
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Click **Submit**.
   If you have changed the default expiration period of the Block List entry, a warning confirmation dialog box is displayed indicating that the period differs from the selected Block List.



Option	Description
Yes	Confirms your expiration override, saves the record, and returns you to the Check Point Block List Entries. If you have email approval configured in your workflow, an approval email request is sent.
No	Cancels the override. At this point, you can change the value for the **Expiration period**. After changing the value, click Submit to return to the Check Point Block Entries list.

9. If not displayed, navigate to **Check Point Block Request List Entries**, and note that the status for the entry is **Pending**.



   The entry is now ready for approval.

Approve block list entries for the Check Point NGTP integration

An approval process for Block List entries is part of the preconfigured workflow. You approve Block List entries before the entries are activated on Block Lists. After you approve the Block List entry, the Gateway retrieves the entry, and your observable is blocked from that point forward.

Before you begin

- Approval for Block List entries is assigned to Security Incident Administrator (sn_si.admin) by default, but this authority can be assigned as required by your organization. In the following example, the ServiceNow AI Platform admin has approval authority.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

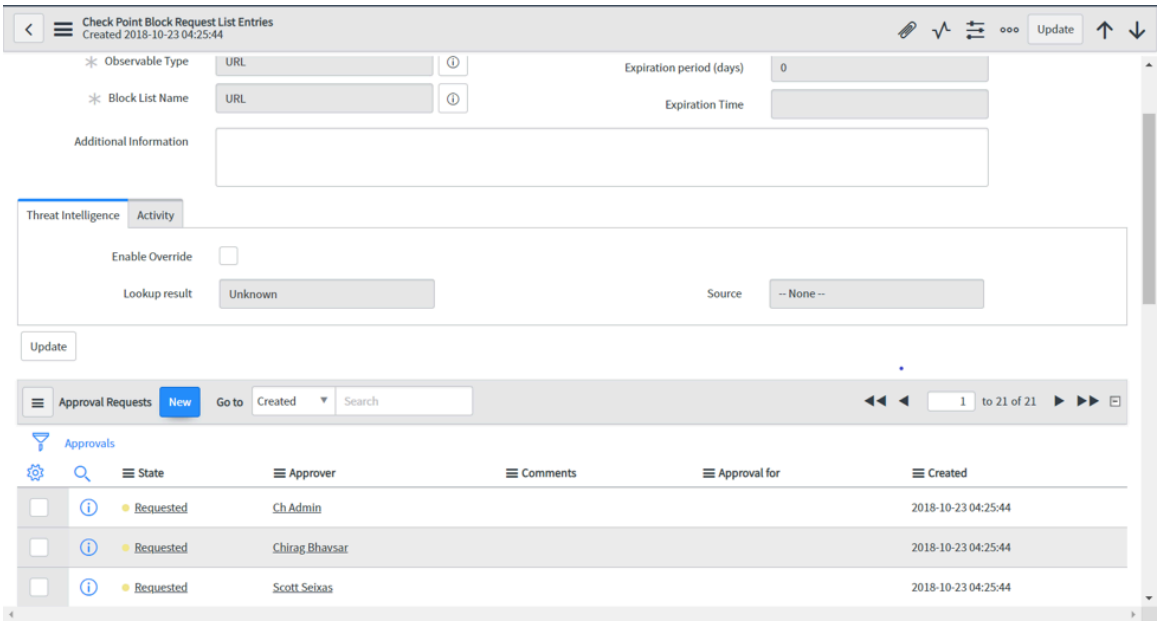
Role required: sn.si.admin

About this task

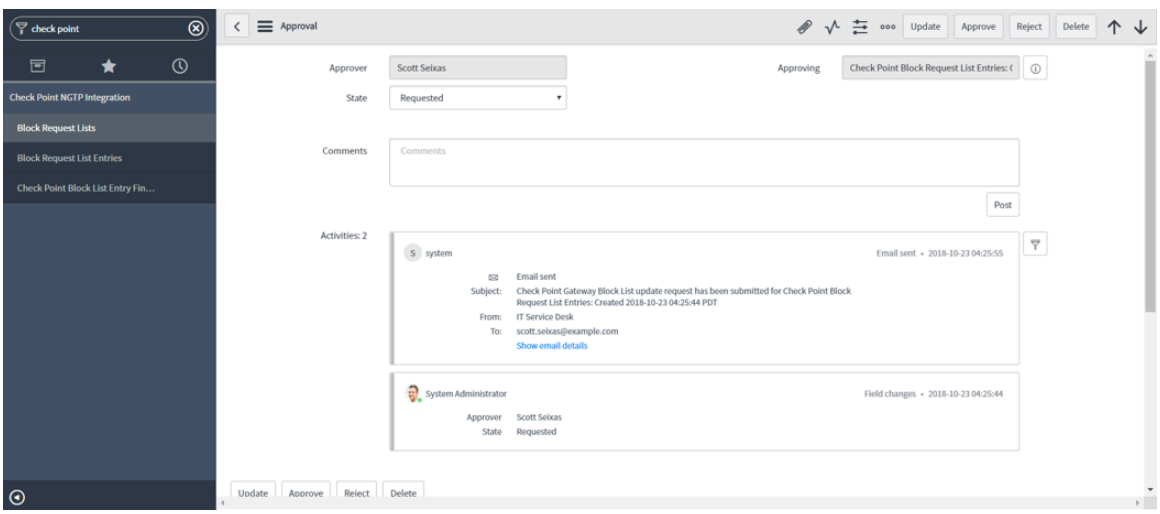
When the approval process is enabled, a Block List entry is not activated or deactivated on the Block List until it is approved.

Procedure

1. Navigate to **All** > **Check Point NGTP Integration** > **Block Request List Entries**, and open the Block List Entry record.
2. On the Block List Entry record, scroll to the **Approval Requests** section.



3. In Approval requests, click an item in the **State** column to open it.
   The approval record is displayed.

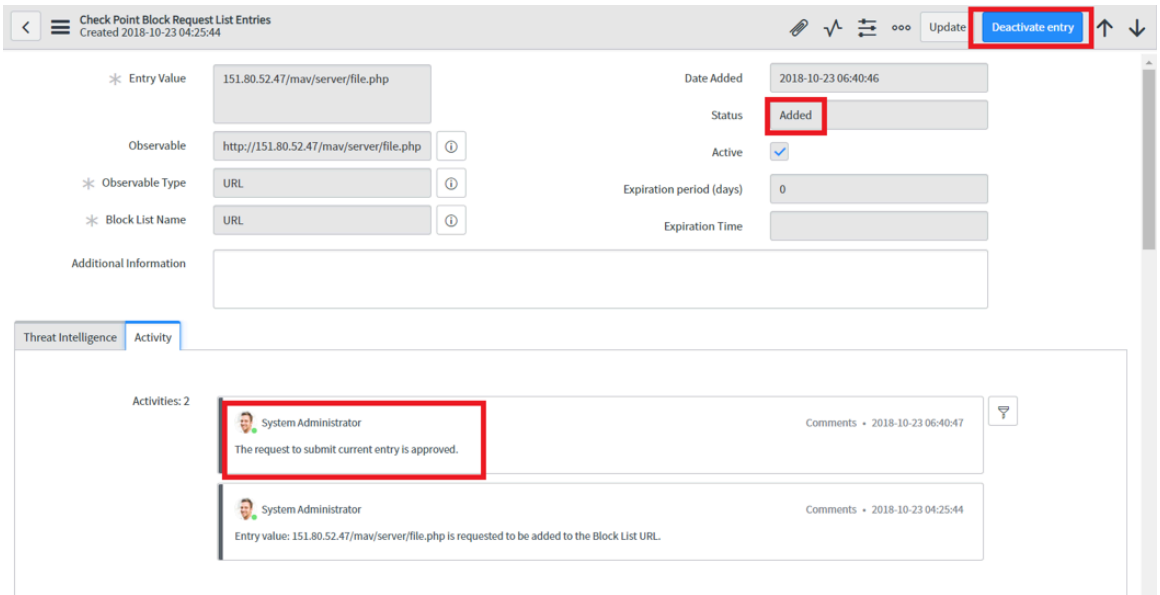


4. Choose one option for approving the Block List entry.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

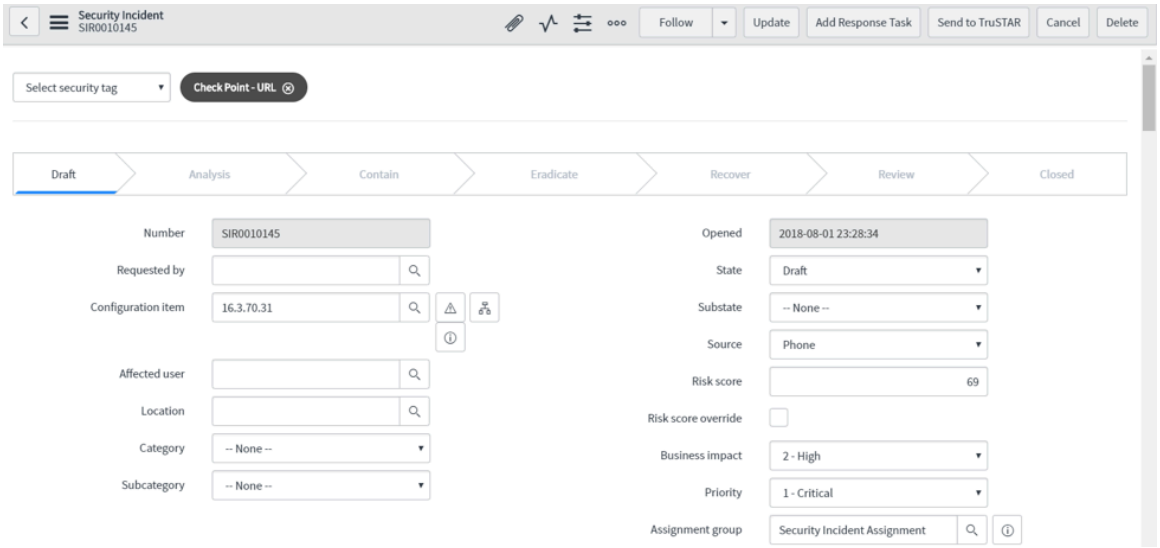
Option	Description
Approve	On the entry record, the Status field changes to Added, and the Active check box is selected. The Deactivate button is displayed and active. Work notes show that the request for the Block List entry has been approved.
Reject	On the entry record, the Status field changes to Rejected, and the Active check box is cleared indicating the entry is not blocked on the Gateway. Work notes show that the request for the Block List entry has been rejected.

After you have approved the Block List entry and it is activated, the Check Point next-generation firewall retrieves the Block List entry after the next retrieval interval. After the entry is retrieved, the observable is blocked from that point forward. In the following figure, note that the Active check box is selected, the status is Added, and the work notes indicate that the request has been approved.

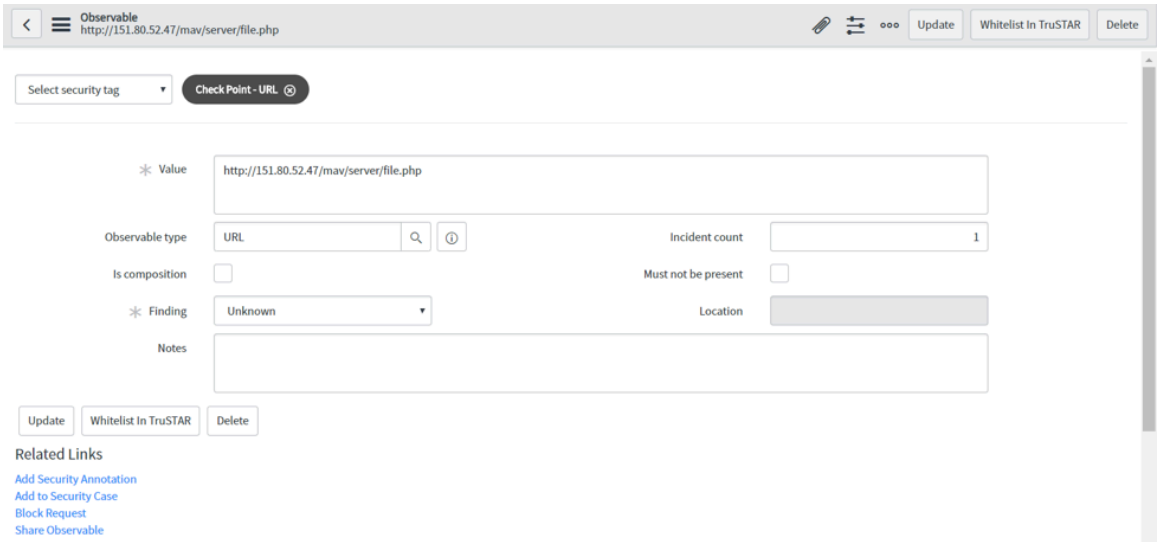


After the Block List entry is approved and activated, the security incident record is marked with a security tag. The tag is displayed at the top of the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The security tag is also displayed on the observable record.



Block list entry exceptions for the Check Point NGTP integration

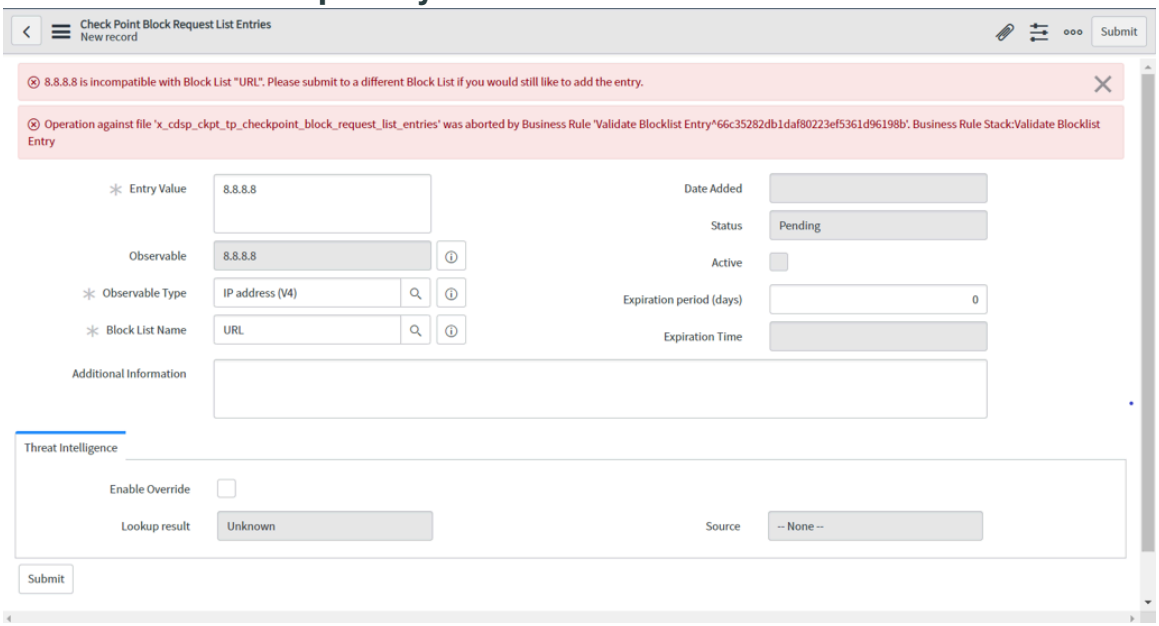
There are restrictions for adding Block List entries to Block Lists. If duplicate, compatibility, or CIDR (Classless Inter-Domain Routing) conflicts exist when you try to add Block List entries to Block Lists, error messages are displayed that help you resolve these errors.

Compatibility exception

Each Block List only accepts entries that are compatible with its observable type. If you create a Domain Block List and you try to attach an IP address observable to it, an incompatible error message is displayed. For example, a domain Block List can only accept domain observables, as illustrated in the following figure.

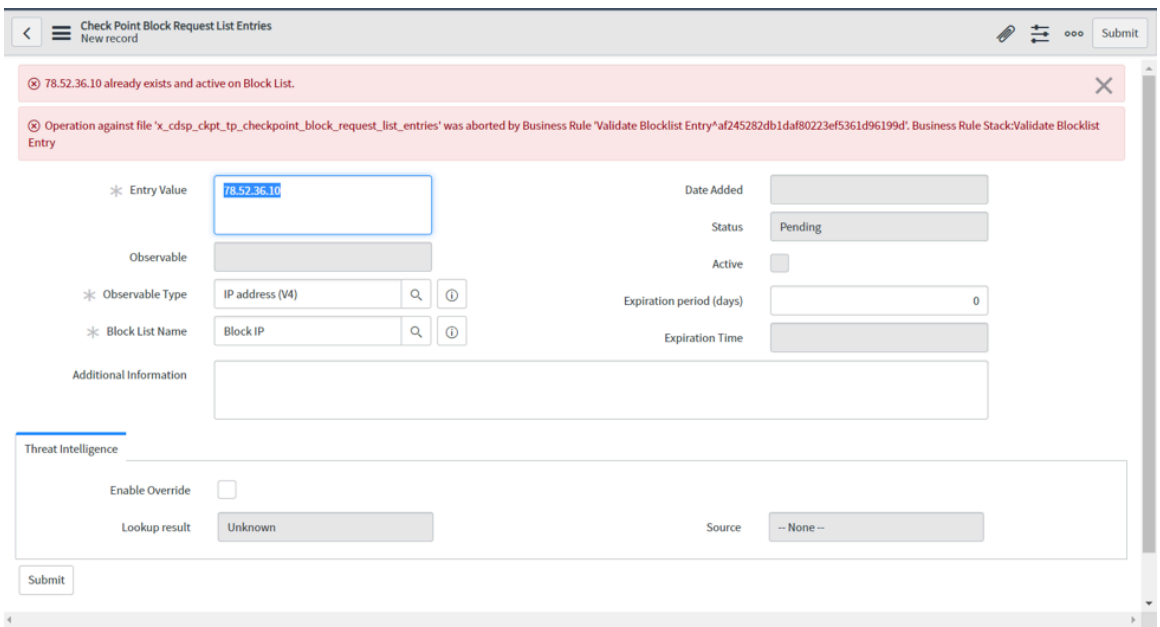
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Block List form with compatibility errors



Duplication exception

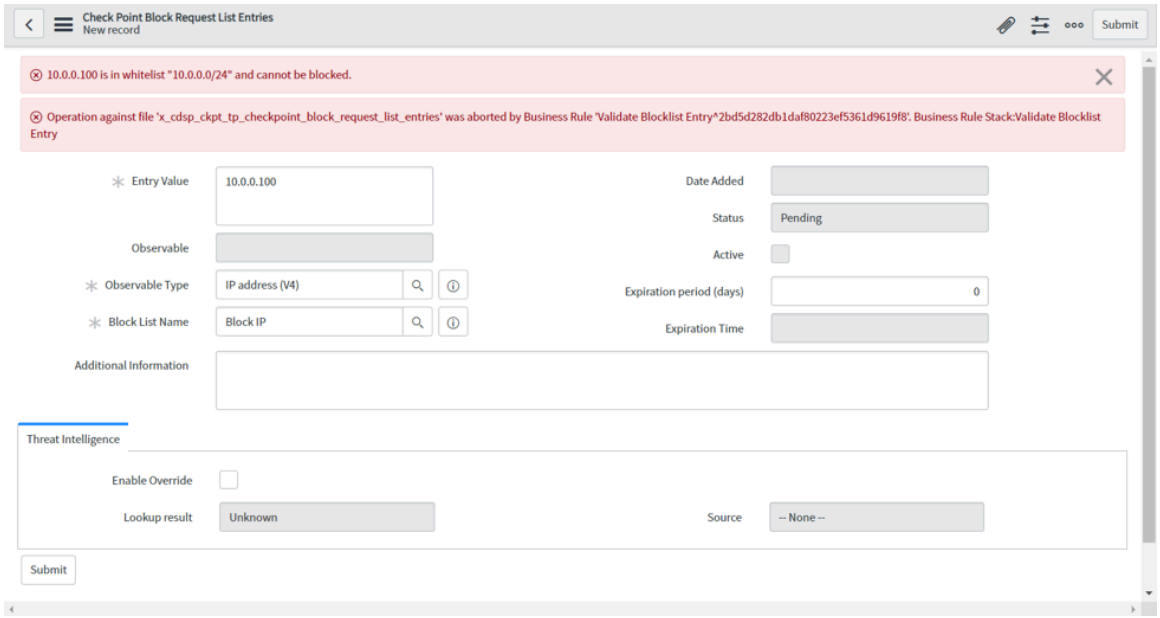
An observable cannot be activated on multiple Block Lists of the same observable type. If a URL observable is already activated on a URL Block List, and you try to activate the same observable on a Phishing URL Block List, a duplication error message is displayed.



CIDR (Classless Inter-Domain Routing) exception

If you attempt to attach a single IP address to an allow list, and this IP address is part of a CIDR observable already on a Block list/Allow list, a CIDR conflict error is displayed. This error indicates that the single IP address is already included on the Block list or allow list as part of the CIDR observable. For example, 192.168.24.25 is part of the CIDR block 192.168.0.0/22.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Edit the security tag name for the Check Point NGTP integration

If the Display tag check box is selected when you create the Block List record, you can edit the tag names and colors of the security tags. Security tags help you track observables that are already blocked.

Before you begin

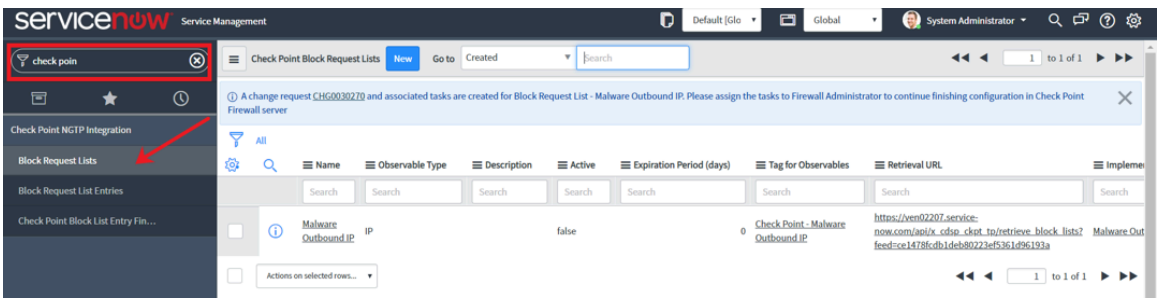
Role required: sn.si.admin

About this task

Security tags help you quickly identify which security incidents have observables on a block list. Tags also help you identify whether an observable is already blocked, or, if it has been removed from a Block List. By default, the color of the security tag is black for block list entries and gray for allow list entries. You can change the names and colors of the tags to help you recognize certain tags more easily.

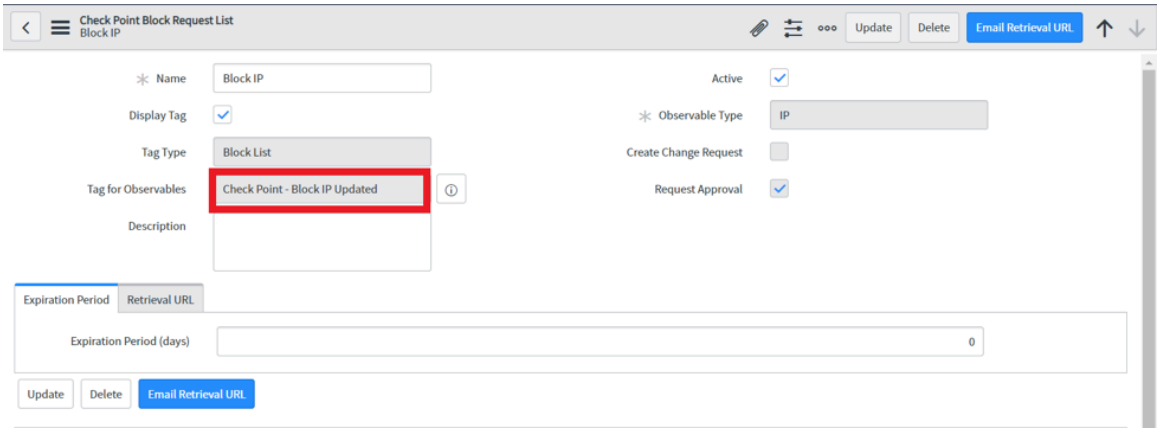
Procedure

1. Navigate to **All** > **Check Point NGTP Integration** > **Block Request List Configuration**.

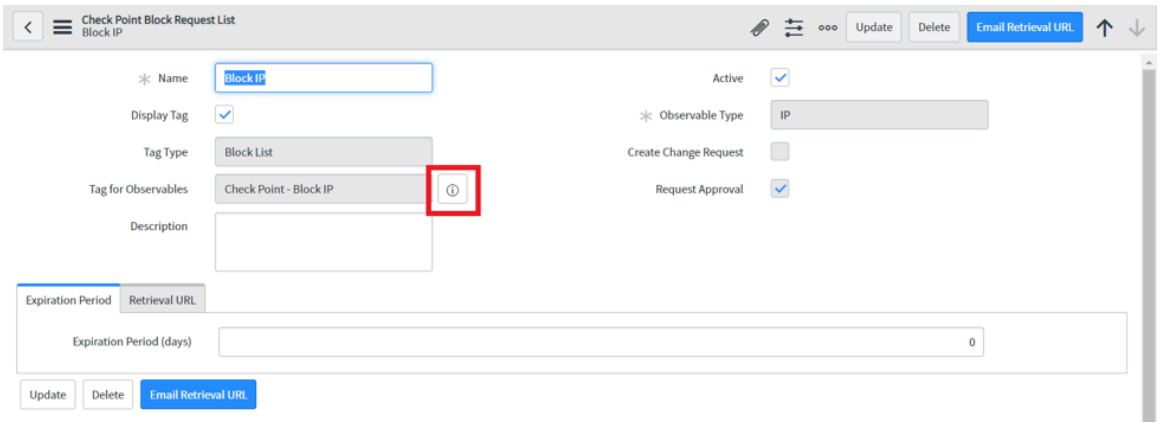


2. Click an item in the **Name** column to open it.
   The Block List record is displayed. By default, the security tag name is the same value you entered in the Name field of the Block List when you created it. By default, the name also includes a Block List prefix, for example, Block List – Malware Malicious URLs.

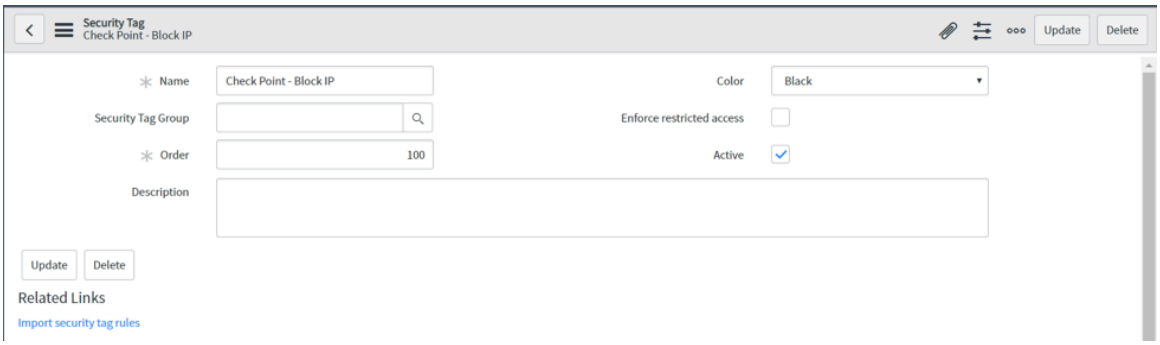
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click the information icon next to tag for observables then Open record.



The Security Tag Form is displayed.

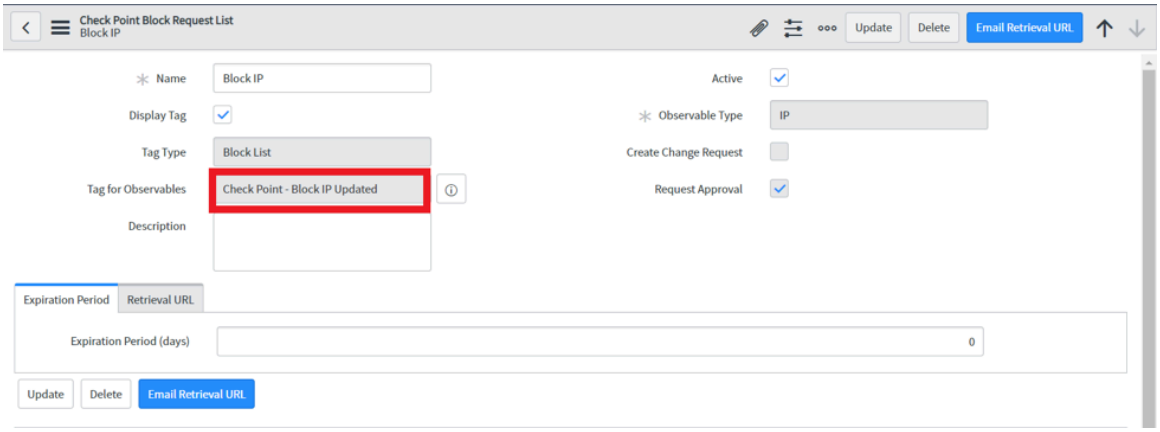


4. In the **Name** field, modify the security tag name.

5. Click **Update**.
The updated Block List record is displayed with the modified tag name.

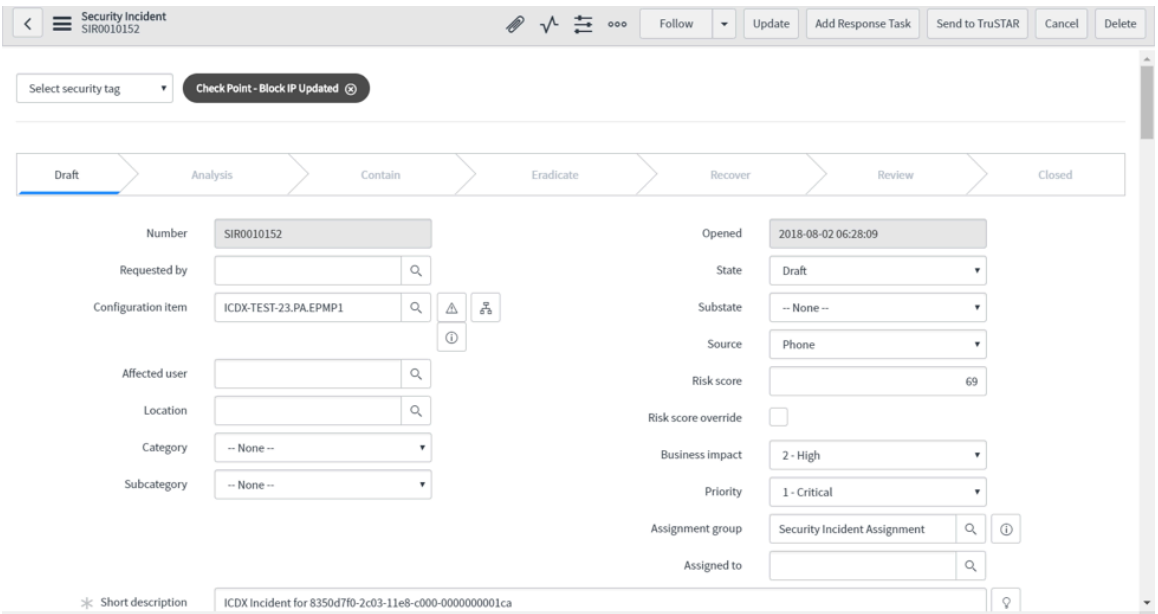
Note: In the following example, Outbound has been added to the tag name. Keep the Check Point prefix in your new tag name to help you identify the tag is associated with the Check Point next-generation firewall integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The security tags are displayed for each observable type (IP, URL, Domain) on the Security Incident record and the Observable record each time that observable is added to Block List.

Result



If an observable has already been added to a Block List, and a security tag is displayed on a security incident for this observable, the Block List security tag also is displayed automatically on any subsequent security incident records that are created. This duplication tells you that the observable is already on a block list. You do not need to add this observable and re-block it.

When an observable is no longer blocked, a security tag is not displayed on the security incident record or the observable record. In this instance, no security tag indicates that the expiration date of the observable may have passed, or the observable has been deactivated from a Block List.

Uninstall the Check Point NGTP integration

If you want to uninstall Check Point NGTP Integration from your ServiceNow AI Platform instance and remove all remnants from the integration, refer to the ServiceNow documentation site for instructions on uninstalling applications.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CrowdStrike Falcon Host integration

The CrowdStrike Falcon Host integration allows you to push observables in a security incident into a watchlist, making them able to generate additional alerts. This integration is an implementation of the CrowdStrike Falcon Host - Publish to Watchlist workflow.

Explore

Security Incident Response integrations

Set up

Get started with the CrowdStrike Falcon Host integration

Use

Perform lookups on observables

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Get started with the CrowdStrike Falcon Host integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the CrowdStrike Falcon Host integration. Before you can use the CrowdStrike Falcon Host integration, you must download it from the ServiceNow Store and then add a user name and password.

Before you begin

- If you are upgrading CrowdStrike Falcon Host integration from a previous version, then you must delete the existing configuration and set up a new configuration. The new integration supports OAUTH2 authentication. This update requires you to enter the **API Client ID** and the **API Client Secret** to authenticate and complete the configuration.
- In the CrowdStrike Falcon Host portal **API Scopes**, enable the **Read** and **Write** setting for **IOCs (Indicators of Compromise)**.

Role required: sn_si_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.
3. In the CrowdStrike Falcon Host card, click **Configure**.
4. On the form, fill in the fields to complete the configuration:

CrowdStrike Falcon Host Configuration

Field	Description
Name	Name of the integration, for example, `demo - 1`.
API Client ID	The client ID that you obtain from the settings section of your account profile in CrowdStrike Falcon Host portal.
API Client Secret	The client secret key that you obtain from the settings section of your account profile in CrowdStrike Falcon Host portal.

5. Click **Submit**.

Result

After it is configured, the CrowdStrike Falcon Host integration can be selected for publishing observables to watchlists in Security Incident Response.

Security Operations CrowdStrike Falcon Host - Publish to Watchlist Flow

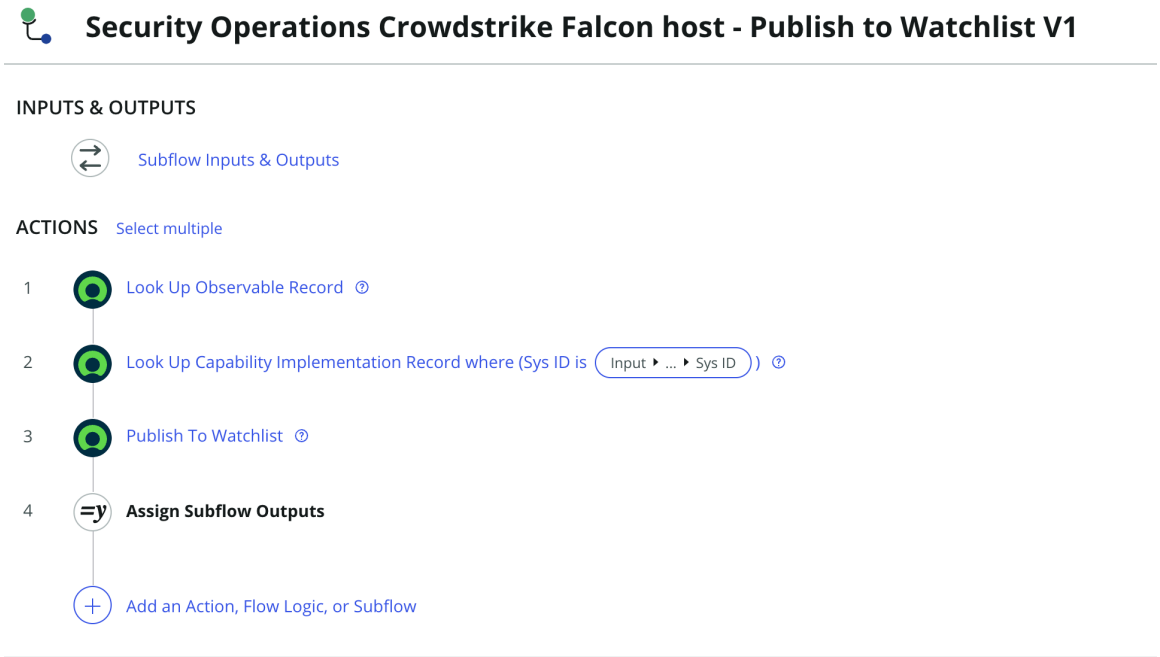
The **Security Operations CrowdStrike Falcon Host - Publish to Watchlist** flow designer is used to specify the watchlist for generating alert or events. The alerts and events are displayed in the CrowdStrike Falcon Host system based on how it is configured.

Publish to Watchlist Flow

This flow designer is triggered by the Security Operations Integration- Publish to Watchlist capability when you select one or more observables associated with a security incident, and use the Publish to Watchlist UI action to push the observables to a watchlist. The observables can then be used to generate

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

additional alerts. For more information, see Publish observables to a third-party



watchlist.

CrowdStrike Falcon Insight for Security Operations integration

With the CrowdStrike Falcon Insight for Security Operations integration, you can make remediation actions on the endpoints in real time, use profiles to gather details about the host, and make specific queries or actions on the endpoint using the ServiceNow AI Platform Security Incident Response product.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The CrowdStrike Falcon Insight for Security Operations integration works with the ServiceNow AI Platform so that you can get additional insight into the scope of an incident. The CrowdStrike Falcon Insight captures all relevant endpoint event activities, you can use the ServiceNow AI Platform to focus on investigations and remediation actions.

Learn about this integration

Document identifier	Document title
ServiceNow product documentation website	ServiceNow Product Documentation website
CrowdStrike Falcon Insight for Security Operations	Getting started with the CrowdStrike Falcon Insight integration

Getting started with the CrowdStrike Falcon Insight integration

You can activate and set up the CrowdStrike Falcon Insight to interface with your ServiceNow AI Platform instance and Security Incident Response product.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: admin

Before you can use CrowdStrike Falcon Insight for the Security Operations integration, you must download it from the ServiceNow Store.

About this task

Checklist

Setup task	Description
Assign and verify the required ServiceNow AI Platform and Security Incident Response roles.	These roles are required for configuration and verification of the expected results: • The admin role installs the integration from the ServiceNow Store and assigns the sn_si.admin role. • The sn_si.admin role configures the integration, creates and activates profiles, and then assigns the sn_si.analyst role. • The sn_si.analyst role responds to security incidents, launches profiles manually, and can submit requests for such actions as isolating the host and removing the host isolation for an approved group.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration.	The ServiceNow Integration Hub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] plugin is required. This plugin enables the execution of IntegrationHub actions and flows: The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications that are required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, you must install and activate each application one at a time in the following order to ensure a smooth installation: **1.** Security Incident Response Dependency (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	4. Security Support Orchestration **5.** Threat Intelligence Support Common **6.** Trusted Security Circles **7.** Security Operations Setup Assistant **8.** Security Incident Response
Set up an approval group.	An optional approval capability is available for isolating host machines, restoring them to the network, and initiating sightings searches. To enable this option, you require prior approval from the sn_si.admin role before host machines are isolated and restored to your network, or when sightings searches are performed. If you require an extra level of control over these actions, enable the **Require approval** option when configuring the profile. The approval authority is assigned to the user with the sn_si.admin role. You can also reassign this approval authority to an approval group.
Assign and verify the CrowdStrike Falcon Platform roles.	The following roles are required on the CrowdStrike Falcon Platform for the integration configuration: • The Falcon administrator role is required to view, create, or modify API clients or keys. • The Real Time Responder – Administrator role is required for creating and executing custom scripts. • The Real Time Responder – Active Responder role is required for creating and executing custom scripts.
Verify that the custom scripts roles and permissions are enabled in the CrowdStrike Falcon Platform.	This integration uses CrowdStrike's custom scripts for few of the enrichment capabilities. • Verify that the Real Time Responder – Administrator and the Real Time Responder – Active Responder roles are available. • Verify that the **Default(Windows) policy** option is enabled in Configuration > Response Policies in the CrowdStrike Falcon UI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	• Verify that the **Real Time Response** and **Custom Scripts** under Real Time Functionality is enabled in the CrowdStrike Falcon UI.
Generate API clients and keys in the CrowdStrike Falcon Platform.	Create the CrowdStrike API clients or keys in the CrowdStrike Falcon Platform to use in the ServiceNow AI Platform integration configuration.

Create CrowdStrike API client and generate keys

Create the CrowdStrike API client and generate the client ID and key, which you use to configure the CrowdStrike Falcon Insight integration.

Before you begin

Role required: CrowdStrike Falcon administrator

Procedure

1. On the CrowdStrike Falcon Platform, navigate to **API Clients and Keys**.
2. In the OAuth2 API Clients table, click **Add new API client**.
3. Enter the following details to define your API client:

Field	Description
Client Name	Enter the client name. This field is required.
Description	Enter the description for the client name.
API Scopes	Defining the scopes is required. **Important:** Ensure that you enable the API account, and make sure that the following scopes are enabled for the API account: ○ Enable Read and Write scopes for Hosts API ○ Enable Read scope for Indicators API

4. Click **Add** to save the API client and generate the client ID and secret key.

Install and configure CrowdStrike Falcon Insight

Install and configure the CrowdStrike Falcon Insight for Security Operations application from the ServiceNow Store on your ServiceNow AI Platform instance.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can associate a capability with only one profile. You can't associate a capability with multiple profiles. When you configure CrowdStrike servers, you can't reuse a CrowdStrike capability with multiple profiles that share the CrowdStrike server. Your profiles can have the same CrowdStrike capability, each profile should use its own CrowdStrike server.

Procedure

1. Download the CrowdStrike Falcon Insight for Security Operations integration from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the CrowdStrike Falcon Insight for Security Operations integration tile, and click **Configure**.
4. On the form, fill in the fields to complete the configuration:

CrowdStrike Falcon Insight Configuration

Field	Description
Name	Name of the integration, for example, `demo - 1`.
CrowdStrike Falcon Insight API URL	Base URL that hosts the CrowdStrike API. Enter the URL with the HTTPS protocol. For example, https://api.crowdstrike.com.
Client ID	The client ID that you obtain from the settings section of your account profile in the CrowdStrike Falcon Insight portal.
Client Secret	The client secret key that you obtain from the settings section of your account profile in the CrowdStrike Falcon Insight portal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.

Result

After the integration is successfully validated and submitted, it's saved on the Security Integrations page as a tile. You can view the CrowdStrike Falcon Insight module in the application navigator.

Create an approval group

Create an approval group for the CrowdStrike Falcon Insight for Security Operations integration that can approve requests for isolating host machines, restoring them to the network, and initiating sightings searches.

Before you begin

You can't reassign the approval authority to a group, unless an approval group is available in your instance.

Note: The approvals option in the profile configuration appears only for Isolate Host and Remove Host Isolation capabilities.

Role required: admin

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. In the groups list, click **New**.
3. On the form, fill in the fields.

Approval group form

Field	Description
Name	Name of the group that you see when you submit an approval request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Group email	Group email distribution list or the email address of the point of contact, such as the group manager.
Manager	Name of the group manager. Click the search icon to view the list.
Parent	Name of the parent group, if associated with a parent.
Type	Categories of groups.
Vendors	vendor_manager role that you assign to users in your organization's vendor management process.
Description	Additional information about the group.

4. Click **Submit**.
   The new group is displayed in the Groups list.

   This group is available to process requests when you enable the **Require approval** option during the configuration of this profile.

   To monitor and process requests submitted by users with the sn_si.analyst role, each member of the approval group navigates to **My Approvals** tab in the ServiceNow AI Platform.

What to do next
The next step is to install and configure the CrowdStrike Falcon Insight application from the ServiceNow Store.

Create a capability profile for the CrowdStrike Falcon Insight integration

Create a profile and select the CrowdStrike Falcon Insight capabilities that you want the profile to run.

Before you begin
Role required: sn_si.admin

About this task
Consider why you want to create a profile before you add CrowdStrike Falcon Insight capabilities to it. The following table lists the capabilities that you must add to a profile when you want the profile to perform certain queries or actions.

You can create a single profile that runs queries for system details, lists logged-in users, fetches running services, fetches running processes, fetches network statistics, isolates the host, and removes the isolated host. Alternatively, you can create multiple profiles, each with its own single capability.

Note: Isolate host, remove isolation, and get file capabilities can’t be merged with any other capabilities while creating a profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Profile types and required CrowdStrike Falcon Insight capabilities

Profile purpose	CrowdStrike capabilities
Gather host details and logged-in users	• **Get Host Details** • **Get Logged On Users**
Fetch the network statistics, processes, and services running for a host	• **Get Network Statistics** • **Get Running Processes** • **Get Running Services**
Isolate a host	**Isolate Host**
Remove isolation for a host	**Remove Isolation**
Obtain a file from a host endpoint	**Get File**

Procedure

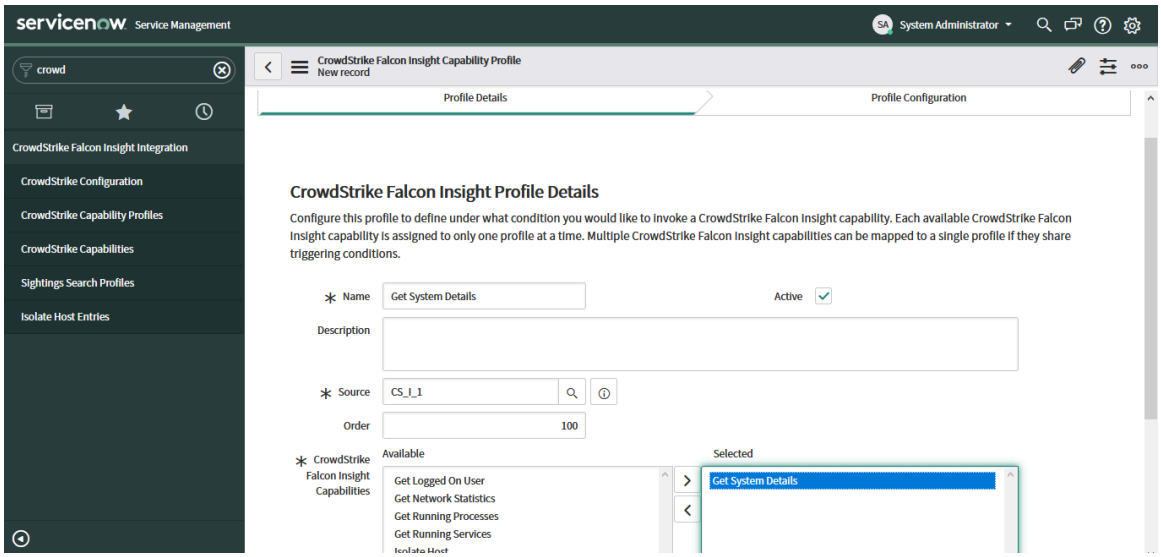
1. Navigate to **All** > **CrowdStrike Falcon Insight Integration** > **CrowdStrike Capability Profiles**.
2. Click **New**.
3. On the form, fill in the fields.

Field	Description
Name	Name for the new capability profile. This name helps you to identify the profile type and is also the default name for the security tag that is associated with this profile.
Active	Indicates if the profile is active or not. When the profile is active, it automatically triggers when a security incident is created that matches the filtering conditions that you've specified in the configuration.
Description	Unique description for the capability profile.
Source	Name of the server. You can only view previously configured servers from the list.
Order	Flow priority. The value for this field indicates the order that flows are executed when two or more profiles share triggering conditions. The flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Default: 100
CrowdStrike Falcon Insight Capabilities	Capabilities of the CrowdStrike Falcon Insight profile. Select the capabilities that you want for this profile from the **Available** to the **Selected**column.

The following example shows a complete form for a profile with the Get System Details capability.



4. Click **Next**.

What to do next

Now you canconfigure your profile. Ensure that you have reviewed the concepts for configuring profiles and trigger conditions before you configure the profile.

Configure profiles and security incidents for the CrowdStrike Falcon Insight integration

Configure your profile settings so that the profile triggers only under the conditions that you set.

Before you begin

Role required: sn_si.admin

About this task

Define the conditions that automatically trigger the CrowdStrike Falcon Insight capabilities that you selected for the profile. You can also select an alternate input field for the Configuration Item (CI) field. In this alternate field, you can set filtering conditions so that only those security incidents that are related to your triggering event automatically trigger the profile.

Note: Navigate to the Profile Configuration page only after you enter the profile details. For more information, see Create a capability profile for the CrowdStrike Falcon Insight integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

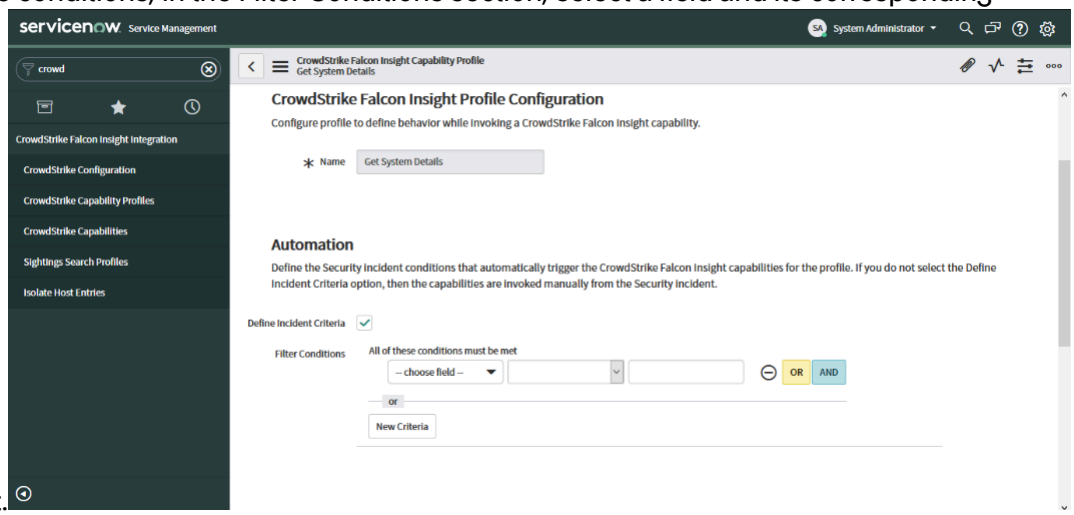
1. In the Profile Configuration page, review and configure the following sections:

Define Incident Criteria (Automation)

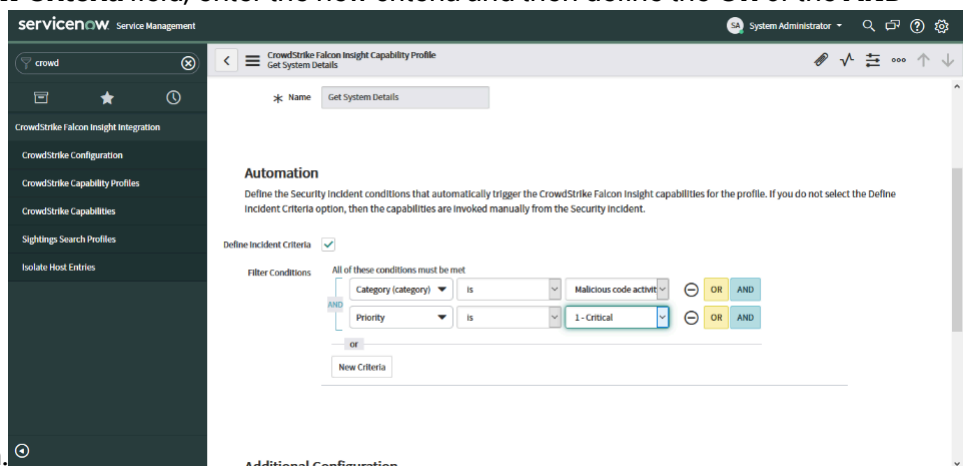
Define the security incident conditions that automatically trigger the CrowdStrike Falcon Insight capabilities for the profile. If you don't select the **Define Incident Criteria** option, the capabilities are invoked manually from the security incident.

a. Select the **Define Incident Criteria** option.

b. To define the conditions, in the Filter Conditions section, select a field and its corresponding requirement.



c. In the **New Criteria** field, enter the new criteria and then define the **OR** or the **AND** condition.

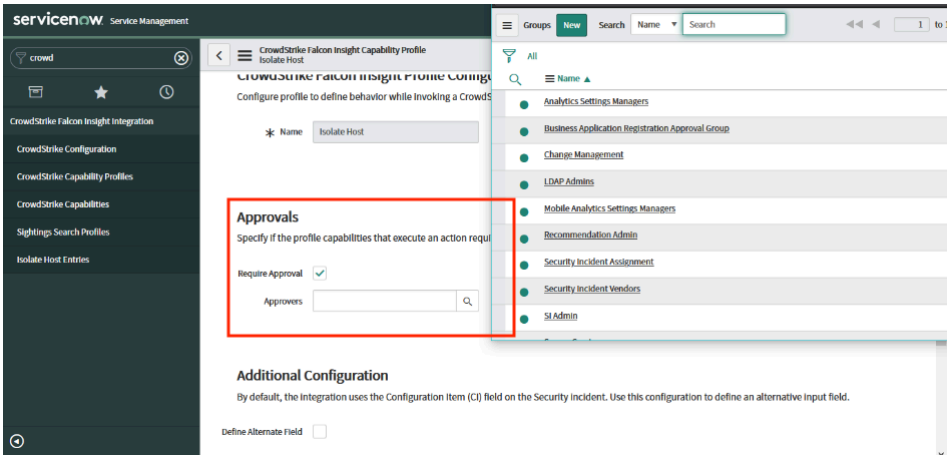


Approvals

To provide an extra level of control when you're using the CrowdStrike Falcon Insight capabilities, select the **Require Approval** option. The approvals option in the profile configuration appears only for the Isolate Host and Remove Host Isolation capabilities.

Note: The approval authority is assigned to the user with the sn_si.admin role. You can also reassign this approval authority to an approval group. For more information, see set up an approval group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Additional Configuration

Select an alternate field on the security incident to display any matching CI data that you find while scanning your assets. By default, the integration uses the Configuration Item (CI) field on the security incident.

a. Select the **Define Alternative Field** option.

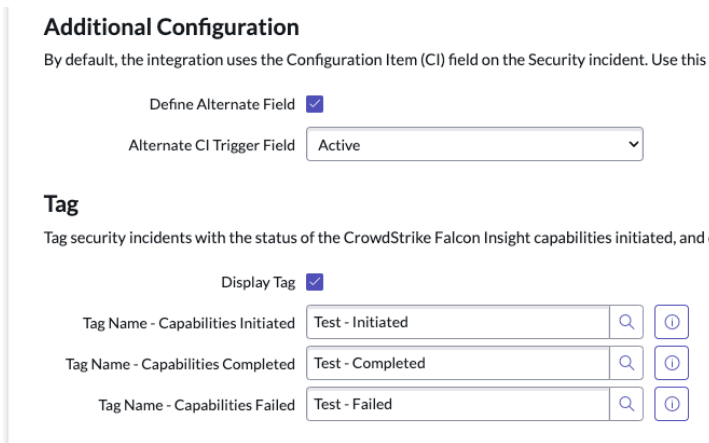
b. In the **Alternate CI Trigger Field**, select an input field.

> **Note:** For more information, see Understand how trigger conditions work with a configuration item for a profile.

Tags

To tag security incidents with the CrowdStrike Falcon Insight Capabilities- Initiated, and Capabilities-Completed, and Capabilities-Failed tags, select the **Display Tags** option. By default, this option is disabled for all profiles.

> **Note:** These tags are provided with the base system. You can create your own tags if required.



2. Click **Done**.

How trigger conditions work with a configuration item for a profile

You can configure the profile settings so that a profile runs only when a set of specific conditions is met or you can set up a profile to search for specific field values on a security incident.

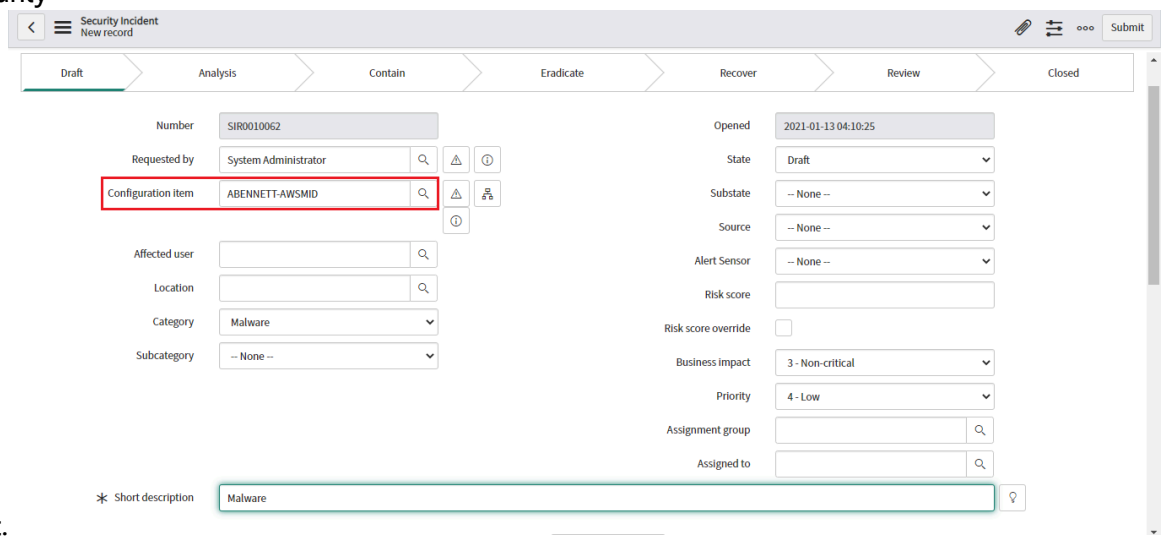
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you create a profile and select the CrowdStrike Falcon Insight capabilities that you want the profile to run on, you can set trigger conditions so that your profile runs automatically when the default field values match the ServiceNow AI Platform security incident.

By default, the integration uses the **Configuration Item** (CI) field on a security incident. This field is used to match your asset IDs with the information that is stored in the ServiceNow AI Platform database. When a SIR security incident is created by a security event and a profile is activated, your assets are scanned for a matching value on the host name or an IP address.

When a matching value is found in the database, that data is gathered from the CrowdStrike Falcon Insight console and is pulled into your ServiceNow AI Platform instance where it is displayed on the related lists of a security incident.

The following example shows a Configuration Item field that is populated with a host name on a SIR security



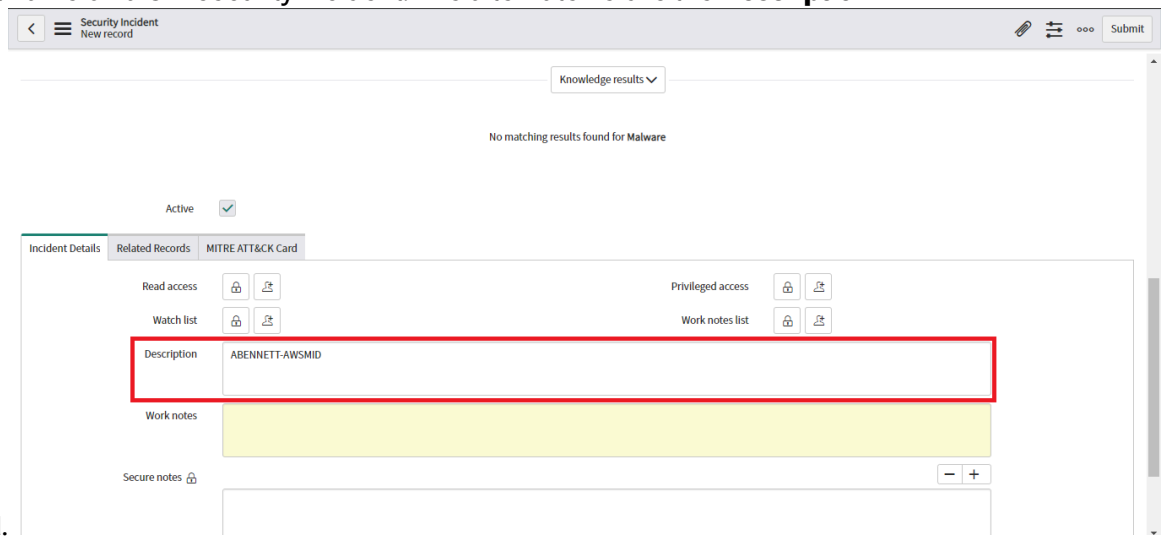
incident.

When the **Configuration item** (CI) field is not populated with a host name or an IP address that matches the database, you can select another field on the security incident to display any matching CI data that you find while scanning your assets.

When you are configuring the profile setup, you can select an alternate **CI trigger** field for endpoint identification to ensure that the CI data from the CrowdStrike Falcon Insight lookup is populated on the associated security incident. You can select any field on the security incident as an alternate CI trigger field, including custom fields that you create. If the CI field is not populated on the associated security incident when the incident is created, select the alternate CI field to ensure that your profiles get triggered.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows an alternate field that is populated with a host name on a SIR security incident. The alternate field is the **Description** field.



Verify CrowdStrike Falcon Insight profile trigger conditions

Test the profile and verify that the trigger condition filters that you have configured work as expected.

Before you begin

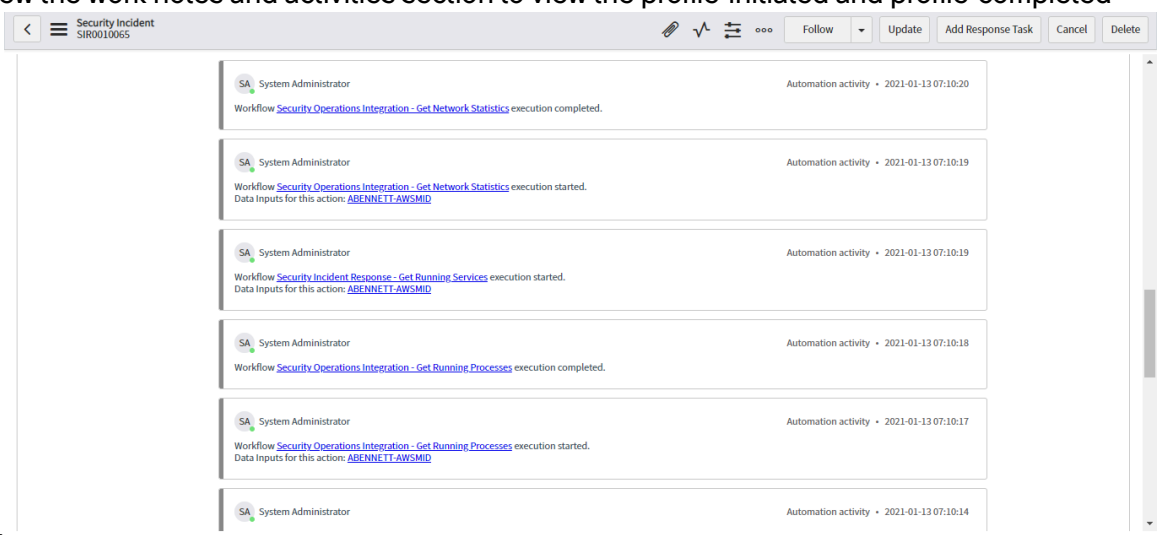
Role required: sn_si.admin

About this task

Activate the profile that is based on the configured trigger conditions you specified so that you can view the query results in the ServiceNow AI Platform security incidents.

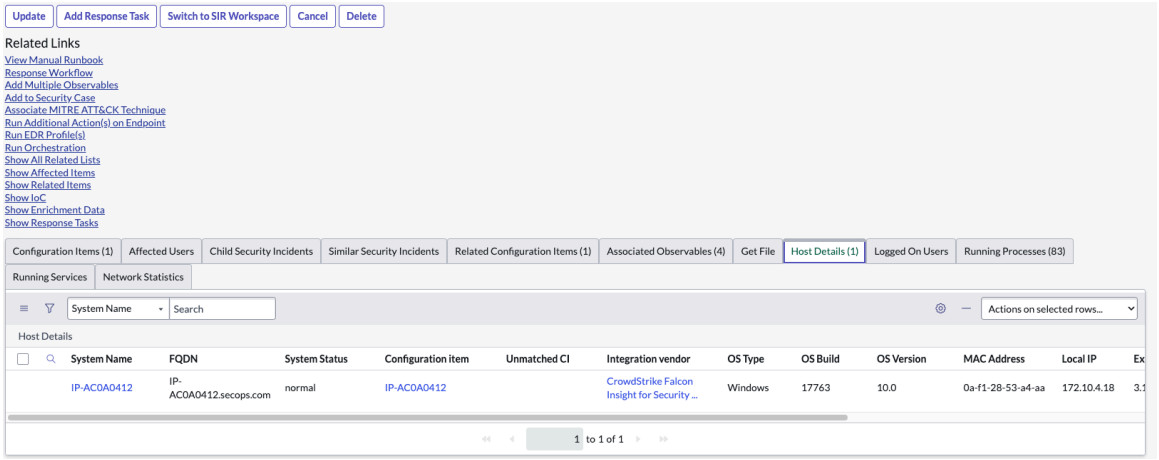
Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select **New** to create a security incident.
3. To create a security incident, fill in the required information and click **Save**.
4. Review the work notes and activities section to view the profile-initiated and profile-completed tags.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Review the details in the CrowdStrike Falcon Insight Details related lists such as Get File, Host Details, Logged on Users, Running Processes, Running Services, Network Statistics, and so on.



Trigger a CrowdStrike Falcon Insight profile manually from a security incident

Trigger a profile manually after you review a security incident.

Before you begin

Role required: admin

About this task

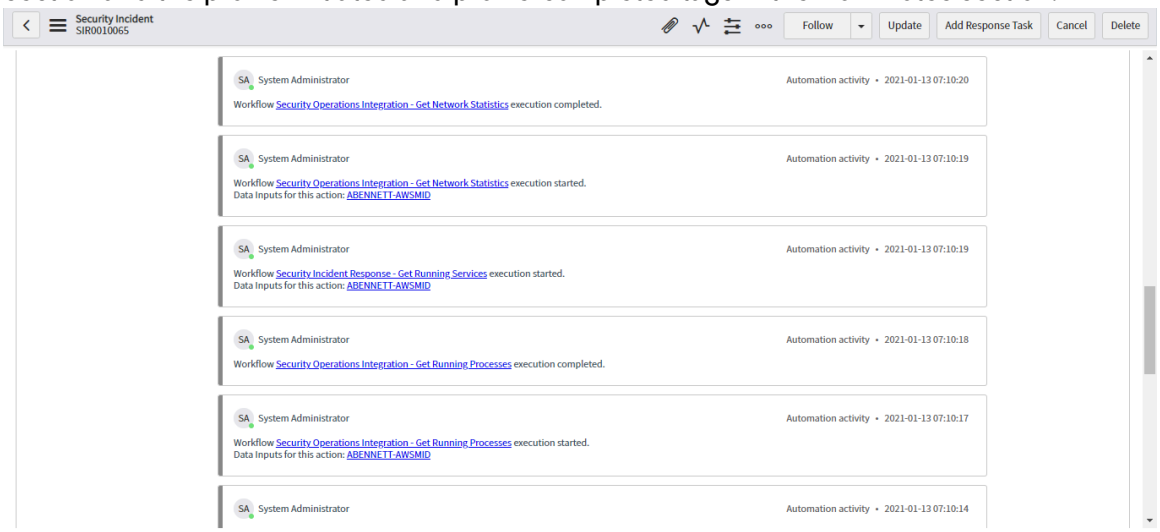
Once you activate the profile, based on the configured trigger conditions, you can view the query results in the ServiceNow AI Platform security incidents. CrowdStrike Falcon Insight also enables you to run individual capabilities on Configuration Items (CIs) without using a profile.

Procedure

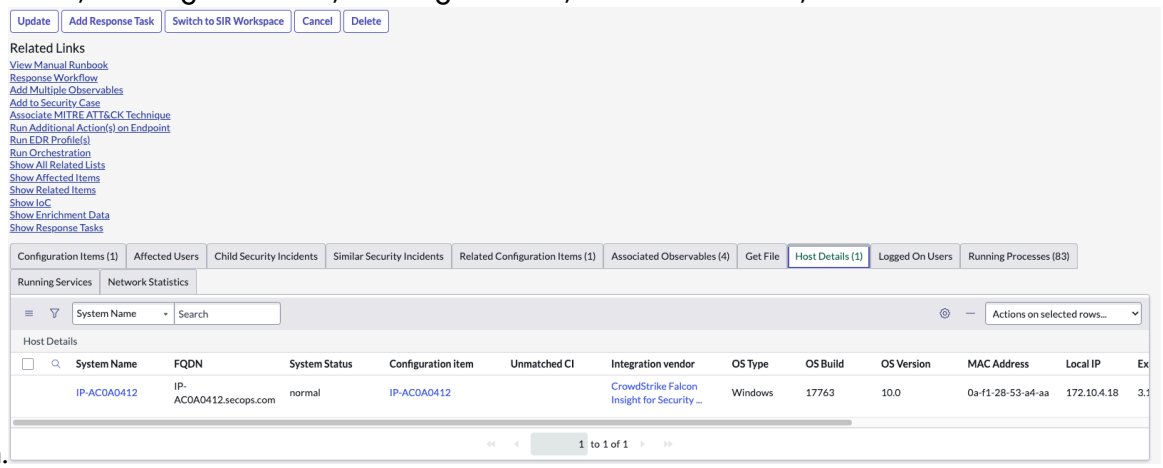
1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the CrowdStrike Falcon Insight information.
3. In the related lists section, select **Run EDR Profile(s)**.
4. Browse and select a profile from the list of available profiles.
5. Select **Include Related CI** to run this profile on all the related CIs of the profile.
   For example, if there are five CIs associated with the security incident, then the selected profile runs on all the five CIs.
6. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected profile is triggered manually. You can review the work notes and activities section and the profile-initiated and profile-completed tags in the work notes section.



7. The results appear in the form of related lists such as Get File, Host Details, Logged on Users, Running Processes, Running Services, Network Statistics, and so on.



8. To run individual capabilities on a CI, perform the following steps:

   a. In the Configuration Items related list, select the required CI.

   b. Click the **Actions on selected rows...** drop-down list, and select the required capability that you want to run for the selected CI.
   For example, Isolate Host.

   c. Look up the required capability implementation for the CI using the search option, and select **CrowdStrike Falcon Insight Isolate Host**.

   d. Click **Isolate Host** to run it on the selected CI.

Create and configure a profile for the sighting search

Use sightings searches for CrowdStrike Falcon Insight to locate infected machines across your organization's network and to address security incident response cases.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Select individual or multiple observables and perform a manual sighting search in CrowdStrike Falcon Insight to determine the prevalence of a threat over time.

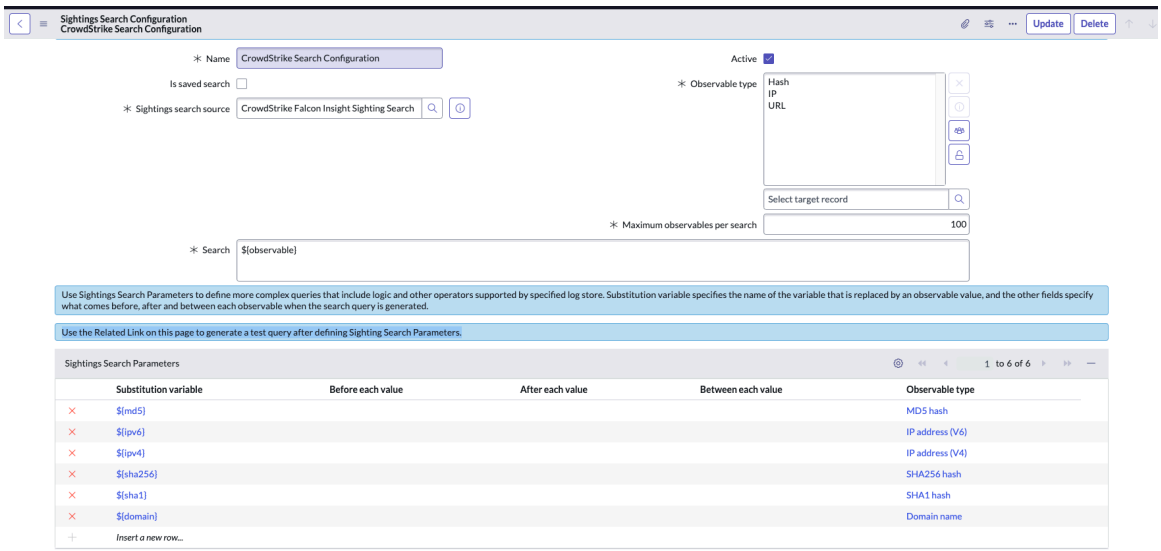
Procedure

1. Navigate to **All** > **CrowdStrike Falcon Insight Integration** > **Sightings Search Profiles**.
2. Click **New**.
3. Configure this profile to determine what servers to search for a specific CrowdStrike Falcon Insight search capability.
4. On the form, fill the fields:

Field	Description
Name	Name for the Sighting Search profile.
Is saved search	Saved search configuration is created if you select this option.
Sightings search source	The source for the sightings search. Select the **CrowdStrike Falcon Insight Sighting Search** as the source.
Active	Option to indicate if the additional is active or not.
Observable type	CrowdStrike Falcon Insight integration supports the following Observable types: ○ Hash ○ IP ○ URL Sighting search is supported for the following Observables types: ○ Domain name ○ IP address (V4) ○ IP address (V6) ○ MD5 hash ○ SHA1 hash ○ SHA256 hash
Maximum observables per search	Maximum number of observables that you can view from a search query.
Search	The default search string is `$(observable)`, but you can define your own search query by specifying parameters that are supported by the CrowdStrike Falcon Insight integration.
Sightings Search Parameters	Parameters to define more complex queries that include logic and other operators supported by the specified log store

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	You can use the Related Links at the bottom of the page to generate a test query after defining Sighting Search Parameters.



5. Click **Submit**.
   The configuration is complete and you can invoke the sightings search from the ServiceNow AI Platform security incident.
6. To verify the configuration and run a sighting search, perform the followings steps:

   a. Open a security incident, scroll to the bottom of the security incident, and click **Show all Related Lists**.

   b. If you select one or more Configuration Items (CI) from the **Running Processes** related lists.

   > **Note:** If you run a sighting search for a CI from the Running Processes related list, then it will only be a Process Hash sighting search.

   c. Click the **Actions on selected rows...** drop-down list, and select **Run CrowdStrike Sightings Search**.

   d. Look up the required Sighting Search Profile using the search option.

   e. Select the required Sighting Search Profile, and click **Submit**.

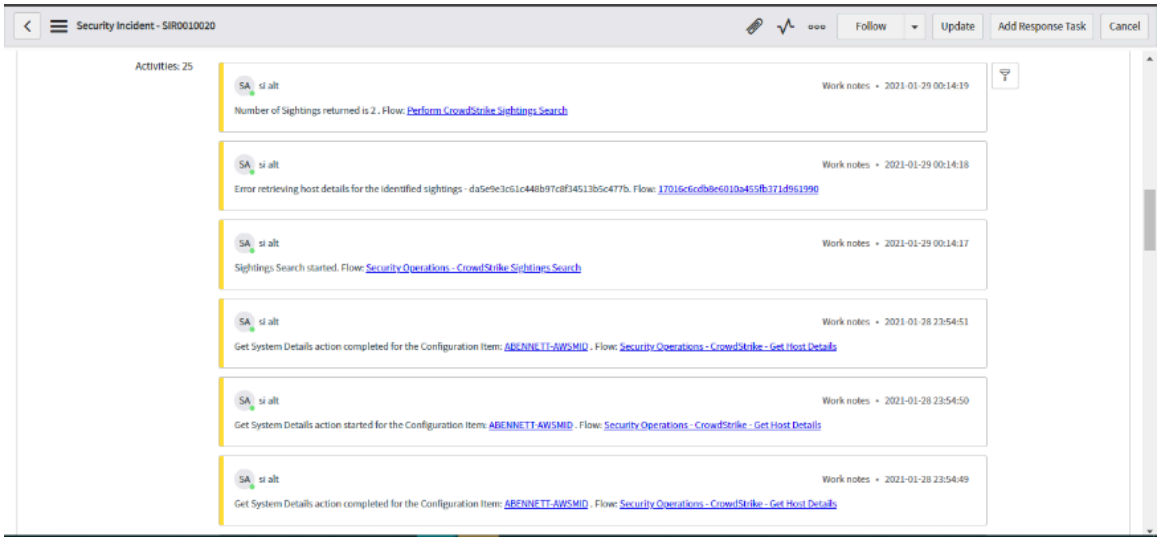
   f. If you select one or more Observables from the **Associated Observables** related lists.

   g. Click the **Actions on selected rows...** drop-down list, and select **Run Sightings Search**.

   h. In the time frame pop-up, select any random value and click **Search**.

   i. On completion of the search, validate the results and details in the work notes and related lists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



j. Select the **Sightings** tab to view the sighting details.

k. Click on the **Preview** icon next to the CI to view more information about CrowdStrike sighting details.

l. Click the **Sightings Search Details** to view the sighting search details, and click the **Sightings Search Results** tab for search results.

Configure and trigger additional actions in CrowdStrike Falcon Insight

The CrowdStrike Falcon Insight integration supports running additional actions like regular expression (regex). The CrowdStrike Falcon Insight integration provides 40 additional actions with the base system.

Before you begin

Role required: sn_si.analyst

Procedure

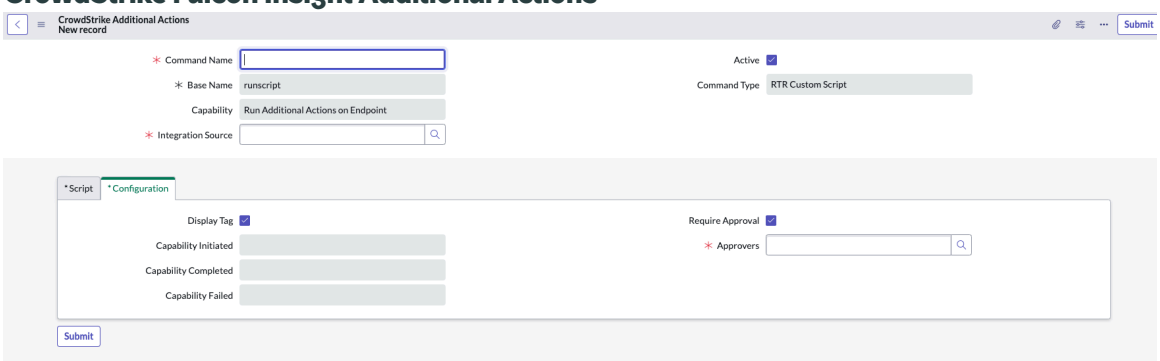
1. Navigate to **All** > **CrowdStrike Falcon Insight Integration** > **CrowdStrike Additional Actions**.
2. Click **New** to create your own additional action or select an existing action that comes with the base system.
   For example, let's create a new additional action.
3. On the form, fill the fields.

Field	Description
Command Name	Command name for the additional action. For example, reg set.
Base name	Base name for the additional action. This field is set by default. For example, reg.
Capability	Capability name for the additional action. This field is set by default. For example, Run Additional Actions on Endpoint.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Integration source	The source for the additional action. For example, CrowdStrike Falcon Insight Integration.
Active	Option to indicate if the additional is active or not.
Command Type	Command type for the additional action. This field is set by default. For example, RTR Custom Script.
Script	○ **OS Type**: Option to select the OS type for your script. Select one of the following: ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ **None** ○ **Script**: Option to enter your script if you selected one of the following OS, except for None option.
Configuration	○ **Display Tag**: Option to display the tag for the configuration. You can select the tag for the following fields: ▪ Capability - Initiated. For example, reg set - Initiated. ▪ Capability - Completed. For example, reg set - Completed. ▪ Capability - Failed. For example, reg set - Failed. ○ **Require Approval**: Option to select an approver or group that needs to approve the configuration.

CrowdStrike Falcon Insight Additional Actions

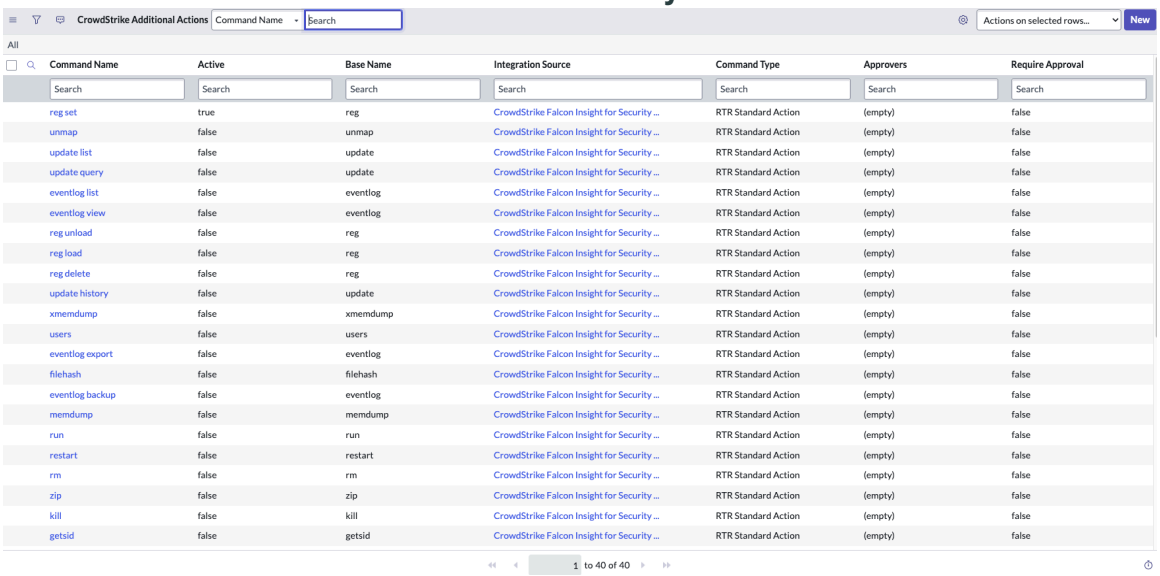


4. Click **Submit**.
5. You can also choose from the following existing additional actions.
   There are 40 additional actions that come with the base system, which you can use to perform additional configurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Ensure that you open the CrowdStrike Additional Actions list and set the required additional action to **true**, else the additional action will not be available in the workspace.

List of additional actions that comes with the base system



CrowdStrike Additional Actions | Command Name | Search | Actions on selected rows... | New

All

Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Navigate to **Security Incidents** > **Show All Incidents**.
7. Select the security incident that you want to review with the run additional actions on Endpoint.
   a. In the related links section, click **Run Additional Actions on Endpoint**.
   b. Browse and select the required capability.
   For example, click **reg set** capability.
   c. Select **Include Related CI** to run the additional actions on all the related CIs of the Endpoint.
   d. You can define the **Subkey** for the run the additional actions on Endpoint.
   This Subkey can be a HKLM/Software/new key.
8. To initiate the run additional actions on endpoint, click **Run Additional Action**.
9. View the automation activities of the execution, and validate them.
10. Validate the status of the action on the Additional Actions on Endpoint related lists.

Using CrowdStrike Falcon Insight integration in Analyst Workspace

Use the CrowdStrike Falcon Insight integration to leverage the CrowdStrike Falcon Insight capabilities on the SIR Analyst workspace.

Before you begin

Role required: sn_si.admin

Before you use CrowdStrike Falcon Insight integration on the Security Incident Response workspace, you must download it from the ServiceNow Store and configure it. For more information, see Getting started with the CrowdStrike Falcon Insight integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can use the CrowdStrike Falcon Insight integration to make remediation actions on the endpoints in real time, use profiles to gather details about the host, and make specific queries or actions on the endpoint using the Security Incident Response workspace.

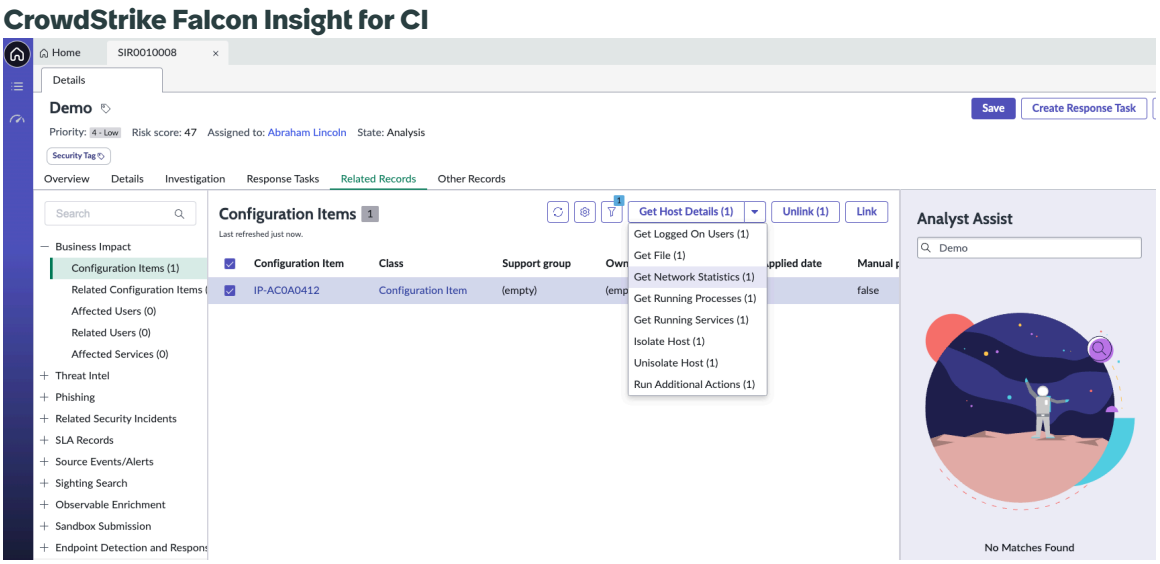
The CrowdStrike Falcon Insight integration enables analysts to use the following CrowdStrike Falcon Insight capabilities on the Security Incident Response Analyst workspace:

- **Get Host Details**
- **Get Logged On Users**
- **Get Network Statistics**
- **Get Running Processes**
- **Get Running Services**
- **Isolate Host**
- **Remove Isolation**
- **Get File**

Procedure

1. In the SIR workspace, open the required security incident and select the **Related Records** tab.
2. You can use the CrowdStrike Falcon Insight capabilities on the Business Impact related list for analysis.

   a. Select a **Configuration Item**, and choose a capability from the dropdown list.



   b. Select the **CrowdStrike Falcon Insight** implementation, and click **Submit**.
   The Get Network Statistics capability is invoked on the CI. You can view the worknotes for the results and findings.

3. You can use the CrowdStrike Falcon Insight capabilities on the **Endpoint Detection and Reponse (EDR)** related list for analysis.

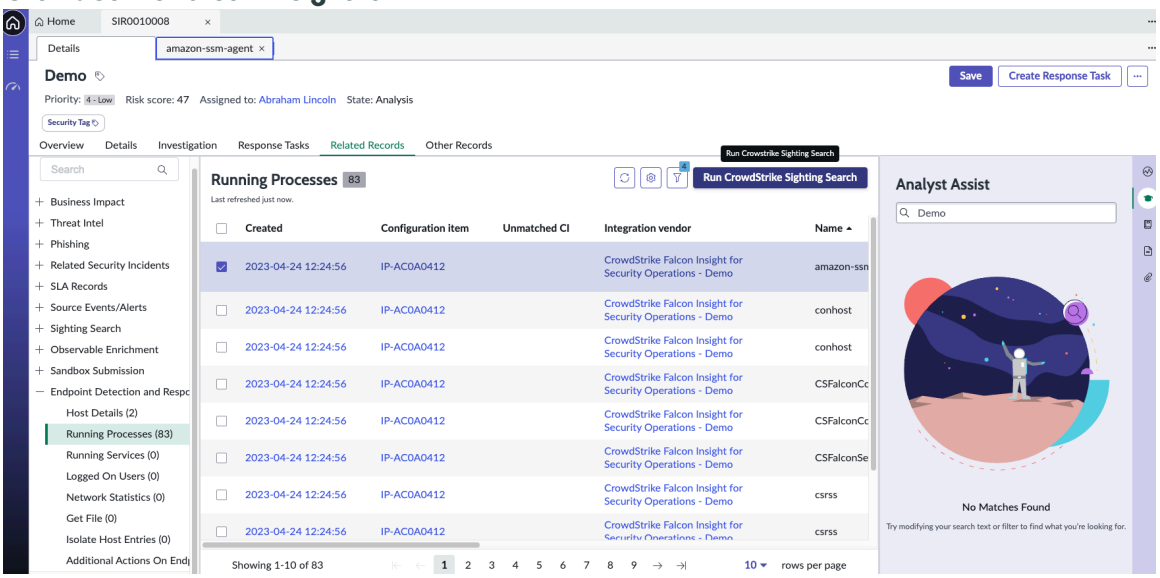
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In the Endpoint Detection and Reponse (EDR) related list, choose an EDR from the list.

b. Click on a particular Running Process to view the CrowdStrike Falcon Insight running process details.

c. To run a CrowdStrike Falcon Sighting Search on a particular running process, select the running process and click **Run CrowdStrike Sighting**.

CrowdStrike Falcon Insight for EDR



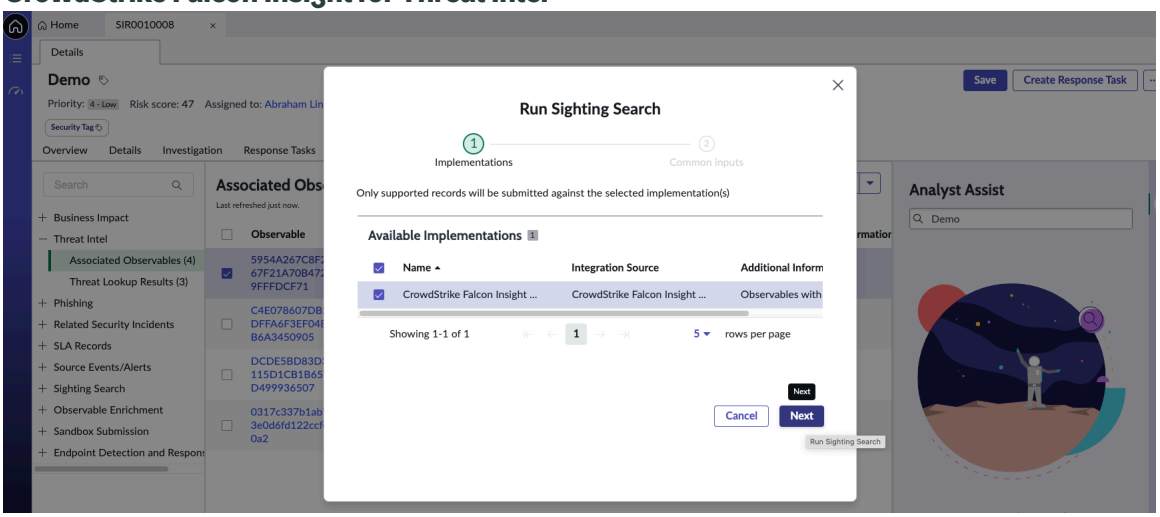
d. Select the **CrowdStrike Falcon Insight** implementation, and click **Run Search**. Then a hash sighting search is run on the selected running process. You can view the worknotes for the results and findings.

4. You can use the CrowdStrike Falcon Insight capabilities on the **Threat Intel** for analysis.

a. In the Threat Intel group, select an **Observable**, and choose a CrowdStrike Falcon Insight capability from the dropdown list.

b. Select the **CrowdStrike Falcon Insight** implementation, and click **Next**.

CrowdStrike Falcon Insight for Threat Intel



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. In the Select Date/Time pop-up, select a random value and click **Submit**.
Then a sighting search is run on the selected observable. You can view the worknotes for the results and findings.

CrowdStrike Next-Gen SIEM integration for Security Operations

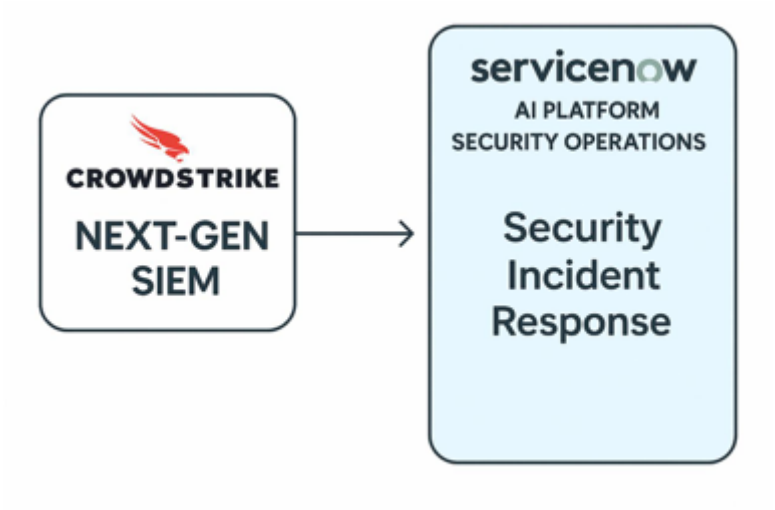
The CrowdStrike Next-Gen SIEM integration automatically ingests detection data that may indicate potential security incidents and streamlines the creation of security incidents in the ServiceNow® Security Incident Response (SIR), ensuring timely and effective response.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview of CrowdStrike Next-Gen SIEM integration

See the following graphic to learn how CrowdStrike Next-Gen SIEM integrates with the ServiceNow AI Platform Security Operations applications.



Key features

Use the key features of this integration to do the following actions:

- Discover CrowdStrike Next-Gen SIEM detections that are candidates for security incidents and automate the creation of these security incidents.
- Map CrowdStrike Next-Gen SIEM defect and entity fields to SIR security incident fields.
- Filter CrowdStrike Next-Gen SIEM defects.
- Aggregate incidents to existing open security incidents so that you don't have to create duplicate security incidents.
- Automate CrowdStrike Next-Gen SIEM detection status updates for Security Incident Response so that you can create and close security incidents.

Note: ServiceNow updates the status of CrowdStrike Next-Gen SIEM detections based on the security incident creation or closure. This update also includes comments of aggregated detections and new detections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Schedule detection ingestion to create security incidents periodically.
- Synchronize CrowdStrike Next-Gen SIEM detection comments with SIR Work notes.

Get started with CrowdStrike Next-Gen SIEM integration

Activate and set up the CrowdStrike Next-Gen SIEM integration for Security Operation plug-in to interface with your ServiceNow AI Platform instance and Security Incident Response product.

Before you can use the CrowdStrike Next-Gen SIEM integration, you must download it from the ServiceNow Store.

Review the following setup checklist and verify that you've completed all the tasks for a smooth integration.

Checklist

Setup task	Description

Assign and verify the required ServiceNow AI Platform and Security Incident Response roles.	The following roles are required for configuration and verification of the expected results:
	• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.ingestion_profile_admin and sn_si.analyst roles.
	• The sn_si.ingestion_profile_admin role performs the following tasks:
	  ○ Configures the integration.
	  ○ Creates detection profiles.
	  ○ Maps the CrowdStrike Next-Gen SIEM detection data fields to the security incident fields.
	  ○ Schedules on-going detection ingestion.
	  ○ Enables detection updates when a Security Incident Response detection is created or closed.

Assign the CrowdStrike required roles.	The following roles are required in CrowdStrike to register and configure your application: • Application developer for registering the application. • Tenant administrator for giving permissions to the application by calling the admin consent endpoint.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration.	The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	install and activate the other Security Operations applications that are required by the integration.
Install and configure CrowdStrike Next-Gen SIEM integration	Install and configure the CrowdStrike Next-Gen SIEM integration for Security Operations application from the ServiceNow Store on your ServiceNow AI Platform instance.

Install and configure CrowdStrike Next-Gen SIEM integration

Install and configure the CrowdStrike Next-Gen SIEM integration for Security Operations application from the ServiceNow Store on your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because this role inherits the required permissions by default.

Procedure

1. Download the CrowdStrike Next-Gen SIEM integration from the ServiceNow Store and install it. For more information, see Download an application from the ServiceNow Store for the first time
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the CrowdStrike Next-Gen SIEM integration tile, and select **Configure**.
4. On the form, fill in the fields.

CrowdStrike Next-Gen SIEM integration form

Field	Description
Name	Name of the CrowdStrike Next-Gen SIEM integration.
Client ID	The client ID that you obtain from the settings section of your account profile in the CrowdStrike portal.
Client Secret	The client secret key that you obtain from the settings section of your account profile in the CrowdStrike portal.
Region	Data center to pull data from. Specify the Region: US-1, US-2, EU-1, US-GOV-1, US-GOV-2 By default, the field is set to US-1

5. Select **Submit**.
   The configured integration tile displays.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Create a detection profile for CrowdStrike Next-Gen SIEM

Create a detection profile for CrowdStrike Next-Gen SIEM

Determine the CrowdStrike Next-Gen SIEM detections that are suitable for creating security incidents by creating a detection profile in your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because the sn_si.admin role inherits the required permissions by default.

Procedure

1. Navigate to **All** > *CrowdStrike Next-Gen SIEM* > **Detection Profile**.
2. Select **New**.
3. On the form, fill in the fields.

CrowdStrike Next-Gen SIEM - Detection Ingestion Configuration form

Field	Description
Name	Name of the profile. This name is also the default name for the security tag associated with this profile.
Active	Option for making the profile active. When a profile is active, the ServiceNow AI Platform actively polls CrowdStrike Next-Gen SIEM detections and corresponding security detections are created in Security Incident Response when the filtering conditions are matched.
Source	CrowdStrike tenant that you configured to ingest detections. If you have multiple tenants configured, select the appropriate tenant for the detection types you are planning to ingest for the profile.
Order	Priority in which the profiles are executed when two or more profiles share triggering conditions. Priority values are usually provided as 100 (the default value), 200, 300, and so on. The profile with the lowest number has the highest priority.
Description	Optional description of the profile.

4. Select **Update** .

The initial detection profile is created with basic information. Saving the profile at this point enables you to continue with defining the profile in case you are interrupted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. **Optional:** Continue with the profile definition process immediately.
   a. On the CrowdStrike-Nextgen Detection Profiles page, select the profile you just created.
   b. In the progress bar, select **Correlation Rules**.

What to do next
Set correlation rules for CrowdStrike Next-Gen SIEM integration

Set correlation rules for CrowdStrike Next-Gen SIEM integration

After creating a CrowdStrike Next-Gen SIEM detection profile, select correlation rules to map corresponding detections to a security incident. Correlation rules are refreshed every time a profile is opened and new rules are available for selection. The CrowdStrike Next-Gen SIEM integration supports multiple profiles.

Before you begin
Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because the sn_si.admin role inherits the required permissions by default.

Procedure

1. If you are not continuing from the previous section of the detection profile definition process, access the profile you are defining.
   a. Navigate to **All** > *CrowdStrike Next-Gen SIEM* > **Detection Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Correlation Rules** in the progress bar.
2. Clear the **All Correlation Rules selected** check box.
3. In the Correlation Rule List search field, enter the correlation rule name created in the CrowdStrike portal.
4. Select the correlation rule.
5. Use the right arrow to move the rule from **Available** to the **Selected** column.
6. Complete this section of the detection profile definition process by selecting **Continue** .

What to do next
Map individual CrowdStrike Next-Gen SIEM detection fields to the fields on the ServiceNow AI Platform Security Incident Response security incident. For more information, see Map the CrowdStrike Next-Gen detection fields.

Map the CrowdStrike Next-Gen detection fields

Map the individual CrowdStrike Next-Gen detection fields to the fields on the SIR security incident so that you can create detections with the mapped data.

Before you begin
Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. On the mapping page, in the CrowdStrike Next-Gen Field Mapping section, select one of the Sample Ingestion Methods.

Sample Ingestion Methods

Field	Description
All default Detection and Events Fields	Use this ingestion method to view the static list of all the detections and event fields. This method contains only default field names without any values. You can use this information to map with the SIR fields.
Retrieve Recent Detections	Use this ingestion method to import the most recent Detections and entities data. If the CrowdStrike Next-Gen detection contains multiple alerts, the earliest alert that is part of the detection is shown in the mapping section. During ingestion as well the earliest security alert field values will be used. You can ingest 5 sample detections. The sample detection field values populate when the profile ingests the sample detections. You can map these detections to the **SIR Incident Target Fields**. The Detection fields and values appear as individual tabs.

2. To add fields to the default fields that are displayed on the security incident, do the following actions:

   a. On the SIR Incident Target Fields section, select the Map another field button.
   It shows a list of SIR fields, from which you can select a field for a new field to be displayed.

   b. In the Security Incident column, expand the list that is displayed and then select a field.

   > **Note:** Multiple observables can be displayed on the same security incident. For example, the **Observable** field can be mapped multiple times with different values. Similarly, the **Configuration Item** and **Work notes fields** support multiple values.
   > If you try to map two values to a field that can't support multiple values, you see an error message that this field does not support multiple values. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field does not populate on the security incident.

   c. From the Detection and Event Fields section, drag and drop your field to map it to your new field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. When you select the check box that corresponds to a field, any new or updated changes made in CrowdStrike will automatically update the respective SIR incident data with the new incident data.

> **Note:** In the base system, the system property sn_sec_cs_ngsiem.detection_updates is by default set to False to receive the CrowdStrike Next- Gen updates related to new alerts that are linked to SIR.

- By default, the Affected Users, Configuration items, and Observables fields are checked. This means that whenever there are new observables or associated configuration items, or affected users that gets added to the incident then that information is automatically extracted and populated in the respective related lists in the Security Incident Response (SIR) during that polling interval.
- For any other fields, you must select the check box that corresponds to a field for any new or updated changes made in the CrowdStrike detection record within CrowdStrike. This will automatically update the respective SIR incident data with the new detection data.

> **Important:** Due diligence is required to be done before selecting this functionality as overriding the existing data may result in unstable data for the analyst to work with and any other automation that is set even by the field values of security incident may also get affected. So, it is very important to do the due diligence before you select any override functionality.

3. To remove a field, use the Remove item button next to the input expression field in the SIR Incident Target Fields section.

4. To map a field value from the Detection and Event Fields section to a field on the SIR incident Target Fields section, use one of the following actions:

a. Drag the Detection field name (for example, id) and drop it next to a field name in the SIR incident Target Fields column.

You can match any value from the Detection and Event Fields section to a field on the SIR incident Target Fields section. Fields are color-coded so that you do not overlook or duplicate detection fields in the mapping process. Light blue fields indicate that an detection field is not yet selected and mapped on the security incident. You may prefer to associate an incoming detection fields with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This way, you can visualize which field values have been added to the security incident and if any remaining important incident information remains unmapped.

b. You can add a combination of text and field.
For example, `Detection name is ${Detections: name}$`. Here `Detection name is` can be manually entered while `${Detections: name}$` is mapped from the Detection and Event Fields section.

c. You can directly manually enter and map a source detection or events fields to a target field.

- To manually map a source detection field use the ${field name}$ format. For example, to map a detection field Severity, the format is`${Detections: severity}$`.
- To manually add a source events fields, use the `${events names: events fields}$` format. For example, to map an events fields Description of events Security Alert, the format is `${Events: description}$`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This integration classifies certain observable sub-types. When you map a CrowdStrike Next- Gen field with the SIR observable field, the ServiceNow AI Platform auto-classifies the observable. If you want to generically map the incoming CrowdStrike Next- Gen observable to the observable type in SIR, then drag and drop the Detection and Event field in the Observable field. However, if you aware of the observable type for the incoming CrowdStrike Next- Gen observable in SIR, then map specifically to the SIR Observable type field. Some examples of specific observable types in SIR include Observable(Domain name), Observable(Email address), Observable(IP address (V4)), and Observable(Host name).

If your incoming CrowdStrike Next- Gen fields contain any MITRE-ATT&CK information, then map it to the MITRE-ATT&CK Technique field. Ensure that the incoming CrowdStrike Next- Gen field contains the MITRE-ATT&CK technique ID or technique name.

Sometimes, detection field values in CrowdStrike Next- Gen may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

5. To format a field translation for a new field from a CrowdStrike Next- Gen detection to match a field value on a Security Incident, select the **Click here** link in the **SIR Incident Target Fields** header.

6. To modify the fields which support field translation, select the  script format field translation icon.
   The fields that support field translation are **Affected user**, **Configuration Item**, and **Priority**.
   For example, click on  icon next to the Category. The CrowdStrike Next- Gen Field Translation script editor opens.

7. Enter any changes to the script and select **Update** to save the changes and return to the Mapping page.
   For example, for Category define the following in the script editor:

   ```
   "<Incoming CrowdStrike Detection Field Value>" : "<Category to
    assign to the Security Incident>".
   ```

   This mapping ensures that a profile uses only configured categories.

8. Continue your mapping by adding or removing field values.
   You can use the same field values in the Detection Generation Conditions builder to define additional criteria that an incoming detection must satisfy to create a security incident.

9. To move to the Filtering and Aggregation section, select **Continue**.

What to do next

Define and set filter conditions so that you can specify which detections should create security incidents. You can use the same field values (defined in the Mapping section) in the detection Generation Conditions builder (in the Filtering and Aggregation section) to define additional criteria that an incoming detection must satisfy to create a security incident.

Defining filter and aggregation criteria

Define and set filter conditions to specify which incoming CrowdStrike Next-Gen SIEM detections should create security incidents. You can also define additional detection field criteria that allows an incoming detection to be appended to an open security incident instead of creating an incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set the filtering conditions for security incidents

Set the filtering conditions so that security incidents are created only when the filtering conditions match.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

This type of filtering helps you to isolate security incidents and limits the number of security incidents that you create. If you set additional filtering criteria, only the required detections are ingested without having to change the query or the triggered detection configuration.

Procedure

1. To define the criteria that an incoming CrowdStrike Next-Gen detection must satisfy so that a security incident is created, select **Filter based on conditions**.

   The options in the first field in the Filter Conditions match the fields that are displayed on the CrowdStrike Next-Gen Sample detection Ingestion section for the detection that you ingested. These fields are dynamic and change depending on the detection that you ingest. The criteria that you enter is case-sensitive. Verify that the criteria that you define matches the values of the detection.

   Use the filter condition *detection_id* for the following fields with multiple values:

   - composite_id
   - host_names
   - seconds_to_resolved
   - seconds_to_triaged

   Because the filter condition can retrieve only strings, you must use the *detection_id* filter condition for the above fields to ensure that the data is filtered correctly.

2. Using the lists and fields of the conditions builder, set the filters for the first row.
3. To add more conditions, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
4. To set a second filter condition, click **New Criteria**.

Define aggregation conditions

Define additional incident aggregation criteria that aggregates an incoming detection to an existing SIR security incident instead of creating similar, potentially duplicate detections. When you use field matching value criteria for each profile, this additional aggregation can reduce the number of active, overlapping security incidents by placing all related detections data on a single security incident.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

If a new incident matches all the values that are selected in the aggregation field conditions in the mapping step, the incident is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.ingestion_profile_admin role working with security incidents, you can view all the added aggregate incidents on a related list on a security incident.

All the aggregated incidents on a security incident are displayed on the CrowdStrike Next-Gen SIEM Aggregated Incidents related list. This list details the associated timestamps and aggregated field values. This information helps you understand why incidents are added to the existing security incidents.

Procedure

1. To define additional incident field criteria that allows an incoming CrowdStrike Next-Gen SIEM detection to be appended to an open security incident instead of creating a new incident, select the **Aggregation Conditions** option as shown in the following figure.
2. In the **Incident fields with matching values** field, enter the field values that you want to match on existing security incidents in your ServiceNow AI Platform instance.
   All field values that you selected in the multi selection input field must match so that the aggregation criteria is met and that this incoming incident can be appended to an existing security incident. This selection implies it is an *AND* condition where fields, such as Observables and Configuration Items that may have multiple field values, are mapped to them. If only a subset of the values is matched, the CrowdStrike Next-Gen SIEM Incident aggregation conditions are not met and a new security incident is created.
3. To add multiple field matching conditions, click **Add New Criteria**
   The aggregation occurs if any one of the multi selection field conditions that you define are met. This selection implies the *OR* condition.
4. To update the work note for a new incident when it is added to a security incident, select **Log work note for new Incident**.

   The work note logs that a new incident is added and includes a link to the incident details. The log work note also updates more details that you add to the work note field in your mapping section.
5. To configure the schedule, click **Continue**.

What to do next

Set a schedule to retrieve the incident data and ingested incidents that match the criteria in the profile.

Schedule the CrowdStrike Next-Gen SIEM detection retrieval

Configure a schedule to define how and when you pull detections from the CrowdStrike Next-Gen SIEM tenant.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. If you are not continuing from the previous section of the Filtering and Aggregation criteria, access the profile you are defining.
   a. Navigate to **All** > *CrowdStrike Next-Gen SIEM* > **Detection Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Scheduling** in the progress bar.
2. On the scheduling form, fill in the fields.

CrowdStrike Next-Gen SIEM Scheduling form

Field	Description
Ongoing detection ingestion	Option to set ongoing detection ingestion that the ServiceNow AI Platform instance pulls from the CrowdStrike Next-Gen SIEM tenant for new detections. Security incidents are created if triggered detections are found and the detection generation filtering criteria matches.
Polling increment (minutes)	Polling frequency defined in minutes.
Set detection ingestion time	Option to add Date and time for the initial ingestion.
Initial detection ingestion time	Date and time that you specify for the detection ingestion.
One-Time Retrieval	Option to enable one-time retrieval of historical CrowdStrike Next-Gen SIEM detections and followed by the reconciliation of the data. When processing the data, both ongoing detections and historical data are pulled. **Note:** The retrieved historical CrowdStrike Next-Gen SIEM detections undergo de-duplication checks to avoid any duplicates within the Security Incident Response application.
Since date	The date since historical detections were ingested from CrowdStrike Next-Gen SIEM.

3. Complete this section of the profile by selecting **Continue**.

What to do next

Automate detection updates and closures

Automate detection updates and closures

Automate detection updates and closures based on the Security Incident Response incident status. The CrowdStrike Next-Gen SIEM integration enables detections to create security incidents and also to update the incidents after they are created or closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because the sn_si.admin role inherits the required permissions by default.

Procedure

1. If you are not continuing from the previous section of the Scheduling process, access the profile you are defining.
   a. Navigate to **All** > *CrowdStrike Next-Gen SIEM* > **Detection Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Additional Options** in the progress bar.
2. On the form, fill in the fields.

Automating Detection Updates form

Category	Field	Description
Security Incident Creation Updates	Update CrowdStrike Next-Gen detection Status upon SIR Incident Creation	Option to use the automated detection update functionality. The CrowdStrike Next-Gen SIEM detection status is updated in CrowdStrike Next-Gen SIEM detection with the comments after the SIR incident is created in the ServiceNow AI Platform.
	Initial detection status update	Initial detection status that is updated in the CrowdStrike Next-Gen SIEM environment, either New or In Progress.
	Initial comments posted back to detection	Initial comments that are posted to the detection in the CrowdStrike Next-Gen SIEM environment.
Detection Closure Updates	Close CrowdStrike Next-Gen detection upon SIR Incident Closure	Option to use the automated detection status update functionality. CrowdStrike Next-Gen SIEM detections are closed in the CrowdStrike Next-Gen SIEM portal with the comments given after the SIR incident is closed in the ServiceNow AI Platform.
	Closure detection status update	Status update in the CrowdStrike Next-Gen SIEM detection when the security incident is closed in SIR.
	Closure Comments Posted back to detection	Comments posted to the detection in the CrowdStrike Next-Gen SIEM detection when the security incident is closed in SIR.
Pull Closed detections	Pull Closed detections	Option to fetch closed detections during ongoing ingestion and one-time retrieval. Closed SIR incidents

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Category	Field	Description
		will not be updated with new data from CrowdStrike Next-Gen SIEM
Detection Comments and SIR Work notes synchronization	Update SIR Automation Activity with CrowdStrike Next-Gen detection comments	Option to update your CrowdStrike Next-Gen SIEM comments in the SIR Automation Activity. The comment in the SIR Automation Activity appears with the prefix *`Comment from CrowdStrike`*.
	Update CrowdStrike Next-Gen SIEM detection comments with SIR work notes	Option to update your SIR work notes in the CrowdStrike Next-Gen SIEM detection comments. The comment in CrowdStrike Next-Gen SIEM appears with the prefix *`Comment from ServiceNow`*.

3. Select **Finish**.
4. Activate the profile.
   a. Select the **Name** section of the progress bar.
   b. Select the **Active** check box.
   c. Select **Continue**.

CrowdStrike Falcon X Sandbox for Security Operations integration

With the CrowdStrike Falcon X Sandbox for Security Operations integration, you can submit files and URLs as part of the security incident response process to CrowdStrike Falcon X Sandbox to perform a detailed malware and threat analysis.

The CrowdStrike Falcon X Sandbox integration provides you with an on-demand, isolated virtual environment where you can perform the malware analysis and provide results to the ServiceNow security incident through the integration.

When you submit your malware incidents they are retained as part of the security incident record. You can use these records for further incident resolution and automate submission of files and URLs.

The integration supports automation of both phishing and malware response playbooks which allows your Security Operations center personnel to be more productive and efficient in responding to security incidents.

Key benefits

With this integration, you can do the following:

- Automate submission of files and URLs from user-reported phishing (URP), email messages, attachments, and other security incidents.
- Manually submit or resubmit previously analyzed files and URLs for updated analysis.
- Create multiple submission configurations that automatically apply CrowdStrike Falcon X Sandbox submission parameters such as operating system, scan type, and runtime options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Analyze malware and threat results in an HTML formatted report within the SIR incident. You can view threat lookup results and the indicator history for files and URLs that have been analyzed multiple times.
- Tag ServiceNow incidents with the submission processing status, as well as threat finding results.

See also

Document identifier	Document title
CrowdStrike Falcon X Sandbox	CrowdStrike Falcon Sandbox FAQ
ServiceNow product documentation website	ServiceNow Product Documentation website

Get started with the CrowdStrike Falcon X Sandbox integration

Activate and set up the CrowdStrike Falcon X Sandbox to interface with your ServiceNow instance and Security Incident Response product.

Before you begin

- Before you can use the CrowdStrike Falcon X Sandbox for Security Operations integration, you must download it from the ServiceNow Store.
- Review the following setup checklist and verify that you have completed all the tasks for a smooth CrowdStrike Falcon X Sandbox integration.

Role required: admin, sn_si.admin

Checklist

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform and Security Incident Response roles.	The following roles are required for configuration and verification of the expected results: • The administrator (admin) installs the sandbox integration from the ServiceNow app store and assigns the security incident administrator (sn_si.admin) role. • The sn_si.admin creates and edits the configuration and global settings and then assigns the security incident analyst (sn_si.analyst) role. • The security incident analyst (sn_si.analyst) responds to security incidents, such as submitting files and URLs to the sandbox and analyzing the submission results.
Verify that the ServiceNow core applications that are required to support the integration are	This integration is supported on Paris and Orlando releases.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
installed and activated before you configure this integration.	Ensure that these dependent plugins are installed. These plugins enable the execution of Integration Hub actions and flows: • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **Note:** If you can't find a plugin, you may have to request it from ServiceNow personnel. To request a plugin, follow the steps in Request a plugin. The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications that are required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. 1. Security Incident Response Dependency (com.snc.si_dep) 2. Security Integration Framework 3. Security Support Common 4. Security Support Orchestration 5. Threat Intelligence Support Common (required to use the sandbox integration capabilities) 6. Trusted Security Circles 7. Security Operations Setup Assistant 8. Security Incident Response For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

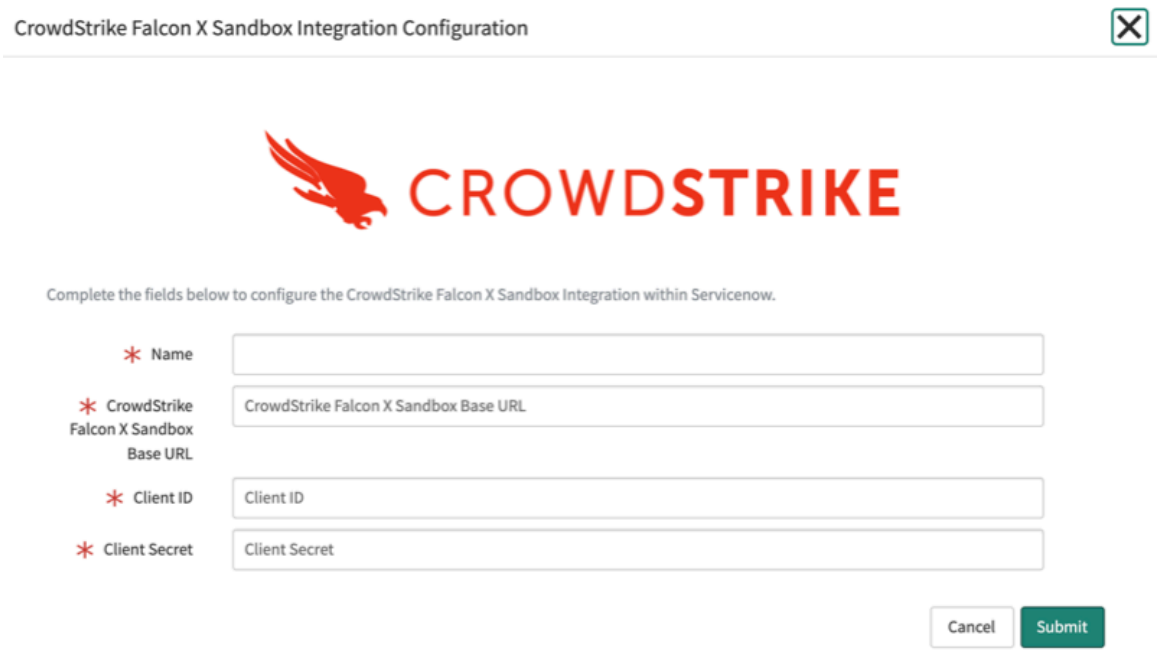
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
Verify that you are licensed for the Falcon Sandbox Private API key, and obtain the CrowdStrike Falcon X Sandbox full API key.	This integration supports the Falcon Sandbox Private Cloud only. **Note:** This release does not support Falcon X integration. CrowdStrike Falcon X Sandbox offers a self-signed restricted API key and an upgraded full API key. Use the full API key for this integration because it enables unrestricted access for automated submissions. For more information, see CrowdStrike Falcon Sandbox Knowledge Base.

Procedure

1. Download the CrowdStrike Falcon Sandbox for Security Operations integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the CrowdStrike Falcon X Sandbox integration tile, and click **Configure**.

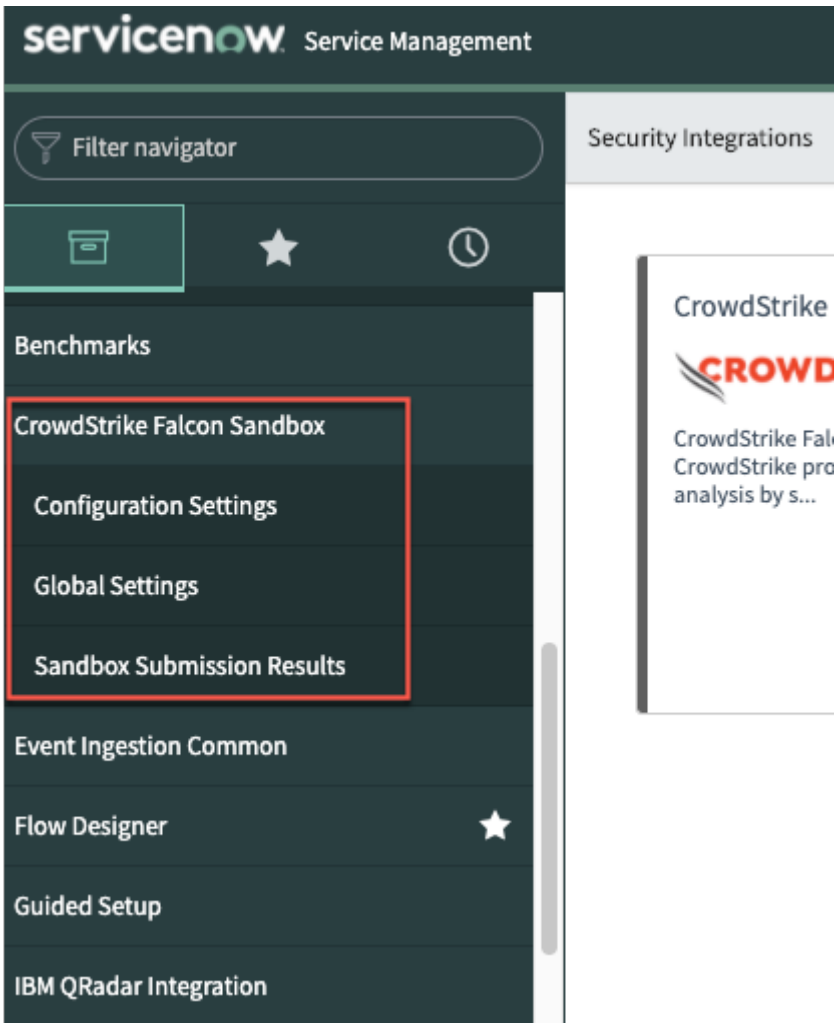


4. Enter the following details to complete the configuration:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name of this integration, for example, `demo-1`. While this is a unique name to identify the sandbox configuration, you can only configure one integration per ServiceNow instance.
CrowdStrike Falcon Sandbox Base URL	Sandbox base URL. This URL is available after you configure the sandbox.For example, `https://servicenow.falcon-sandbox.com` is a base URL.
Client ID	OAuth2 API client ID. For more information see, API Clients and Keys.
Client Secret	OAuth2 API client secret key. For more information see, API Clients and Keys.

5. Click **Submit**.
   After the sandbox is successfully validated and submitted, it is saved on the Security Integrations page as a tile. You can now view the Sandbox module in the application navigator.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
After you successfully complete the integration, the next step is to set up Sandbox submission configurations.

Set up Sandbox submission configurations

Set up the Sandbox configuration to define the analysis environment and runtime options for your security incident record submissions for the malware analysis.

Before you begin
Role required: sn_si.admin

About this task
Before you can submit files or URLs to the CrowdStrike Falcon X Sandbox using the integration, you must configure at least one submission configuration. The submission configuration defines the Sandbox operating system, scan type, run time options, and other incident handling characteristics. You may want to create multiple configurations to use the different options that available in the CrowdStrike Falcon X Sandbox environment.

Procedure

1. Navigate to **All** > **CrowdStrike Falcon X Sandbox** > **Configuration Settings**.
2. Click **New**.
3. Complete the following fields to create a configuration for a Full **Scan type**.

Field	Description
Name	Unique name for the submission configuration. This name appears to analysts when they submit a file. It is important to ensure that the name is descriptive and easily distinguishable from the other configurations (example, Win 10 Full Scan). If the name is not unique, an error appears and duplicate configuration record names do not save.
Scan type	Scan type as **Full**. A **Quick** scan type provides a limited threat analysis.
Operating system	Analysis VM environment that the sandbox scans the file or URL in.
Active	Option that you select when manually submitting files or URLs.
Default configuration for automated submission	Option that is cleared by default. Selecting this option enables this configuration to be available for automating malware analysis submissions. **Note:** You can have only one active submission configuration as the default configuration for automated submissions.
Display tags	Option that is cleared by default. When you select this option, tags are displayed

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	to provide the status of a file or URL submission. The analysis may take several minutes to process. The display tags are submission initiated, submission completed, or submission failed.
Additional runtime options	Option that is cleared by default. When you select this option, additional runtime parameters that Sandbox supports are available.
Runtime action scripts	Option that enables you to use an action script that simulates human behavior and interacts with the file or URL during the analysis. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ See CrowdStrike Falcon X Sandbox documentation for more details.
Network Settings	Option that allows you to select the type of network settings used while submitting an URL or file to Sandbox.

4. Click **Submit**.
   After you submit the configuration, it is saved on the Configuration Settings page as a record. The configuration must be **Active** to be used in sandbox submissions.

What to do next
After you configure sandbox submissions, the next step is to manually submit files or ULRs to Sandbox

.

Manually submit files or URLs to Sandbox

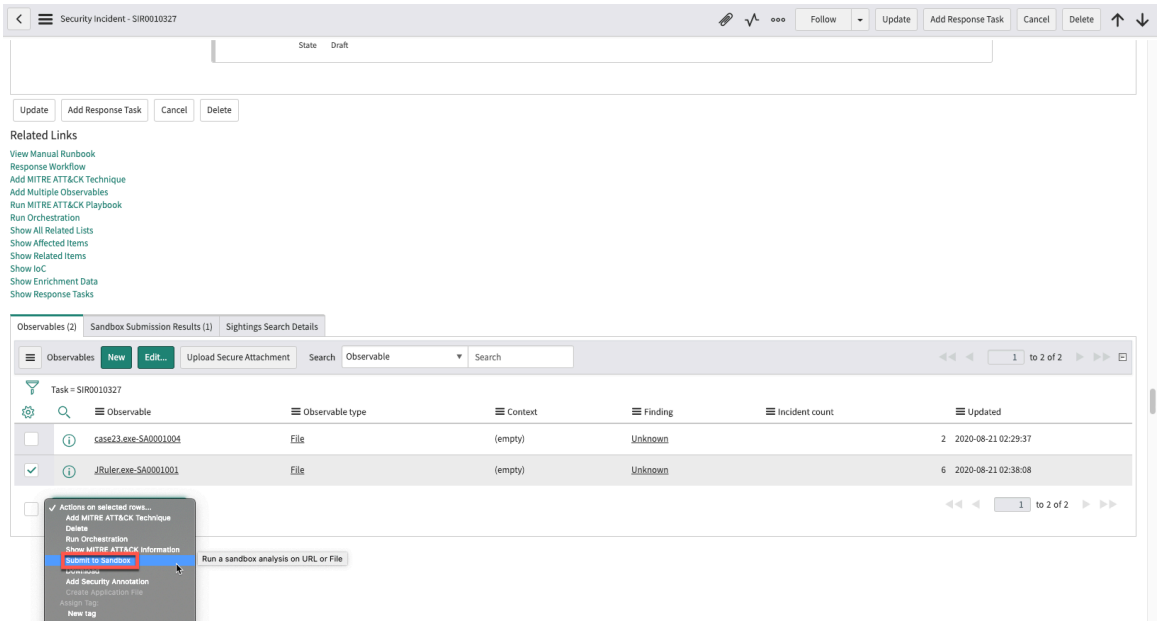
You can manually submit a file or URL to a sandbox when certain incident criteria, such as category is phishing, are met.

Before you begin
Role required: sn_si.analyst

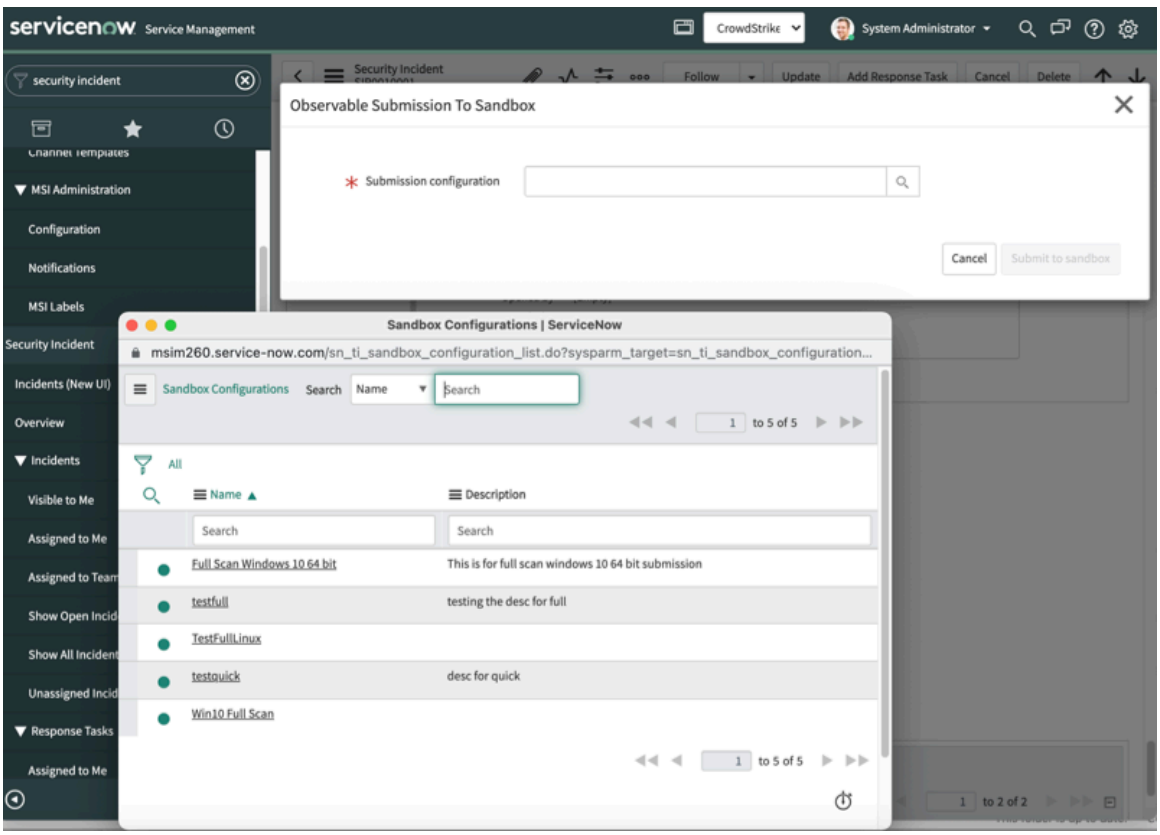
About this task
After reviewing the security incident and the file or URL, you can select the **Submit to Sandbox** option to perform a malware analysis.

Procedure
1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents** and open a security incident to which you want to submit a file or URL observable type record.
2. Click the **Show IoC** related link.
3. On the **Observables** tab, select a record or multiple records for which you want to perform malware or threat analysis and click **Submit to Sandbox**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

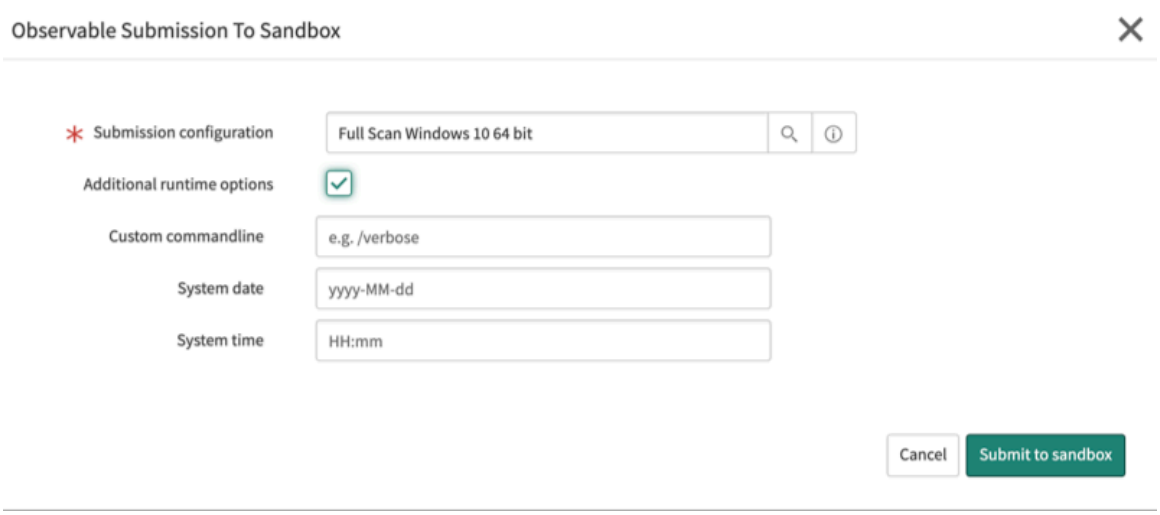


4. When the File Submission filter appears, select your preferred sandbox configuration in **Submission configuration**, and click **Submit to Sandbox**.



5. **Optional:** Select **Additional runtime options** if you want to provide further custom options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Field	Description
Custom commandline	Regular application command line or a special operation.
System date	System date in yyyy-MM-dd format.
System time	System time in HH:mm format.

After you initiate the submission, you can view the Work notes to see the status of your submission. For further information on the status of the submission or to analyze the results, view the **Sandbox Submission Results**.

Note: In CrowdStrike Falcon X Sandbox, quick scan isn't supported for URLs. If the worknotes has too much information, you can use the Filter option to drill down to the required worknotes that is relevant to you.

What to do next

When you submit the observables to the sandbox for malware analysis, view the sandbox submission results to take the next steps on potential threats.

Automate CrowdStrike Falcon Sandbox submissions using Flow Designer

The CrowdStrike Falcon X Sandbox integration includes flow templates created using the Workflow Studio that work with security incident records.

Before you begin

- Verify that you have created a Sandbox submission configuration and have enabled one configuration as the **Default configuration for automated submission**. When the flow is triggered, the sandbox submission occurs on your default configuration.

Role required: sn_si.admin

About this task

These flows are primarily designed to get you started when you want to automate file or URL submissions as part of your incident response workflow.
When you activate a sample flow, your phishing file attachments are automatically submitted if you define the security incidents as phishing in your sample flow. Alternatively, you can submit all .exe files when this file type is attached to an observable record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can modify these sample flows to trigger an automated submission under different conditions, categories, compound conditions, and so on.

The sandbox integration consists of two base system flows that are deactivated by default.

- **Submit file when category is phishing**: This flow submits a file to the sandbox for malware analysis when the security incident category is defined as phishing. You must attach a file to the observable record on the security incident. If you are using the User Reported Phishing (URP) functionality, any email attachment is automatically parsed and added to the SIR incident record as an observable record. No further action is required to automate the submission.
- **Submit when file type for observable is exe**: This flow submits a file to the sandbox for malware analysis when the security incident observable is an exe. Similar to the phishing category flow, a you must attach a file to an observable record on the security incident. You can do this manually by uploading the file or automatically if a phishing email attachment, or other mechanism that is creating the incident, is associated with the observable records.

When the flows are configured and incident conditions satisfy the parameters, the sandbox submissions trigger automatically when you review the security incident. Review the Work note that indicates that a submission has been initiated, a tag appears if enabled in the configuration, and a pending submission results record.

The sandbox integration also contains multiple subflows. The subflows are internal components of the overall integration submission capabilities. You can customize and edit the subflows to suit your security criteria.

You can refer the subflows to troubleshoot issues with sandbox submissions. An Execution record is created every time you invoke a subflow. This record indicates where in the flow a particular error occurred and enables you to fix the problem.

Sandbox Integration- Multiple workflows

Flows | Subflows | Executions | Help

+ New

All > Application Name contains Sandbox

Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

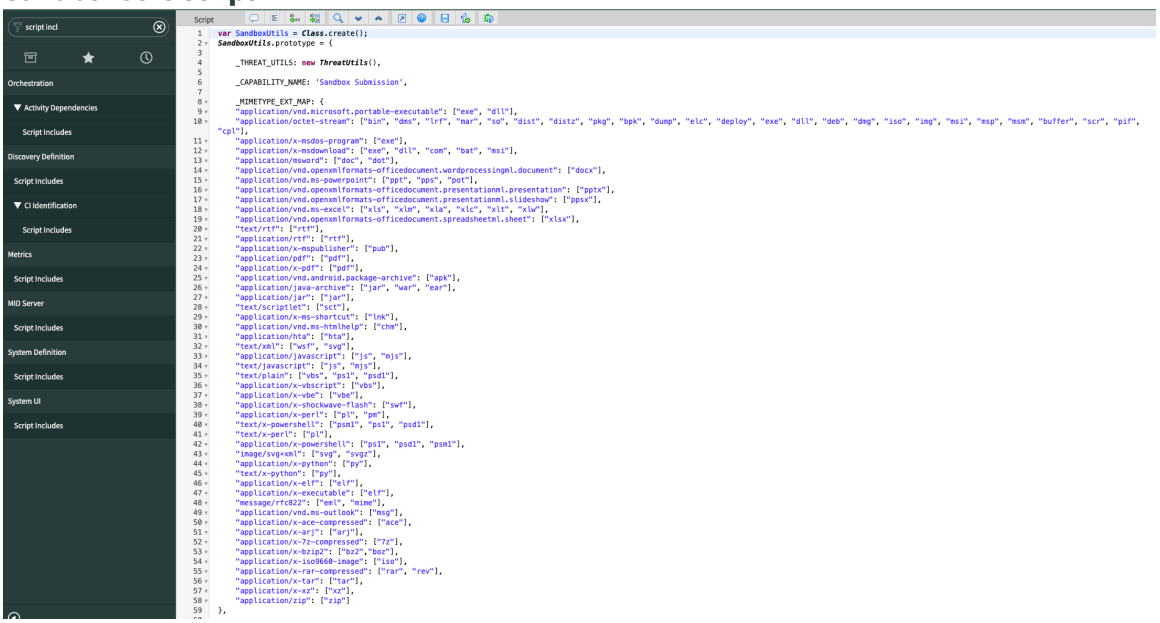
Actions on selected rows... 1 to 11 of 11

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

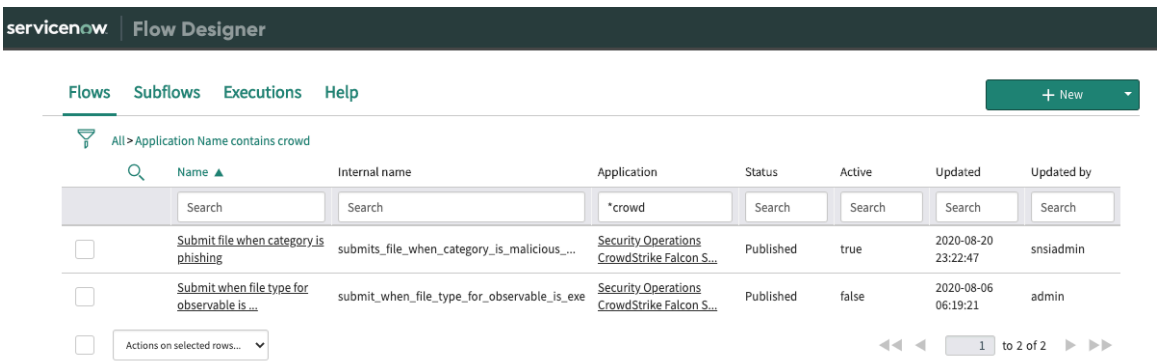
- If you choose to customize the default flows, then you should verify that the Submit Observable for Automated submission subflow is included in your flow to trigger automatic submissions.
- You can customize and define your file extensions for an exe. Create a copy of the flow **Submit when file type for observable is exe**, and make changes to the copy. The content type and file extensions are mapped in the SandboxUtils script. To access script includes, navigate to **System Definitions > Script Includes** and search for SandboxUtils.

SandboxUtils script



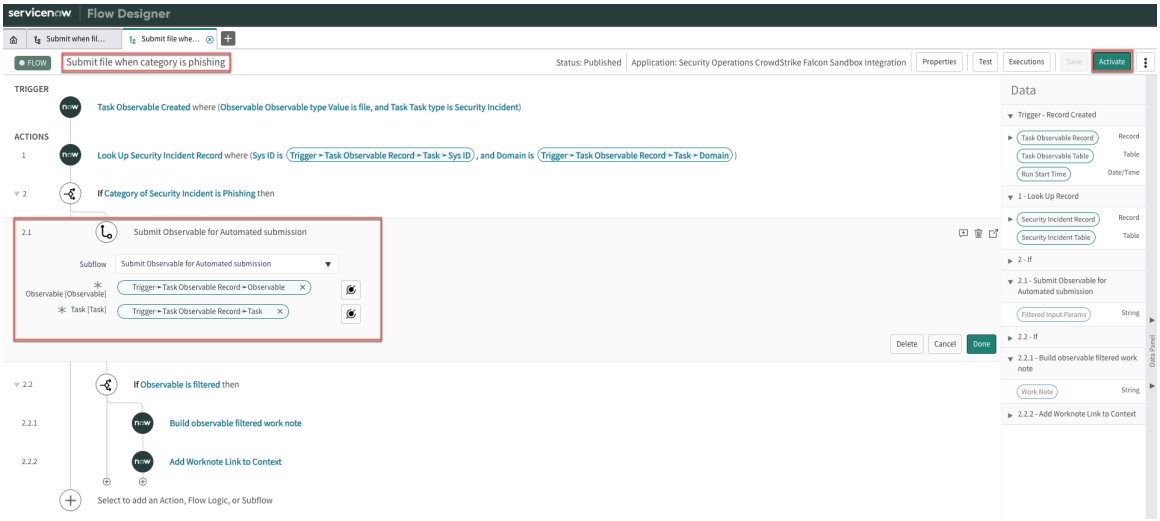
Procedure

1. Navigate to **All** > **Flow Designer** > **Designer** > **Flows**.
2. Filter the flows by the **Application** type.
   For example, *crowd filters the two CrowdStrike Falcon X Sandbox flows.



3. Select a flow to view the details.
   The example below shows the Submit file when category is phishing flow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click **Activate** and then click **OK** when the confirmation message appears.

What to do next

After you configure automated submission flows, you can View the sandbox submission results to analyze any threats.

Monitor the submission results in the sandbox

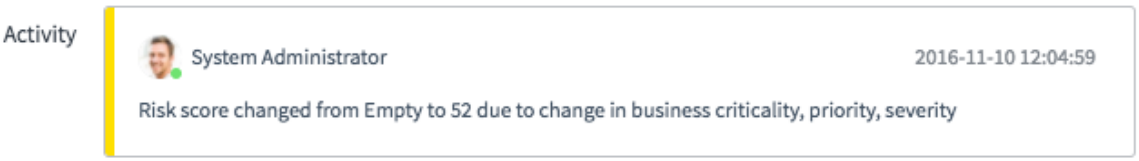
Results for all Sandbox submissions are shown in the **Sandbox Submission Results** tab for every security incident.

Before you begin

Role required: sn_si.analyst

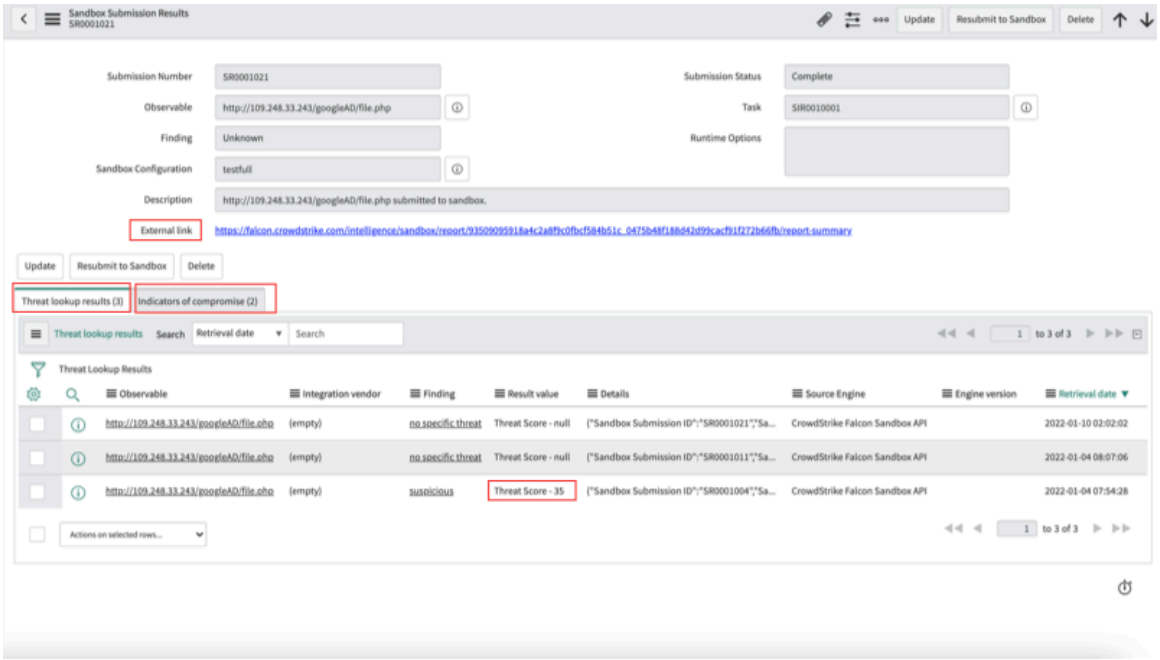
Procedure

1. Open the security incident that you are working with and verify that the sandbox submission is successful.



2. Review the Work notes for more information and learn how to proceed if you can't verify that the scan is successful.
3. Either click the complete results link in the Work notes or at the bottom of the security incident, navigate to **Show All Related Lists> Sandbox Submission Results**.
   Results are displayed in the Sandbox Submission Results tab.
4. Click open any record to view the complete sandbox analysis.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. **Optional:** Click **Resubmit to Sandbox** to reprocess the observable.

Result

- The **Threat lookup results** tab provides the threat assessment, including malicious findings, threat scores, and additional details. These details are provided in the standard threat lookup format structure for all ServiceNow threat lookup integrations.
- The **Indicators of compromise** tab provides the malicious or suspicious sandbox results with the Confidence scores. The Confidence scores are similar to other Indicator information that is stored in the ServiceNow platform. Indicators that are classified as informational are not included in this tab.
- The external link provides you with a view the Sandbox results in the CrowdStrike Falcon X Sandbox portal.

> **Note:** This option requires that you have the CrowdStrike Falcon X Sandbox role to view the results.

You can also monitor the sandbox submission results for all security incidents by navigating to **CrowdStrike Falcon Sandbox** > **Sandbox Submission Results**.

Tag security incidents with the Sandbox submission status

Tag security incidents with the Submission Initiated and Submission Complete tags.

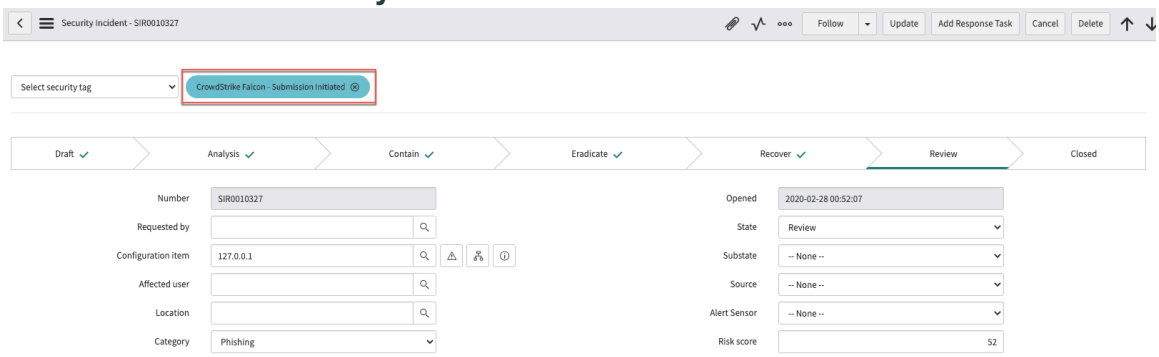
When you select the **Display tags** option in the Sandbox submission configuration, tags are displayed to provide the status of a file or URL submission. Checking the status this way is useful because the sandbox analysis may take several minutes to process.

The display tags are called submission initiated, submission completed, and submission failed.

The following example shows a security incident where the submission has been initiated.

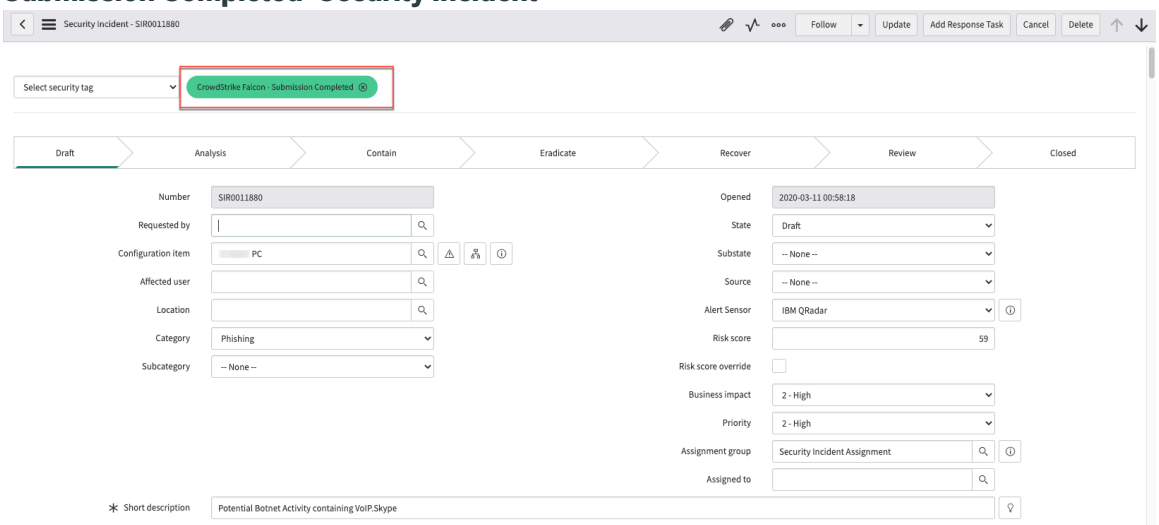
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Submission Initiated- Security Incident



The following example shows a security incident where the submission has been completed.

Submission Completed- Security Incident



Review the sandbox global settings

If you experience issues with file or URL submission results, review and modify the global sandbox settings.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **CrowdStrike Falcon Sandbox** > **Global Settings**.
2. Review and modify the settings as required.

Field	Description
File Size Limit (MB)	Sandbox upload file size limit in megabytes. **Note:** The file size limit of 256 MB is configured by default. Do not increase the value beyond 256 MB. However, you may want to reduce the maximum file size limit to avoid submitting large files.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Maximum time out for submission results (minutes)	Maximum timeout for submission results from the sandbox. **Note:** The default timeout is 30 minutes. If your results take longer than 30 minutes, you can increase the time. Also, you can view the results in the sandbox portal.

3. Click **Save** .

Elasticsearch Incident Enrichment integration

The Elasticsearch - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

Explore

Security Incident Response integrations

Set up

- Get started with the Elasticsearch - Incident Enrichment integration
- Create sightings search configuration records

Use

- Run a Sightings Search
- Security Operations Integration - Sightings Search Flow
- Security Operations - Elasticsearch Sightings Search Flow

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started with the Elasticsearch - Incident Enrichment integration

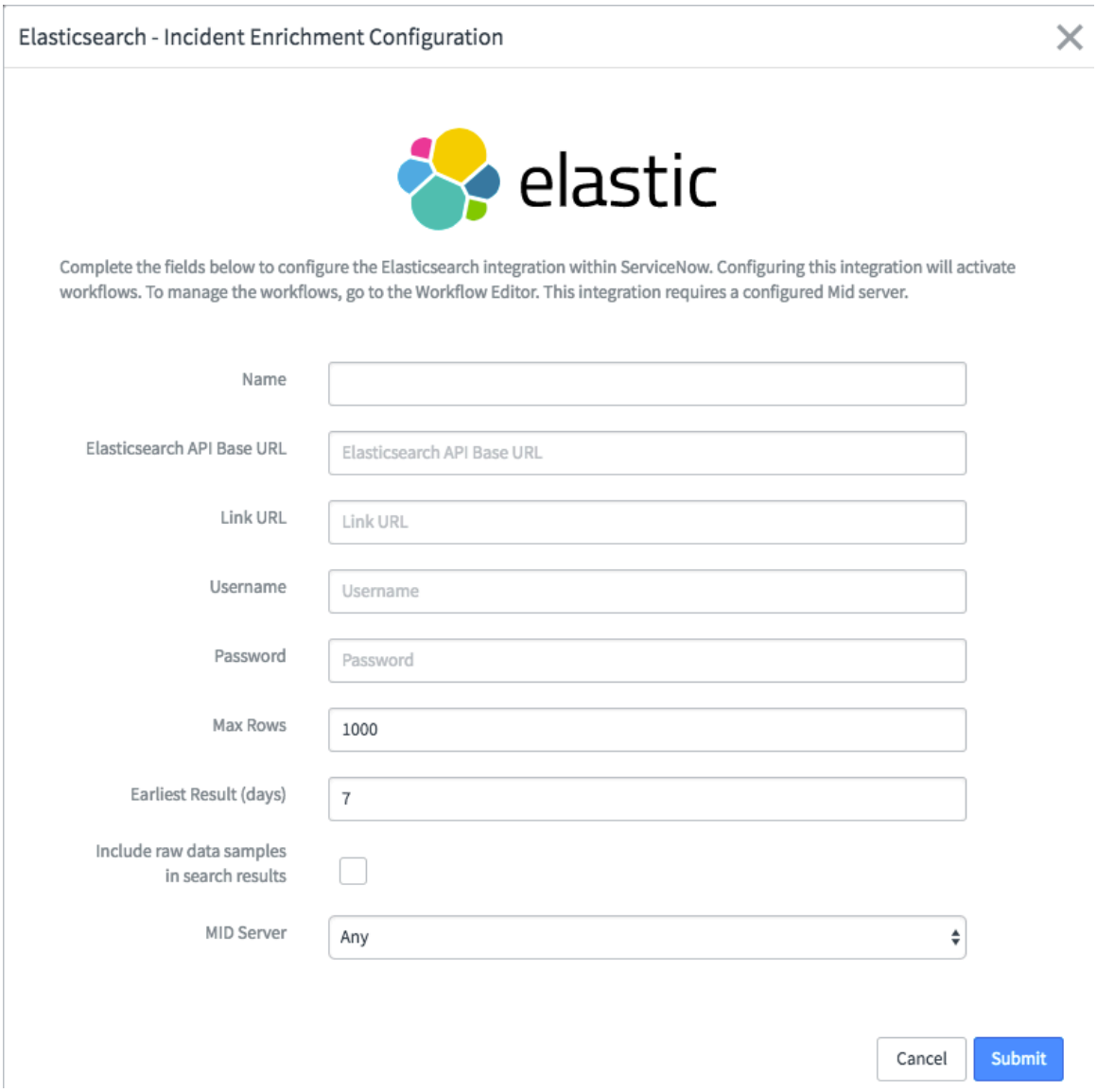
Elasticsearch is a distributed, RESTful search and analytics engine that easily integrates with Security Operations. Before you can use the Elasticsearch - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.

Before you begin

Role required: sn_si.admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access Elasticsearch and obtain the API Base URL under your Elasticsearch profile.
3. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configurations**. The available security integrations appear as a series of cards.
4. In the Elasticsearch - Incident Enrichment card, click **New**.



5. Fill in the fields, as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	The name of this configuration.
Elasticsearch API Base URL	The base URL you acquired from the Elasticsearch site.
Link URL	[Optional] Links to a Kibana instance, when available
Username	Your Intel Elasticsearch username.
Password	Your Intel Elasticsearch password.
Max Rows	The maximum number of rows you want to search.
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.
7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Result

After it is configured, the Elasticsearch - Incident Enrichment integration can be selected for publishing observables to watchlists in Security Incident Response.

FireEye Endpoint Security integration

FireEye Endpoint Security (HX series) helps organizations to inspect and analyze which contains known and unknown threats on any endpoint.

Skilled attackers today bypass traditional defences most security teams have relied on for years to protect their endpoints. Even when a traditional defence stops a known threat, it can't determine what that threat was trying to do. FireEye HX Endpoint Security helps your security team hunt down and stop known and unknown advanced threats against your endpoints.

The Gold Standard Security Incident Response integration with FireEye HX, makes it easier and efficient for Security Analysts to investigate and remediate security incidents in an instant without having to navigate between tools. You can use network containment to perform remediation actions on the endpoints, implement profiles to gather specific details about the host, and perform specific queries or actions on the endpoint.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key features

- Ability to perform host enrichment actions to gather more details about the endpoint such as host details, network statistics, user details, file details, process details, and service details.
- Ability to perform Enterprise Security Search to sight potential malicious observables across endpoints, and take remediation actions.
- Ability to gather Triage and Data Acquisition for in-depth endpoint inspection and analysis.

Limitations

Following are the known limitations of this integration:

1. Mid Application field value should be entered manually.
2. Isolate Host and Get Running Services cannot be performed on Linux agent.
3. Remove Isolation does not support for Linux agent.
4. Triage Acquisition does not support for Linux agent.
5. Users need to configure Show Enrichment Data related links. It is not available out of the box.
6. For Sightings search only five active searches can be present at once. Remaining will be queued and will start after the completion of any one of the ongoing sightings.
7. Sightings are available out of the box, which will be active false by default.
8. Hash is not supported for Get Running Processes.

Set up your NowPlatform instance for FireEye integration

Verify and review the following configuration procedure to set up NowPlatform instance for Fireeye integration.

Before you begin

Role required: ServiceNow AI Platform administrator (sn_si.admin)

The following section lists the setup tasks that are required to complete in your NowPlatform instance prior to installing the application for the FireEye integration.

Verify that you have completed the following tasks before you install the application from ServiceNow Store.

Task	Description
Verify that you have assigned the required NowPlatform and Security Incident Response (SIR) roles.	The following roles are required: 1. User with system administrator (admin) role is required to install the application for the integration. 2. User with security incident administrator (sn_si.admin) role is required to configure the integration, create, activate, and remove profiles. 3. User with security incident analyst (sn_si.analyst) role is required to work with

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	security incidents. A user with this role can initiate any of the capabilities available in the integration.
Verify that you have installed and configured a MID Server.	Configure MID Server: A MID Server in your NowPlatform instance is required to manage files and connect to the FireEye service deployed within your organization network. For more information on MID servers, see https://www.servicenow.com/docs
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application.	The following applications must be installed and activated from the ServiceNow Store before installing this application. Install and then activate one application at a time in the order listed below to ensure a smooth installation: **1.** Security Incident Response Support **2.** Security Support Core **3.** Security Support Common **4.** Security Incident Response **5.** Threat Intelligence Support Common **6.** ServiceNow Integration Hub Enterprise Pack Installer
Before you enable the approval option for profiles, verify that you have created an approval group.	An optional approval workflow is available for isolating host machines, restoring them back to the network, getting file, and running additional actions on end point. If your organization wants an extra level of control over these actions, enable the Require approval option during the configuration of the profiles. In the absence of a profile if a capability is invoked from the Related List directly, Approvals can be handled from the FireEye default setting module. As a Security Administrator, you can set up approval while configuring the profiles and the default settings. An approval group must be available on the Groups list in your instance.

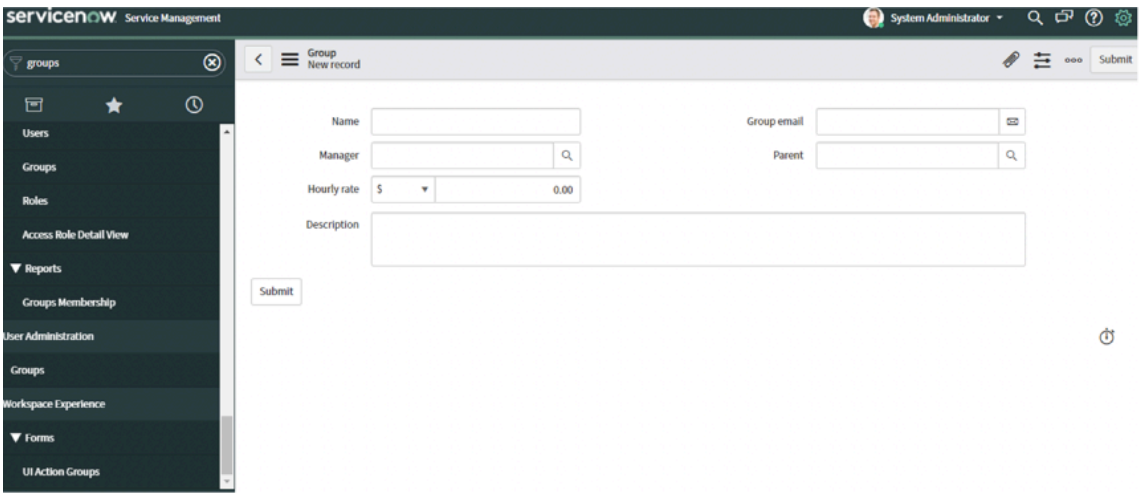
Procedure

1. Navigate to **User Administration** > **Groups**.
2. Click **New** in the Groups list.
3. Fill the form with the following details:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name of the group that is displayed when an approval request is submitted.
Group email	(Optional) Group email distribution list or the email address of the point of contact, such as the group manager.
Manager	(Optional) Name of group manager. Click the search icon to view the list.
Parent	(Optional) Name of the parent group, if associated with a parent.
Hourly rate	(Optional) The amount paid for every hour worked.
Description	(Optional) Additional information about the group.

4. Click **Submit**.



The new group is displayed in the Groups list. You have successfully created an approval group. Add users to your new group as required who can approve the requests submitted by the security analyst. A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user.

To monitor and process requests submitted by users with the sn_si.analyst role, each member of the approval group should navigate to My Approvals in the ServiceNow AI Platform. Alternatively, the approvers can find the requests submitted specifically for FireEye integration under the FireEye Approvals.

What to do next

The next step is to install and configure the application from ServiceNow Store.

Configuring Timestamp Settings for Triage Acquisition

Configure and verify the timestamp settings before the installation procedure.

Before you begin

Role required: NowPlatform Security incident administrator (sn_si.admin)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before installing the FireEye application, there are some pre-requisites that need to be performed on FireEye.

Triage Acquisition can be requested with an input of 'Around Timestamp' field or 'Standard' field. Around timestamp requests information collected during a specified amount of time before the timestamp until a specified amount of time after the timestamp. The timestamp is the time the event that generated the alert occurred. If you select Standard, the Endpoint Security appliance requests information from the host for all data around an event.

When an Endpoint Security user requests a triage collection based on a specific date and time the agent returns information for a specified window of time before and after the alert. The timestamp settings control the length of the window for the triage collection. Timestamp settings apply only to agent URL events (URL Monitor Events) and registry key events (Reg Key Events).

You can use the Timestamp Settings tab to specify the length of time before and after the timestamp during which information is collected. Timestamp Settings can range from 0- 86400 seconds. The default for both settings is 600 seconds.

You can use the Timestamp Settings tab on the Automatic Triage Settings page to specify the length of time before and after the timestamp during which information is collected. The timestamp is the time when the event that triggered the alert occurred.

Procedure

1. Navigate to **Endpoint Security Web UI**.
2. Select **Admin** > **Triage Settings**.
3. Click **Timestamp Settings** tab on the **Automatic Triage Settings** page.
4. Specify the length of time before and after the timestamp for which the information is needed.
5. Enter the number of seconds before the specified timestamp for which the information is needed.
6. Enter the number of seconds after the timestamp for which the information is needed.
7. Click **Save**.

> **Note:** You can change all values on the page back to the default settings by clicking **Reset to Defaults**, and clicking Save.

- **Acquisition Space Area**: The Acquisitions page shows how much disk space is remaining for acquisitions.
- **Setting Disk Utilization Limits for Acquisitions:**
  - Triages, file acquisitions, and data acquisitions can accumulate over time and use an increasing amount of disk space. To control this, you can allot a set amount of disk space for them. Ten percent of the disk space you specify is reserved for automatic triage acquisitions. When the total allotted acquisition space is exceeded, the oldest automatic triages are deleted.
  - When the total disk size of completed acquisitions exceeds a specified limit, the Endpoint Security appliance deletes the oldest completed acquisitions until enough disk space is cleared to bring the total under the specified limit. Acquisitions that are not yet completed are not affected.
  - The Endpoint Security appliance automatically deletes acquisitions if an Administrator, Analyst, or Investigator uses the Endpoint Security Web UI to manually delete the associated agent.

  To set disk utilization limits for complete acquisitions using the Web UI:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Navigate to **Endpoint Security Web UI**.
- Select **Disk Utilization Limits** from the **Admin** menu.
- In the **Acquisition space limit** area, specify the maximum amount of disk space (in GB) that can be used to store triage, file and data acquisitions. Valid values and defaults vary based on your Endpoint Security appliance model. The values appropriate for your model are shown on the Disk Utilization Limits page.
- Click **Save**.

Note: All the mentioned settings are honoured and in case of any failures or errors, ServiceNow AI Platform just returns those errors.

Install the application and configure a source for the integration

Install and configure the application from ServiceNow Store on your ServiceNow AI Platform instance.

Before you begin

Role required: NowPlatform administrator (admin)

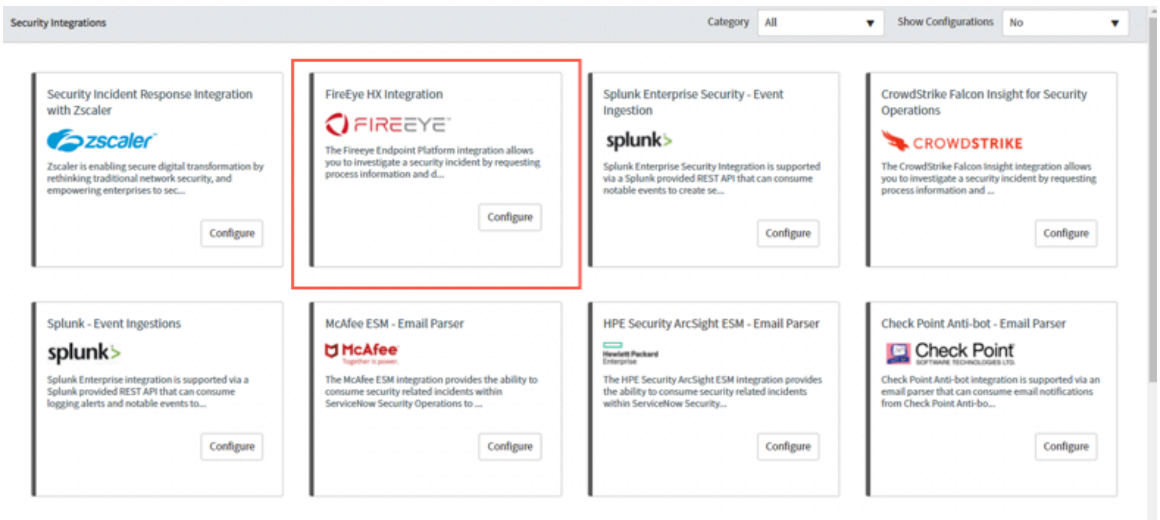
Note: An active MID Server is mandatory to configure a source.

Download the Security Incident Response integration with FireEye HX application from the ServiceNow Store and install.

After you have successfully installed the application, follow the below steps to configure it:

Procedure

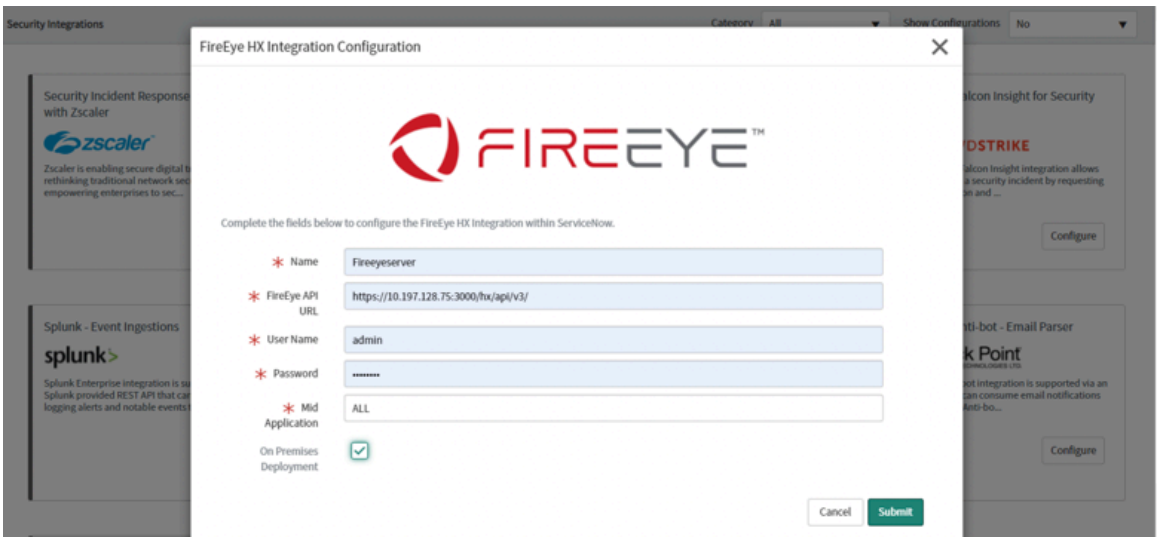
1. Navigate to **Integrations** > **Integration Configurations**.
2. Select the **Integration Configurations** module to display the available integrations, and locate the **FireEye** tile.



3. Click **Configure** on the FireEye tile.
4. Provide the following details to set up the FireEye integration:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

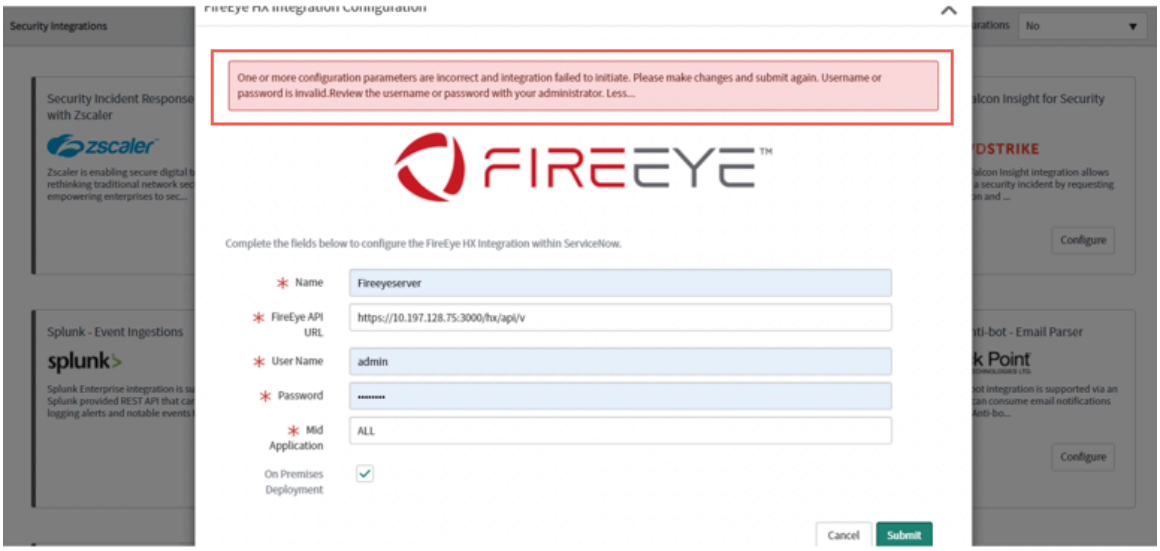
Field	Description
Name	Name of the FireEye configuration. This name is used to identify the source and the associated credentials and configuration. This name help you distinguish the credentials and accounts and identify each source to avoid conflicts with profiles.
API URL	Base URL hosting the FireEye API.
User Name	Enter the username of the FireEye account.
Password	Enter the password of the FireEye account.
Mid Application	MID Application that is set up in your environment. Mid server is required to process zip files for some of the enrichment capabilities. By default, it will be ALL. Users should provide valid application name manually.
On Premises Deployment	Default is disabled. If you are using the cloud-based version of FireEye, verify that the check box is cleared.



5. Click **Submit**.
   The FireEye Configurations list is displayed with your new configuration record. You have completed the configuration for a FireEye server. If you cannot connect to the FireEye, or your

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

credentials are incorrect, a validation error message is displayed as shown in the following figure. Verify that your credentials are correct and try again.



FireEye Default Settings

Following are the additional configuration settings after you complete the installation.

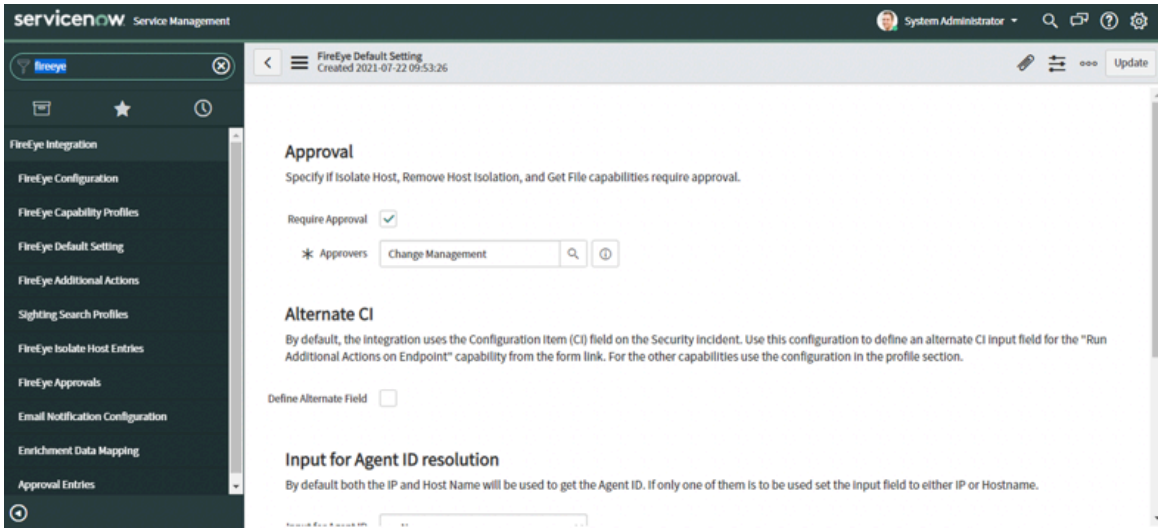
Once you complete the installation, you can find FireEye Default Settings module in the left navigation. It contains default settings for different FireEye functionalities.

Additional Configurations

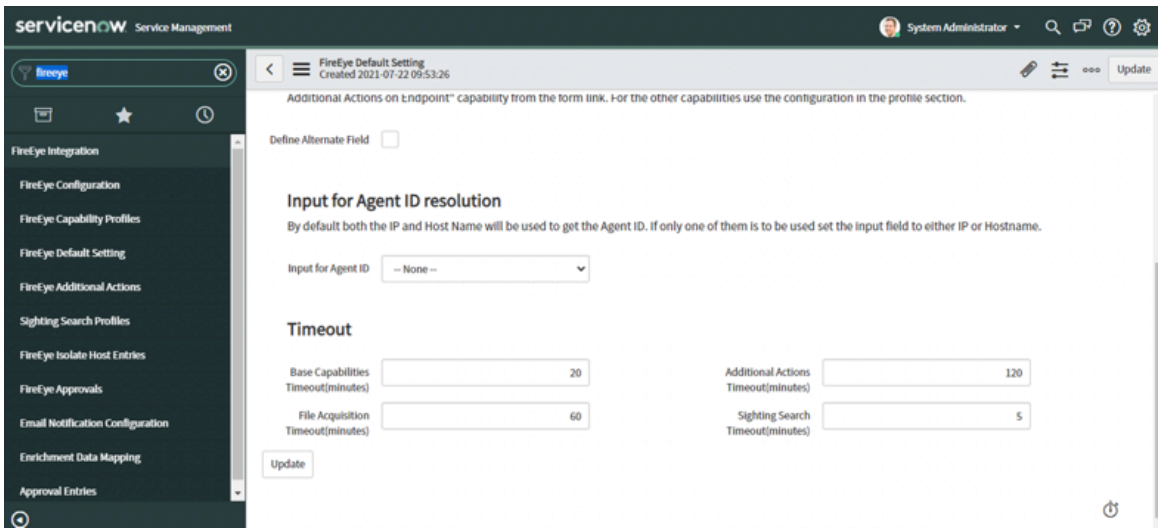
Following are the additional configuration settings:

1. **Approval**: This approval is specifically for the Isolate Host, Remove Host Isolation, and Get File capabilities when they are triggered directly from the Related list, and in the absence of profiles for them. If there is/(are) (an) existing profile(s) for these capabilities, then the approval configuration in the profile will be honored.
   - **Require Approval:** When you enable Require Approval, the Approvers field is available on the form.
   - **Approvers**: List of approver groups. After you submit a request, approval is required from the group to complete the request.
2. **Alternate CI**: Enabling this check box will provide list of fields available to pass an alternate CI to the capability. By default, the integration uses the Configuration Item (CI) field on the Security incident. This configuration is applicable only for the “Run Additional Actions on Endpoint” capability. So, use this configuration to define an alternate CI input field for the “Run Additional Actions on Endpoint” capability only. For the other capabilities use the configuration in the profile section. If the profiles do not define an alternate CI, then the capabilities would pick the CI field from the Security Incident form.
3. **Input for Agent ID resolution**: By default, IP and Host Name will be used to get the Agent ID. If only one of them is to be used set the input field to either IP or Host Name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. **Timeout**:
   - **Base Capabilities Timeout(minutes):** The Enrichment, Isolate Host and Remove Host Isolation capabilities will fail if no response is rendered in the set time.
   - **Additional Action Timeout(minutes):** The Run Additional Actions on End point capability will fail if no response is rendered in the set time.
   - **File Acquisition Timeout(minutes):** The Get File capability will fail if no response is rendered in the set time.
   - **Sighting Search Timeout(minutes):** The Search will be stopped after the set time.



Create a new capability profile for the FireEye Endpoint integration

Create a profile and select the FireEye HX capabilities that you want the profile to run.

Before you begin

Role required: NowPlatform Security incident administrator (sn_si.admin)

About this task

Profiles are created to club capabilities together, and would help Analysts perform the investigation/remediation easily.

Following are the list of capabilities that you could add to profile(s):

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Get Host Details
2. Get Logged On Users
3. Get Network Statistics
4. Get Running Processes
5. Get Running Services
6. Get File
7. Isolate Host
8. Remove Isolation

You cannot club Get File, Isolate Host, and Remove Host Isolation capabilities with other capabilities while creating a profile. Profiles for these have to be individually created. On the other hand, Get System Details, Get Logged on Users, Get Network Stats, Get Running Processes, and Get Running Services can be clubbed together. You could create profiles individually or by clubbing them in full or parts as per your need. Once a capability is included in a profile, it cannot be included in another profile.

To create a new capability profile, follow these steps:

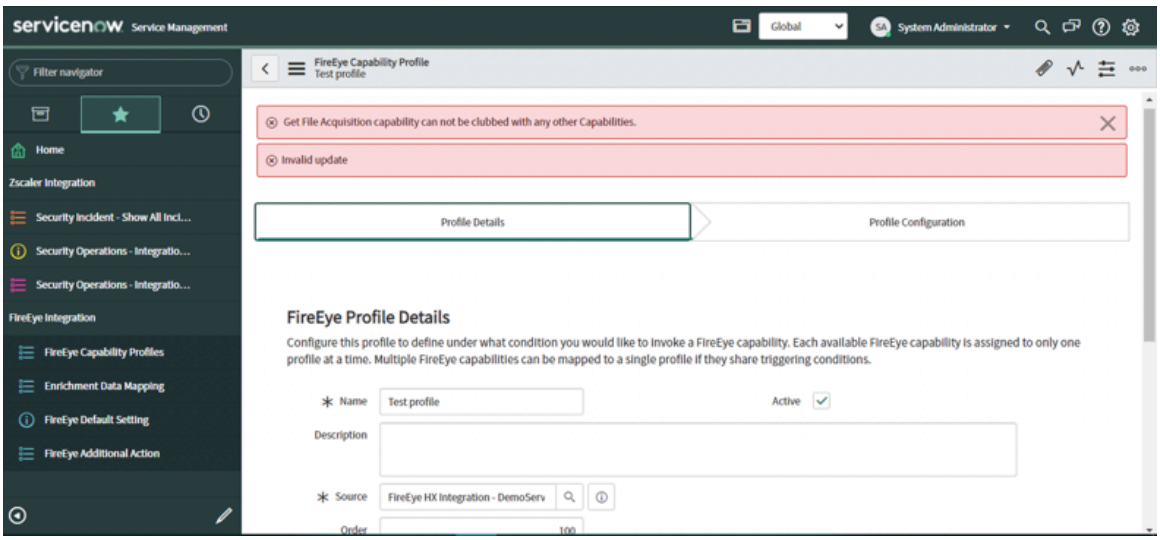
Procedure

1. Navigate to **FireEye Integration** > **FireEye Capability Profiles**.
   The capability profiles list is displayed.
2. Click **New**.
3. On the form, fill the fields.

Name	Name for the FireEye HX capability profile. This name helps you identify the profile type and describe it.
Description	Additional information about the profile that further describes the profile.
Source	Name of the FireEye HX source. Only configured sources are available from the choice list.
FireEye HX Capabilities	Capabilities of the FireEye HX profile. Select the capabilities you want for this profile from the Available column and move them to the Selected column.
Order	Flow priority. Default is 100. The value of this field indicates the order that Flows are executed when two or more profiles share triggering conditions. The Flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400.

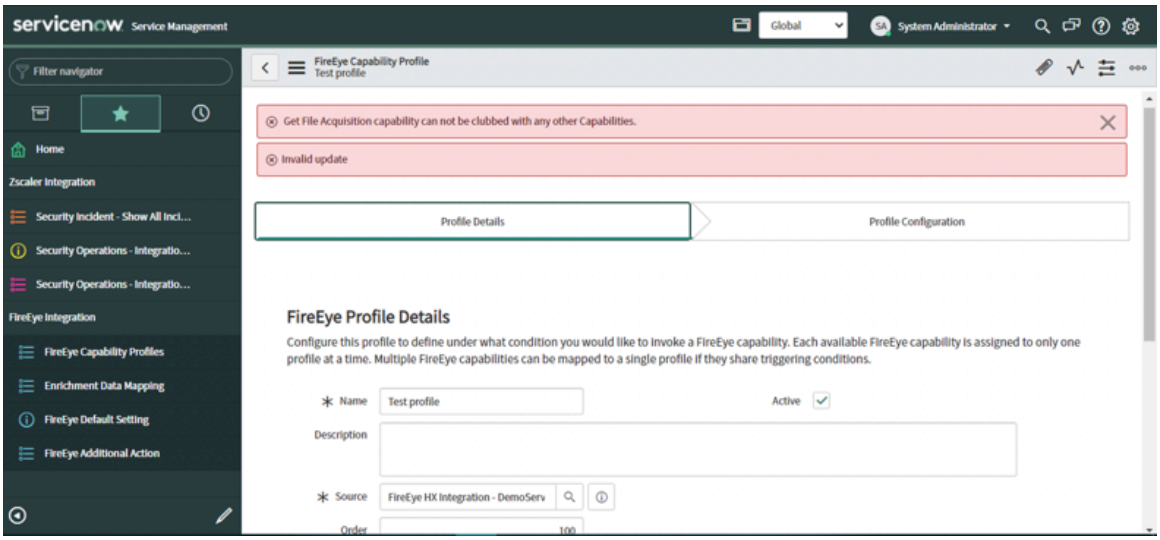
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Active	This indicates that the profile is active. When the profile is active, it automatically triggers when a security incident is created that matches the filtering conditions that you have specified in the configuration.



The following figure is an example of a completed form for profile details with Get Host Details capability.

4. Click **Next** to continue to Profile Configuration.



Note: Isolate Host, Remove Host Isolation and Get File capabilities cannot be clubbed with other capabilities.

What to do next

The next step is to configure your profile. Before you configure the settings for the profile, you may prefer to review the concepts for configuring profiles and triggering conditions. For more information, see Understand how trigger conditions work with a configuration item for a profile.

Understand how trigger conditions work with a configuration item

After you create a profile and select the FireEye capabilities that you want the profile to run, configure the profile settings so that it runs only when a set of specific conditions are met.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

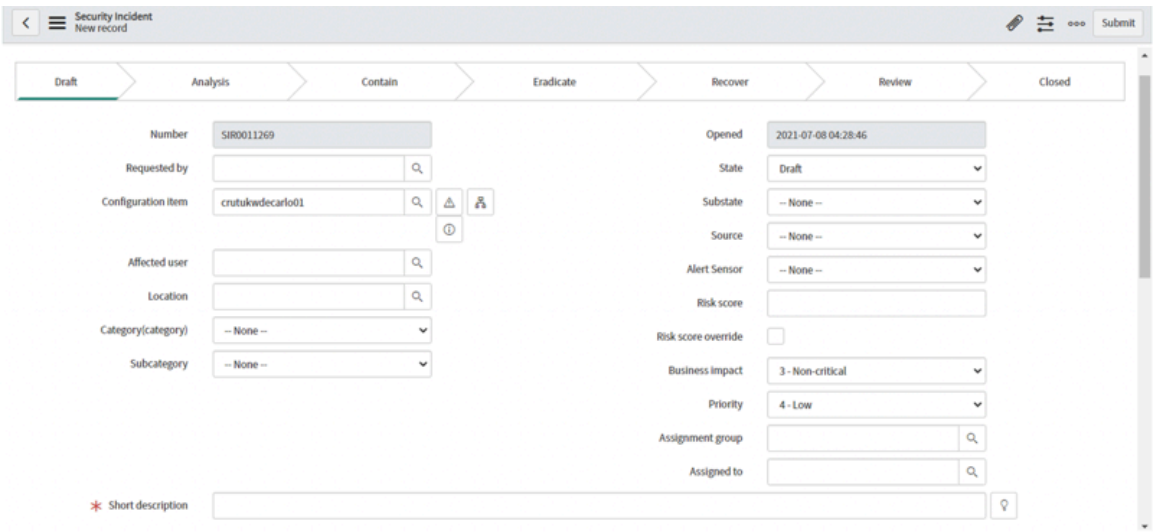
You can set trigger conditions so the profile runs automatically whenever a security incident matching the trigger condition is created. If the trigger condition is not set, these profiles can be manually run by clicking the form 'Run EDR profile(s)' on the security incident, and selecting the profile.

By default, the integration uses the Configuration Item (CI) field on the Security incident. This value is used to match the IDs of your assets with the information stored in the Now Platform CMDB. When a security incident is created, and a profile is run either automatically or manually, the CMDB is searched to retrieve the hostname and/or IP address based on the value of the CI field. The host name and or IP is used to resolve the Agent ID on FireEye HX to identify the endpoint.

In an ideal case, a matching value is found in the database, and data is gathered from the FireEye HX console for the matching asset. The data for various capabilities are pulled into your ServiceNow AI Platform instance and displayed in the related lists of a security incidents. When the Configuration item (CI) field is not populated on the security incident with a host name, or an IP address that matches the database, you can select an alternate field on the security incident that contains either the host name or the IP to perform the Agent ID resolution.

During the configuration step of the profile setup, you can select an alternate CI field for endpoint identification to ensure that the you are able to identify the endpoint on FireEye HX. You can select any field on the security incident as an alternate CI trigger field including custom fields that you create. By selecting this alternate CI field as a backup, you ensure that your profiles run even if the CI field is not populated on the associated security incident upon incident creation.

Note: The alternate CI fields are considered only for capabilities that could be added to a profile. For all the additional actions, the alternate CI is picked from the default settings page.



Configure profiles and security incidents for the FireEye HX integration

After you create a profile and select the FireEye HX capabilities that you want the profile to run, configure the settings so that the profile can be invoked only under the defined conditions.

Before you begin

Role required: sn_si.admin

Configure the profile so that it runs only when the conditions you specify are fulfilled. Select an alternate input field for the Configuration Item (CI) field, if required, and set filtering conditions so that the profile can be triggered automatically when a security incident meeting the trigger conditions is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can navigate to the **Profile Configuration** page only after you have entered the **Profile Details**.

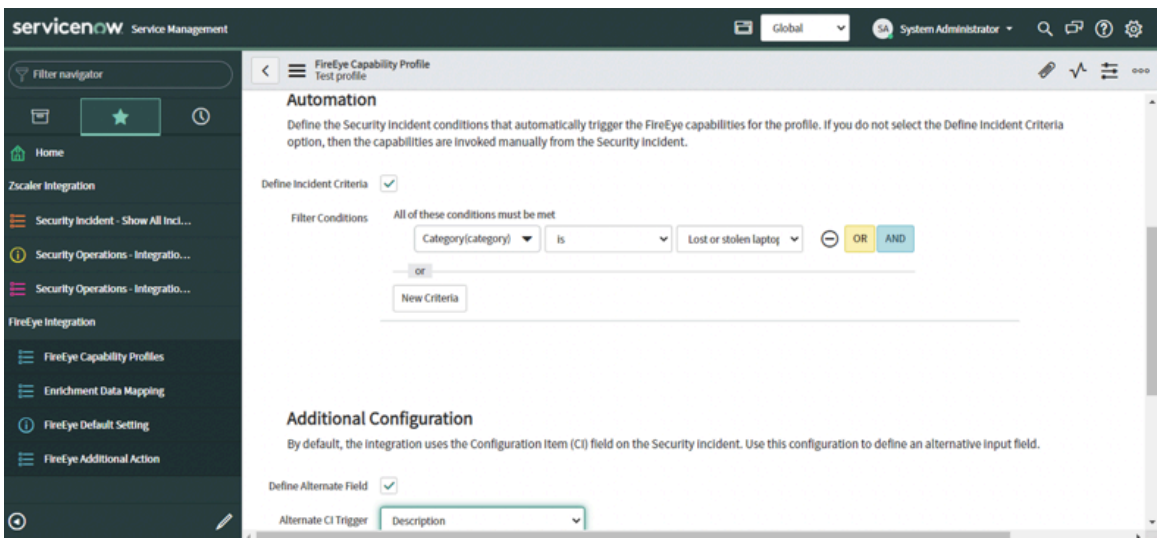
Procedure

1. Navigate to **FireEye Integration** > **FireEye Capability Profiles**.
2. Click **Next** on the **Profile Details** page after completing the Profile details section.
3. Review and configure the following sections:
   - **Define Incident Criteria (Automation)**: Define the security incident conditions that would automatically trigger the FireEye HX capabilities for the profile. If you do not select the **Define Incident Criteria** option, then the profile and the underlying capabilities can be invoked manually from the Security incident.
     - Select **Define Incident Criteria** option to automatically trigger FireEye HX capabilities in the profile.
     - In the **Filter Conditions**, select the required field.
     - You can add **New Criteria** and also define the OR or the AND condition.

     Note: Isolate Host, Remove Host Isolation, Get File cannot be triggered automatically.

   - **Additional Configuration**: When the Configuration item (CI) field is not populated on the security incident with a host name, or an IP address that matches the database, you can select an alternate field on the security incident to query the FireEye HX APIs.
     - Select the **Define Alternative Field** option to define an alternative input field.
     - Select the input field from the **Alternate CI Trigger Field**.

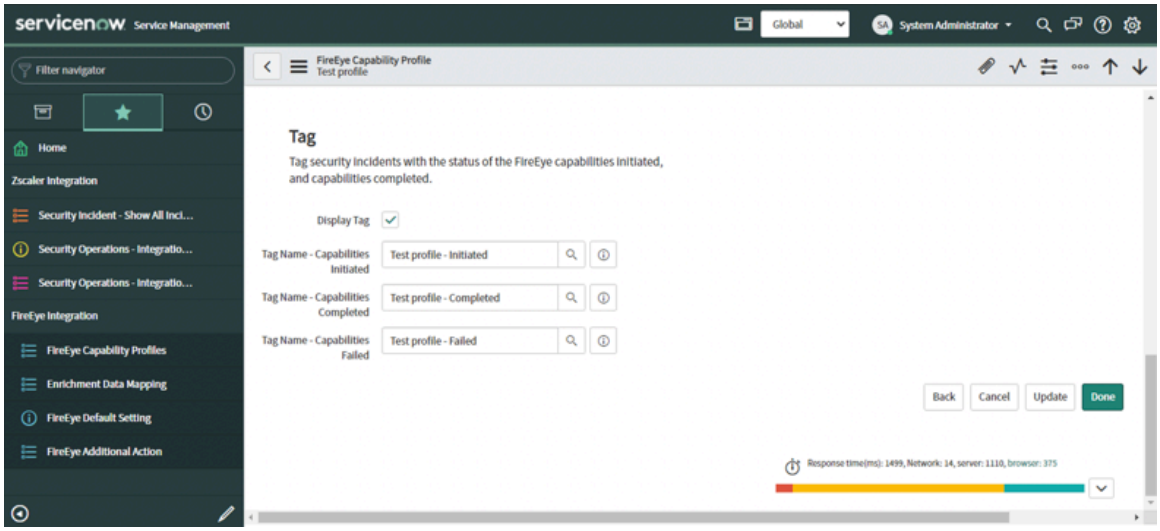
     Note: For more information, see Understand how trigger conditions work with a configuration item.



   - **Tags**: You can optionally tag security incidents with the FireEye HX profile initiated, profile completed, and profile failed tags.

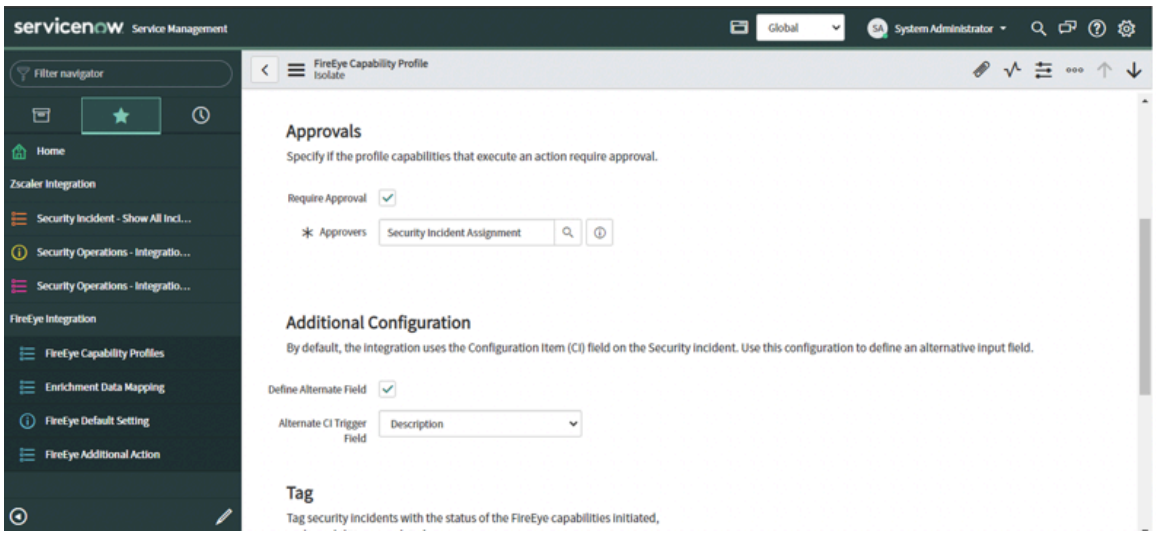
     Select the **Display Tag** check box to enable tagging security incidents, profile name is prefixed on enabling the tag. By default, this option is disabled for all profiles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **Approvals**: Select the **Require Approval** check box to provide an extra level of control when using the FireEye HX capabilities for isolating host machines, restoring them to the network, and to get the files.

  The approvals option in the profile configuration appears only for Isolate Host, Remove Host Isolation, and Get File capabilities.



4. Click **Done**.
5. Verify FireEye HX trigger conditions.

Verify the Trigger Condition Filters

Test the profile and verify that the trigger condition filters that you have configured are working as expected.

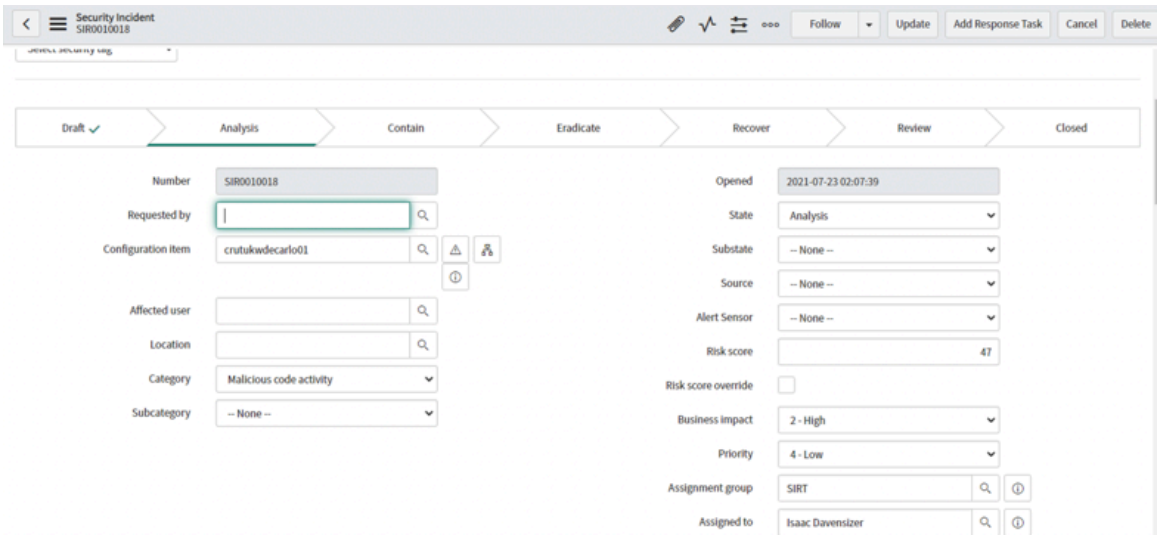
Before you begin
Role required: sn_si.admin or sn_si.analyst

Once you activate the profile, based on the configured trigger conditions you can view the query results in the ServiceNow AI Platform security incidents.

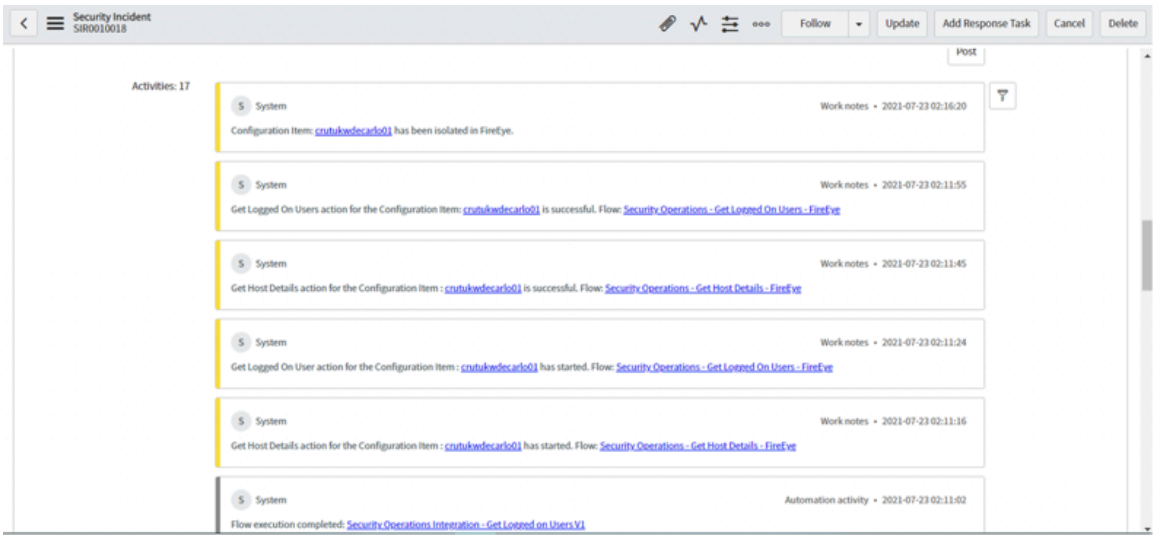
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select **New** to create a new security incident.
3. Provide the filter conditions as given in the capability profile to trigger the respective profile.



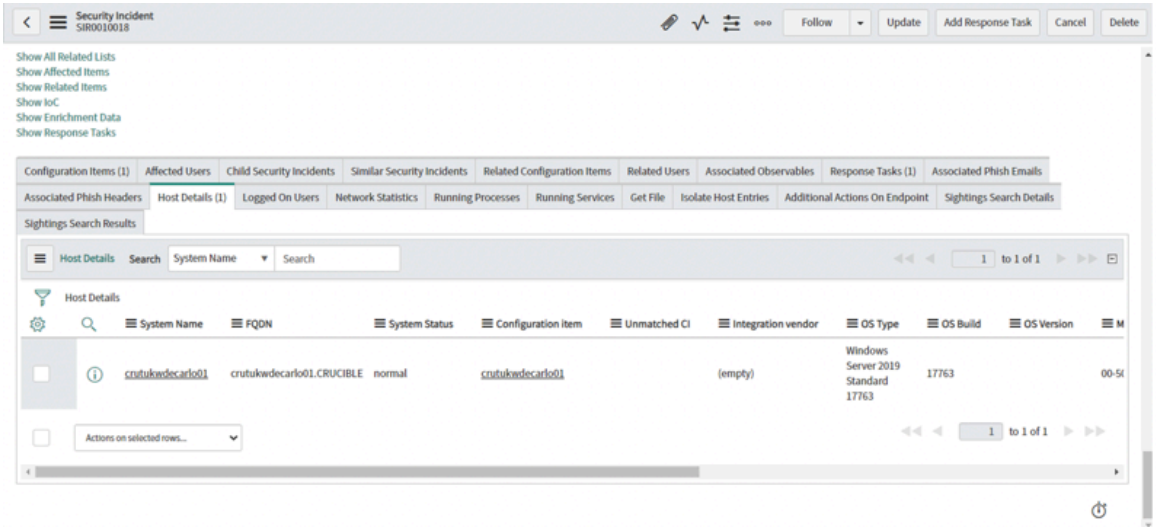
4. Click **Save**.



5. Review the work notes and activities section.
6. View the profile initiated, profile completed, or profile failed tags.
7. Click **Show all Related lists**.
8. Click any related list (tab).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, Host Details.



Trigger a FireEye capability profile from Related Links

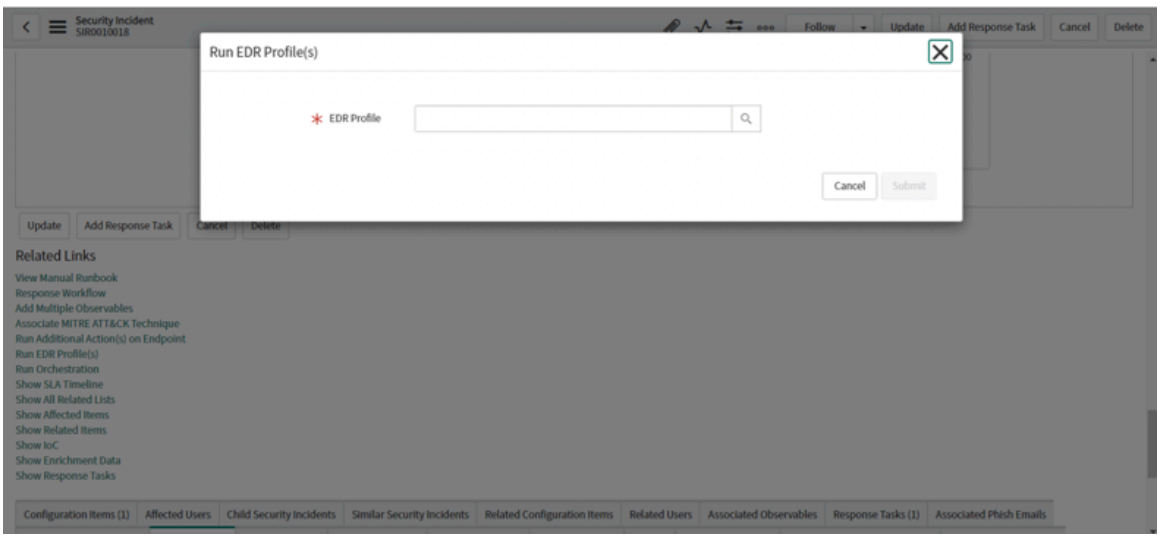
Trigger a capability profile manually after reviewing a security incident from related links.

Before you begin

Role required: sn_si.admin or sn_si.analyst

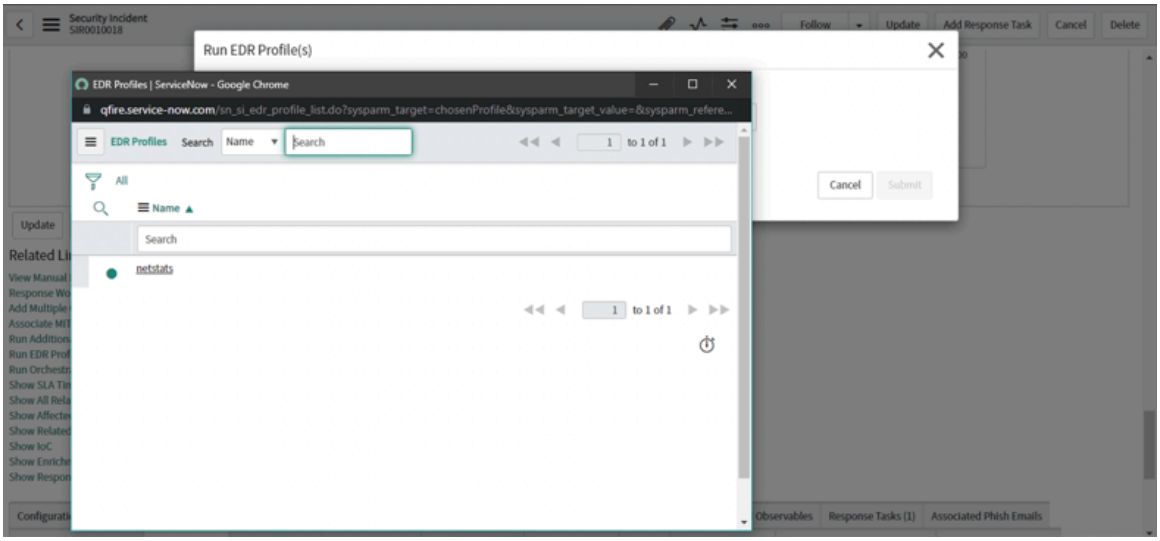
Procedure

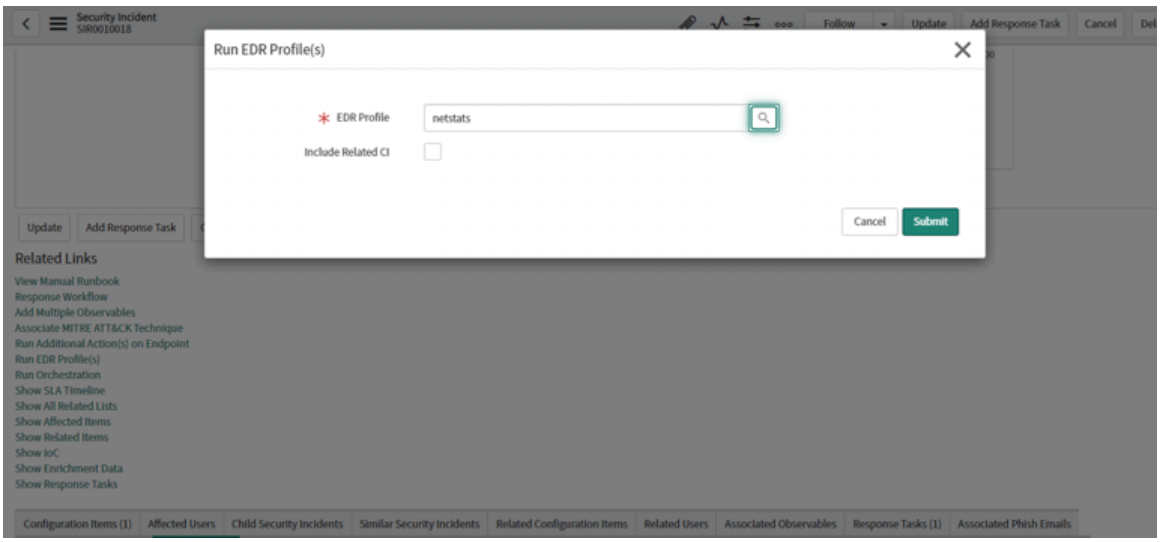
1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review.
3. Click **Run EDR Profile(s)**in the related links section.



4. Browse and select a profile from the list of available profiles and click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.





5. The selected profile is triggered manually.
6. Review the work notes and activities section.
7. View the tags and check the related lists for the data.

> **Note:** In addition to running the profile for the CI or the Alternate CI of the security incident, you could also run the profile for CI values present in the Configuration Item Related list by checking the Include Related CI on the dialog box. This will fetch data for the CI values present in the related list as well. Alternatively, you could run the profile just for the CI values present in the related list.

Trigger a FireEye Capability profile from Configuration Item related list

Trigger a capability profile manually from the configuration item related list.

Before you begin

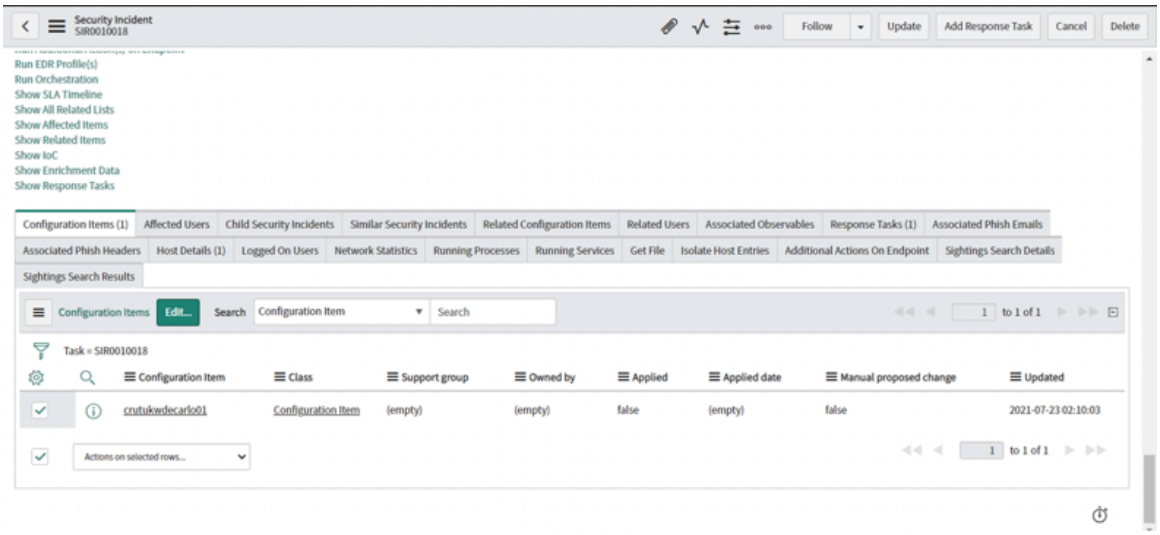
Role required: sn_si.admin, sn_si.analyst

Procedure

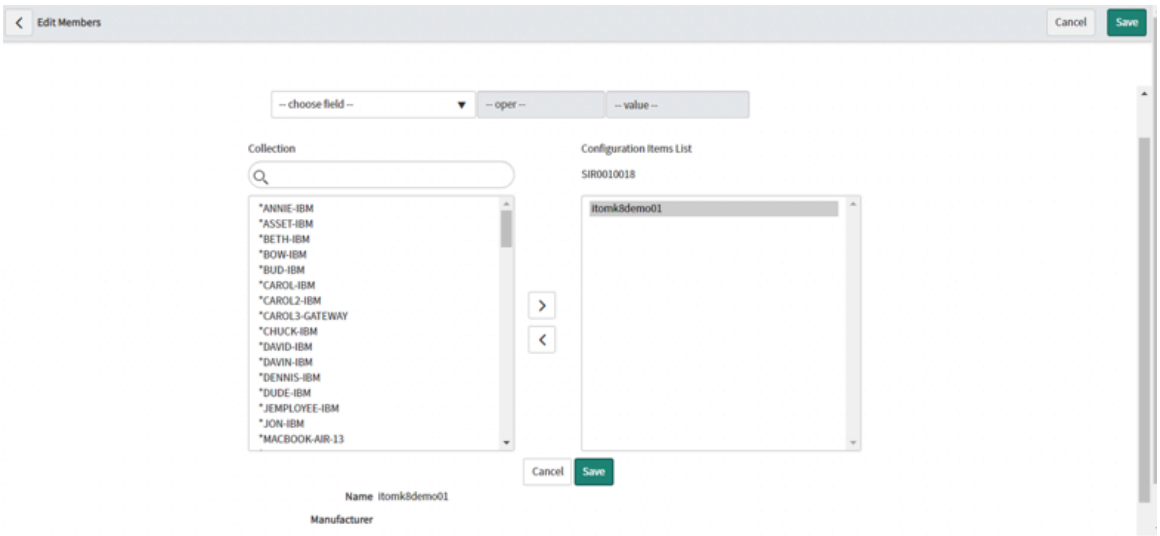
1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the FireEye HX information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Show all related lists** in the related lists section.
4. Click the **Configuration Item** related list.

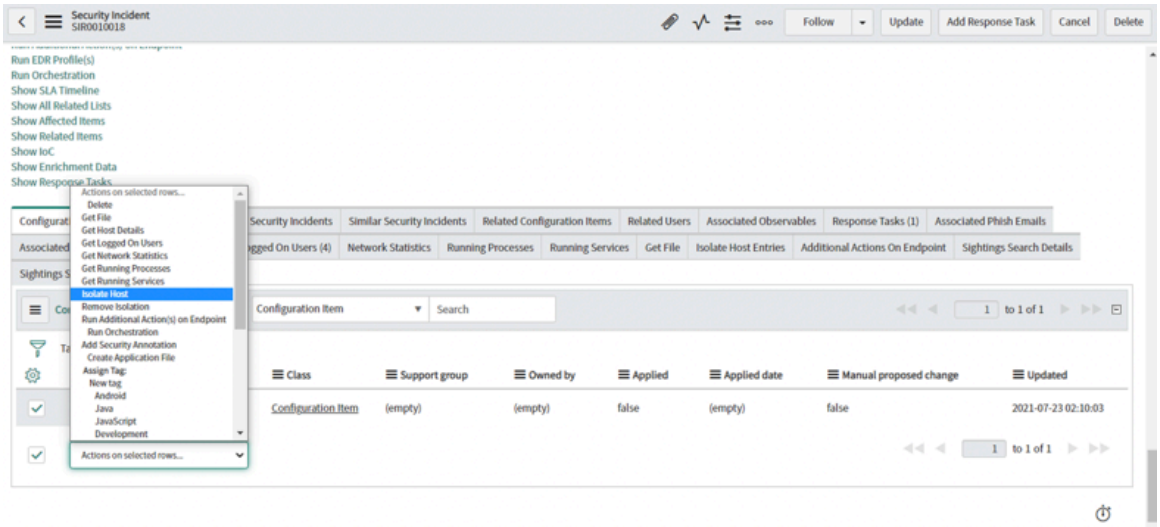


5. Click **Edit** to add the available configuration items, if values are not already present, and click **Save**.



6. Select the added configuration item(s), and from the Actions on selected rows, select a capability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. The selected capability is triggered manually.
8. Review the work notes and activities section.
9. View the tags, and check the data in the related lists.

FireEye Get File Capability

File acquisition requests instruct an Endpoint Security Agent to obtain a file from its host endpoint. File acquisitions are used for static or dynamic analysis of potential or verified compromises, as well as for evidence retention during insider threat investigations. Get File capability should be created as a separate profile.

Before you begin

Role required: admin

Triggering Get File Profile and create a FireEye HX capability profile with **Get File** capability.

Procedure

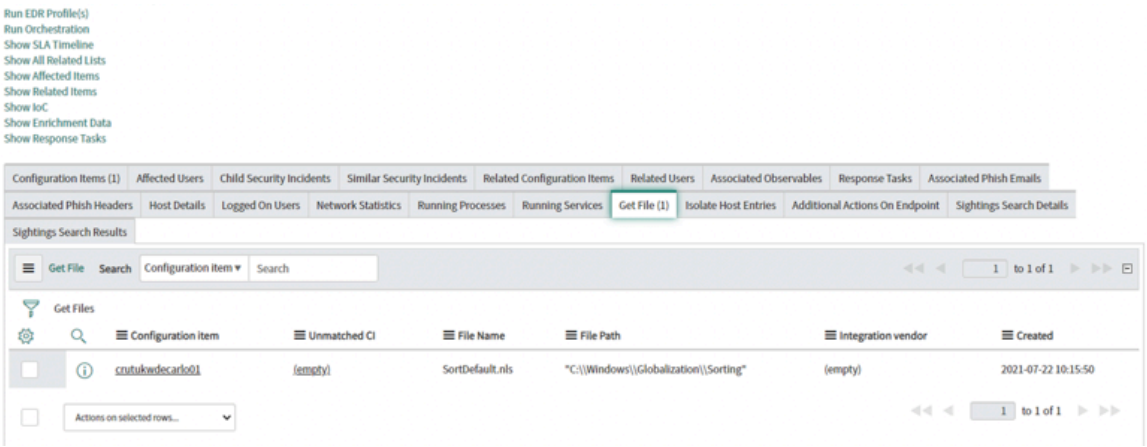
1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review.
3. Click **Run EDR Profile(s)**in the related links section.
4. Browse and select Get File profile from the list of available profiles.
5. Provide the **File name** and **File path**.

> **Note:** Enter the name of the file for which you want to acquire. Specify a precise path name or another appropriate path-based Windows environment variable. You must specify the drive letter or path names. Different endpoints may have different drive mappings. If you explicitly specify a folder name, you can end the path with a backslash. However, the final backslash is not mandatory.

6. Click **Submit**.
7. Review the work notes and activities section.
8. View the tags and check the results in the **Get File** related list.

> **Note:** The Get File profile is now triggered manually.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



To review a downloaded file acquisition:

- Open the file acquisition .zip file.
- Enter the password required to open the file. Password can be viewed by hovering over download link in FireEye HX Console. Follow the below steps to view the password:
  - Login to FireEye HX console.
  - Navigate to **Acquisitions** and filter by Acquisition type – File.
  - Select the desired record.

    Note: You will be able to see the details of the file acquired on the right tab.

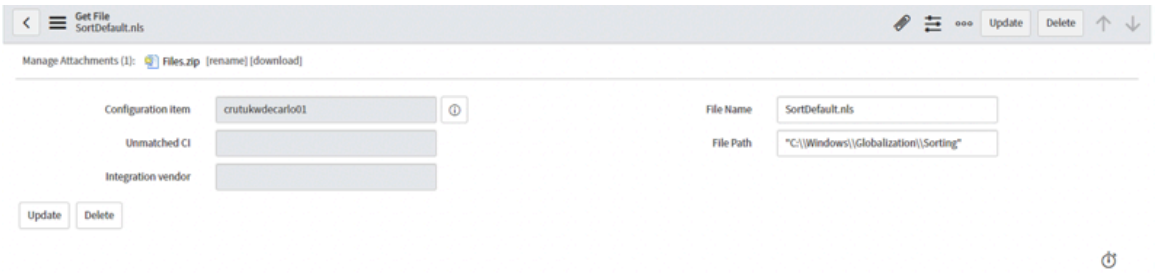
  - Hover over the **Download** link available at the top to get the password.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

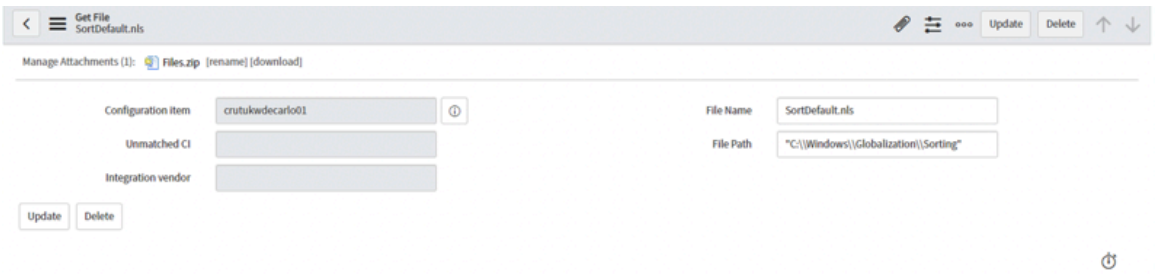
- Open and review the files within the .zip file using any text or XML editor.

Note:

- It is recommended that the file retrieved is added as an observable manually, so that it can be tracked as an evidence against the security incident. This will also help view the files in future, when password is forgotten or changed.
- The maximum file size supported for Get File action is 1024 MB, and this value can be configured by changing **com.glide.attachment.max_size**, and the default timeout is 60 minutes that can be configured from the FireEye HX Default Settings page.



- Get File can also be triggered from configuration item related list.



FireEye Additional Actions on Endpoint

FireEye integration supports running additional actions beyond the gold standard actions.

These actions comprise of Triage Acquisition and Data Acquisitions. Out of the box, two data acquisitions are supported:

- Comprehensive Investigative Details Script
- Standard Investigative Details Script

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In addition, Triage Acquisition is also supported out of the box. All these three are created by default along with the source. The customers can also create their own actions i.e., Data acquisitions from the FireEye Additional Actions Module.[1] The maximum file size supported for FireEye Additional Actions is 1024, and this value can be configured by changing **com.glide.attachment.max_size**, and the default timeout is 120 minutes that can be configured from the FireEye Default Setting page.

Comprehensive Investigative Details Script

Enables collecting all forensic and investigative artifacts from the endpoint but is the most prohibitively expensive option. This configuration is ideal for situations where there will only be one window for collecting data from the endpoint in question, and the ability to acquire more data cannot be guaranteed later. So, use this action with caution.

Standard Investigative Details Script

Enables the most common options for collecting forensic and investigative artifacts from an endpoint. Meant to be the primary response tool when you have suspicion that an endpoint may be compromised and need to perform a deep dive analysis of that endpoint. Aims to strike a balance between collecting the most relevant and valuable data whilst avoiding the costly options that can be collected later once further investigation proves them necessary.

Triage Acquisition

Triage collections contain information from within the lookback cache as well as additional forensic audit information, such as URL download history, file download history, process and ports listings, and standard system information. You might want to examine such information when anomalous network traffic is detected, and you want more visibility into endpoint actions.

Maintaining Data Acquisition Scripts on FireEye

Data acquisition requests (sometimes referred to as Live Response requests) allow you to acquire any data you need from a single running endpoint. Using the Data Acquisition Scripts page on FireEye, you can create, edit, copy, and delete the data acquisitions scripts used for data acquisition requests.

Accessing the Data Acquisition Scripts Page on FireEye

To access the Data Acquisition Scripts page:

1. Navigate to Endpoint Security web user interface.
2. Select Data Acquisition Scripts on the Admin menu.

Creating a Script on FireEye

To create a data acquisition script:

1. Select **Data Acquisition Scripts** > **Admin** menu of the Endpoint Security web user interface.
2. Click **Create Script**.
3. Enter a name for the new script in the **Script Name** field.
4. Optionally, enter a description of the script.
5. Select the operating system to which the script applies. You can only select a single operating system on the Create Script dialog.
6. Click **Create** to start the script definition.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select an acquisition data type in the **Add an acquisition type**drop-down box and click **Add**. Options for the acquisition type you requested appear to the right of the script list.
8. Supply values for the acquisition type options or use the default values that are already selected. The Web UI does not warn you or remove tabs, spaces, or unwanted characters (such as \n) in your specifications.
9. Repeat the previous 2 steps to request additional data for the data acquisition script. Some acquisition data types are available only once for a script, while others can be specified more than once. After adding an acquisition type to a script, the list of acquisition types available in the **Add an acquisition type**drop-down box adjusts appropriately.
10. To remove an acquisition data type from the script, click the x icon ( ) on the acquisition tab on the left side of the page.

Note: This integration does not support **Allow Edits before acquiring** option while creating scripts. So, ensure that the check box is unchecked.

Exporting a Script from FireEye

You can export a data acquisition script to a JSON file. To export a data acquisition script:

1. Select **Data Acquisition Scripts** > **Admin** of the Endpoint Security web user interface.
2. Select Data Acquisition Scripts on the Admin menu.
3. Select the script you want to export on the left side of the page.
4. select **Actions** > **Export Script**.
5. A JSON file is downloaded to your computer. The JSON file name includes the operating system so you can easily determine which scripts are for which operating system.

Creating a new Data Acquisition Action in the ServiceNow AI Platform

To create a new action, follow these steps:

1. Navigate to **FireEye Integration** > **FireEye Additional Actions**. The FireEye Additional Actions list is displayed.
2. Click **New**. The form for the new action is displayed.
3. Fill out of the form.

Action Name	Name of the FireEye action that is performed. This name helps you identify the Action type and describe it.
Acquisition	An acquisition obtains the data to analyze. This is a read only field, and is defaulted to Data Acquisition.
Source	Name of the FireEye source. Only configured sources are available from the choice list.
Capability	This is a read only field and is populated with Run Additional Action(s) capability
Acquisition Type	Type of acquisition action that needs to be obtained, and analyzed.
Active	This indicates that the Action is active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Require Approval	When you enable the Require Approval option, the Approvers field is available on the form. After you submit a request, approval is required from the group to complete the request.
Display tag	Type of operation system such as Windows, Mac, Linux for adding scripts. **Note:** Only one type of OS is supported currently. You can create one action per operating system. For other operating systems, create new actions as required.
Scripts	Imported script from FireEye needs to be provided for the selected OS Type. Only one script can be added to each OS type.

4. Click **Submit**.

Triggering Data Acquisitions from Security Incident

The Additional actions created can be run via the Related Link called **Run Additional Action(s) on Endpoint** on the security incident.

Note: **Allow Edits before acquiring** FireEye functionality is not supported for the Additional Actions on Endpoint.

Create and configure a profile for sightings search with the FireEye Integration

Configure the sightings search profile using the following procedure.

Before you begin

Role required: NowPlatform Security incident administrator (sn_si.admin)

Whenever a source is created, individual sightings search configurations for five types (File, IPs(v4), MD5, SHA1 and SHA256) will be created and inactive by default. You should make it active before using Sighting Search. Each Observable type is having different search query to retrieve sightings. We would be initiating a different search for each observable type. Multiple observables search for a sighting search is not possible in FireEye as it would perform an AND operation on the observables and the result might be inaccurate.

Note: For Sightings search only five active searches can be present at once. Remaining will be queued and will start after the completion of any one of the ongoing sightings.

If you want to create a new sightings search profile, follow the steps below to create one:

Procedure

1. Navigate to **Integrations** > **Sightings Search Configuration**.
2. Click **New**.
3. On the form, fill the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name for the capability profile.
Is saved search	This will run a saved search i.e. the Name field should match the name of the saved search.
Sightings search source	Defines the source configured for the integration.
Search	Add a native search string to form a query.
Active	Query will run only if it is active.
Observable type	Defines the type of observable category.
Maximum observables per search	The number of observables before the search query is split into multiple queries. Set this value to 1 for this integration.
Sightings search parameters	Use Sightings Search Parameters to define more complex queries that include logic and other operators supported by specified log store.

4. Click **Submit** to complete the configuration.

Invoke Sighting Search from a Security Incident

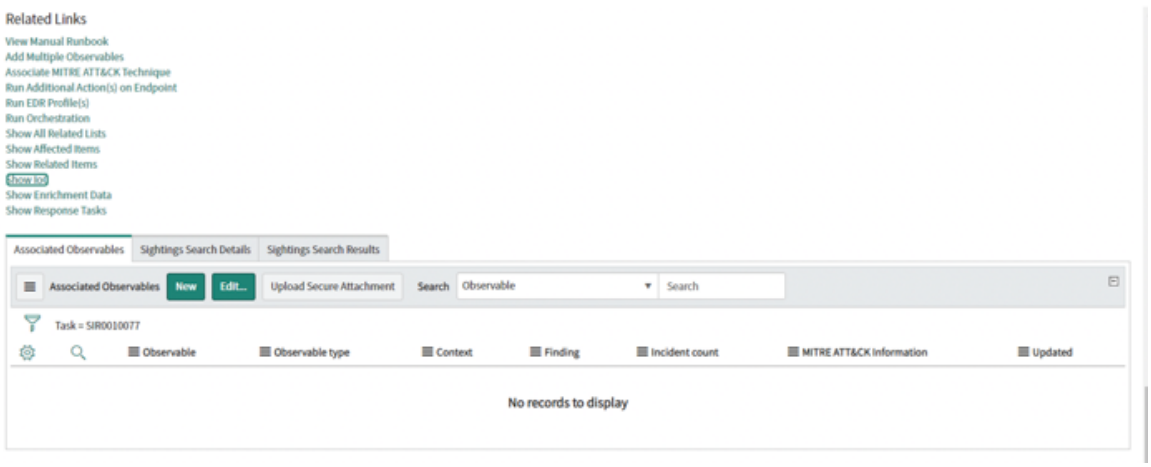
Invoke the sightings search from a SIR security incident by following the below procedure.

Before you begin

Role required: ServiceNow AI Platform administrator (sn_si.admin)

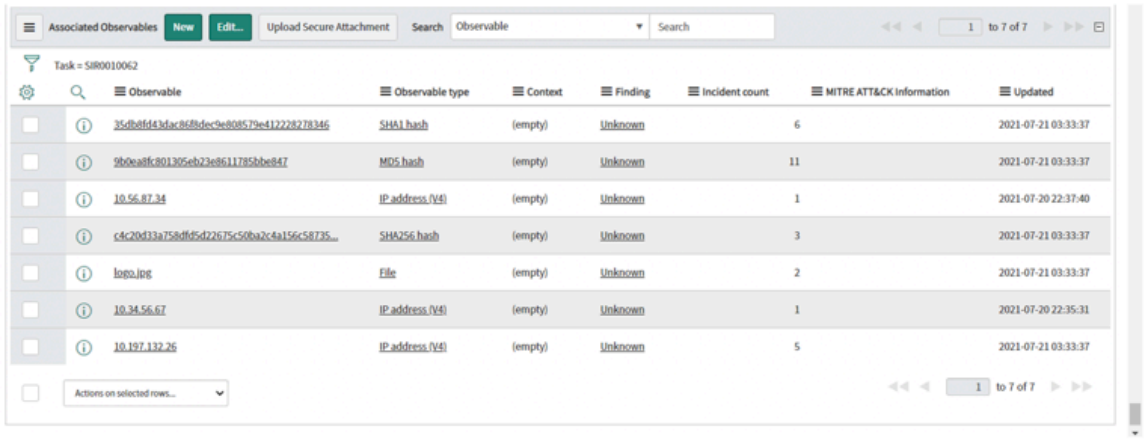
Procedure

1. Navigate to the Security Incidents.
2. Open any existing SIR or create a new SIR.
3. Click Show IoC in Related Links.
4. Click **Associated Observables** related lists.

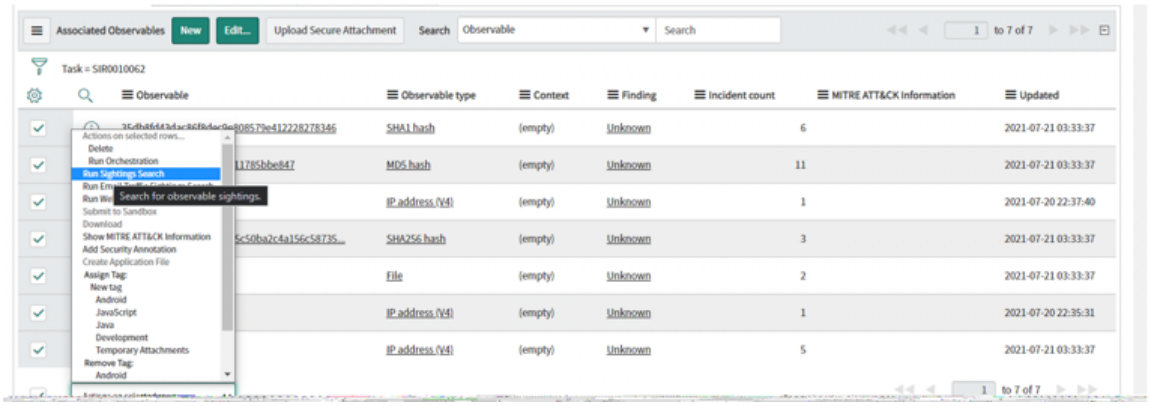


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

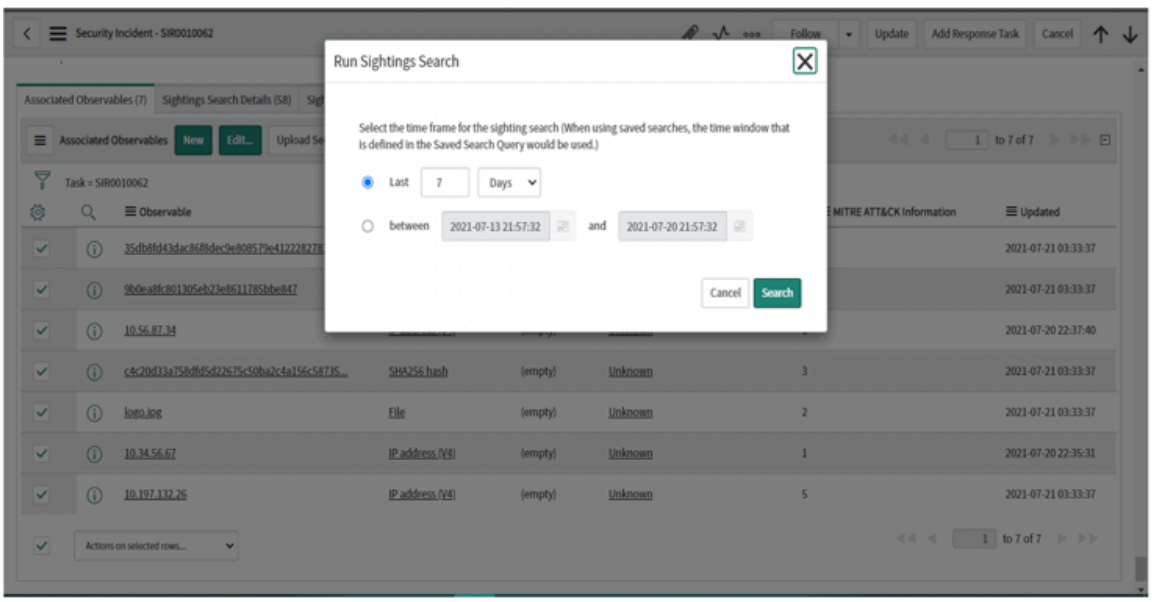
5. Add any existing observables or create new observable.



6. Select the observables and from Actions on selected rows, click **Run Sightings Search**.

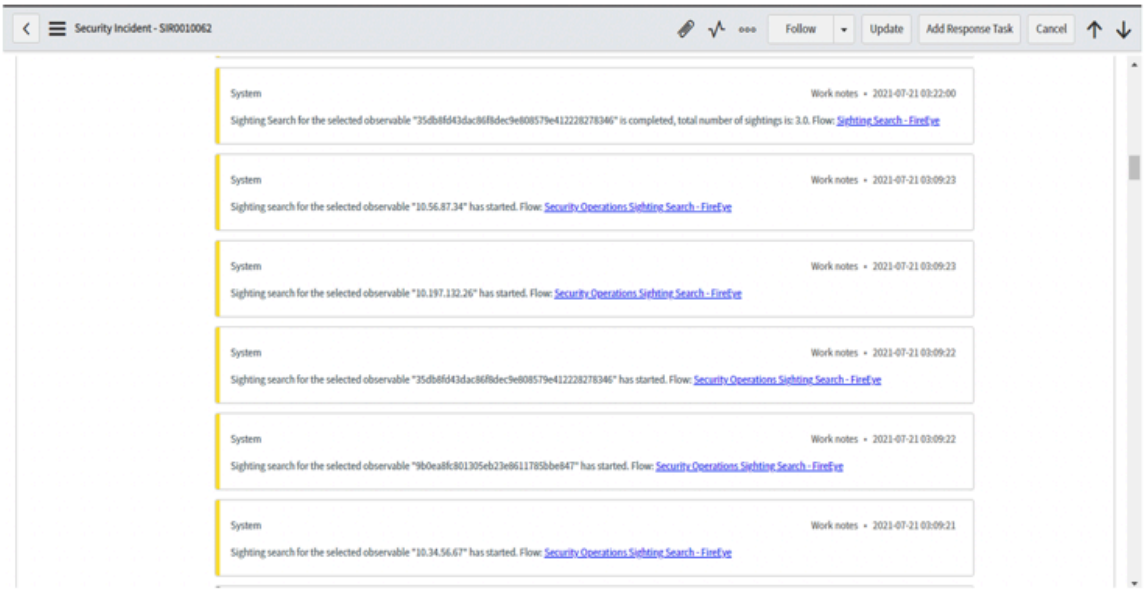


7. Ignore the inputs in the next dialog box that asks for time data.
There are default values populated. However, the search is performed real time and the time values are ignored for this integration.



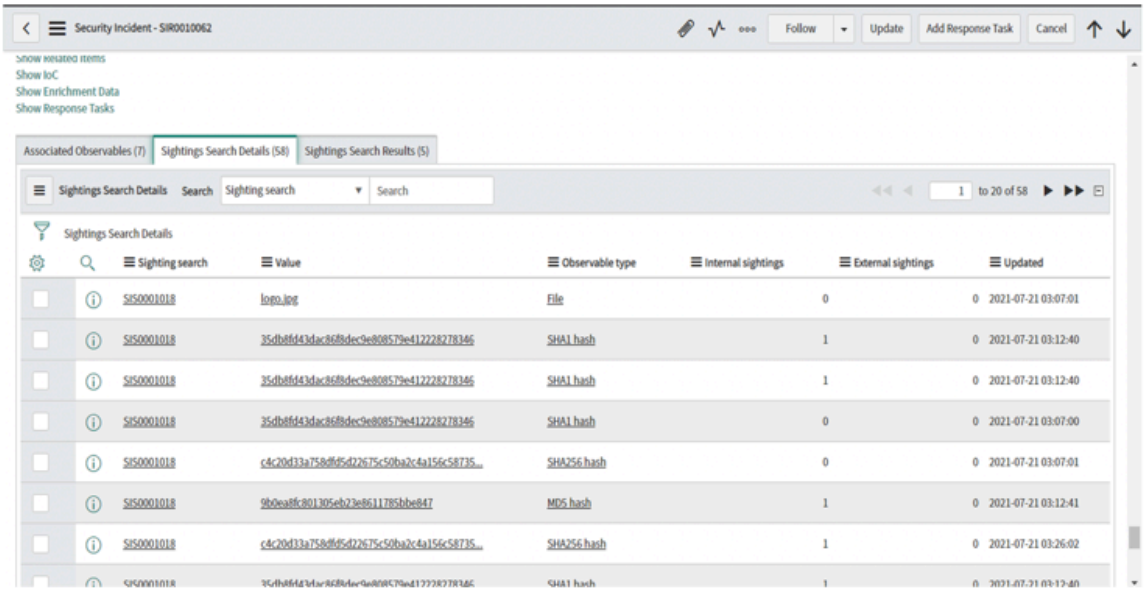
8. Check the worknotes for status.

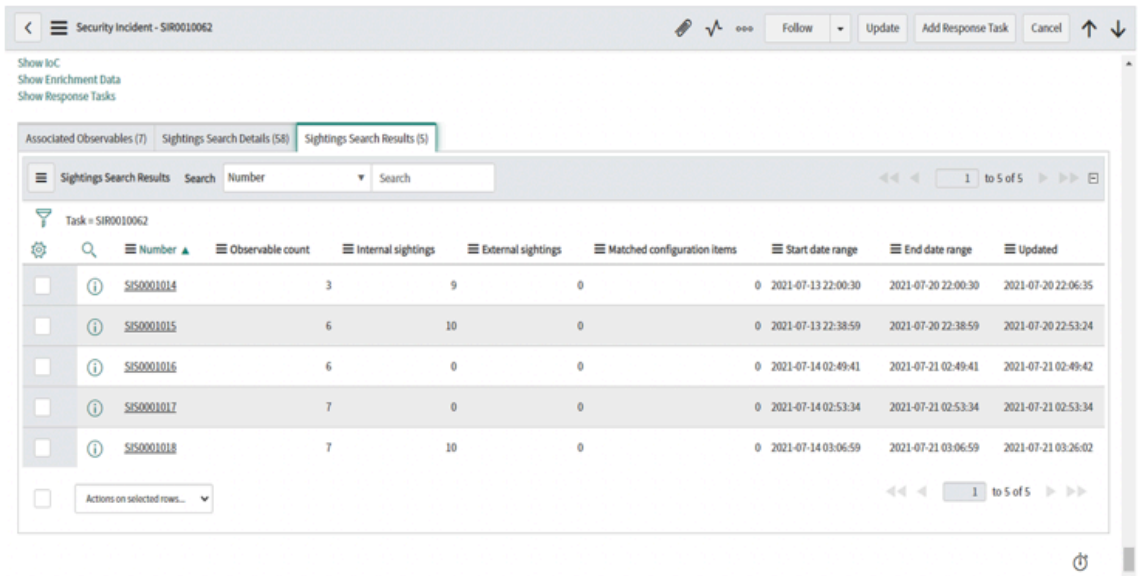
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. On completion of the search, check the results and details in the related lists.
10. Click on **Sightings Search Details** tab for details and **Sightings Search Results** tab for search results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.





Have I been pwned? integration

The Security Operations Have I been pwned? integration enables you to submit lookups on domain names and email addresses to determine whether user personal data has been compromised by data breaches.

Explore

Security Incident Response integrations

Set up

- Security Operations Have I been pwned? integration setup
- Activate the Security Operations Have I been pwned? integration

---

Use

Develop

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

Perform lookups on observables Threat Lookup - Have I been pwned? flow

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Security Operations Have I been pwned? integration setup

Have I been pwned? is a free resource used to assess if someone may have been put at risk due to their online account being compromised or "pwned" in a data breach. It easily integrates with Security Operations.

Before you can use the Have I been pwned? integration, you must activate the plugin. If necessary, you can also update your X509 SSL certification.

The Security Incident Response, Threat Intelligence, and Security Operations Have I been pwned? plugins are required to implement the Security Operations Have I been pwned? integration.

Threat Lookup - Have I been pwned? flow

The Threat Lookup - Have I been pwned? flow performs a lookup on selected observables. If the observables are of a type recognized by Have I been pwned?, the observables are scanned for malware, and the results are returned.

Role required: sn_si_admin

This flow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the Have I been pwned? implementation is selected. For more information, see Perform lookups on observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Have I been pwned flow



For information on the activities used by this flow, see Common Security Operations integration flows and orchestration Flow Actions.

Activate the Security Operations Have I been pwned? integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Have I been pwned? integration. Before you can use the Have I been pwned? integration, you must download it from the ServiceNow Store.

Before you begin

- The Threat Intelligence plugin must be installed and activated before you can use the Security Operations Have I been pwned? Integration.

Role required: sn_si_admin

Procedure

Download the integration from the ServiceNow Store.
This integration supports an open API and does not require further configuration. Have I been pwned? can now be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related topics

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Acquire the SSL certificate from the third-party vendor.
   For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.

   a. Enter the endpoint URL into the browser address bar.
      For example: `https://<3rdparty>/`.

   b. Click the lock icon in the address line.

   c. Click **More Information** and click the **Security** tab.

   d. Click **View Certificate** and click the **Detail** tab.

   e. Click **Export** to save the PEM into your local file system.

   f. Open the saved file in any text editor tool and copy the content to the clipboard.
      It must begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

2. Navigate to **System Definition** > **Certificates**.
3. Click **New** and create a new record for the integration.
4. In **PEM Certificate**, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Add the certificate to the Identity Provider record.
   a. Navigate to **Multi-Provider SSO** > **Identity Providers**.
   b. Select the active default identity provider for which you created the new certificate.
   c. Scroll down to **X.509 certificates** related list, and click **Edit**.
   d. Move the newly created certificate to the **Selected** column.
6. Click **Save**.
   The other fields in the record are generated automatically.

> **Note:** If you have a certificate that has expired, you need to remove it. For information on how to remove the expired certificate, refer to KB0691439 Replacing an expiring SAML certificate.

HPE Security ArcSight ESM - Email Parser integration

The HPE Security ArcSight ESM - Email Parser integration is supported using an email parser that consumes email notifications from ESM to create security incidents.

Configure HPE Security ArcSight ESM - Email Parser integration

HPE Security ArcSight ESM - Email Parser integration uses email notifications from ESM to drive enrichment, and response workflows.

Before you begin

Role required: sn_si_admin

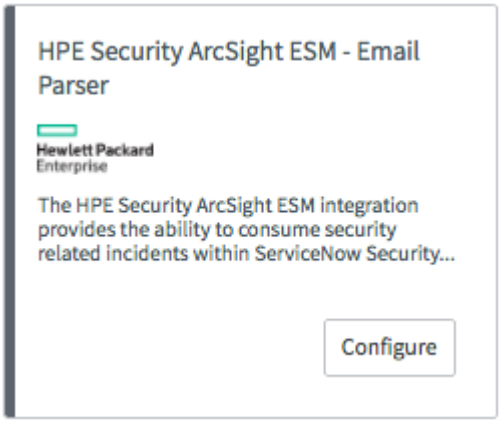
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

An HPE Security ArcSight ESM - Email Parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.

Procedure

1. Navigate to **All** > **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.



2. In the HPE Security ArcSight ESM - Email Parser card, click **Configure**.
3. In the **HPE Security ArcSight ESM - Email Parser Configuration** dialog box, click the **Configure Email Parser** link.
4. Click the **ArcSight ESM** link to edit the settings in the template email parser provided.
   At a minimum, fill in the `Email is from` field. To create you own email parser, see Create email parsers in Security Operations.
5. Check the **Active** box.
6. Click **Update** in the **Email Parser** form.
   The email parser is active. You do not need to return to **Integration Configurations**.

HPE ArcSight Logger - Incident Enrichment integration

The HPE ArcSight Logger - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

Explore

Security Incident Response integrations

Set up

- Get started with the HPE ArcSight Logger - Incident Enrichment integration
- Create sightings search configuration records

Use

Develop

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Run a Sightings Search
- Security Operations Integration - Sightings Search Flow
- Security Operations - Arcsight Logger Sightings Search Flow
- View Sightings Search Details
- View Sightings Search Results
- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Get started with the HPE ArcSight Logger - Incident Enrichment integration

HPE ArcSight Logger streams real-time data and categorizes them into specific logs and easily integrates with Security Operations. Before you can use the HPE ArcSight Logger - Incident Enrichment integration, you must download it from the ServiceNow Store and add API URL and login credentials.

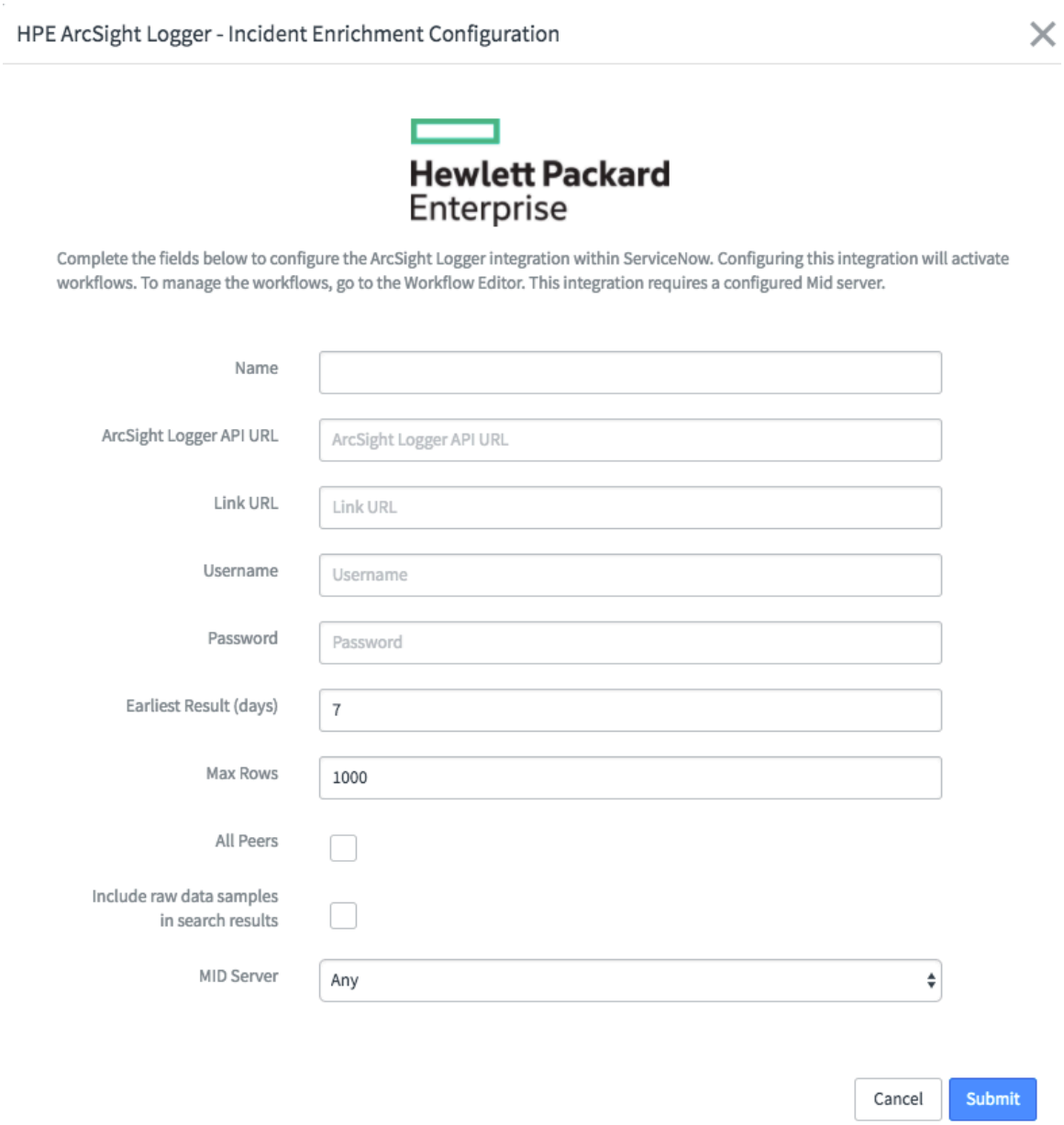
Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.
3. In the HPE ArcSight Logger - Incident Enrichment card, click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.
ArcSight Logger API Base URL	The base URL you acquired from the HPE Security ArcSight Logger site.
Link URL	[Optional] The Link URL that links to an HPE Security ArcSight Logger instance, when available.
Username	Your Intel HPE ArcSight Logger username.
Password	Your Intel HPE ArcSight Logger password.
Earliest Result (days)	The earliest results you want to see in number of days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Max Rows	The maximum number of rows you want to search.
All Peers	The default is unchecked and searches only the local logger you are connected to. When checked, it searches all the loggers that are connected to one another.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

5. Click **Submit**.
   The integration configuration card displays.
6. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Hybrid Analysis integration

The Hybrid Analysis application is part of an open online community in which users analyze files and URLs for threats. You share results and utilize research from the community for more effective incident responses. When integrated with the ServiceNow AI Platform Security Operations product, the shared threat intelligence provides you with additional insight into the severity of specific observables.

The Hybrid Analysis integration performs threat lookups on the following observables:

- File hashes
- IP addresses
- URLs

The flow checks for new observables as they arrive in security incidents. If the observables are of a type recognized by the API integration, the observables are evaluated. Observables determined to be malicious are tagged.

Install and configure Hybrid Analysis

Before you run the integration on your instance, complete the installation and configuration steps so the Hybrid Analysis application properly integrates with ServiceNow AI Platform Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform and Security Incident Response roles.	The following roles are required for installation, configuration, and verification of expected results: • The administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module and assigns the sn_si.analyst role.
Obtain an API key.	Visit the Hybrid Analysis website for information on API keys and to create an account: Hybrid Analysis website. The configuration requires that you enter the API keys.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	For the Madrid release and later family releases, the com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications. The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation: **1.** Security Integration Framework **2.** Security Support Common **3.** Security Support Orchestration **4.** Security Incident Response For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Role required: admin

About this task

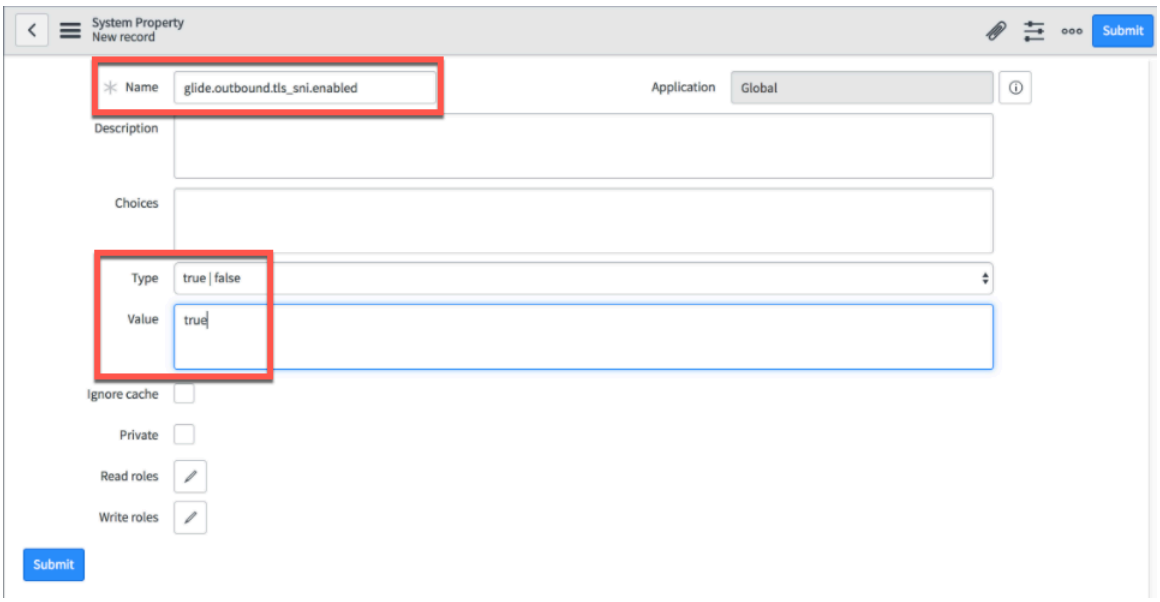
Perform the following steps to update system properties and install and configure the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

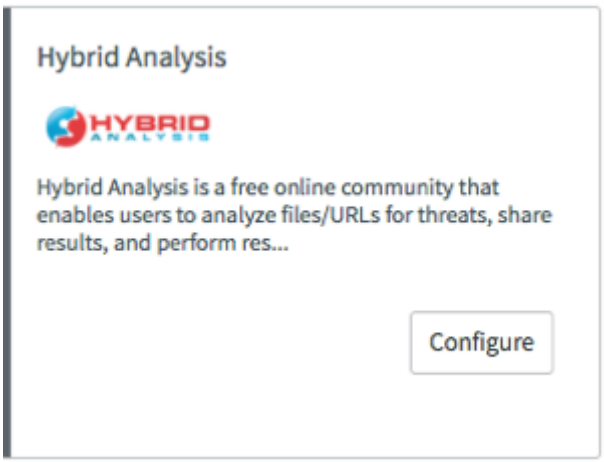
Procedure

1. In the navigation filter, enter `sys_properties.list` and press **Enter**.
   The **System Properties** list is displayed.
2. Click **New**.
   A new record is displayed.
3. Fill in the fields, or select the values listed in the following table and click **Submit**.

Field name	Value
Name	`glide.outbound.tls_sni.enabled`
Type	Select **true I false**
Value	`true`

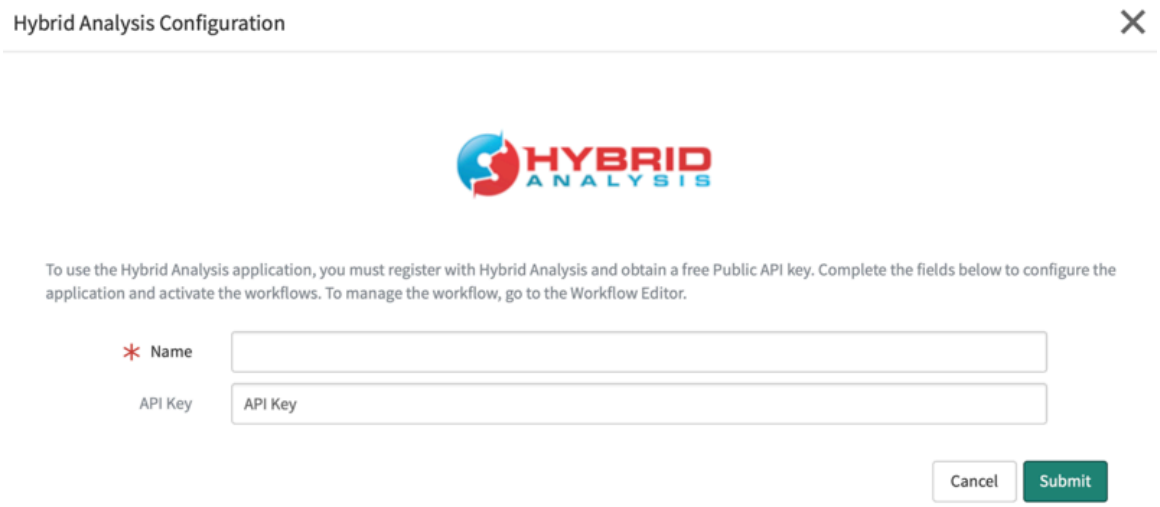


4. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
5. After the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the Hybrid Analysis tile.
6. Click **Configure**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. In the **Hybrid Analysis Configuration** dialog box, enter the API key you obtained from the Hybrid Analysis website and click **Submit**.



8. Verify successful configuration.
   Configuration is successfully completed unless an error message is displayed.

   Trouble?

   If an error message is displayed during the configuration, the Hybrid Analysis API key may be invalid.

Verify expected results for Hybrid Analysis

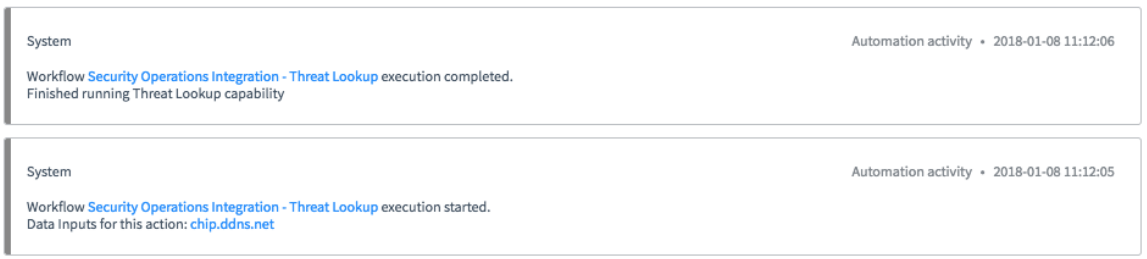
Observables are generated automatically by a security incident and scanned by the application. Locate the lookup results on the security incident to verify the threat lookup has run successfully. Also view raw data and run threat lookups on child observables.

Before you begin

Role required: sn_si.analyst

Procedure

1. Open the security incident record you are working with and verify that the lookup has run successfully.



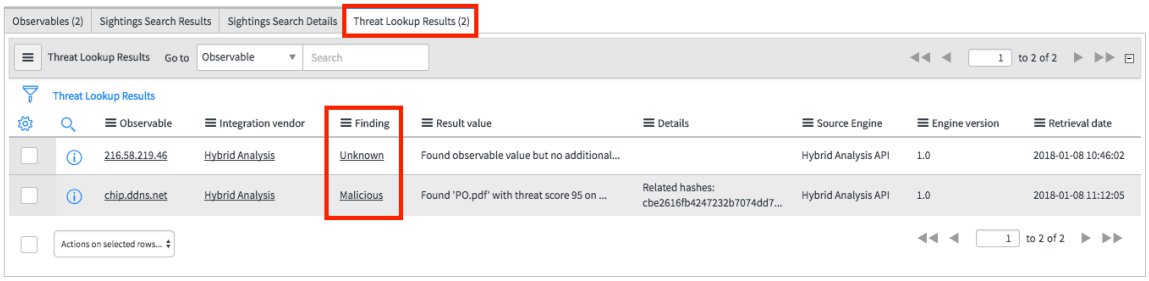
   After the application is configured, the flow launches automatically upon incident creation. The execution and completion status of the lookup is then displayed in the work notes in the security incident.

2. Review the work notes for more information on how to proceed if you cannot verify that the lookup ran successfully.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

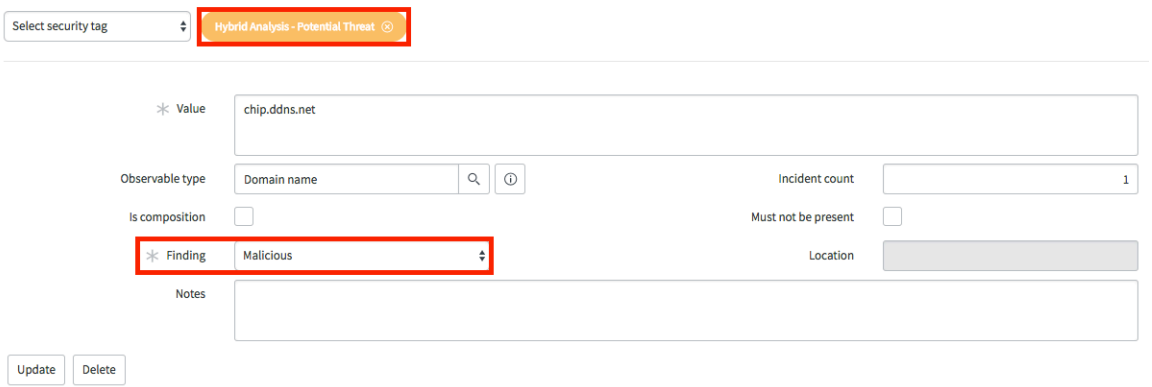
3. Navigate to the bottom of the security incident record and click the **Show All Related Lists** related link to view results.

   Note: The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. In the upper-right corner of the banner frame, click the Settings gear icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.



   The **Threat Lookup Results** tab displays the lookup results at the bottom of the security incident record. Note the **Finding** column displays `Unknown` for records not determined to be malicious. For results matching malicious, the **Finding** column displays `Malicious`.

4. In the **Observable** column, click an observable to open the record.



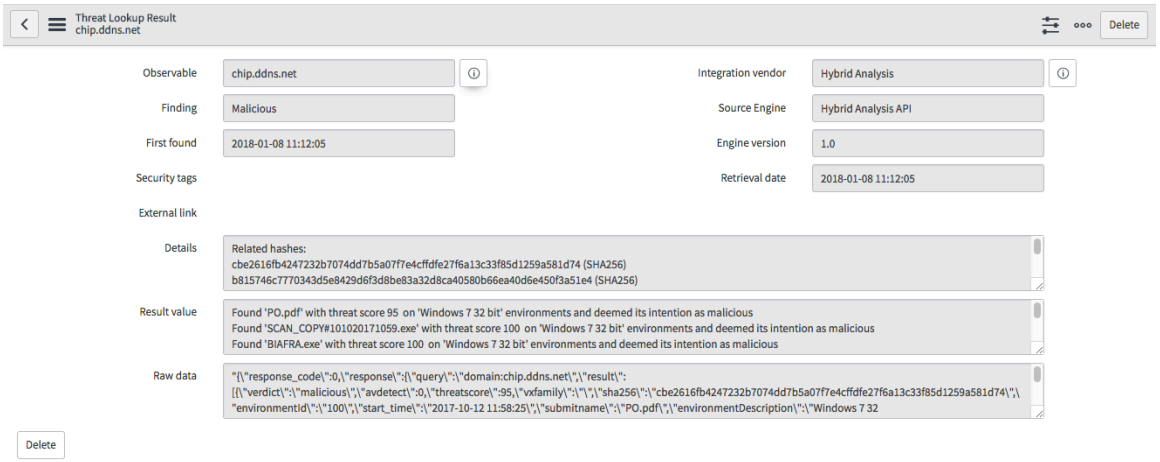
   For lookups matching malicious, the **Finding** field displays `Malicious`, and the observable is tagged with the Threat Intelligence source that found it to be malicious, in this case, the Hybrid Analysis integration.

5. **Optional:** Follow the steps to view raw data, view a list of child observables, and run a threat lookup on selected child observables.

   a. Navigate back to the security incident and on the **Threat Lookup Results** tab, click the blue information icon next to an observable.

   b. In the window that is displayed, click **Open Record** to view the data.
   From any observables viewable in the raw data that is displayed from the lookup, the Hybrid Analysis integration also creates child, or related observables.

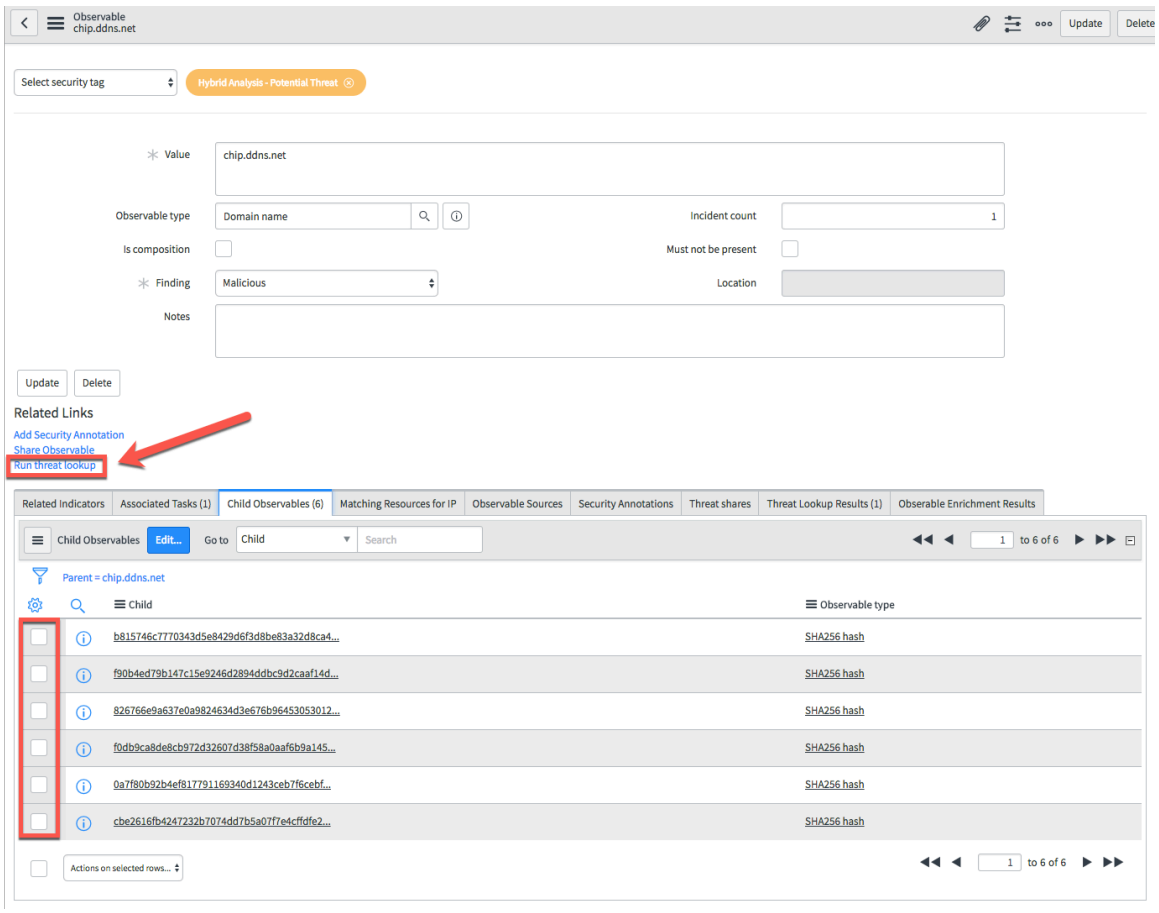
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The link created by the API, the raw data, and other information are displayed.

c. Navigate back to the security incident and click the **Show IoC** related link.
The child observables are displayed on the **Child Observables** tab on the security incident, because the lookup has found an existing connection between these related observables and the observable initially submitted.

d. Click the field next to an observable in the **Child** column to select it, followed by the **Run threat lookup** related link to perform a lookup.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. In the dialog box that is displayed, verify that the Hybrid Analysis integration is selected and click **Submit**.

f. In the work notes, verify that the lookup has run successfully, and on the **Threat Lookup Results** tab in the security incident, locate lookup results for the child observables.

Trouble?
If you do not see results under the **Threat Lookup Results** tab, verify that the observable is a type that is supported for lookup by the integration.

(Optional) Manually attach an observable for Hybrid Analysis

You can manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

Before you begin

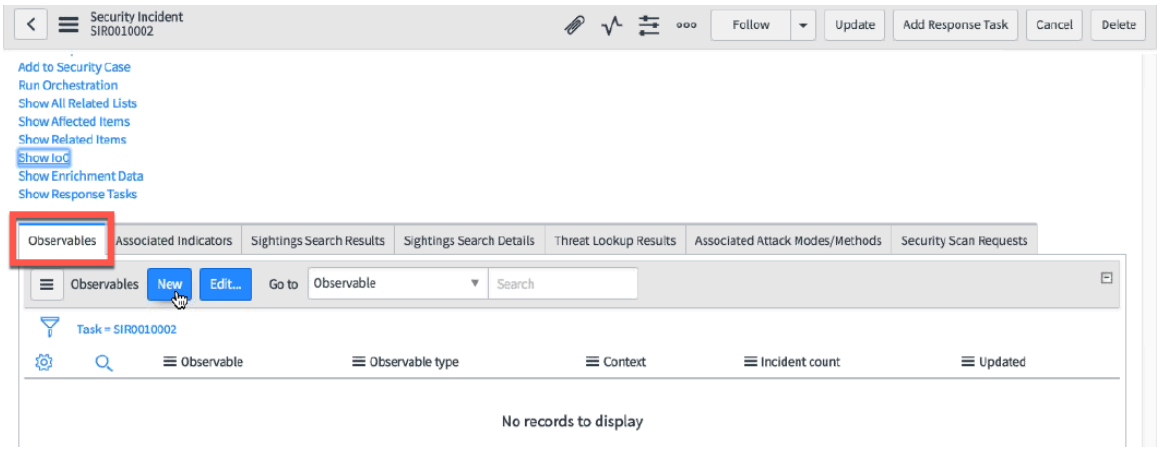
Verify the observable is of a type supported by the integration. The integration performs lookups on the following types of observables:

- File hashes
- IP addresses
- URLs

Role required: sn_si.analyst

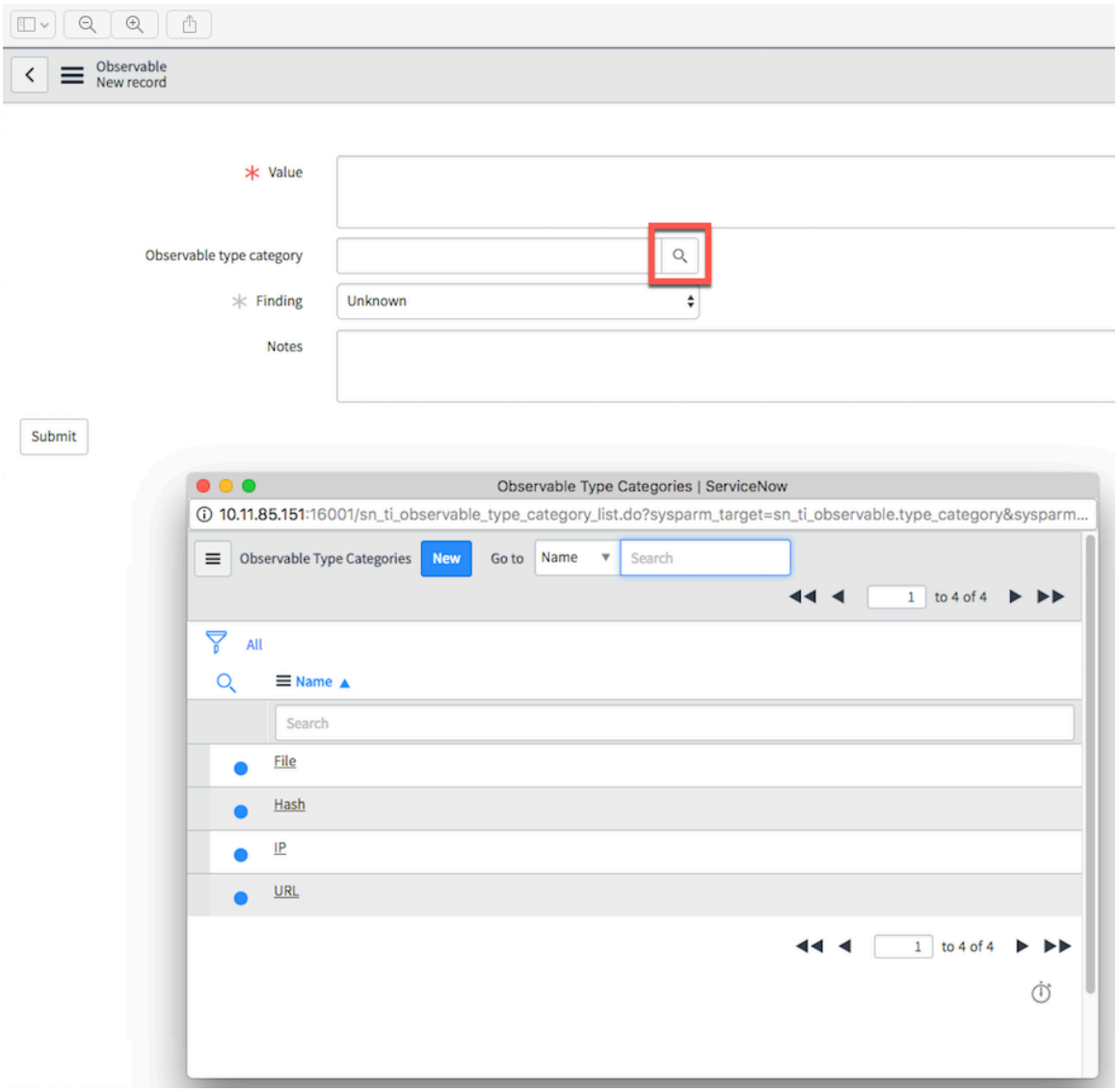
Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents** and open a security incident to which you want to attach the observable.
2. On the open security incident, click the **Show IoC**link in **Related Links**.

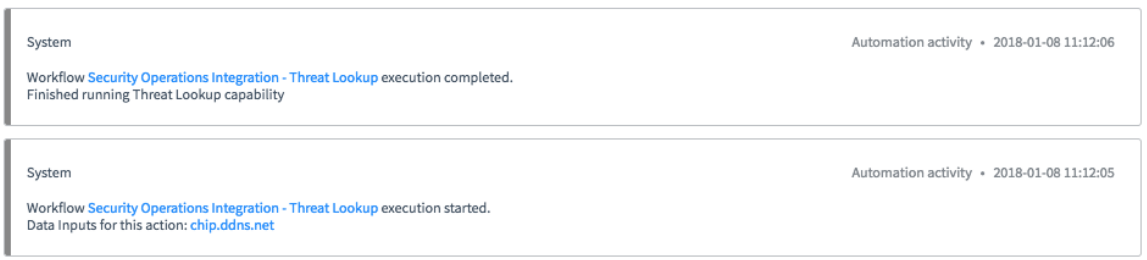


3. On the **Observables** tab, click **New**.
   The Observable form is displayed.
4. In the **Value** field, enter an observable (file hash, IP addresses, or URL).
5. Click the search icon and from the **Observable Type Categories** dialog box, click the desired observable type in the list to populate the field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

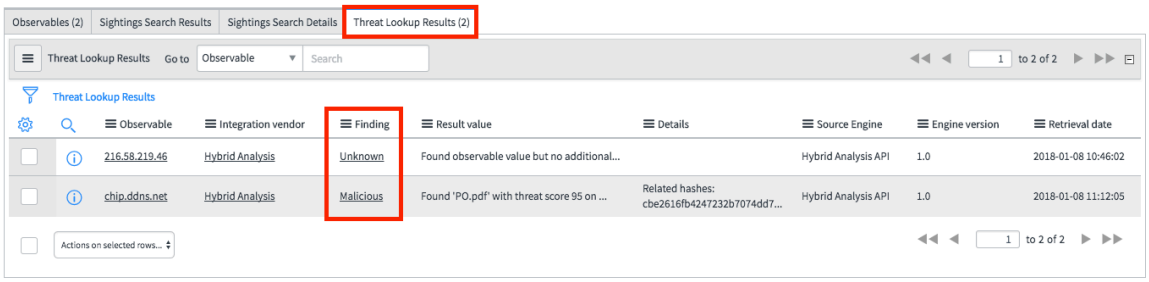


6. Click **Submit**.
   The flow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the security incident record.
7. Navigate to your security incident and review the work notes.

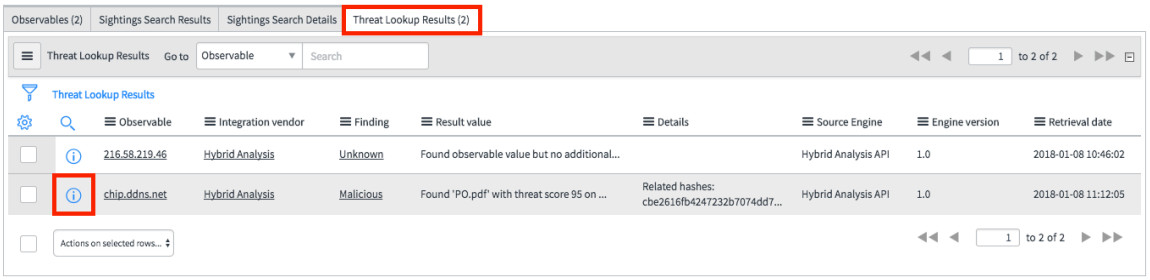


8. At the bottom of the record, click the **Show All Related Lists** related link.
9. Click the **Threat Lookup Results** tab to view the results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



10. In the **Observable** column, click the blue information icon next to a given observable for more information and raw data.



11. In the dialog box that is displayed, click **Open Record** to view the raw data and more details. Alternatively, you can also attach an existing observable to the security incident record.
12. **Optional:** With the **Observables** tab selected, click **Edit**.
13. **Optional:** In the **Edit Members** form that is displayed, move an existing observable from **Collection** to **Observables List** and click **Save**.
    You are returned to the security incident.
14. In the far left column, select the observables you want to run the lookup on, and from the **Actions on selected rows...** choice list, select **Run threat lookup**.
    A message is displayed across the top of the record that the request is being processed. Verify that the lookup has run successfully.

Trouble?
Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

IBM QRadar Offense Ingestion Integration

The IBM QRadar Offense Ingestion integration allows you to automatically fetch IBM QRadar offenses and convert them into security incidents and enable automated response actions.

This integration supports the following:

- Discovery of IBM QRadar offenses that are candidates for security incidents.
- Fetching recent events or flows associated with an offense.
- Track key updates to offenses periodically.
- Mapping of offense, event, and flow fields to security incident fields.
- Preliminary view of the mapped fields.
- Setup scheduled ingestions of offenses to create security incidents periodically.
- Close the offenses when the security incidents are closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install and configure the ServiceNow application for the IBM QRadar offense ingestion integration

Before you run the integration on your ServiceNow AI Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.admin

Procedure

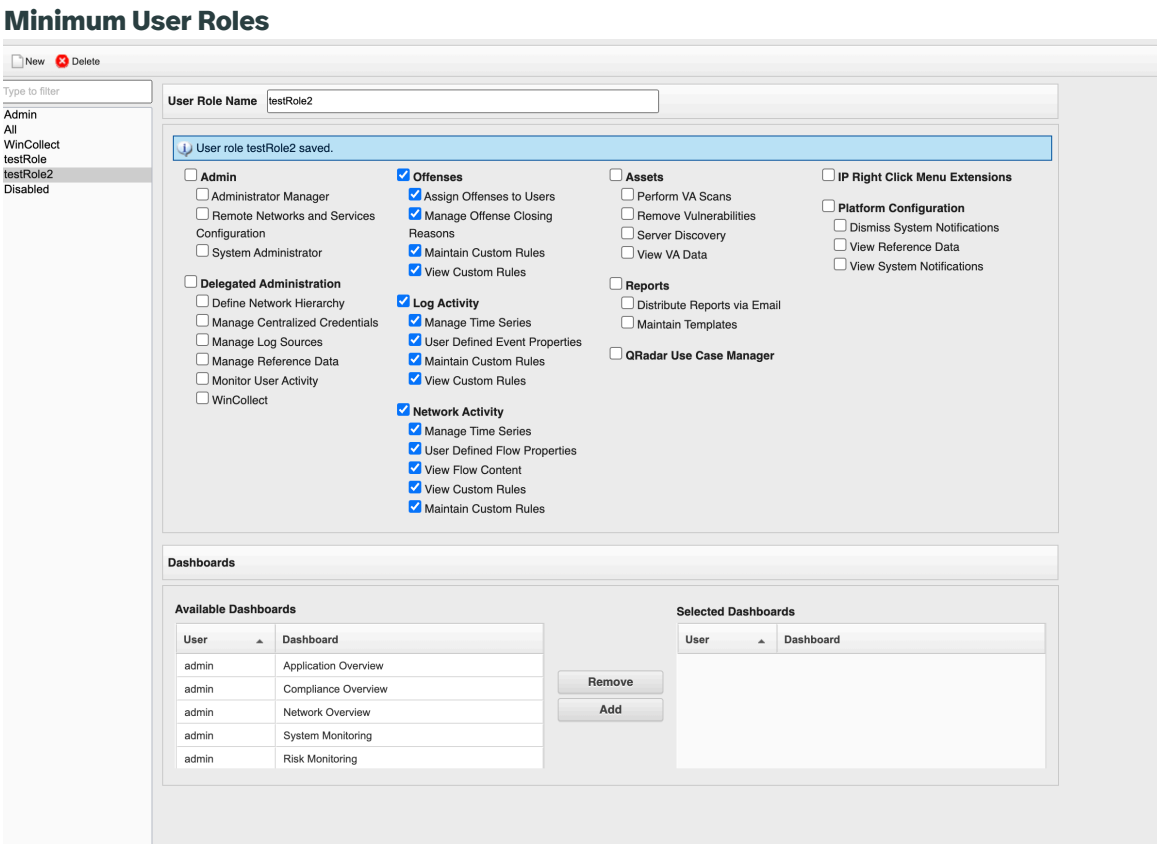
1. If you have not installed the IBM QRadar application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **Integrations** > **Integrations Configurations** and locate the IBM QRadar tile.
3. To configure the application, click **New**.
4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.
5. In the **Offense Ingestions Configuration** dialog that is displayed, fill in the fields.

Field	Description
Name	Name of the IBM QRadar console or the IBM QRadar instance used for the integration. Spaces are supported for names, but paren theses are not supported.
IBM QRadar API Base URL	Host URL for your IBM QRadar instance. **Note:** You need to enter only the URL and the port number here. For example, https://ibm-qradar.com:8443. If the port number is 443, it need not be explicitly entered.
IBM QRadar Dashboard URL	The URL for the IBM QRadar dashboard or the console. This URL is used to auto con struct the hyperlinks for offenses in the IBM QRadar dashboard. Enter only the host URL, for example, https:// qradar.com. Do not include the .jsp in the URL, for example, https://qradar.com/con sole/qradar/jsp/QRadar.jsp is an invalid for mat. **Note:** If the dashboard URL is not avail able, enter the IBM QRadar API Base URL here.
IBM QRadar API Version	Version 10 and above are supported.
IBM QRadar API Authorized Service Token (on premises)	The IBM QRadar authorized service token is used for authentication. The authorized ser

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

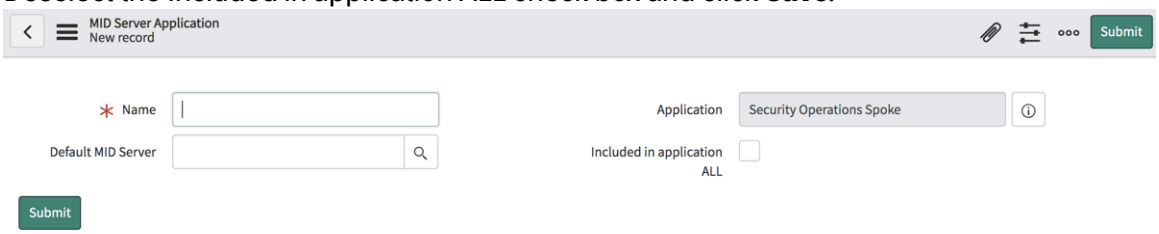
Field	Description
	vice token must have the following minimum user roles: **Offenses**, **Log Activity**, and **Net work Activity** along with a user security pro file that has no restrictions. To generate the authorized service token, fol low these steps: ○ In the IBM QRadar console, navigate to the **Admin** tab and click **Authorized Services**. ○ If a valid authorized service token exists, check the expiry date and use this token. If an authorized service token is not avail able, follow these steps: ○ In the IBM QRadar, navigate to the **Admin** tab and click **Authorized Service**. ○ Click **Add Authorized Service** and create a token with the user role and security pro file. Ensure that you specify an expiry date for a long validity period.
IBM QRadar API Authorized Service Token (for QRoC)	If you are using IBM QRadar on Cloud (QRoC), use the self service application to generate the authorized service token with admin user role and admin security profile for authentication.
On Premises Deployment	Default is disabled. If this option is enabled, you must specify a MID Application Name. If you are using IBM QRadar on Cloud (QRoC), verify that the check box is cleared.
MID Application Name	Specify a MID Server Application that is set up in your environment. If you do not have a Mid Server Application configured,you must create a new MID Server application for this integration. **Note:** The MID Server Application can be configured only by users with sys tem administrator role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



To create a new MID Server Application, follow these steps:

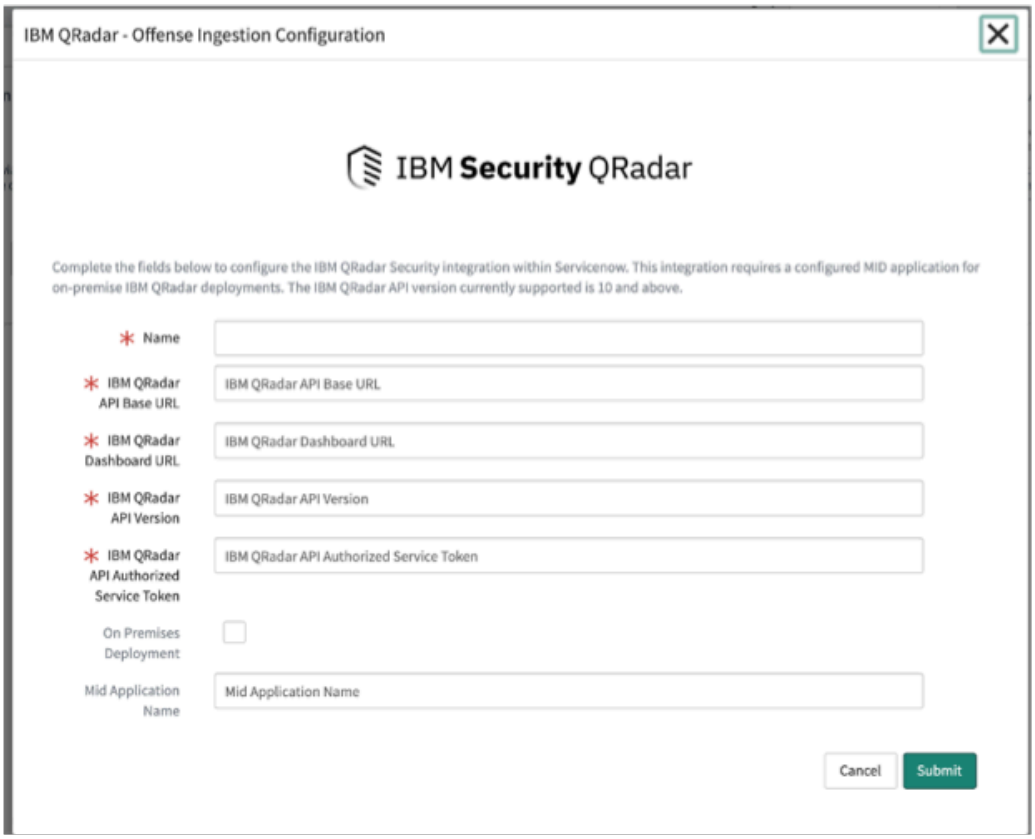
- Navigate to **MID Server** > **Applications** and click **New**.
- Enter a name for the MID Server Application and select a MID Server to be used as the default.
- Deselect the Included in application ALL check box and click **Save**.



- Click **Edit**. In the **Edit Members** page, select all available MID Servers, move them to the MID Servers List, and click **Save**. Depending on the availability, one of the MID Servers configured with the MID Server Application will be used.

6. Enter the configuration details and specify the MID Server Application you have created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The source that you configure on the **IBM QRadar Offense Ingestion Configuration** form can be reused for multiple ServiceNow AI Platform profiles as long as each profile ingests offenses.

7. Click **Submit**.
   After it is successfully validated and submitted, each IBM QRadar server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.

   Note: If you encounter some issues with the IBM QRadar domain segmentation feature, contact IBM QRadar Customer Support for assistance.

What to do next
You have successfully installed and configured the application. The next step is to create the profile.

Set up your ServiceNow AI Platform® instance for the IBM QRadar offense ingestion integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the application from the ServiceNow Store.

Before you begin
Role required: sn_si.admin

About this task
Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description

Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.	The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform® instance.
	• A user with the ServiceNow AI Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.
	• A user with the sn_si.admin role oversees the following tasks in the ServiceNow AI Platform®:
	  ○ Names, creates, and edits offense profiles.
	  ○ Selects and maps IBM QRadar offense data fields to the security incident fields.
	  ○ Previews security incident details for accuracy prior to finalizing the configuration.
	  ○ Schedules on-going offense ingestion.
	  ○ Enables offense updates when a SIR incident is created and closed.
	  ○ Assigns the security incident analyst (sn_si.analyst) role.
	  ○ Users with the sn_si.analyst work with security incidents.
	For more information about roles and assigning roles to users, see Roles on the Servicenow Product Documentation website.

Verify that you are using the following versions: • IBM QRadar version 7.3.2 or later. • IBM QRadar API version 10 or later. Earlier versions are not supported.	If you have access to the IBM QRadar console, you have access to the API that is required for this integration. There is no other special setup required for the API.
Verify that you have installed and configured a MID Server Application.	Configured MID Server Application. A MID Server in your ServiceNow AI Platform® instance is required to connect to the IBM QRadar service if the IBM QRadar server is deployed within your corporate network. See the ServiceNow Product Documentation website for information about MID Servers. If you are using the IBM QRadar Cloud service, a MID Server is not required.
Verify that the ServiceNow core applications that are required to support the integration are installed	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
and activated before you install the application for the integration.	one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Event and Alert Ingestion for Security Operations: This application requires: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST **Note:** The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance. For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

What to do next

You have successfully set up your ServiceNow AI Platform® instance for the integration. The next step is to install the IBM QRadar application from the ServiceNow Store for the integration.

Create a profile for IBM QRadar offense ingestion integration

As a user with the sn_si.admin role, you create an offense profile in your ServiceNow AI Platform instance and determine which offenses create security incidents. Before ServiceNow AI Platform Security Incident Response (SIR) security incidents are created from offenses, the field values from offenses are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident will be created.

Before you begin

Role required: sn_si.admin

About this task

From an integration perspective using available APIs, IBM QRadar offenses are automatically ingested into the Security Operations environment of your ServiceNow AI Platform instance depending on the profile type defined. The integration workflows ingest different types of offenses such as unauthorized access attempts and malware, for example. These offenses are ingested based on the profiles that you configure in the Security Operations environment of your instance. All offenses are initially ingested for a configured offense type in a profile. Ingested offenses can then be further filtered to specify which offenses create security incidents. For example, you may prefer filters that create security incidents only for offenses that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested offenses, individual field values on the offenses are mapped to corresponding fields on a layout of security incident for a preview.

Names for the offense profiles in your ServiceNow AI Platform instance must be unique. You can create multiple configurations for multiple sources and you can also create multiple profiles for a single source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create profiles for ingesting IBM QRadar offenses

You can set up a profile to ingest offenses.

Before you begin

Role required: sn_si.admin

Procedure

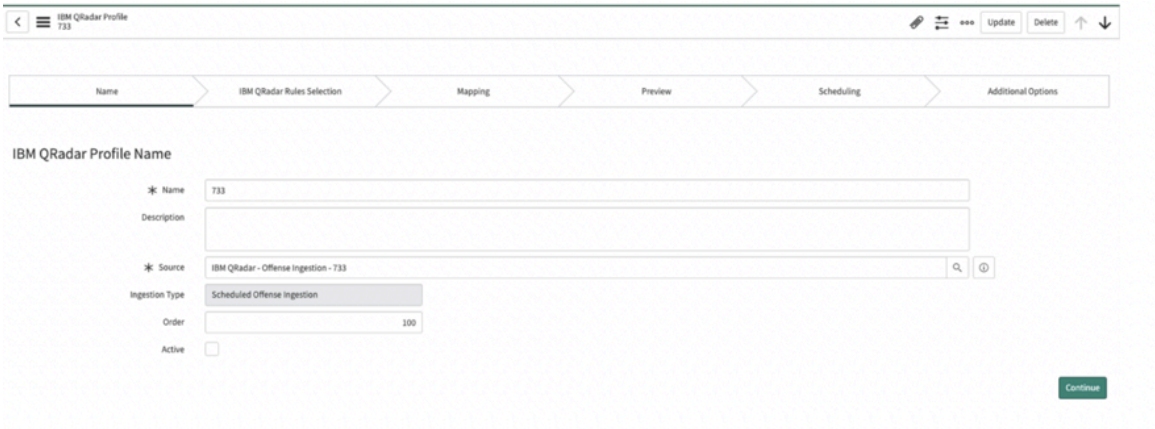
1. To create a profile for an offense in your ServiceNow AI Platform instance, navigate to **IBM QRadar Integration** > **IBM QRadar Profile**.
2. Click **New**.
3. Fill in the fields.

   An example of a completed form follows the table.

Field	Description
Name	Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Active	Check box is cleared by default. If this option is disabled, the profile is not active and ingestion will not take place. **Note:** You should complete all sections in the profile before making it active.
Source	The IBM QRadar server that you configured to ingest offenses. If you have multiple IBM QRadar servers configured, select the appropriate server for the offense types that will be ingested for the profile. You are required to enter a value.
Order	Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Additional text to help you distinguish this profile from other profiles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure is an example of a completed form.



What to do next

The next step is to select the offenses for ingestion.

Select IBM QRadar rules

Based on the IBM QRadar Source, select one or more IBM QRadar rules for the profile.

Before you begin

Role required: sn_si.admin

About this task

View the available IBM QRadar rules in your ServiceNow AI Platform instance so you know the active IBM QRadar rules for which you want to ingest and create security incidents.

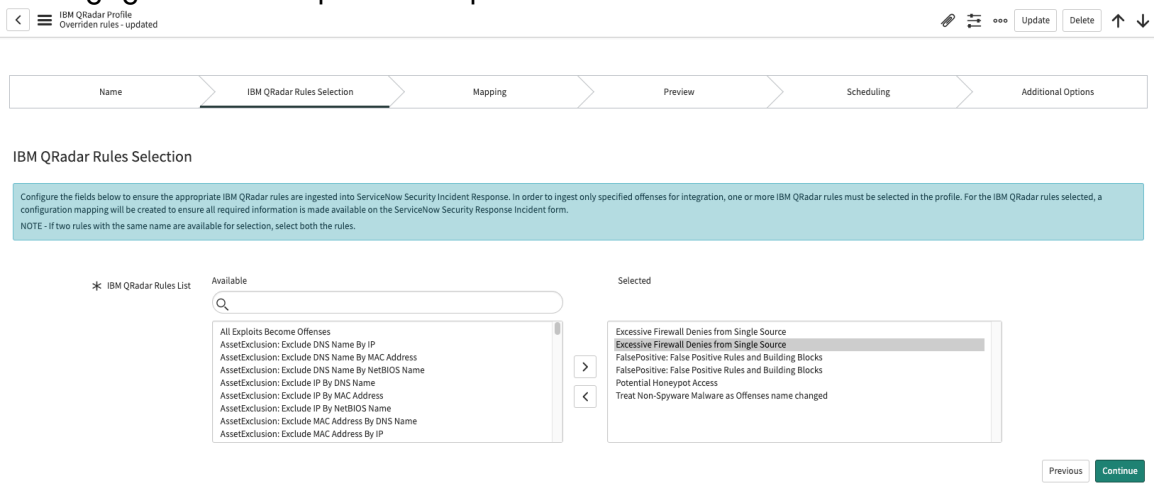
In IBM QRadar, you can identify rules by their origin as System, Override, and User rules. By default, the origin of a rule is linked to a System rule. When you modify a System rule in IBM QRadar, its origin is set as Override.

Click the list in the IBM QRadar Rules List field. A list of active IBM QRadar rules that are present in the IBM QRadar Console is displayed. Select one or more rules from the list and move them to the **Selected** column. Offenses triggered by one or more of the IBM QRadar rules selected are ingested in this profile.

Rules with the same name: In the ServiceNow AI Platform instance, a list of active or enabled rules are displayed. If you modify an active or enabled System rule in IBM QRadar, a new Override rule is created. This results in two rules being displayed with the same name in the ServiceNow AI Platform. When this scenario occurs, select both the rules to ingest and create security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure is an example of a completed



form:

Click **Continue** to proceed to the next step in the wizard.

Mapping of offense fields for the IBM QRadar integration

After you have selected the rules, the next step is to map offense, event, or flow fields to the fields in the security incident form.

Overview

For the mapping step, you must first ingest sample offenses for one or more selected IBM QRadar rules. Then you must ensure that all relevant offense field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

Mapping of the sample offense fields involves the following:

- Fetching and populating of the sample data: See Ingesting the sample IBM QRadar offenses.
- Mapping the offense fields to the security incident: See Mapping IBM QRadar offense fields to security incident response fields.

Ingesting the sample IBM QRadar offenses

You can ingest sample offenses for one or more selected IBM QRadar rules.

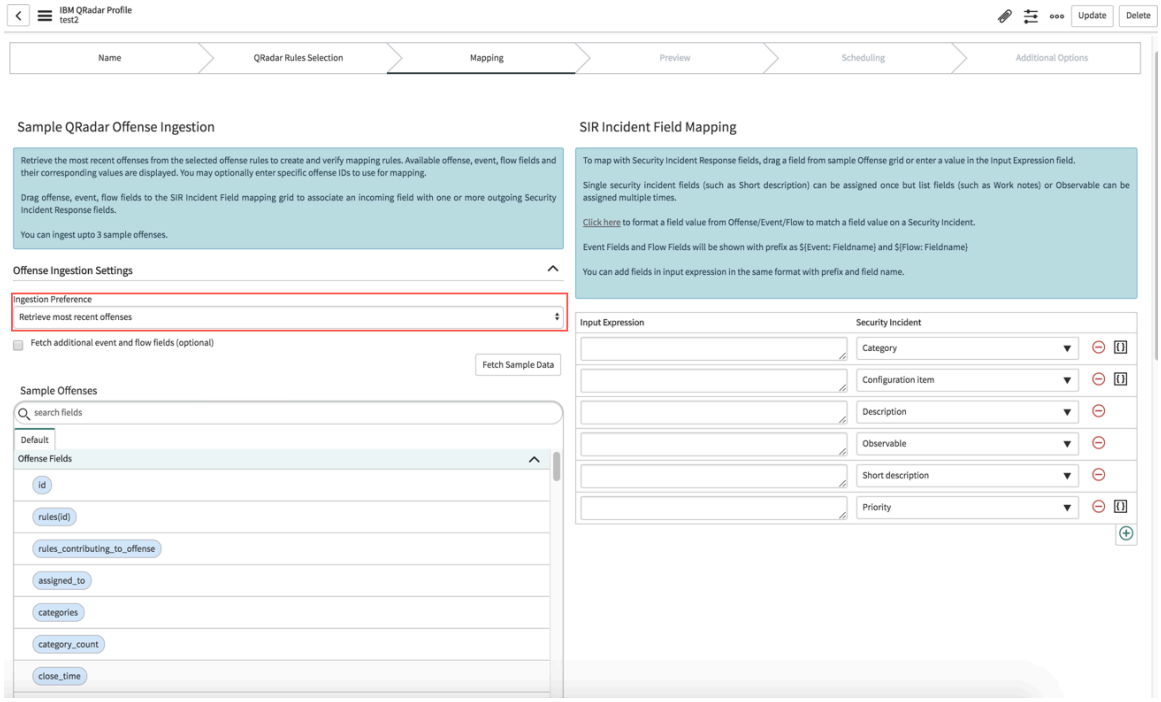
Before you begin

Role required: sn_si.admin

Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. You can either pull the three most recent sample offenses or provide the unique offense IDs for the specific offenses that you want to use for your mapping experience.
   From the **Ingestion Preference** choice list, select one of the following:
   - Retrieve most recent offenses: The three most recent offenses for the selected rules are retrieved.
   - Select offenses based on offenses ID: Specify the offense ID for the offenses to be retrieved. You can specify a maximum of 3 offense ids separated by commas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



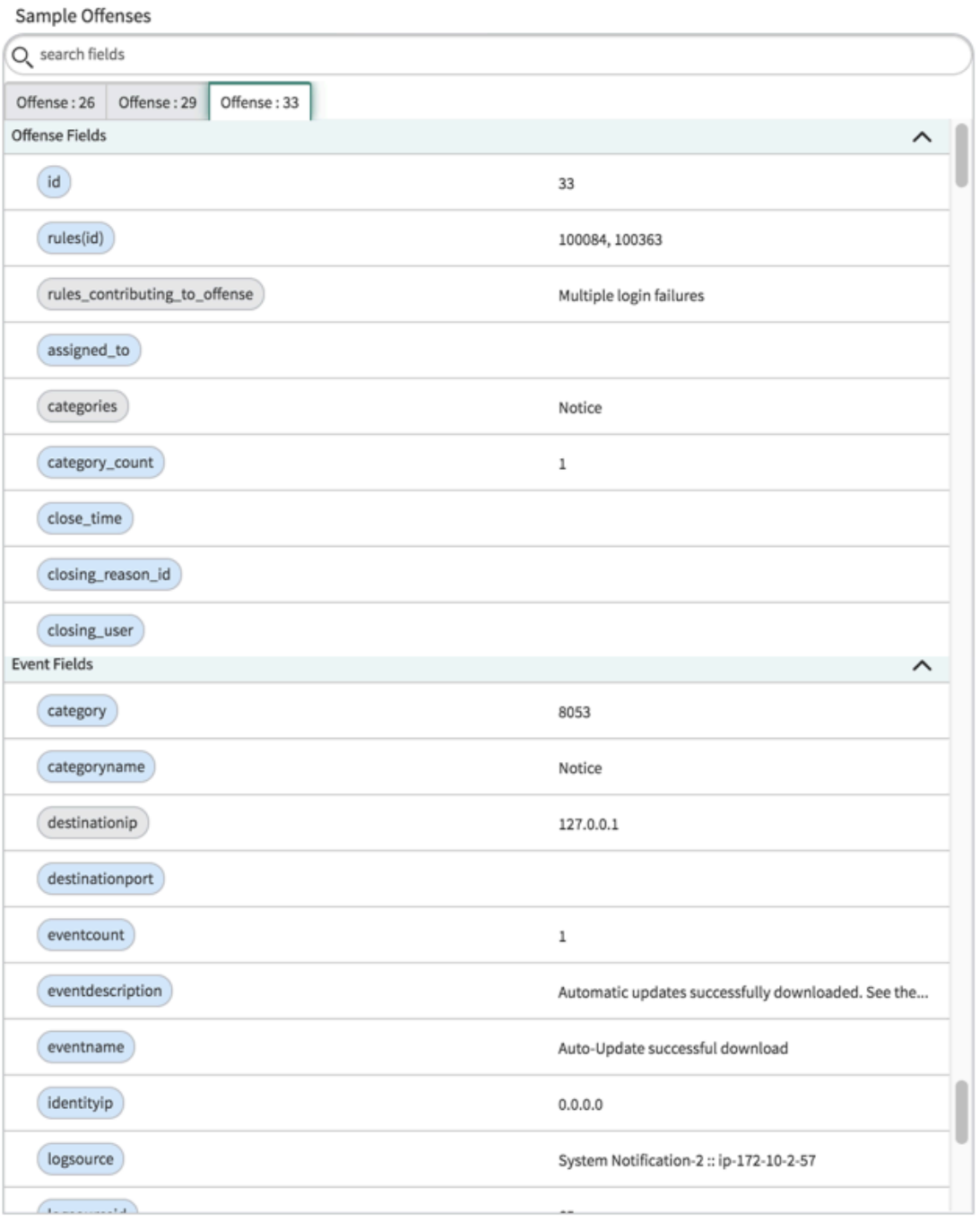
3. Click **Fetch Sample Data** to pull the latest sample offense data from the IBM QRadar console for the selected offense rules.

   The offense fields and values results are displayed as individual tabs. An offense can be triggered by three types of rules:

   - Event: In this rule, event logs are checked and if the specified criteria is met, an offense is created.
   - Flow: Network data and traffic is checked and if certain conditions are met, an offense is created.
   - Common: In this case, you can specify conditions for events or flows and either or both conditions are met, an offense is created.

   The pull for sample offenses may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen. Depending on the rule or rules that triggered the offense, along with the offense fields, the event or flow fields are populated as shown in the figure below:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: The event or flow fields displayed belong to the first event or flow field that triggered the offense based on the corresponding event or flow rule.

4. The following are custom offense fields created for this integration.
   Standard offenses fields in addition to these custom fields are available for mapping.
   - rules_contributing_to_offense: IBM QRadar rules that contributed to the offense based on the Rule ID.
   - users: User names for the offense
   - remote_destination_ip: The remote destination IPs for the offense.

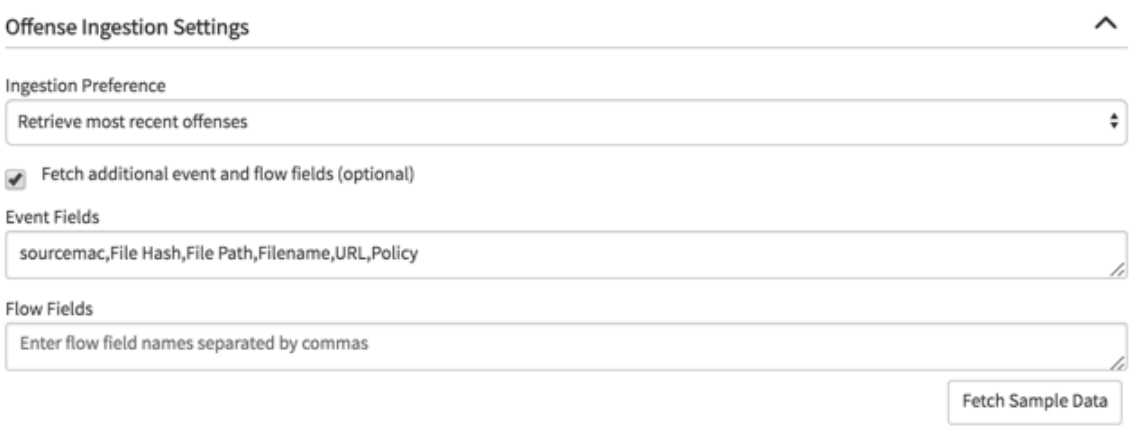
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Based on the local destination IDs for the offense, the following custom local destination address fields are available:

- local_destination_address (domain_id)
- local_destination_address (event_flow_count)
- local_destination_address (first_event_flow_seen)
- local_destination_address (id)
- local_destination_address (last_event_flow_seen)
- local_destination_address (local_destination_address_ids)
- local_destination_address (magnitude)
- local_destination_address (network)
- local_destination_address (offense_ids)
- local_destination_address (local_destination_ip)

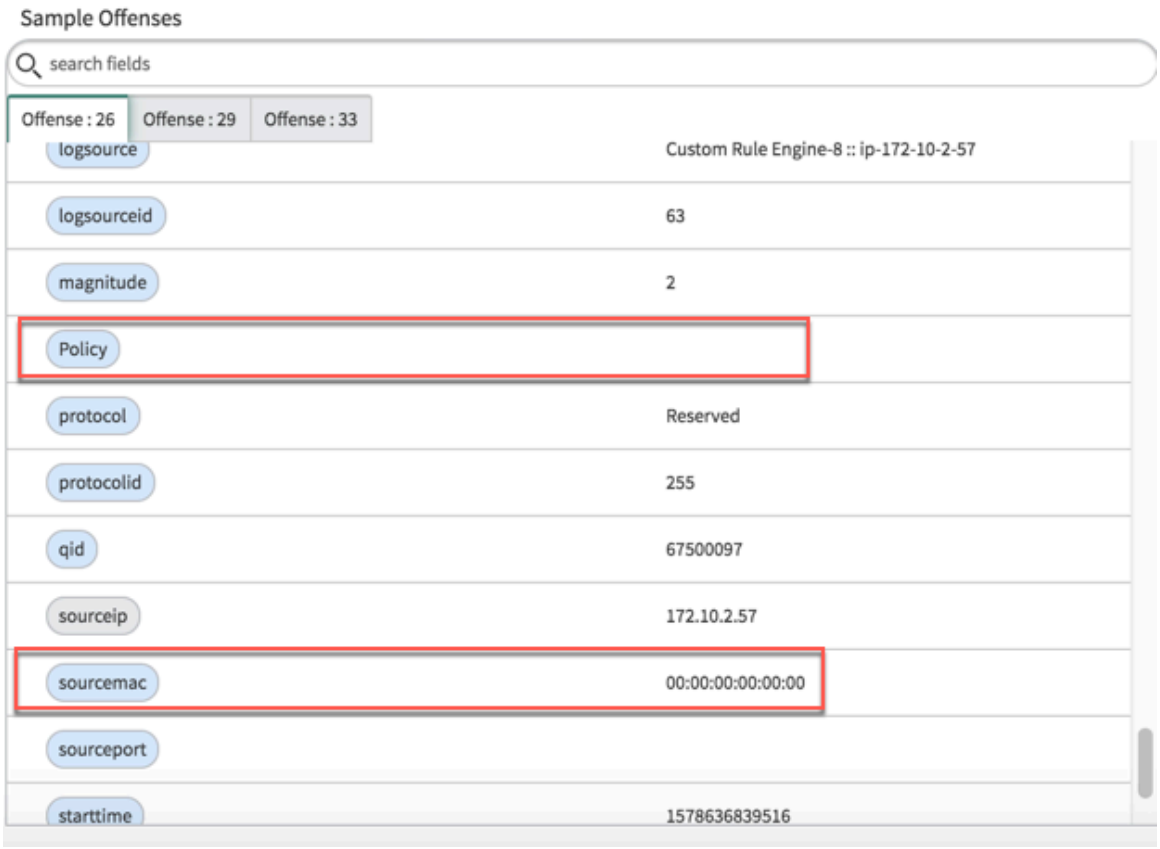
- The following source addresses are available based on the source IDs of the offense:
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (id)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (magnitude)
  - source_addresses (network)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

Select the **Fetch additional event and flow fields (Optional)** check box. You can fetch sample event and flow data from any active, valid custom event and flow fields. Specify the custom fields separated by commas as shown below:

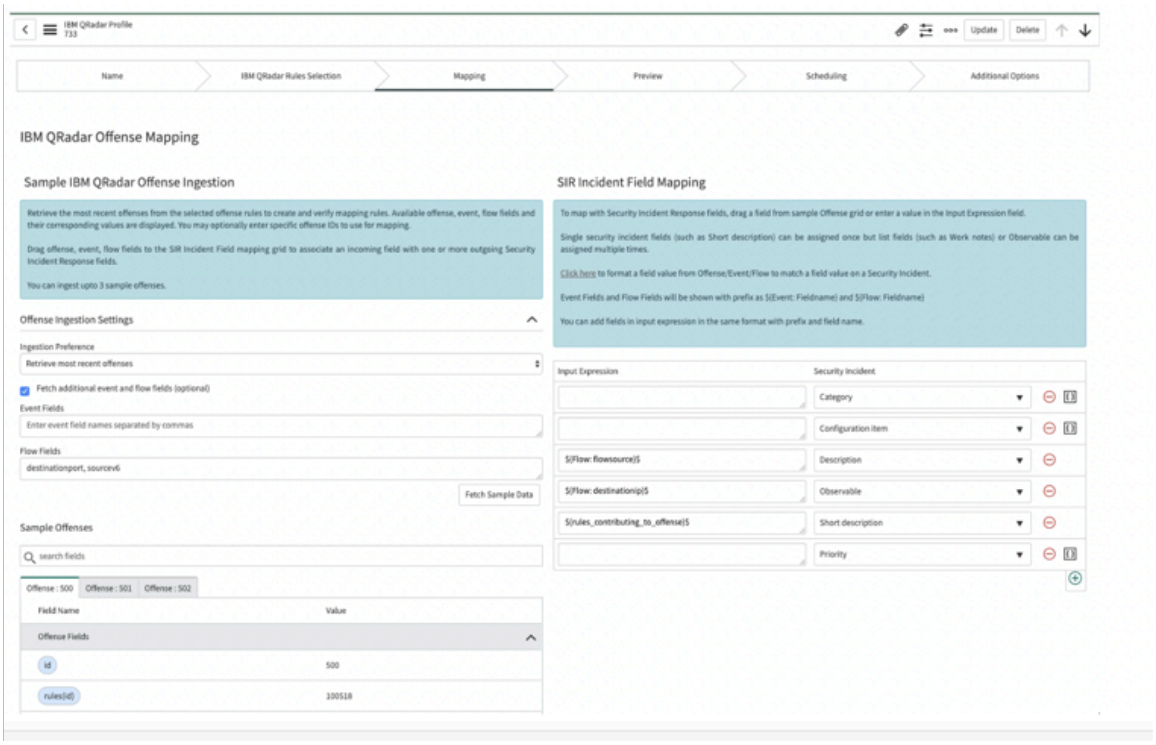


Click **Fetch Sample Data**. The specified event or flow fields along with their values (if available) are appended to the Event or Flow section as shown below:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



After you fetch the sample data, the corresponding values for these fields are populated on the left side of the form.



What to do next

After you have fetched the sample data, the next step is map the offense fields to the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mapping IBM QRadar offense fields to security incident response fields

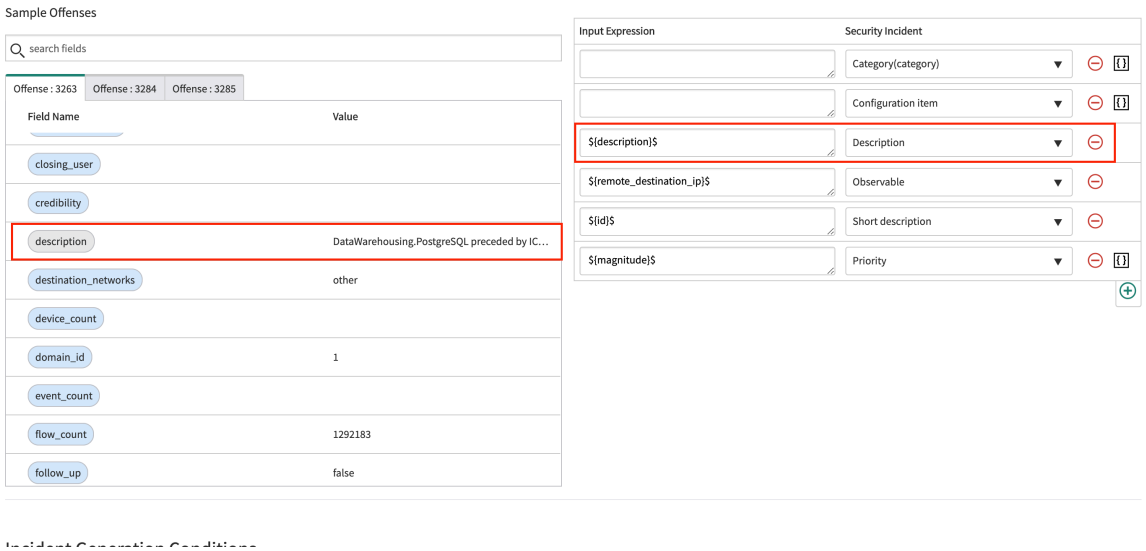
Map individual offense, event, and flow fields to fields on a ServiceNow AI Platform SIR security incident.

Offense field mapping

As a user with the sn_si.admin role, use the fields from the Sample Offenses section on the left and map them to the security incident fields in the SIR Incident Field Mapping column. Edit the mapping configuration by dragging offense, event, or flow fields from the left side and dropping them on the ServiceNow SIR incident mapping section on the right. The mapping on the right associates the incoming offense field with an outgoing security incident field.

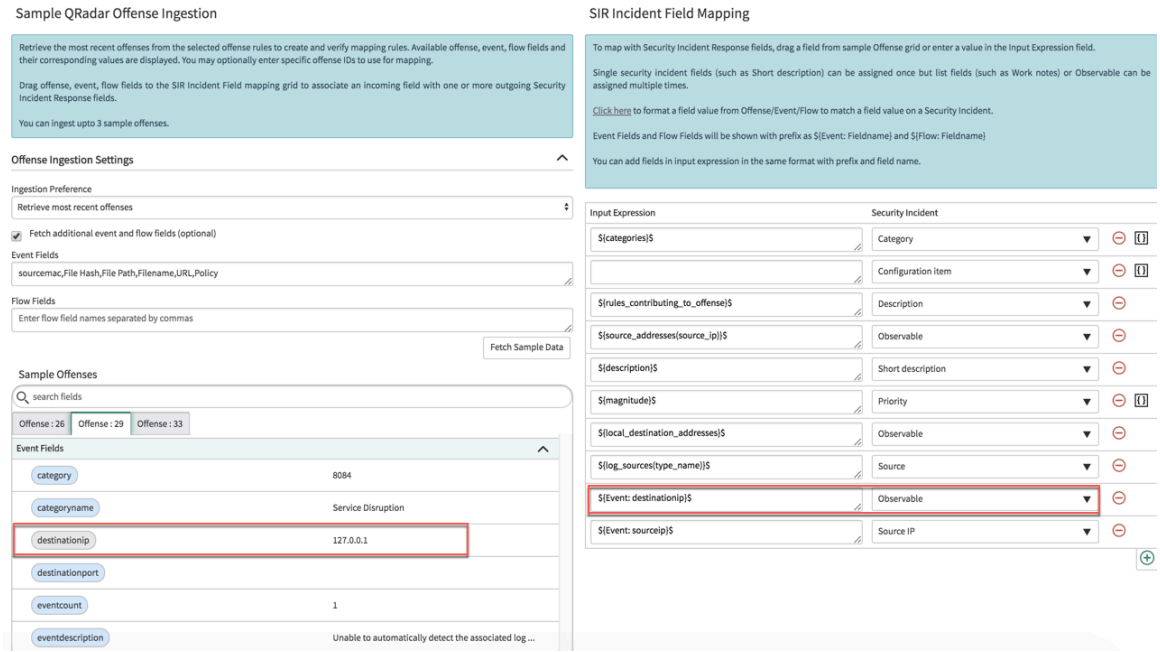
1. After you have fetched the sample data, the next step is map the offense, event, or flow fields to the security incident. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
2. Drag the field name, for example, `description`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

   The field value is displayed in the Input Expression column. In the following image, `description` is mapped to the `Description` field on the security incident.



Note: If you enter the event or flow field name manually in the Input Expression section, you must add a prefix as *`${Event:eventfield}$`* or *`${Flow:flowfield}$`* before the name of the field being mapped.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



To help you ensure that no offense, event, or flow fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the offense fields helps you keep track of the offense values that you have already mapped as they become greyed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important offense information remains unmapped.

Light blue fields on the left indicate that an offense field is not yet selected and mapped on the security incident. You may prefer to associate an incoming offense, event, or flow field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

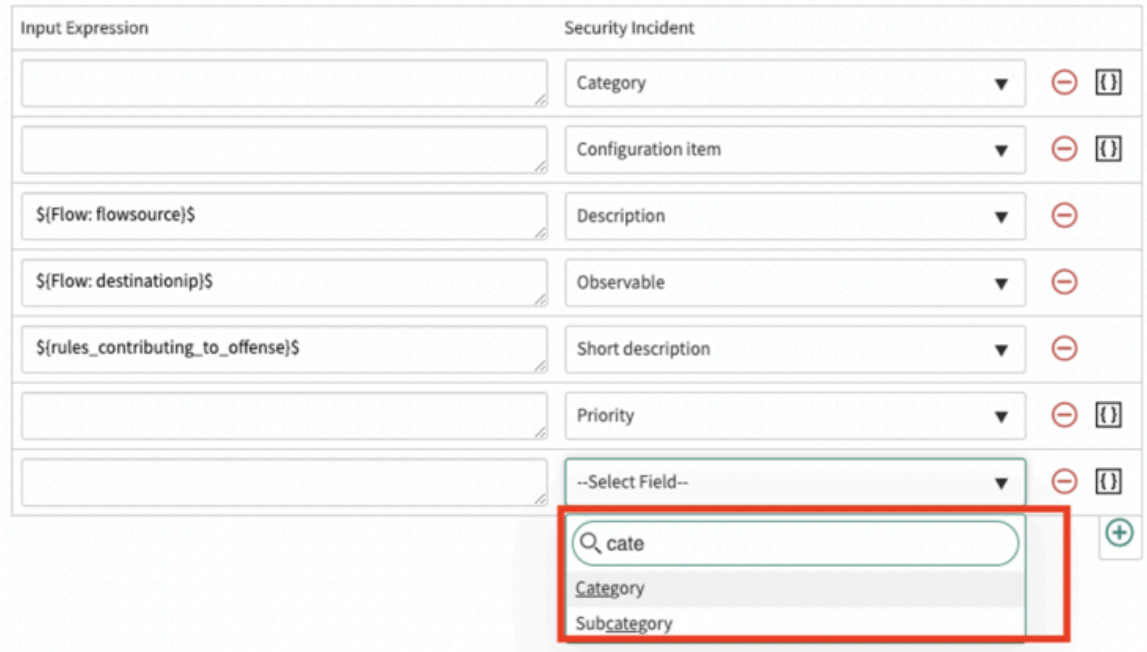
3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps:

   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.

   b. In the Security Incident column, expand the choice list that is displayed, and select a field.

      In the expanded choice list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the offense fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, select the offense field and drag-and-drop it to an appropriate security incident field on the right.

4. Remove fields by using the - icon next to the field name in the SIR incident field mapping section.

5. Continue mapping by adding or removing field values to the mapping.

Offense fields with multiple values

- Security incident fields such as **Category** and **User** fields, (for example, Affected user, Assigned to) available with the base product do not support multiple values.
- The following IBM QRadar fields support multiple values:
  - *categories*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_offense*
  - *users*

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

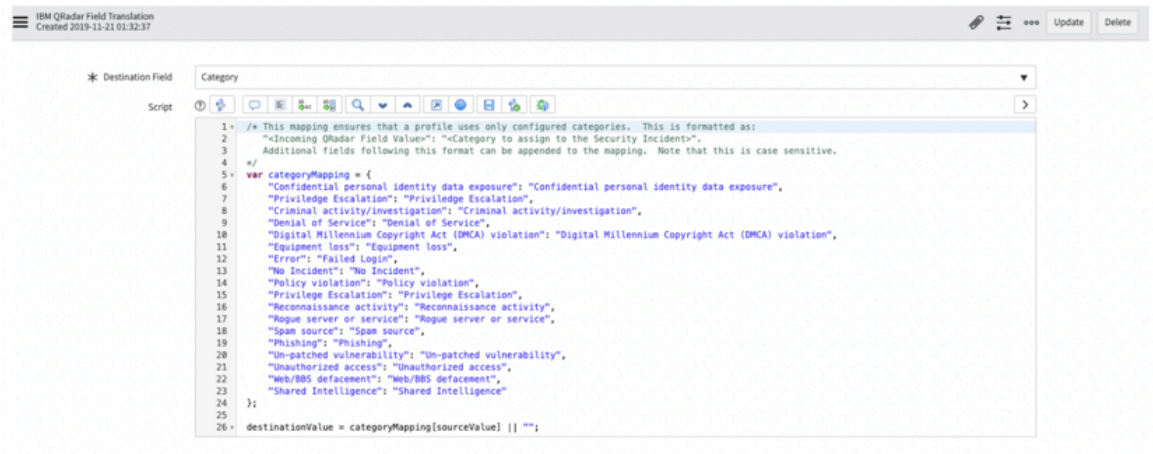
If you need to map the above fields to any Security Incident Response fields apart from CI and Observable type fields, you must create new Security Incident Response fields of type **List** and use them for mapping.

Note: By default, only non-reference **List** type fields are supported.

Format Field Translation

In certain cases, offense field values in IBM QRadar may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the {0}. The script editor is displayed.



Enter any changes to the script and click **Update** to save the changes and return to the Mapping page.

Incident generation conditions

Once the mapping section is complete, you can set filter conditions so that you can specify which offenses should create security incidents versus which offenses should be filtered out, for example, low priority offenses. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming offense must satisfy to create a security incident. To set incident generation conditions, follow these steps.

1. Scroll to the **Incident Generation Conditions** section on the form and select the **Filter based on conditions** check box to enable the option.

   The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

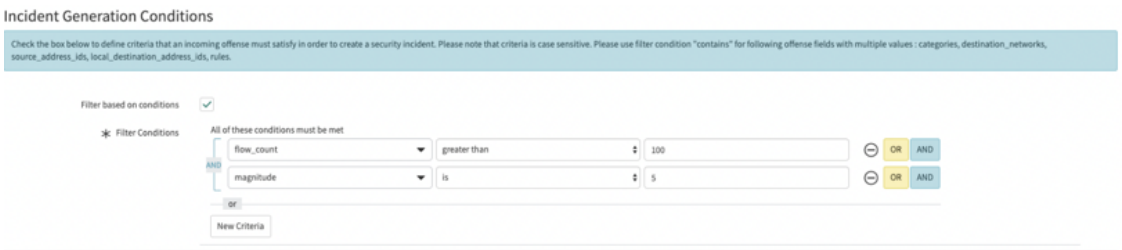
   The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the Sample QRadar Offense Ingestion section for the offenses you ingested. These fields are dynamic and change depending on the offenses that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the IBM QRadar offense. If you are not sure about the values to enter in the filter fields, you may prefer to return to your IBM QRadar console and review your offenses for the keywords.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The *categories*, *destination_networks*, *source_address_ids*, *local_destination_address_ids*,*remote_destination_ips*, *rules_contributing_to_offense*, and *users* offense fields can have multiple values (as the values are stored in arrays). As the filter condition can retrieve only strings, you must use the *contains* filter condition for these fields to ensure that the data is filtered correctly.

2. Using the choice lists and fields of the conditions builder, set filters for the first row.
3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
4. (Optional) In the second row, set a second filter condition.

   The following image is an example with two conditions that must be matched before security incidents are created.



   You have set the incident generation conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

   This type of incident generation condition filtering helps you narrow down the offenses, and limit the number of unnecessary security incidents that you create without modifying the underlying rule or filters in IBM QRadar. If additional filtering criteria are set, only offenses that match all criteria are mapped to incidents.

Note: If any of the offense field names have special characters such as quotes (“),hyphens (‘), underscores (-), or ampersands (@), these characters may need to be replaced for filtering purposes but a numerical suffix is appended to differentiate fields with duplicate offense names. For example, if the first offense field is `alerts.alert` and the second offense field is `alerts@alerts`, these fields cannot be uniquely identified as the remaining standard text characters are the same. In this case, a suffix is added to the second offense field and the field is renamed to `alerts@alert(1)` when displayed in the Filter Conditions list.

Offense aggregation criteria to handle similar offenses and prevent duplicate incidents

Define additional offense aggregation criteria that aggregates an incoming offense to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related offense data on a single security incident. To set the criteria, follow these steps below:

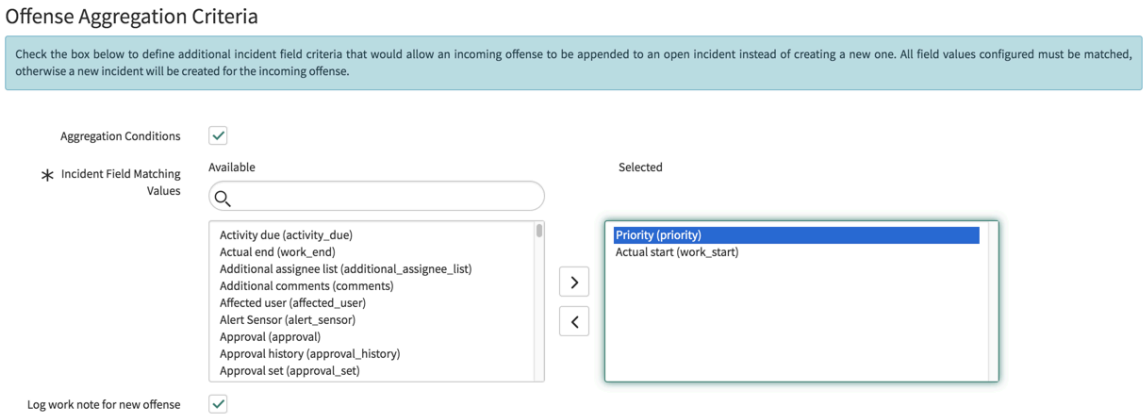
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Scroll to the Offense Aggregation Criteria section on the form and select the **Aggregation Conditions** check box to enable this option.

   The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

2. From the Available list, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform and move them to the Selected list.

   All the field values that you select must be matched to append this incoming alert to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple offense field values mapped to them. All values must match. If only a subset of the values are matched, the offense aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.



   If a new offense matches all the values that are selected in the aggregation field conditions in the mapping step, the new offense is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregated offenses on a related list on a security incident. This list details associated time stamps and aggregated field values. This information helps you understand why these offenses are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the **Show All Related Lists** link.

3. (Optional) To log a work note for a new offense that is recently added on the security incident, select the check box to enable this option. The work note logs that a new offense has been added along with a link to the offense details and any other details that may have been added to the work note field in your mapping section.

   You have successfully mapped values from an IBM QRadar offense to fields on a security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also appended offenses to existing security incidents when offense field values match the configured aggregation criteria.

4. Click **Continue** to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident

Preview the security incident for the IBM QRadar integration

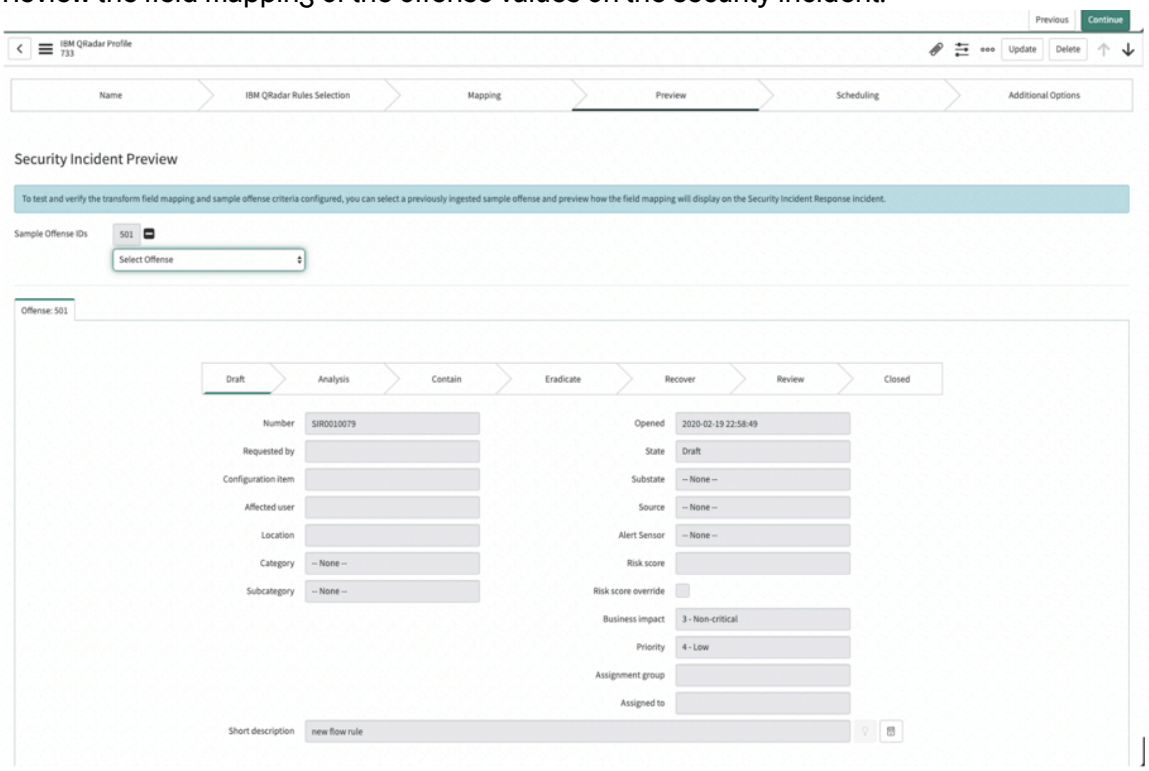
After you complete the mapping step, preview the values that you mapped in a SIR security incident. This preview step permits you to verify that you have mapped all the offense fields that you want displayed on the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.admin

About this task
As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Procedure
1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. From the Sample Offense IDs choice list, select an item.
   The security incident is displayed. This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the offense values on the security incident.



   The preceding image is an example of a preview with a mapping error of the samples that were ingested.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

What to do next
If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Define schedule for the IBM QRadar integration

You can define the schedule for the offense ingestion. During this step, you can verify the default settings for the offense retrieval or modify the scheduling as needed. This step also permits you to retrieve historical offenses using a date range.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.admin

About this task
You can choose whether you want to ingest any historical offenses during the Scheduling step. You also choose how often you will poll for future new offenses and updated offenses that match the profile configuration.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the IBM QRadar offense ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the IBM QRadar server against a desire to be notified as soon as possible when an offense is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

Pulling new and updated offenses

When the polling schedule is set, the scheduled job pulls both new and updated offenses that were pulled previously but did not meet the incident filtering criteria. This provides you with the flexibility to create incidents based on criteria that may not be present when a offense is first created but becomes available after an update occurs, for example, during the investigation phase. Once an incident is created for a specific offense, its subsequent updates are ignored since it is expected that the offense is now being treated as an active ServiceNow security incident. However, all other offenses that have been previously ingested but failed to meet the incident generation criteria, will continue to be pulled and checked against the incident generation criteria until they become part of an active incident.

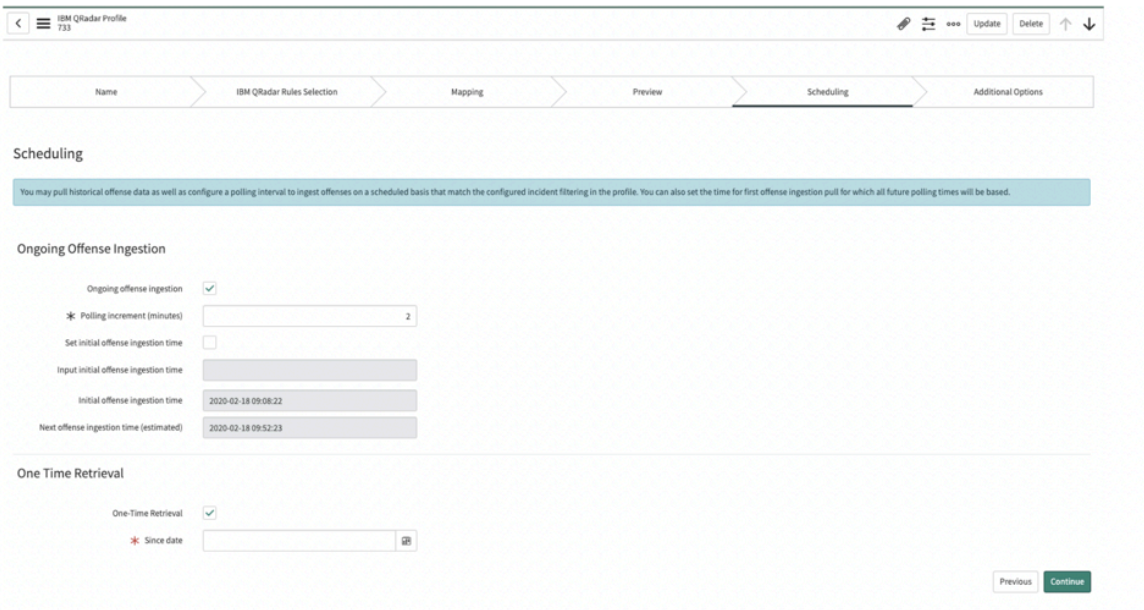
Procedure
1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when offenses are pulled from the IBM QRadar console.

Option	Description
Ongoing offense ingestion field selected	On-going Offense Based on the default setting, the Service Now AI Platform instance pulls from the IBM QRadar server for new and updated offenses every five minutes. Security incidents are cre ated if offenses are found and incident gener ation filtering criteria are matched. To balance ingestion polling overhead desire to get the most current data, five minutes is the default setting. However, this value can be modified to as low as one minute if needed.
○ **Ongoing offense ingestion selected** ○ **Set initial offense ingestion time**	Initial ingestion time If you want to schedule the initial ingestion at a specific time, follow these steps: ○ Select the Ongoing offense ingestion and Set initial offense ingestion time fields. ○ Specify the time in the Input initial offense ingestion time field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	The initial ingestion will take place at the time specified here. Subsequent ingestions will be based on the schedule defined in the Polling increment (minutes) field. As an example for scheduling an initial of fense ingestion time, if you have a daily IBM QRadar security check that runs once a day at 4 AM local time, you can set up the corre sponding offense profile in your ServiceNow AI Platform instance to run at 4:05 AM local time to capture the security failure right away and create a security incident. Enter `<date> 04 05 00` in the Initial of fense ingestion field. In the Polling increment (Minutes) field, enter `<date> 1440` (24 hours) to schedule the next offense ingestion for 24 hours from the initial offense ingestion. Both the initial offense ingestion time and next offense ingestion time are displayed in the fields. The initial ingestion will take place at 4:05 am. The subsequent ingestions will be based on the polling interval. In this case, since the Polling increment is 24 hours, the next inges tion will take place on the next day at 4:05 am.
One Time Retrieval field selected	One-Time Retrieval Use this configuration if you want a one-time pull to ingest historical offenses. When this setting is configured, a profile is used once to retrieve offenses from historical events that are based on a date range. To the right of the Since date field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling offens es. Starting with the Since date value, offens es are retrieved up through the current date. Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of historical offenses from IBM QRadar for archival reasons but rather a minimal amount of in-flight offenses that are being actively worked at the time of profile activation. After the offenses are pulled, this setting will not retrieve more offenses for this profile go ing forward from the current date. This setting populates the security incident with all the of fenses that are found for the range you enter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click **Continue** to navigate to the Additional Options page.

Automate offense updates and closure based on SIR incident status

The IBM QRadar integration has a bi-directional interface that allows for both offenses to create security incidents, as well as an ability to update the offenses once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, security incident URL, and so on.

Before you begin

Role required: sn_si.admin

Procedure

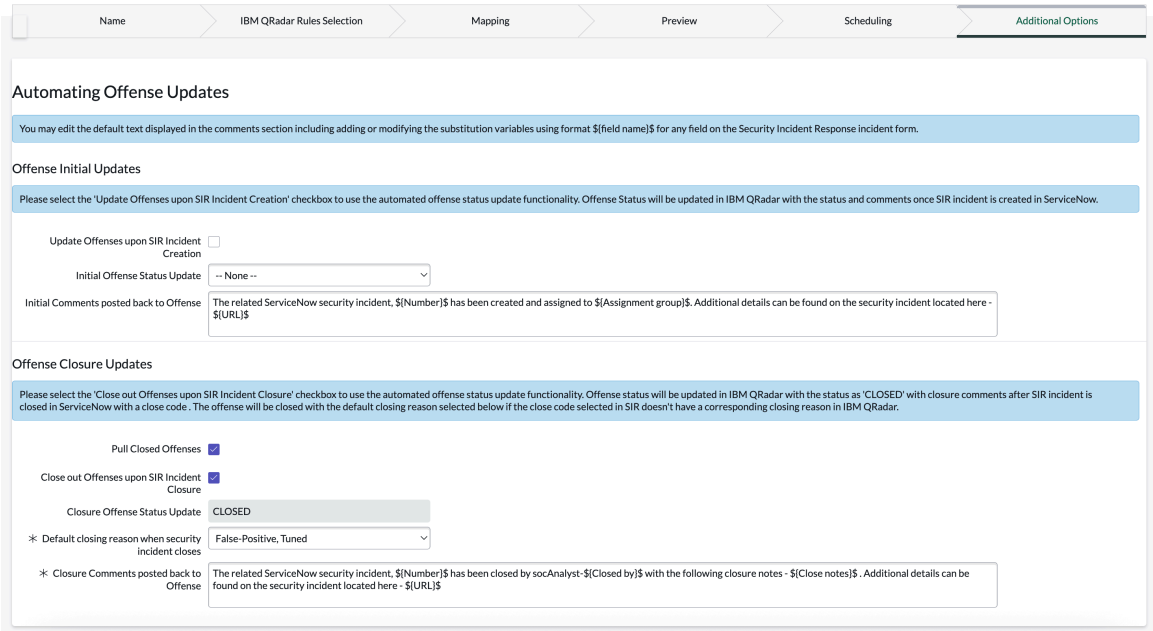
1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.
2. Follow the instructions below to complete the configuration for updating offenses when the security incident is created.

Option or Field	Description
Update Offenses upon SIR Incident Cre ation	Select this option if you want to update the of fense status and add additional comments when a security incident is created from the offense. This can occur for both the initial trig gering offenses that create the security inci dent, as well as aggregated offenses.
Initial Offense Status Update	You can select: ○ Open: The status of the offense is set to **Open** and a comment is added indicating that a security incident has been created for the offense. ○ Hidden: The status of the offense is set to **Hidden** and this offense is hidden in the IBM QRadar dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or Field	Description
Initial Comments posted back to Offense	Based on the stage you have selected, the ini tial comments as defined in the IBM QRadar console are displayed here.
Pull Closed Offenses	Select this option if you want the integration to fetch **Closed** offenses from IBM QRadar. These offenses will be evaluated for security incident creation, correlation, and historical visibility in ServiceNow®. By default, closed offenses are ignored and open offenses are retrieved from IBM QRadar during polling.
Close out offenses upon SIR Incident Clo sure	Select this option if you want to use the auto mated offense closure option. When the secu rity incident is closed in ServiceNow with a rel evant close code, the offense status is updat ed in IBM QRadar to **Closed** with closure com ments. **Note:** The close code specified for the security incident must correspond to the closing reason specified in the IBM QRadar dashboard. The offense is closed in IBM QRadar only if a corre sponding closing reason is found. If a corresponding reason is not found, the offense is closed with a default close code.
Closure Comments Posted back to Offense	The closure comments as defined in the IBM QRadar dashboard are displayed here.
Default closing reason when security inci dent closes	The default reason to be used when a secu rity incident is closed, When a security inci dent is closed, a close code (or the reason for closing) is specified in the security incident record, If the close code does not match the closing reason specified in the IBM QRadar dashboard, and you try to close the security incident, an error message is displayed. In such cases, the default closing reason speci fied here is used when the security incident is closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Select **Finish** to complete the configuration and move the profile to the **Waiting** state.
   A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull offenses from the IBM QRadar console based on your scheduling.

Configuration settings

Use this option to modify the IBM QRadar ingestion integration default system properties.

To modify the system properties, log in as a user with the *sn_si.admin* role and navigate to **IBM QRadar Integration** > **IBM QRadar Integration Settings**.

IBM QRadar Integration Settings

Property Name	Description
Enforce a limit on number of security incidents that can be created in 24 hour period. sn_sec_qradar.max_si_per_day	Specify the maximum number of security incidents that can be created in 24 hours. • Type: integer • Default value: 1000
Enforce a limit on number of offenses that can be aggregated to a single incident. sn_sec_qradar.max_aggregation_per_si	The offense aggregation limit for a security incident. For example, if there are 102 offenses, the first 100 offense are aggregated to security incident_1 and the remaining 2 to security incident_2. • Type: integer • Default value: 100
This property sets the time period of AQL to fetch recent event/flows for a particular offense.	Specify the number of days to fetch recent events or flows for a particular offense.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IBM QRadar Integration Settings (continued)

Property Name	Description
sn_sec_qradar.on_demand_recent_days_limit	• Type: integer • Default value: 7
This property limits the number of recent events fetched for a particular offense. sn_sec_qradar.on_demand_event_limit	Specify the number of events that are retrieved for an offense. The most recent events are retrieved first based on the event timestamp. • Type: integer • Default value: 100
This property limits the number of recent flows fetched for a particular offense. sn_sec_qradar.on_demand_flow_limit	Specify the number of flows that are retrieved for an offense. The most recent flows are retrieved first based on the flow timestamp. • Type: integer • Default value: 100
This property sets the timeout value(seconds) for the AQL which fetches recent flows/events for a particular offense. sn_sec_qradar.on_demand_timeout	• Type: integer • Default value: 300
Search IDs timeout(seconds) for records in queue for polling AQLs of an offense. sn_sec_qradar.sid_ttl	The AQL's time out for an offense in the queue before creating a security incident. For example, if there are 90 offenses, the first 50 offenses are processed for AQL data in the first batch, and the remaining 40 offenses in the subsequent batch in the same polling interval. • Type: integer • Default value: 300
Threshold to control the number of searches that can be running in IBM QRadar at a time which is triggered by the integration scheduled job.sn_sec_qradar.records_threshold_in_que_for_aql	Specify the number of offenses that you fetch in a single batch in a polling interval. • Type: integer • Default value: 50
This is the number of days for integration tables clean up. sn_sec_qradar.queue_item_expire	The following are the integration tables: • sn_sec_qradar_events - IBM QRadar Events • sn_sec_qradar_flows - IBM QRadar Flows • sn_sec_qradar_offense_updates - IBM QRadar Offense Updates

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IBM QRadar Integration Settings (continued)

Property Name	Description
	• sn_sec_qradar_offense_to_task - IBM QRadar Offense to Task • Type: integer • Default value: 30
Offense limit per scheduled job runs per profile either in one-time retrieval or on-going ingestion. sn_sec_qradar.max_offense_limit_per_run	Specify the number of offenses that you fetch into the ServiceNow AI Platform in a single retrieval. • Type: integer • Default value: 1000
Set this property to activate the Offense Updates feature. sn_sec_qradar.get_offense_updates	**Note:** Enabling this setting may cause a delay in creating a security incident. • Type: true| false • Default value: false
Enables adding overlapping interval while fetching offenses from QRadar. sn_sec_qradar.allow_overlapping	Option to enable the use of an overlapping time window when fetching offenses from IBM QRadar. When enabled, the system includes a small overlap between consecutive polling intervals to ensure that no offenses are missed due to timing delays or ingestion latency. • Type: true| false • Default value: false
Logging Level-debug,info,warn,error. sn_sec_qradar.logging.verbosity	Logging verbosity level for the QRadar integration. Supported values include debug, info, warn, and error. • Type: Character • Default value: debug
Time in minutes to be added as overlap interval. sn_sec_qradar.overlapping_time	Number of minutes to be added as an overlap interval when fetching offenses from IBM QRadar. • Type: integer • Default value: 30
Number of rules that will be included in a single cell.	Specify the maximum number of correlation rules that will be grouped and sent together in

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IBM QRadar Integration Settings (continued)

Property Name	Description
sn_sec_qradar.rules_batch_size	a single request to IBM QRadar during offense polling. This setting will help control batching behavior and performance. Lower value result in more API calls with smaller payloads, while higher value reduces the number of API calls and increases the size of each request. Adjust this value based on QRadar performance and API limits. • Type: integer • Default value: 50
Fetch ADE Rules sn_sec_qradar.fetch_ade_rules	Option to ingest ADE Rules in IBM QRadar Rules list. ADE Rules will fetch Anomaly Rules created in IBM QRadar. • Type: true| false • Default value: false

Any modified integration settings will be applied during the next polling interval as defined in the profile.

Optional: Copy a IBM QRadar profile

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

Before you begin

Role required: sn_si.admin

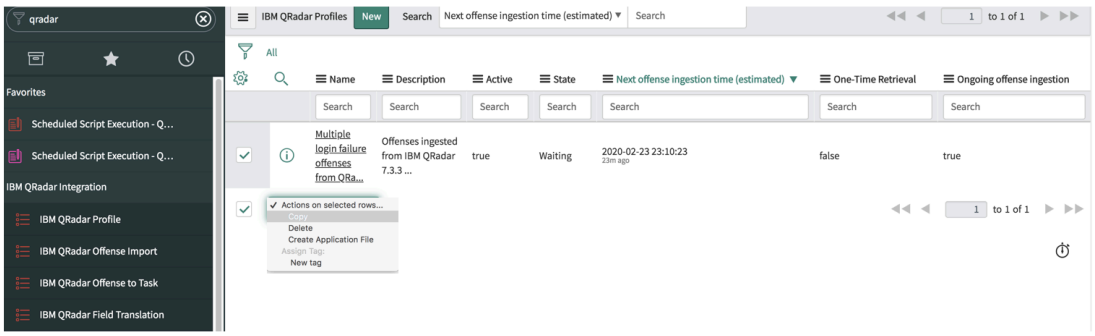
About this task

As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure

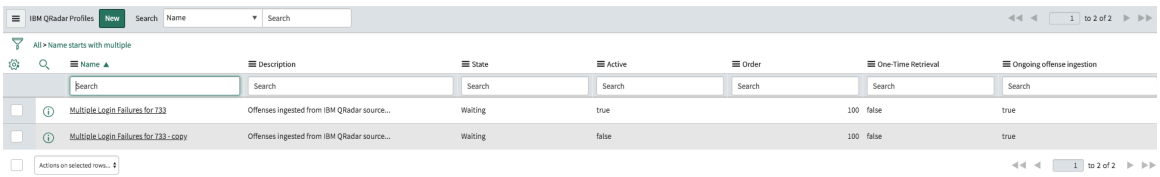
1. Navigate to **All** > **IBM QRadar Integration** > **IBM QRadar Profile**.
2. In the IBM QRadar Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

Note: If you select a different source for the profile, you must select new rules (Select IBM QRadar rules) for the profile. But if you use the same source and select new rules, the sample offenses will be cleared.



You have successfully copied the settings from an existing profile to a new profile. Note that the **Active** column status is set to false as the profile needs to be activated.

What to do next

You are prompted to activate (enable) the new profile after you complete the configuration steps.

Domain separation and IBM QRadar Offense Ingestion

Domain separation is supported in IBM QRadar offense ingestion. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on support levels, see Application support for domain separation.

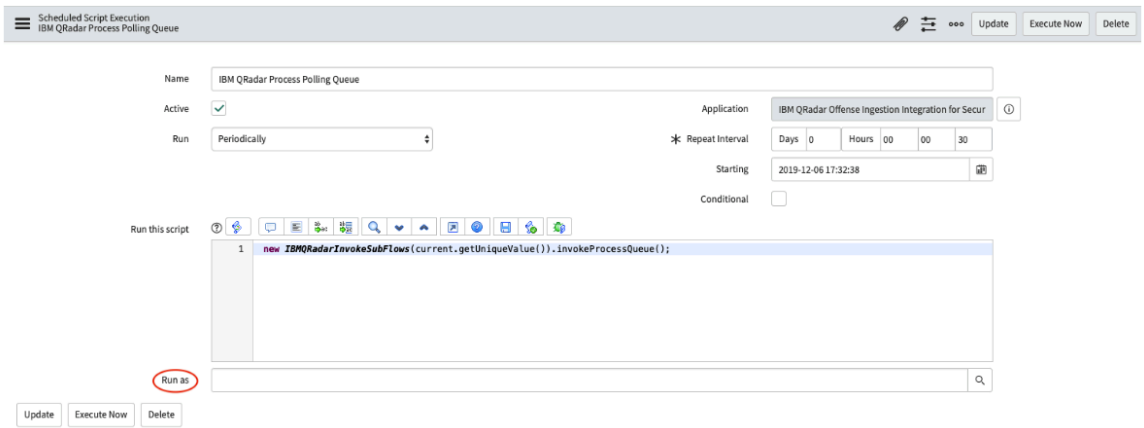
How domain separation works in IBM QRadar Offense Ingestion

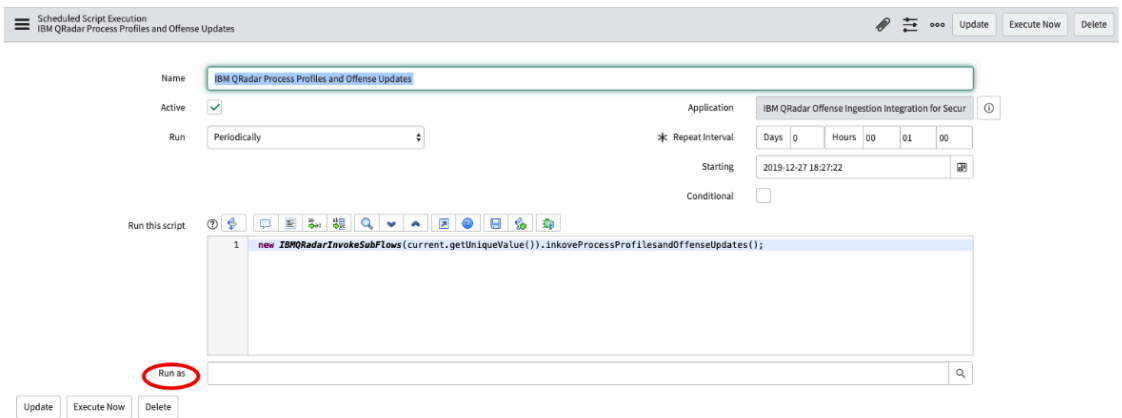
Follow these steps to achieve domain separation:

- Create a user with the *sn_si.admin* role in the respective domain.

  Note: When you create the profile, use the domain picker to select the specific domain. Do not create the user in the parent domain and later change the domain of the profile. You should have a specific user for each domain for your profile with the *sn_si.admin* role. Use this user to create or modify settings in the profile.

- Disable existing scheduled jobs.
- Replicate the IBM QRadar Process Polling Queue, the IBM QRadar Process Profiles, and the Offense Updates scheduled jobs for every domain.
- Change the **Run as** from the system user to the user with the *sn_si.admin* role in the respective domain and run the scheduled job.





Related topics

Domain separation for service providers

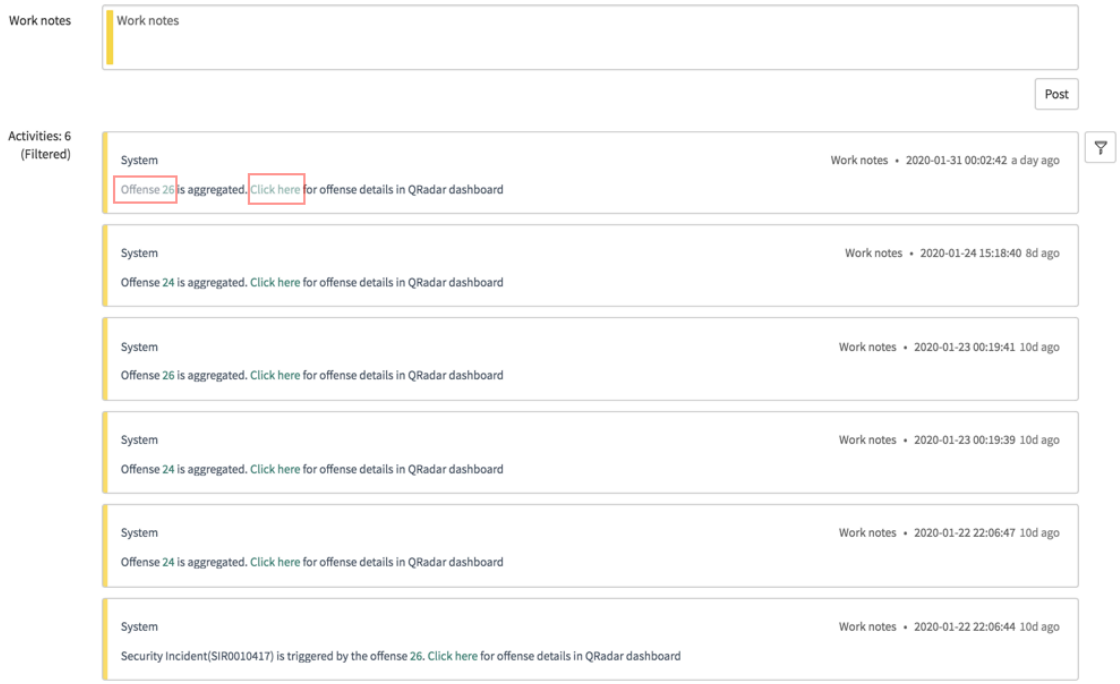
Security Incident Response form after offense ingestion

After an IBM QRadar offense has been ingested, a security incident is created and the corresponding updates are made to the security incident record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

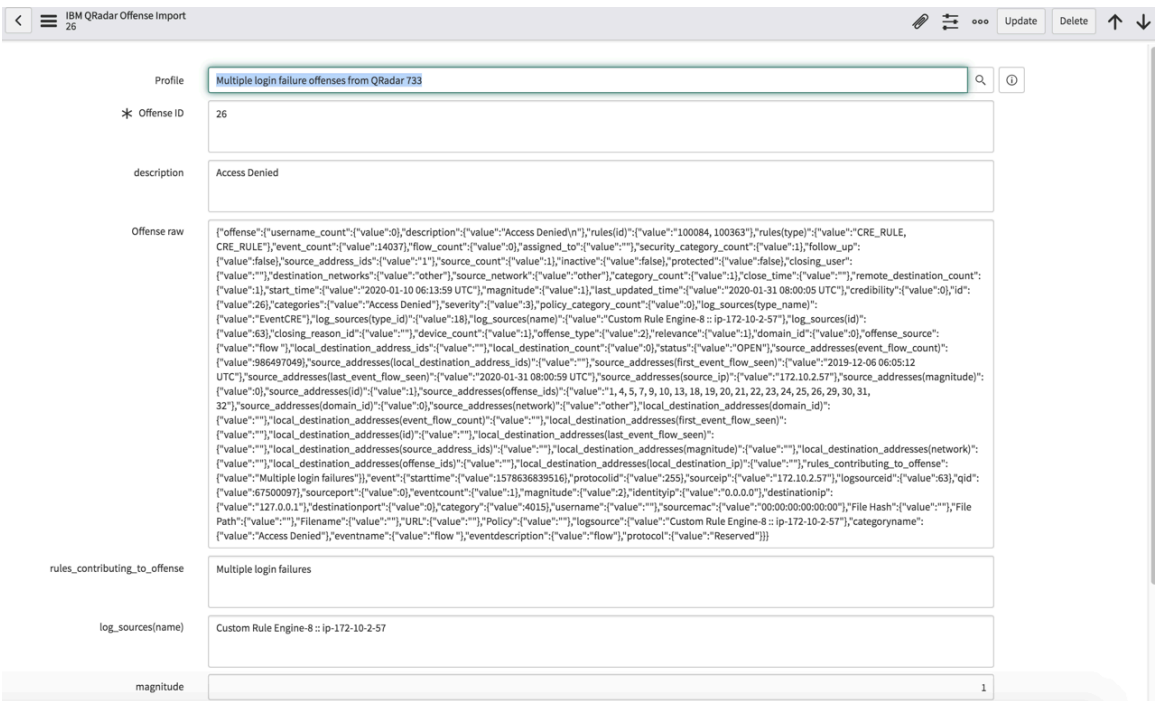
Worknotes

A worknote is posted with details of the offense that triggered the security incident.



Click the offense link to navigate to the internal security incident record. The **Click here** hyperlink takes you to the IBM QRadar dashboard where you can view the offense details.

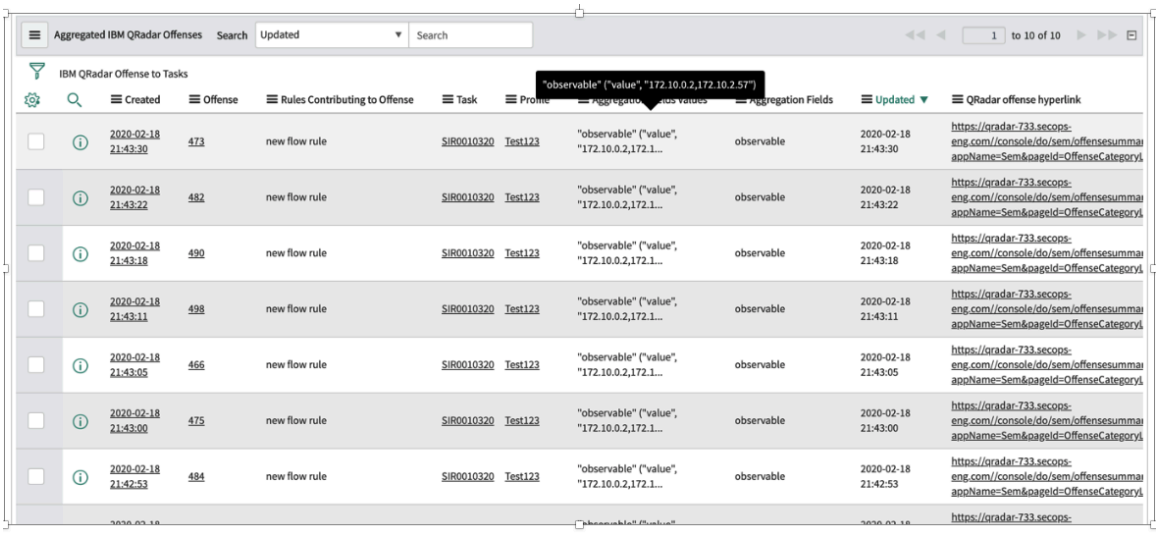
If you had selected the **Log work note for new offense** option in the Offense Aggregation Criteria as described in the Mapping IBM QRadar offense fields to security incident response fields, a worknote is posted when the offense is aggregated.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

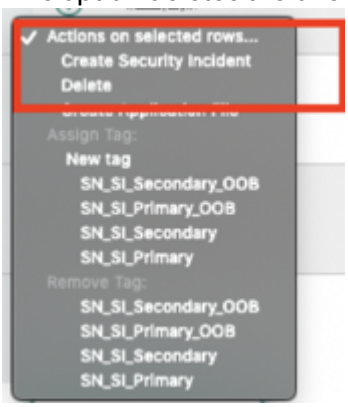
Aggregated offenses

Click **Related Lists** > **Aggregated IBM QRadar offenses** to view the offenses aggregated to the security incident. Click the QRadar offense hyperlink to view the offense in the IBM QRadar dashboard.



Create security incident: Select an offense from the list, click the **Actions** menu, and click **Create security incident**. This option creates a security incident for the offense and this offense is de-aggregated from the parent security incident.

Delete offense record: Select an offense from the list, click the **Actions** menu, and click **Delete**. This option deletes the offense record.

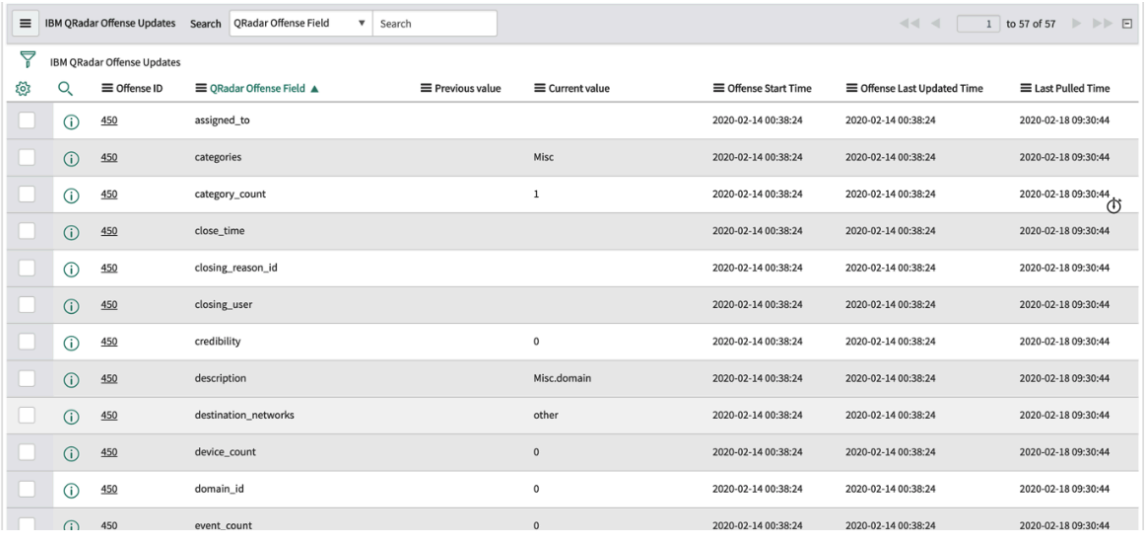


IBM QRadar offense updates

This shows the standard and custom offense fields and tracks changes to the offense during every polling interval. This is helpful as you can view any offense updates directly without navigating to the IBM QRadar dashboard. Any changes to the values are displayed in the Previous value and Current value fields.

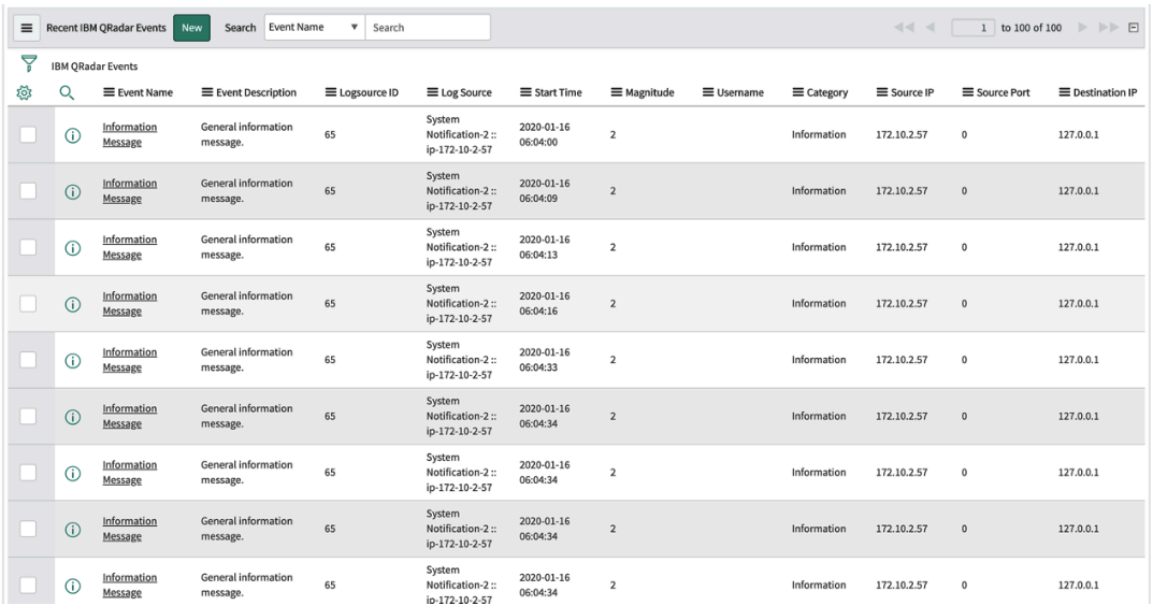
To enable the offense updates feature navigate to **IBM QRadar Integration** > **IBM QRadar Integration Settings** and enable **Set this property to activate the Offense Updates feature**. By default, this setting is disabled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Recent IBM QRadar events

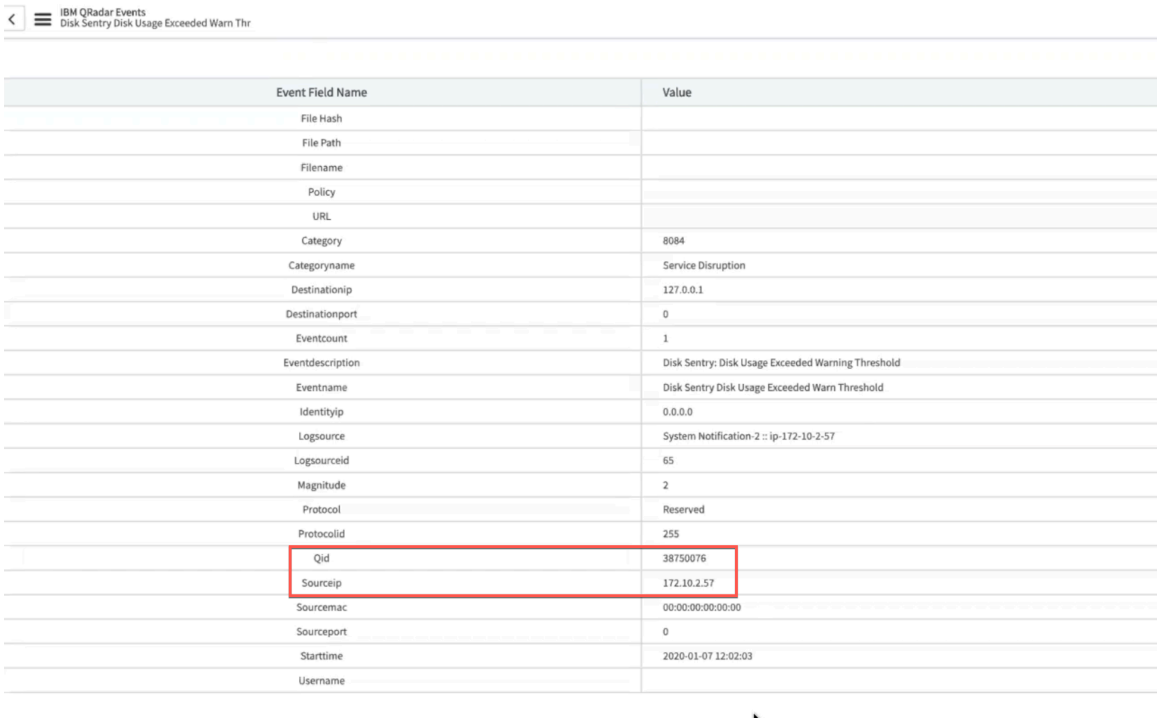
Click the **Fetch Recent IBM QRadar Events** option under the **Related Links** to view the most recent IBM QRadar events.



By default, a maximum number of 100 events are displayed. You can modify this default setting in the Configuration settings.

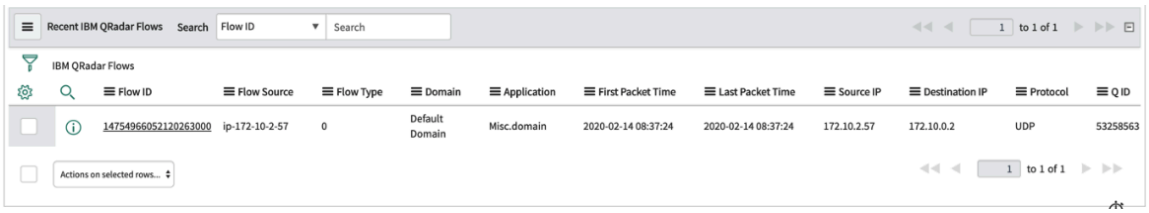
Note: The above image shows the standard event fields associated with the offense. If you have configured and mapped any custom event fields (See Mapping IBM QRadar offense fields to security incident response fields), you can view them in the List View by clicking the Event Name link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Recent IBM QRadar Flows

Using the Integration Hub and Flow Designer, several flows, subflows, actions are available with the IBM QRadar integration. When you click the **Fetch Recent IBM QRadar Flows** option under the Related Links, the most recent flows are retrieved. To view these flows, click **Recent IBM QRadar Flows**.



By default, a maximum number of 100 flows are displayed. You can modify this default setting in the Configuration settings.

Note: The above image shows the standard flow fields associated with the offense. If you have configured and mapped any custom flow fields (See Mapping IBM QRadar offense fields to security incident response fields), you can view them in the List View by clicking the Flow ID link.

Flow Designer and Integration Hub usage with IBM QRadar offense ingestion integration

Using the Flow Designer and Integration Hub functionality, several subflows and actions have been built as part of the IBM QRadar offense ingestion integration.

The following IBM QRadar subflows are available:

- Connection and Credential Validation: This is used in the configuration tile for validating the host and credentials in the initial setup.
- IBM QRadar Rules Retrieval: This is used in the Rules section of the profile setup to retrieve all active rules in IBM QRadar. This subflow is triggered asynchronously.
- Fetch Sample Offenses Data From IBM QRadar: This is used in the Mapping section of the profile setup to fetch sample data. This subflow is triggered asynchronously.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- IBM QRadar Offense status updates: This is triggered by a scheduled job every minute and updates the offense in IBM QRadar when the security incident is created or closed.
- Process Profiles from Scheduled Job and Queue Offenses: This is triggered by a scheduled job every minute to pull offenses per profile based on polling interval. This pulls offenses and queues them to the polling table for further processing.
- Process Polling Queue and Poll in Batches: This is triggered by a scheduled job every 30 seconds to process the Polling table Queue.
- Fetch Recent IBM QRadar Flows: This is triggered from the security incident form link to get latest flows of offense.
- Fetch Recent IBM QRadar Events: This is triggered from the security incident form link to get latest events of offense.

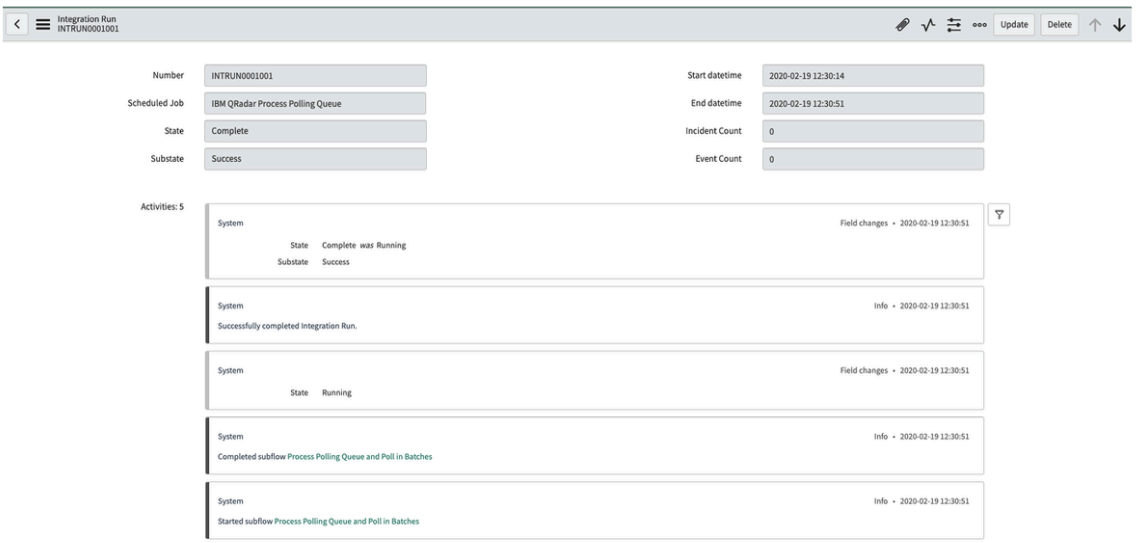
To view these subflows, login as a user with the *sn_si.admin* role and navigate to **Flow Designer** > **Designer**. Click on the Name link of any of the subflows listed above to view the subflow in detail.

Troubleshooting IBM QRadar offense ingestion integration

This section covers important troubleshooting tips and frequently asked questions related to IBM QRadar offense ingestion.

- Integration run: When a scheduled job starts executing, an integration run record with logs, errors, and warnings is displayed. The number of offenses pulled and the number of incidents created in a scheduled job run are also displayed. Users with the sn_si.analyst role can see if any errors/profiles pulling failed during the integration run.

  Worknotes in the integration run provide links to the executed subflows. Users with the sn_si.analyst role can check the `sn_event_ingestion_integration_run` table for any errors that have occurred. To troubleshoot any integration issues, you must first check the integration run. Errors are logged as worknotes in the integration run records for every scheduled job run.



- SSL issues: When connecting to IBM QRadar cloud instances, ensure that the instance has a valid CA certificate which has not expired. You can import RSA or your own certificates into the platform and ensure that the common name of the certificate matches host name. See https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 for details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Incomplete profile: While configuring the profile, in the Additional Options (Automate offense updates and closure based on SIR incident status) section, you must click the **Finish** button to ensure that the profile is moved to Waiting state indicating that it is waiting for ingestion.
- Validate profile: To validate if the integration is working correctly, check the profile states, last pulled date of profile, offense import table, offense to task table records.
- MID server configuration: If you are installing the IBM QRadar application on-premise, after configuring the MID server, you must create a MID server application. The MID server application name should be used in integration configurations tile instead of the MID server name.

> **Note:** The default MID serve timeout is 30 seconds. To see instructions on disabling the timeout period, see <link>. Note that this is a system-wide change and may impact other integrations.

- Offense Updates: If you have enabled the *sn_sec_qradar.get_offense_updates* property and you notice a delay in the creation of security incidents, then disable the property. Do not enable this property when the polling interval is low and the offenses load on QRadar is high as this increases the queue load.
- Missing event, flow data, remote_ip, or users data in a security incident: If you observe that event, flow data, remote_ip, or users data is missing in a security incident, then increase the timeout (seconds) for *sn_sec_qradar.sid_ttl* parameter. Increasing the duration delays the creation of the security incident until the AQLs complete parsing each offense.
- Timeouts: If you view timeout errors in the application logs, review and modify the following flow designer actions:

Flow designer actions

Parameters	Action
Fetch Sample Offenses `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);`	Review and update the duration in milliseconds.
Fetch Sample Offenses `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);`	Add a parameter for the *executeAction* and enter the duration in milliseconds.
Fetch Offenses for profile and queue records in polling table `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);`	Review and update the duration in milliseconds.
Wrapper for testing connection REST `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);`	Add a parameter for the *executeAction* and enter the duration in milliseconds.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parameters	Action
Wrapper for validating API credentials REST `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);`	Add a parameter for the *executeAction* and enter the duration in milliseconds.
REST step for IBM QRadar Offense updates `var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);`	Review and update the duration in milliseconds.

IBM QRadar - Incident Enrichment Integration

The IBM QRadar - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

Explore

Security Incident Response integrations

Set up

- Get started with the IBM QRadar - Incident Enrichment integration
- Create sightings search configuration records

Use

- Run a Sightings Search
- Security Operations Integration - Sightings Search Flow
- Security Operations - QRadar Sightings Search Flow
- View Sightings Search Details
- View Sightings Search Results

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started with the IBM QRadar - Incident Enrichment integration

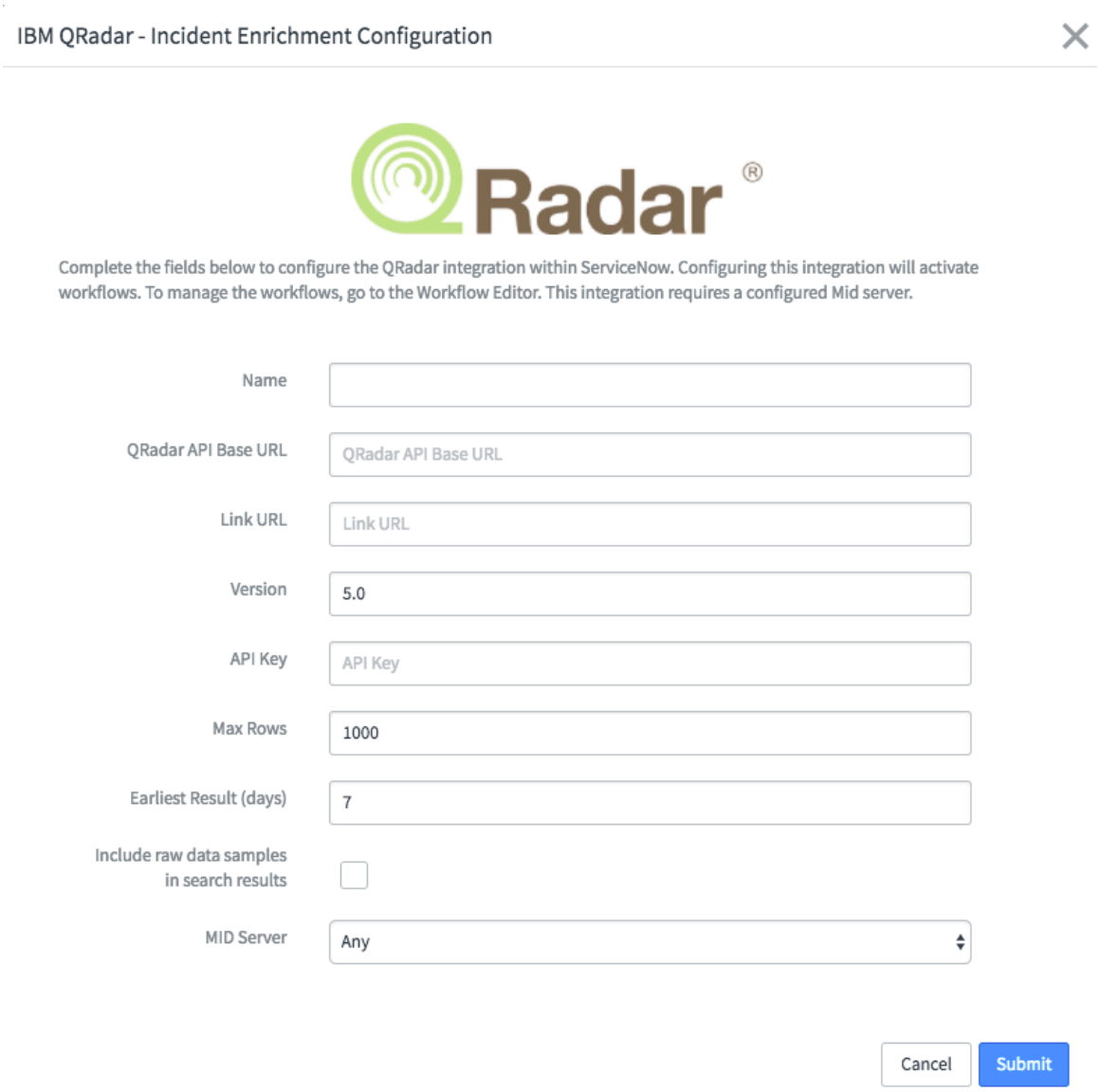
IBM QRadar is an enterprise security information and event management (SIEM) product that integrates easily with Security Operations. Before you can use the IBM QRadar - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and API Key.

Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access IBM QRadar and obtain the API Base URL and API Key under your IBM QRadar profile.
3. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configurations**. The available security integrations appear as a series of cards.
4. In the IBM QRadar - Incident Enrichment card, click **New**.



5. Fill in the fields, as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	The name of this configuration.
QRadar API Base URL	The base URL you acquired from the IBM QRadar site.
Link URL	[Optional] The Link URL that links to an IBM QRadar instance, when available.
Version	The IBM QRadar version; 5.0 is the default.
API Key	The API key you obtained from the IBM QRadar site.
Max Rows	The maximum number of rows you want to search.
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.
7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

LogRhythm Overview

The mapping flexibility of this integration provides an analyst with visibility to events and related alarm data that can be integrated into ServiceNow AI Platform security incidents for further investigation and remediation.

Alarm profiles are created in your ServiceNow AI Platform instance to customize how different LogRhythm alarm fields are displayed on a ServiceNow AI Platform security incident. A default mapping of alarm fields is provided, which can be edited to meet customer-specific needs.

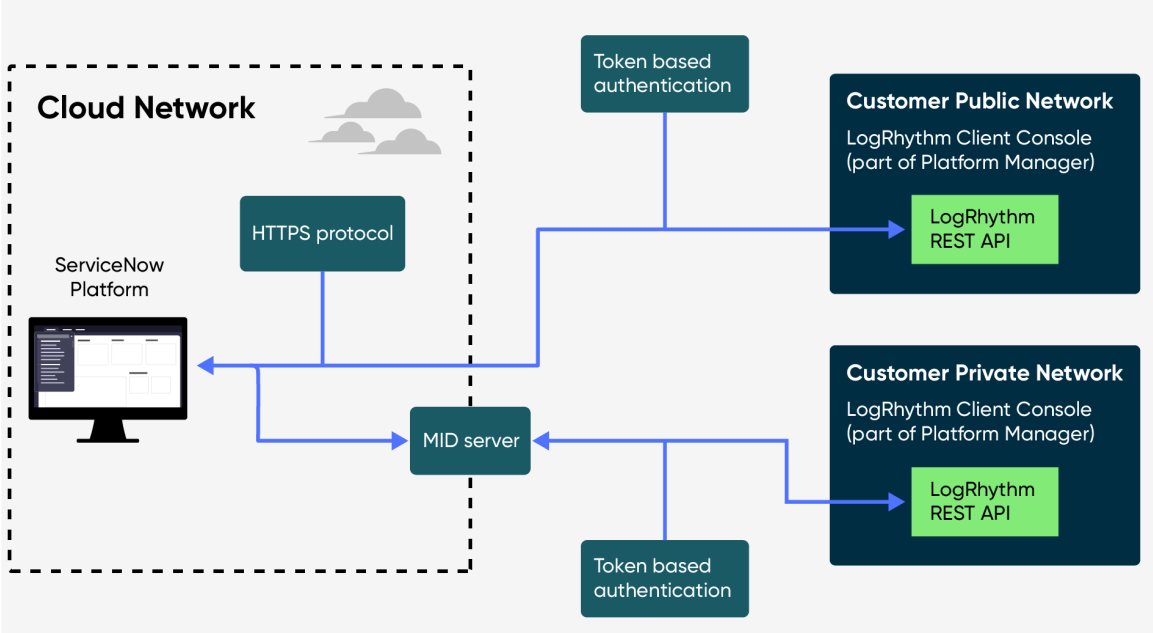
The following figure is an example of a customer environment. When an event triggers the creation of a security incident in the ServiceNow AI Platform® instance, a request is sent from your ServiceNow AI Platform® instance to pull alarms from the LogRhythm Client Console either through a MID Server or even without it.

The REST API key is used by the ServiceNow AI Platform® to authenticate with the LogRhythm Client Console. This connection allows your ServiceNow AI Platform instance to pull individual LogRhythm alarms based on configured profiles.

The REST API is used to gather message details not accessed by the REST API.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

LogRhythm integration



Key features

This integration includes the following key features:

- Flexibility to create multiple alarm profiles for different alarm types such as Phishing and Malware.
- Drag-and-drop mapping of LogRhythm alarm field values to associated SIR security incident fields.
- A Preview of the SIR security incident layout based on LogRhythm sample alarms.
- Ingest historical alarms as well as ongoing future alarms on configurable intervals.
- Automated LogRhythm alarm closure upon SIR incident closure. A URL to the SIR incident as well as an incident ID is provided for easy reference.

Supported releases of the ServiceNow AI Platform

This integration is compatible with the Quebec or later releases of the ServiceNow AI Platform®.

Supported versions of LogRhythm

This integration is compatible with LogRhythm 7.8 or later. The earlier versions aren't supported due to API limitations.

Note: The following topics are numbered. For a smooth installation and to help you verify expected results, follow the topics in the order they're presented.

Set up the REST API for LogRhythm

You use the LogRhythm REST API key to gather additional event details for individual alarm fields. The API key provides details that are unavailable using the LogRhythm REST API.

Before you begin
Role required: LogRhythm Client Console/Platform Manager Administrator

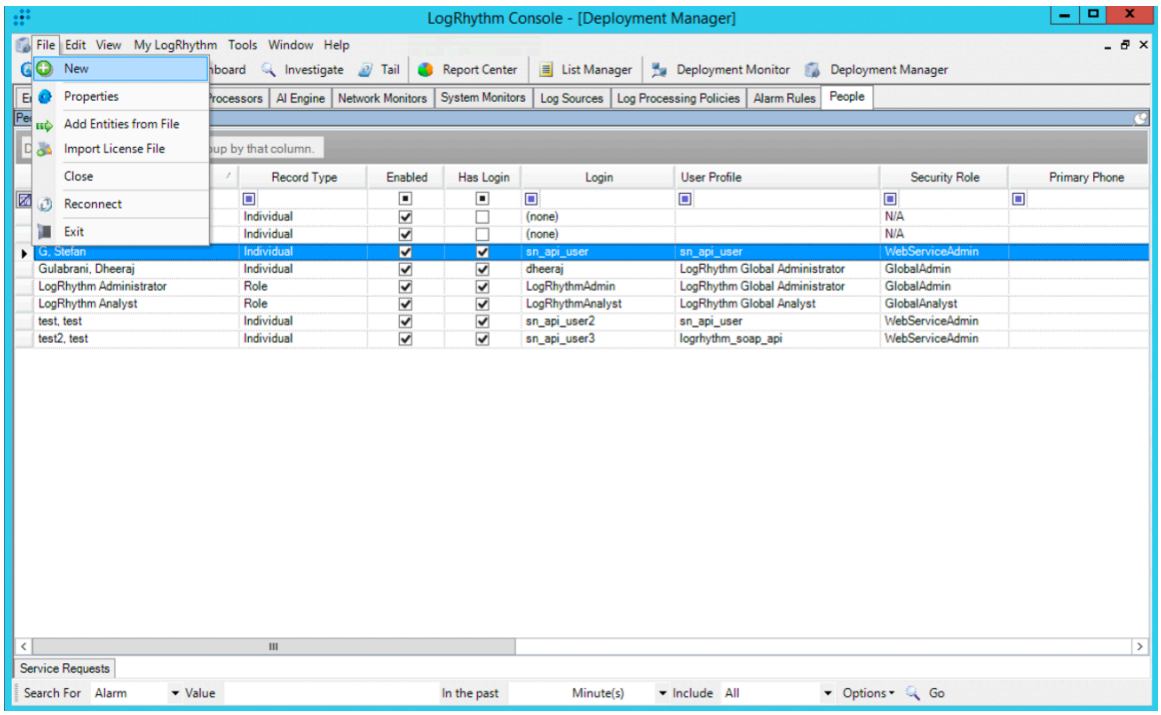
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

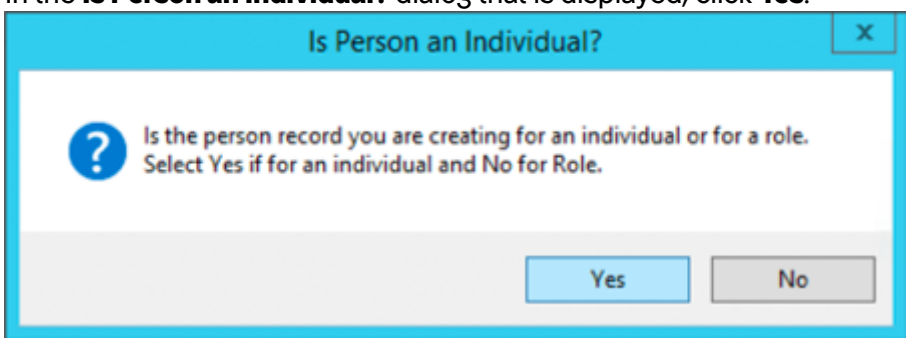
This task is performed on the LogRhythm Client Console. Set up the LogRhythm REST API prior to installing the plugin from the ServiceNow Store.

Procedure

1. Navigate to the LogRhythm Client Console and select the **File** menu.
2. Click **New** to create a new user.



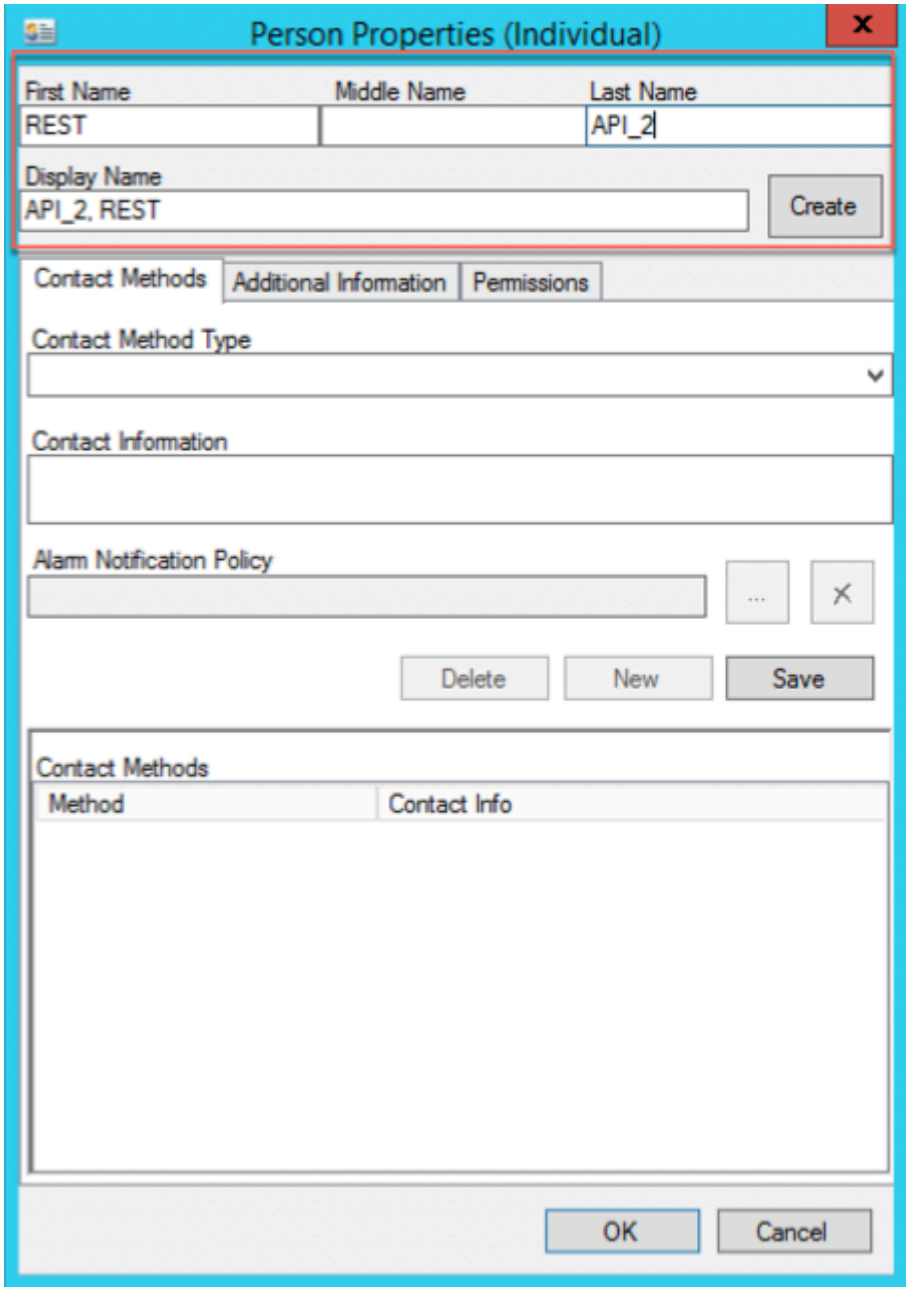
3. In the **Is Person an Individual?** dialog that is displayed, click **Yes**.



4. In the Person Properties dialog that is displayed, fill in the Name fields.

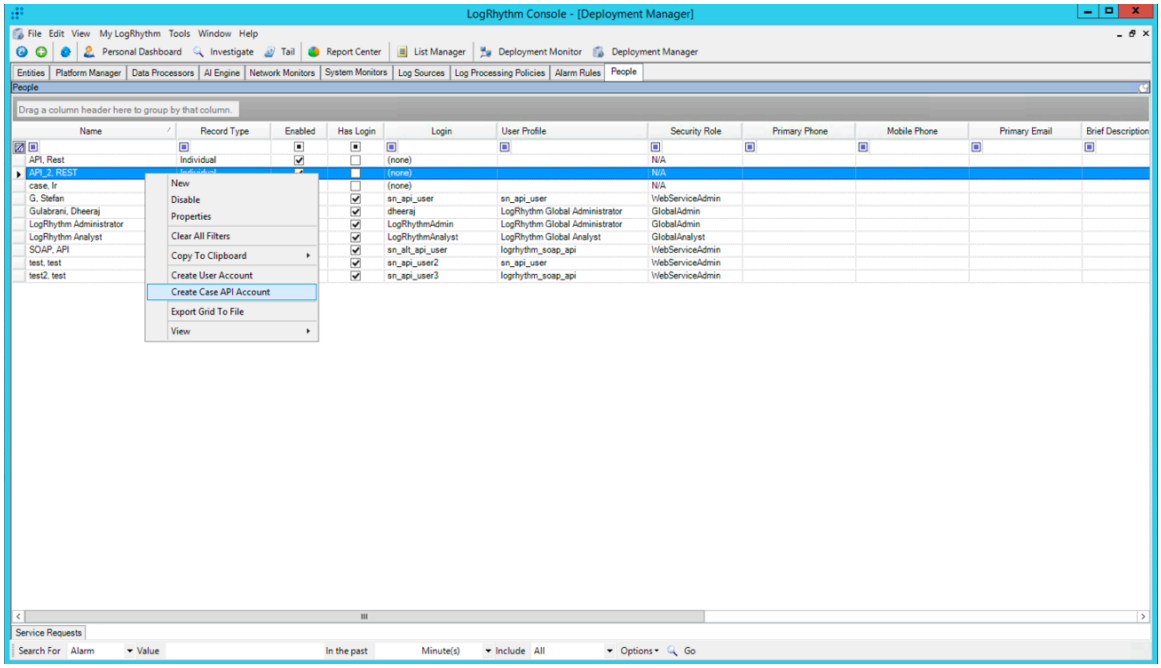
   Use a different name for the LogRhythm REST API than the one you used to create the REST API, for example, `REST API_2`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



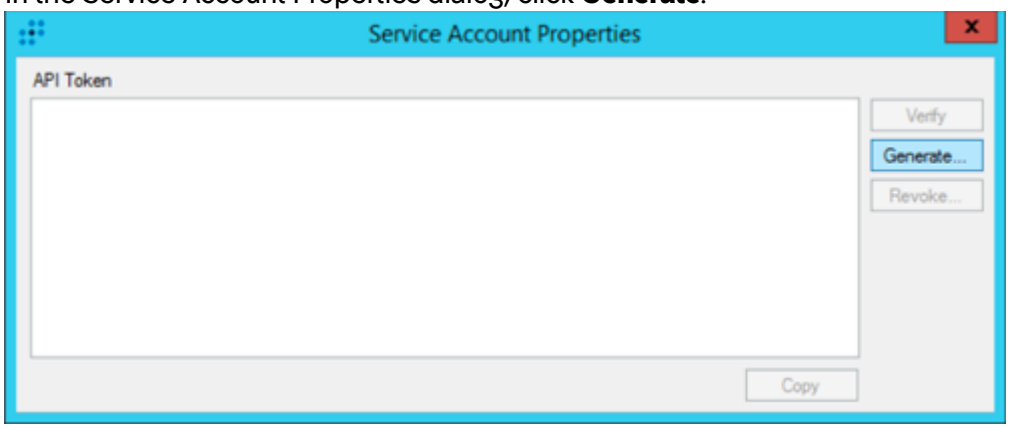
5. Click **OK**.
6. Right-click the new listing in the Name column (**API_2_REST**) and, in the choice list, select **Create Case API Account**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

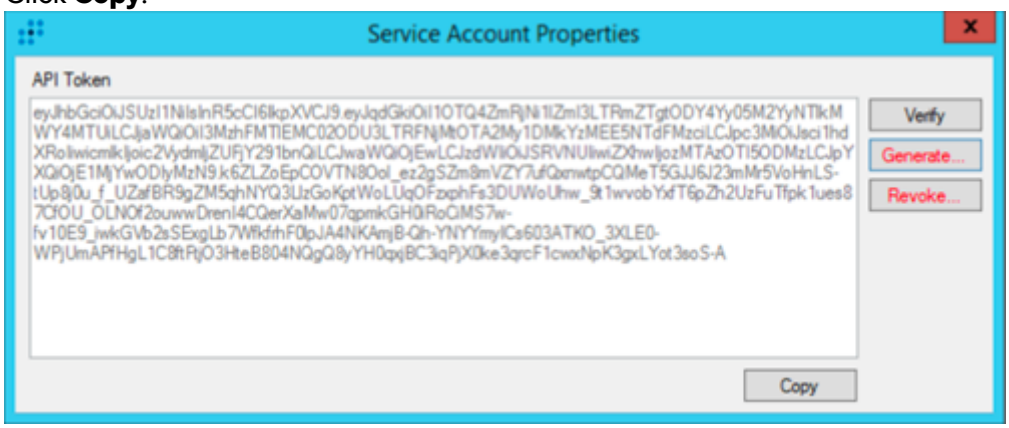


Note: The Case API is not used, but the credentials for the Case API Account and the LogRhythm REST API are the same.

7. In the Service Account Properties dialog, click **Generate**.



8. Click **Copy**.



You have now set up the LogRhythm REST API. You paste the string you copied in the previous step into your ServiceNow AI Platform instance in the LogRhythm REST API Token field during the configuration steps listed in Install the plugin and configure LogRhythm.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

You are now ready to Install the plugin and configure LogRhythm.

Install the plugin and configure LogRhythm

Before you run the integration on your instance, complete the installation and configuration steps so the application properly integrates with Security Operations on the ServiceNow AI Platform®.

Before you begin

Role required: admin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration. The latest LogRhythm version is 7.8 or later.

Note: Your existing alarm profiles will no longer be supported on the latest LogRhythm version, so you need to create new alarm profiles and perform the required configurations.

Setup task	Description

Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.	The following roles are required for installation, configuration, and verification of expected results:
	• The system administrator (admin) installs the application plugin and assigns the security incident administrator (sn_si.admin) role.
	• The (sn_si.admin) oversees the following tasks:
	  ○ Names, creates, and edits alarm profiles.
	  ○ Maps and filters alarms – identifies specific LogRhythm alarms that create security incidents and configures how these alarm fields map to a ServiceNow AI Platform® security incident.
	  ○ Previews security incident details for accuracy prior to finalizing the configuration.
	  ○ Ingests historical alarms and schedules pulled alarms.
	  ○ Assigns the security incident analyst (sn_si.analyst) role.
	  ○ This role also has access to the Security Operations module.
	• The security incident analyst (sn_si.analyst) responds to security incidents that are created based on the alarm profile settings.

Obtain a LogRhythm API user name and password and verify that you are using version LogRhythm 7.8 or later.	Visit the product website for information on API keys and to create an account: LogRhythm Enterprise website. The user accounts, credentials, and certificates must

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	be configured properly prior to installing the application. The integration requires LogRhythm version 7.8 or later and the LogRhythm REST APIs. See Set up the REST API for LogRhythm.
Verify that you have installed and configured a MID Server.	A MID Server is required in your ServiceNow AI Platform environment. See the ServiceNow Product Documentation website for information about how to set up and configure MID Servers.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	For the Rome release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

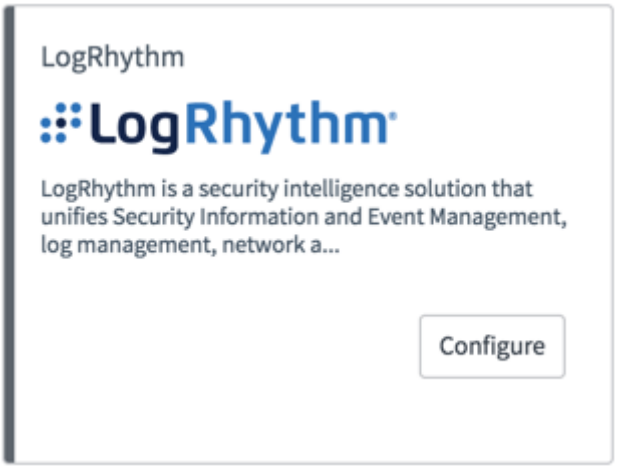
Important: If you have any connectivity issues to the LogRhythm client console, refer to the Verify connectivity for LogRhythm.

Procedure

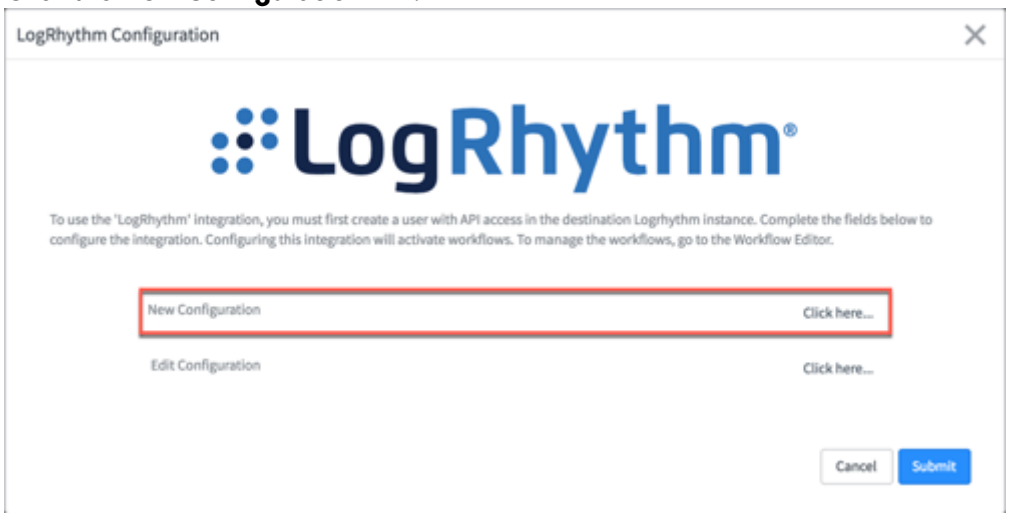
1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
2. Once the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the LogRhythm tile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Configure**.



4. Click the **New Configuration** link.



5. On the form, fill in the fields:

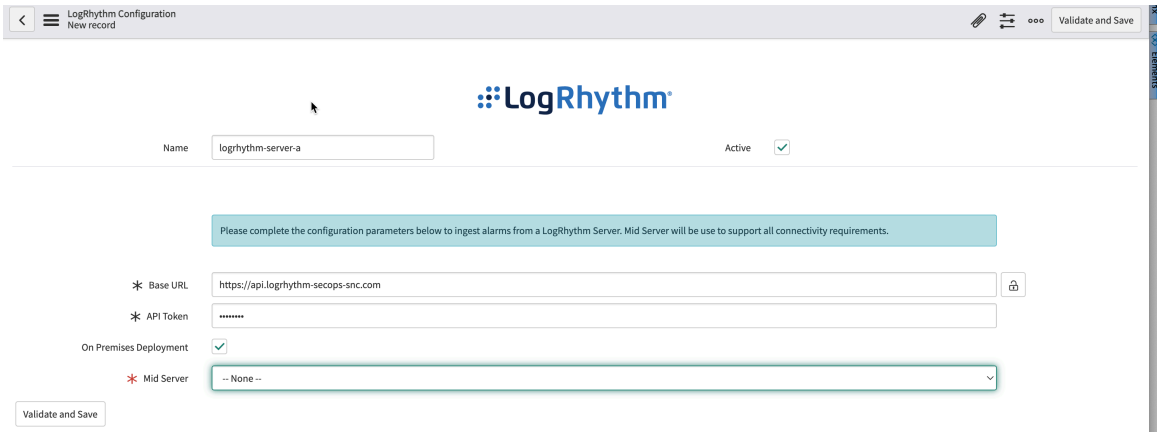
LogRhythm configuration

Field	Description
Name	LogRhythm server name, for example, `logrhythm-server-a`.
Base URL	Base URL hosting the LogRhythm REST API. The MID Server permits access to the network where the LogRhythm Client Console is hosted. This URL is where the LogRhythm server is hosted within that network. Click the lock icon on the right-end to edit the field and enter text for a URL, for example, `https://logrhythm.secops-eng.com:8501/`.
API Token	Enter the token that is associated with your REST API that you created on the LogRhythm Client Console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
On-Premise Deployment	Option to select if it's a LogRhythm on-premise deployment.
MID Server	Specific MID Server that is set up in your environment. Only the MID Servers that are active and have been validated are available from this choice list.

The following figure is an example of a completed form.



6. Click **Validate and save**.
   After validation is successfully completed, a message is displayed and the LogRhythm Configurations page is reloaded. The next step is to create an alarm profile.

What to do next

After you successfully complete the validation, the next step is to Creating an alarm profile for LogRhythm.

Creating an alarm profile for LogRhythm

In an alarm profile that you create and name, you specify which alarms you want to pull from the LogRhythm Client Console. You also define how they are mapped to fields on a ServiceNow AI Platform security incident.

Before you begin

Role required: sn_si.admin

About this task

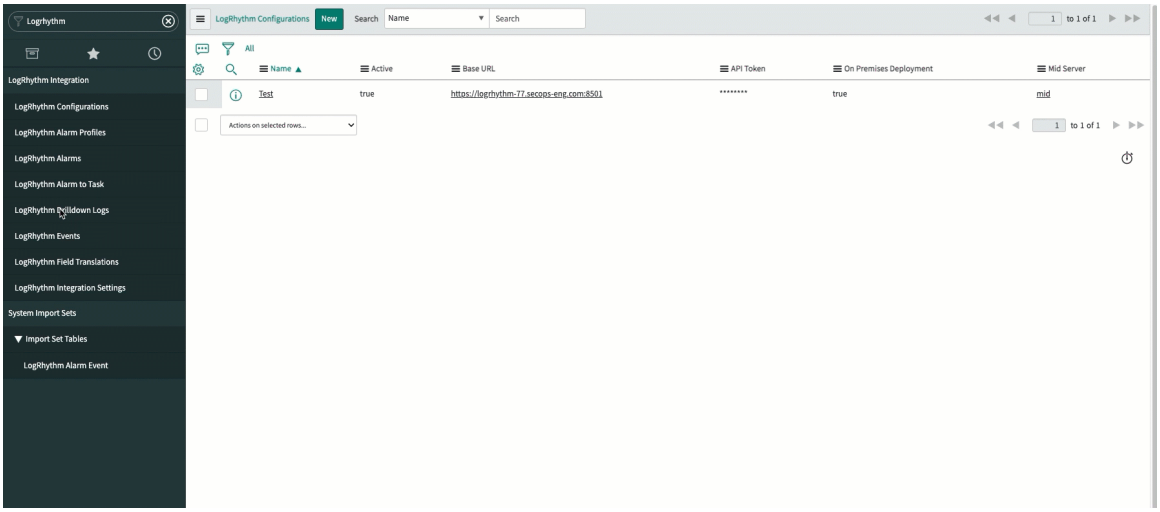
Based on the Alarm Profile configured, one alarm profile can ingest all types of alarms out of the box, but you can use filter criteria to ingest specific types of alarms. Using this ServiceNow AI Platform integration, all configured alarm rules or specific ones based on the profile created are ingested. Alarm rules such as only high-risk level alarms can then be filtered to specify which alarms should create security incidents. Before security incidents are created, individual field values on the filtered alarms are mapped to corresponding fields on the ServiceNow AI Platform security incident. This configuration is done via an alarm profile within your ServiceNow AI Platform instance.

Procedure

1. Navigate to **All** > **LogRhythm Integration**.
2. Select the **LogRhythm Alarm Profiles** module to display the **Alarm Profiles** list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Alarm Profile



3. To create a new alarm profile, click **New**.
   A new alarm profile form is displayed. At the top of the page in the progress bar, **Name** is selected. This bar tracks your progress during the configuration.
4. On the form, fill the fields.

Alarm Profile

Field	Description
Name	Name for the alarm profile. This name helps you identify the alarm types such as Unauthorized access (VPN), malware, or phishing.
Short description	Short text for additional information about the alarm profile, which may include the type of alarms, or an alarm category. An example description: All alarms associated with unauthorized Powershell and Sudo access attempts.
Source	Source server from the choice list. The list consists of LogRhythm configurations you have already set up, for example, `logrhythm-server-a`. See Install the plugin and configure LogRhythm.
Order	Alarm profile priority. This field indicates the order in which the alarm profiles are executed when two or more alarm profiles share the triggering conditions.
Active	By default this option is not selected. After you complete all alarm profile setup steps and click **Finish**, you are prompted to select this check box to activate the alarm profile. When the alarm profile is active, it pulls

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	alarms from the LogRhythm Client Console automatically.

5. Click **Continue** to save your data and proceed to the Mapping form.

   If the validation is successful, the page reloads and the **Mapping** form is displayed. You cannot proceed with the configuration until you have successfully validated your connection and credentials.

Related topics

Mapping LogRhythm alarms to the security incident

Mapping LogRhythm alarms to the security incident

After selecting the LogRhythm source that you want to ingest, you need to map individual LogRhythm alarm fields to the ServiceNow AI Platform security incident fields.

Mapping alarms includes the following tasks:

- Map LogRhythm alarms. For this task, you list and ingest (Pull) sample alarms using the alarm IDs or most recent alarms from the LogRhythm client console.
- The Sample Alarm fields are categorized into three groups:
  - Alarm fields: The alarm fields that are available and their corresponding values are displayed.
  - Event fields: The event fields that are available and their corresponding values are displayed.
  - DrillDownLog fields: The drilldown log fields that are available and their corresponding values are displayed.
- Each Alarm ID that you pulled is displayed as a tab. On the Alarm ID tabs, verify that all critical alarm fields from the Alarm Sample Ingestion section on the left of the form are mapped to the SIR Incident Field Mapping section on the right of the form.
- After you map the alarms to the SIR Incident Field Mapping field, you can see the alarm category also being display in the Input Expression field. For example, `${Alarm: alarmid}$`.
- You can modify the configuration by adding or removing fields on the security incident. Track overlooked or duplicated fields with the color coding that is provided.
- You can filter alarms to specify which alarms are ingested into the SIR application. You can either filter the alarms directly or use the alarm categories to drill down your search based on Alarms, Events, or DrillDownLogs.
- Use the script editor if you want to format values for the Priority and Category fields on the security incident.

The next step is to Map LogRhythm alarm fields to security incident fields.

Related topics

Map LogRhythm alarm fields to security incident fields

Use the script editor to format LogRhythm values

Filter alarms for LogRhythm

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Map LogRhythm alarm fields to security incident fields

You map individual alarm fields to the security incident fields. The preconfigured mapping can be edited, and color coding provided for the fields helps you monitor alarms you have already mapped. This step helps you visualize how your edits impact the fields on the security incident.

Before you begin

Role required: sn_si.admin

If you are unfamiliar with the LogRhythm alarms, navigate to the LogRhythm Client Console and review a few sample Alarm IDs. For the following example, LogRhythm alarms `9468` and `9474` were used to map the alarms to the security incident.

About this task

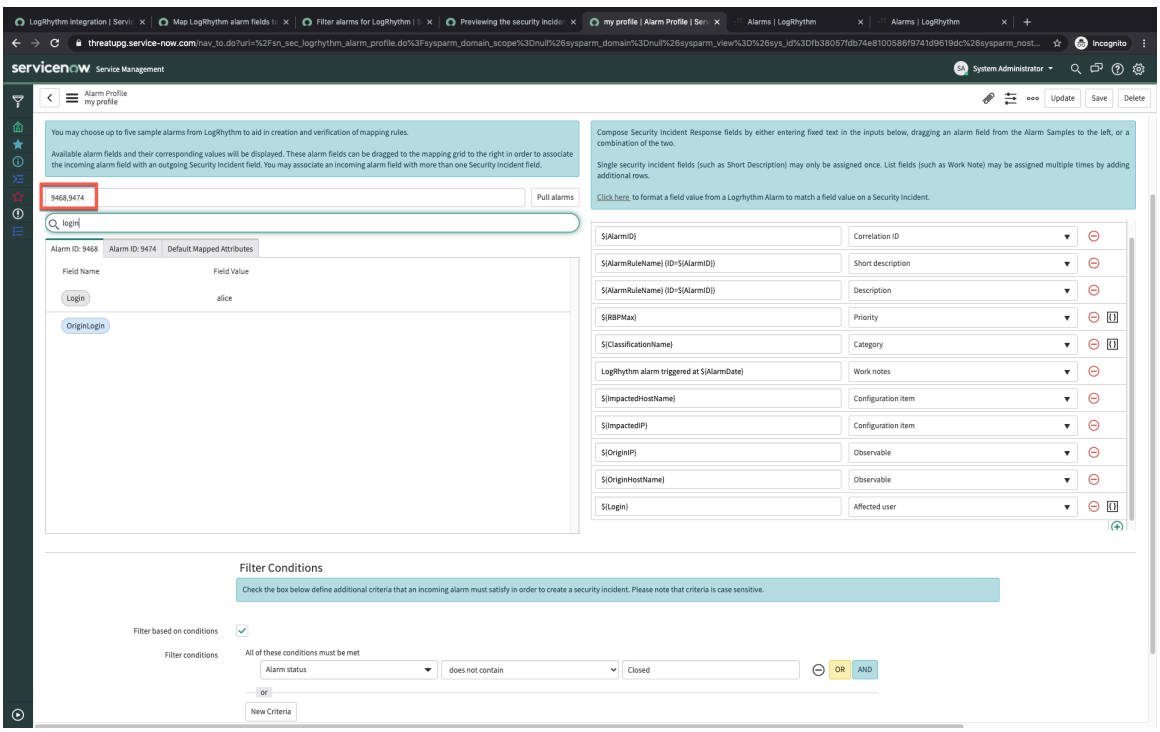
Using this form, you map the LogRhythm alarm rules on the left to the security incident fields on the right.

The following figure shows the default mapping of alarms that is preconfigured for each alarm profile. This default mapping can be edited, and with this form, you customize the fields that populate the security incident. After you complete this mapping, you can see how adding or removing alarm fields potentially impacts the field values on the security incident.

On the left side of this form in the following figure, the LogRhythm alarm rules are outlined. The values of these alarm rules are mapped to the security incident fields on the right side of the form.

Procedure

1. After creating an alarm profile for LogRhythm, click **Mapping** on the progress bar.
2. In the **Alarm Sample Ingestion** field, enter up to five sample LogRhythm Alarm IDs separated by commas (`9468 , 9474`).



3. Next to the alarm field, click **Pull Alarms**.

   The pull for sample alarms may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the sample Alarm IDs are submitted and successfully pulled from the LogRhythm server, the alarm fields and their corresponding values are displayed in tabs.

Note: After an alarm ID is successfully pulled, the ServiceNow AI Platform may return the following message: `The following new fields will be available for filtering shortly. Please reload this profile in a few minutes if filtering based on these fields is required. itemspacketsin, itemspacketsout`.

This message occurs when the single alarm that has been pulled contains field names not previously processed by the ServiceNow AI Platform. These fields are available for mapping, however, if this message is displayed, reload the form so that these fields are displayed and available in the filter choice lists of the conditions builder when you are ready to set filtering conditions.

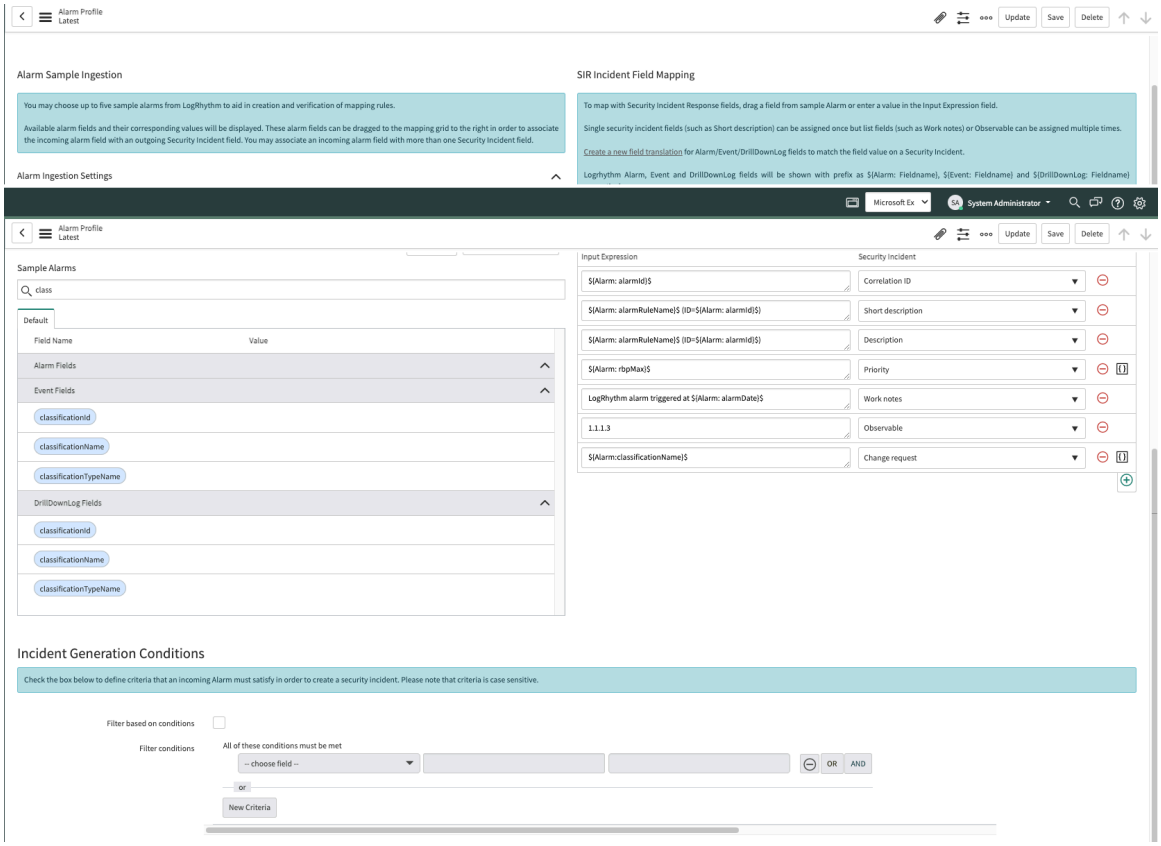
Ingesting these sample alarms in the alarm profile configuration helps you prevent mapping alarm fields to the security incident that contain no values. It also aligns alarm fields with values to the appropriate fields in the security incident. This step ensures that all critical alarm fields are mapped and that there are no missing field values on the security incident.

To help you ensure that no alarms are overlooked or duplicated in the mapping process, alarm fields are color-coded. A light blue alarm field (`Account`, `AlarmRuleID`, `AlarmStatus`, etc.) indicates that a field is not yet selected for mapping to a security incident.

A gray field (`AlarmDate`, `AlarmID`, and `AlarmRuleName`) indicates that a field has already been selected and has been mapped to a field on the security incident. This color coding helps you track the mapping, because in certain cases, an alarm field can be mapped to more than one field on a security incident. For instance, the `Observables` and `Work Note` fields can have more than one value.

4. To clear the sample alarm data, click **Clear Sample Alarm Data**.
5. To edit the default configuration on the security incident, follow these steps to add a field:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



a. On the lower right of the form, click the plus icon.
A new field is displayed.

b. In the Security Incident column, select an available field from the choice list.

In the expanded choice list, some of the fields are shaded. For example, `Category` has a gray background, which indicates it has been mapped in the security incident. Similar to the color coding for LogRhythm alarm fields, this color coding for the security incident fields ensures that values from the alarm fields are not inadvertently mapped to the same security incident field.

In the illustration above, the alarm rule `${Alarm:classificationName}$` is already mapped to the `Category` field in the security incident in this profile.

Note: The Observable field can be mapped to more than field on the same security incident so that multiple observables can be displayed. Similarly, the `Configuration Item` and `Work notes` fields can be mapped to display multiple values.

On the Alarm Sample Ingestion side of the form, blue indicates that an alarm rule field has not been mapped. Gray indicates that it has been mapped. In the choice list on the SIR Incident Field Mapping side of the form, white indicates that a field has not been mapped. Gray indicates that a field has been mapped. Use this color coding to help you track your field mapping.

In the above illustration, `Affected user` has been selected from the choice list as a new field on the security incident.

c. From the Alarm Sample Ingestion section on the left side of the form, left-click to select the Alarm ID you want in the Input Expression field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the above illustration, `Login` has been selected.

d. Drag it to the cleared field and release it.
In the left column in the SIR Incident Field Mapping section, the new value for the `Affected User` field is displayed. In this case, the `Login` value from the LogRhythm alarm is displayed in the `Affected user` field on the security incident.

6. Alternatively, to manually enter a value for fields in the Input Expression column, place your cursor in the input expression field, and enter a desired alarm value.

For example, in the above illustration another field has been added (`Assignment group`) to the security incident form, and `Security Incident Assignment` has been entered manually in the field.

7. Continue editing the preconfigured mapping as required.
If you need to translate values from LogRhythm alarm fields to values that are supported by the fields on the security incident, you can use the script editor. See Use the script editor to format LogRhythm values.

What to do next
After you complete the field mapping, the next step is to Filter alarms for LogRhythm.

Filter alarms for LogRhythm

Setting filtering criteria for alarms after you have mapped fields helps you determine which alarms should be ingested into the SIR application. Filtering alarms helps you significantly reduce the number of alarms you ingest when the alarm profile is activated.

Before you begin
Role required: sn_si.admin

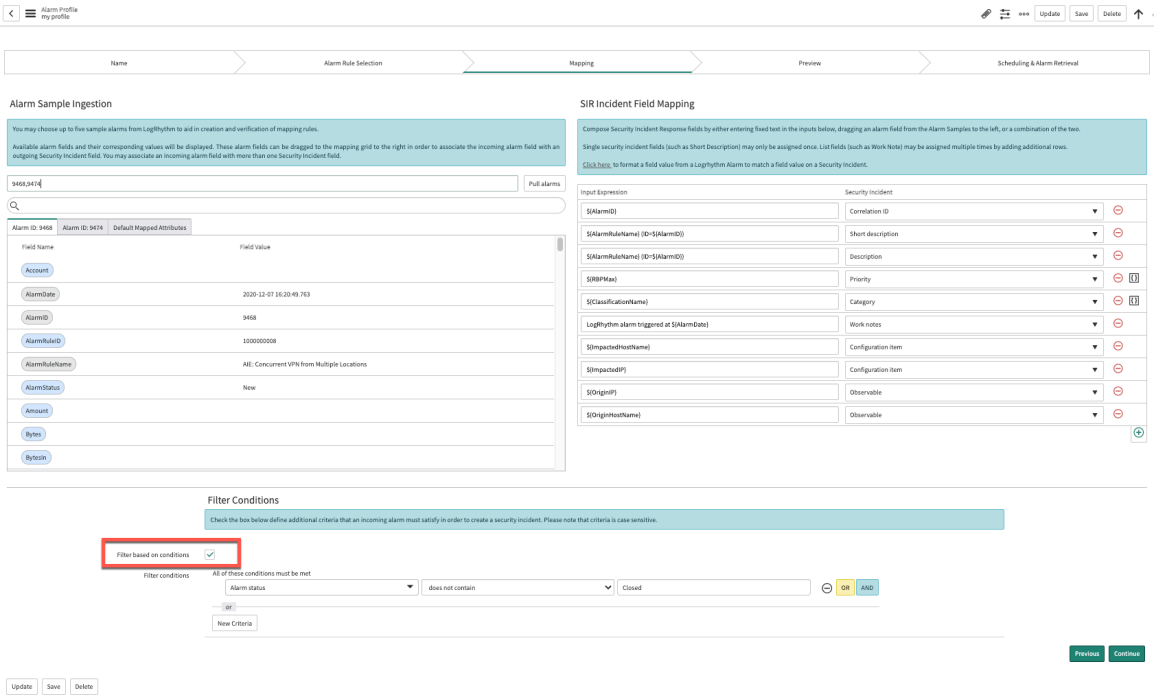
About this task
Use the filtering conditions at the bottom of the mapping form to filter out specific alarms or limit ingestion to only alarms that meet certain field-level criteria. Filtering significantly reduces the number of alarms you ingest once the alarm profile is activated. Use filtering to ingest a manageable quantity of alarms that your Security Operations Center (SOC) staff can support.

Note: The following example shows a default filter setting in which `Alarm status - does - not - contain - Closed` is the default setting. This filter only pulls active alarms, and this setting reduces the number of pulled alarms. The following steps illustrate how to add another useful filter which includes only alarms with the highest severity or priority values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

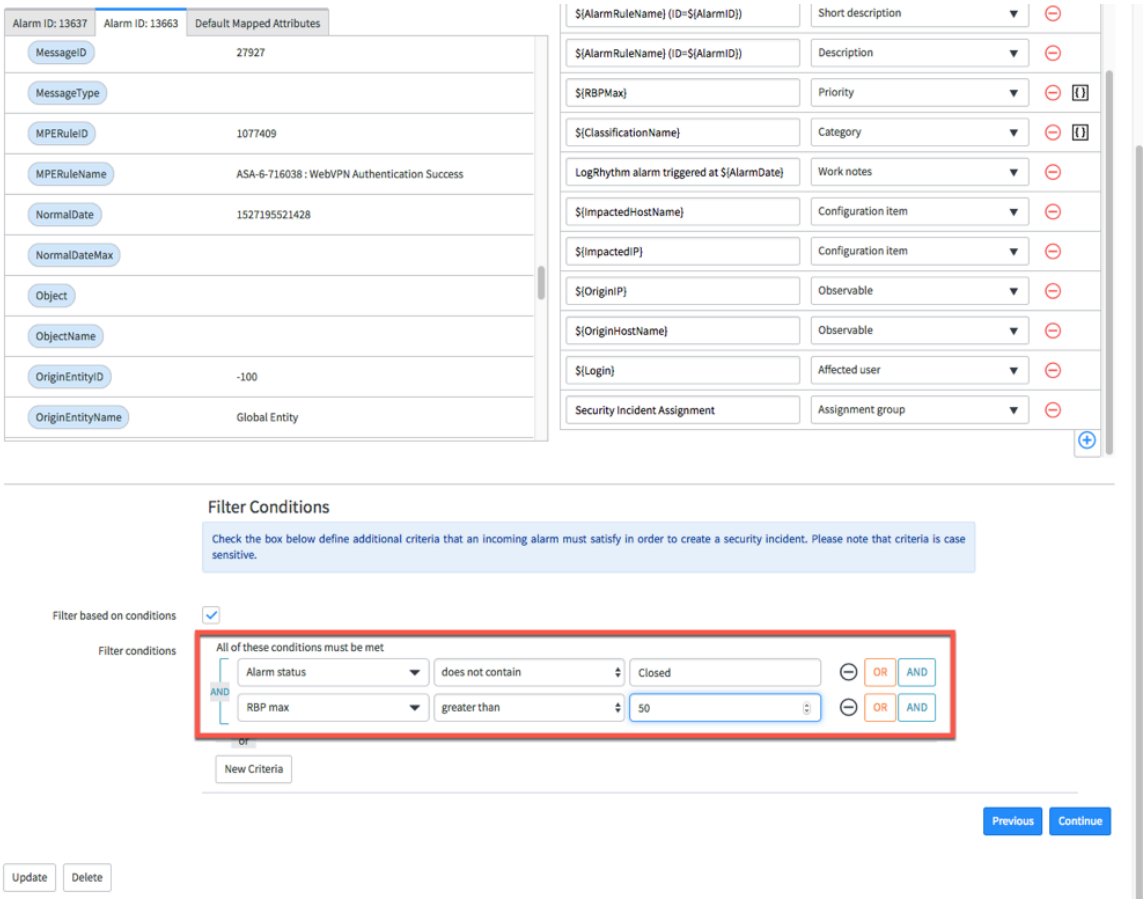
1. To edit the filtering criteria, select the **Filter based on conditions** check box.



2. To the right of the **Filter conditions** field, click **OR** or **AND**.
3. In the new line that is displayed, select the filtering conditions from the choice lists.

   The following image shows an additional filter added to the criteria in which risk-based priority (RBP max) is greater than 50. With this filter setting, only LogRhythm alarms with a risk-based priority value that is greater than 50 are pulled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. After you have verified that all critical LogRhythm alarm fields are mapped to the ServiceNow AI Platform security incident, and you have set filtering criteria to limit alarm ingestion, choose one to continue the configuration.

Option	Description
Continue or Preview	The Preview form of the security incident with your mapping configuration is displayed. **Preview** is selected on the progress bar. The next step is to view the security incident with your mapped alarms.
Update	Save your data and return to the **Alarm Pro files** list.
Previous	The alarm profile record is displayed.
Delete	Delete this alarm profile and the **Alarm Pro files** list is displayed.

What to do next

The next step is to preview your mapped fields on the security incident. See Previewing the security incident with mapped LogRhythm alarm values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Previewing the security incident with mapped LogRhythm alarm values

After you have completed the mapping step, preview the values that you mapped to the fields on the security incident. This preview step permits you to verify that you have mapped all the critical LogRhythm alarm fields you want displayed on the security incident.

Role required: sn_si.admin.

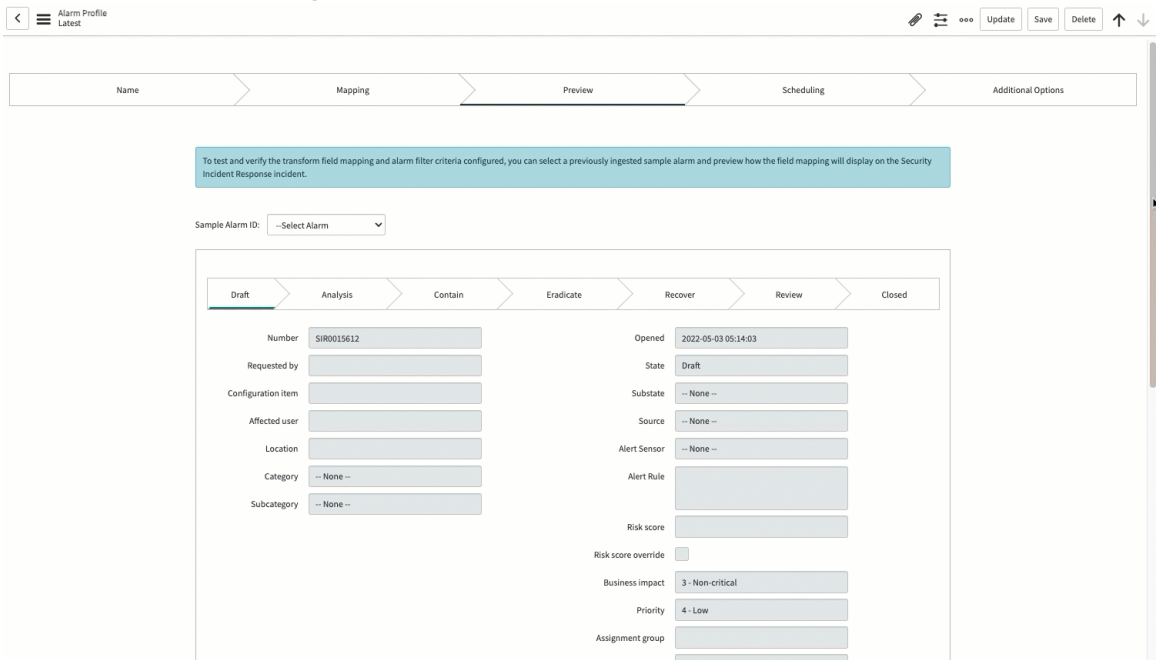
Security incident

If the security incident preview is not displayed, click **Preview** in the progress bar.

An example of the preview for the entire ServiceNow AI Platform security incident is displayed in the two following figures. This example of the preview of the security incident is populated with the LogRhythm alarms fields mapped from sample alarm `13663`.

In the following figure, the `Configuration item`, `Affected user`, `Priority`, `Assignment Group`, and `Short description` fields of the security incident are populated.

Upper half of the security incident



On the lower half of the security incident form, the `Description` field is populated. Under the Related Items section, the `Configuration item`, `Observable`, and `Work note` fields are populated with values. If multiple values for these fields are mapped, each value is displayed on the security incident, because each of these fields can accept more than one value.

Error conditions in preview

The following warning messages may be displayed when previewing the security incident. If a sample alarm does not pass the filtering criteria, the entire security incident is not populated.

Input value not found

If the alarm ID is included within the filtering conditions, a warning message may still be displayed if specific input values are not found for certain mapped fields. For the sake of the following example, in the preview of the record, assume that there is no value in the `Assigned to` field, although it was mapped.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For this type of message, in the Mapping record, verify that the input value is correct. In this case, the person in the `Assigned to` field in security incident is incorrect in the ServiceNow AI Platform instance. When this alarm is ingested and it creates a security incident with this condition, fields with this input value (`Abel Tuter`) are left blank in the security incident.

The remaining messages in blue are informational, and they indicate that these fields have no value to display in the preview. This preview permits the security incident administrator configuring the alarm profile to verify that these fields should have no value at the initial creation stage, because in certain cases, security incident fields may be populated later automatically. Other mapping errors are also displayed.

After you are satisfied with the mapping and the security incident preview, choose one to continue the configuration.

Option	Description
Click **Continue** or **Scheduling** in the progress bar.	Advance to the **Scheduling & Alarm Retrieval** form. **Scheduling & Alarm Retrieval** is selected on the progress bar. The next step is to schedule alarm retrieval.
Click **Previous**.	Return to the alarm profile and continue mapping.
Enter another alarm ID in the **Sample Alarm ID** choice list at the top of the preview form.	The **Sample Alarm ID** choice list is displayed for every alarm ID you have entered. You can select up to five alarms. This option permits you to preview another LogRhythm alarm ID on a security incident.

After you preview the security incident and are satisfied with the results, the next step is to Schedule and retrieve LogRhythm alarms.

Schedule and retrieve LogRhythm alarms

After you preview the security incident with the LogRhythm alarms that you have selected and mapped, you are ready to schedule alarm retrieval. After you complete this step, the alarm profile is ready to be activated.

Before you begin

Role required: sn_si.admin

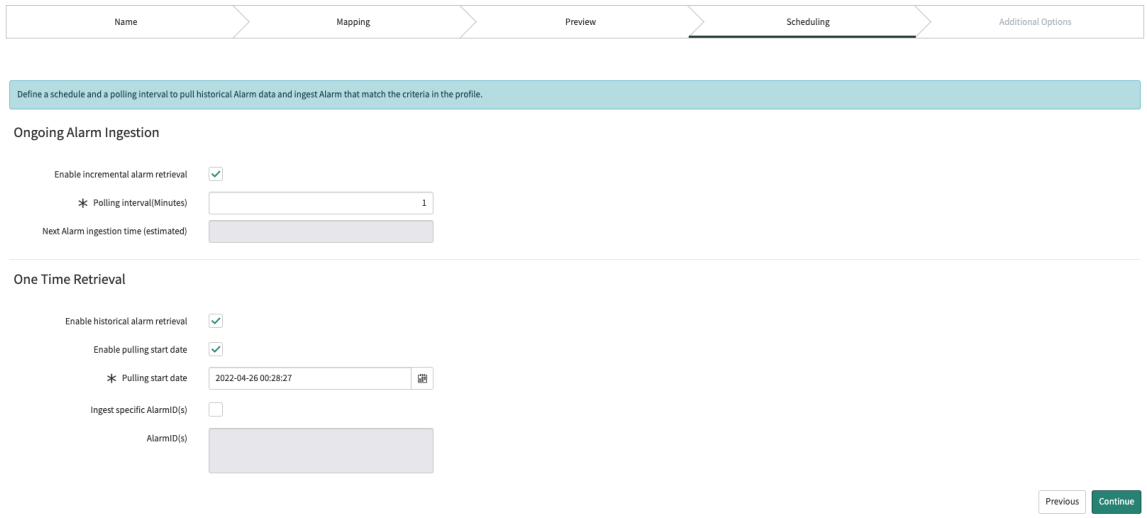
About this task

Scheduling permits you to modify the scheduling and the types of alarms selected for retrieval. You filter the alarms you ingest based on a date range or on specific alarm IDs. With this step, you determine whether you want to ingest historical alarms, and how often you poll for future alarms that match the alarm profile configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Click the **Scheduling** step on the progress bar.



2. Choose from the following options to configure your alarm retrieval.

Option	Description
Enable incremental alarm retrieval	Default is selected. Select this option to re trieve incremental alarms.
Polling interval (in minutes)	The ServiceNow AI Platform instance pulls from the LogRhythm Client Console for new alarms every one minute. If mapped alarms are found, and filtering criteria are matched, security incidents are created. This setting can be changed, however, the de fault setting balances alarm ingestion against server load and retrieves the most current da ta.
Next Alarm ingestion time (estimated)	Displays when the next scheduled ingestion would occur for the current alarm profile. This is only an estimated time.
Enable historical alarm retrieval	Default is cleared. No historical data is pulled. If selected, the following fields are displayed. Choose one to configure retrieval either by date or alarm ID. **Enable pulling start date** Default is cleared. Select this op tion to enable the pulling date. **Pulling start date** Default is cleared. Select this op tion to set the pulling start date. Click the calendar icon to enter a date and time. Alarms are pulled

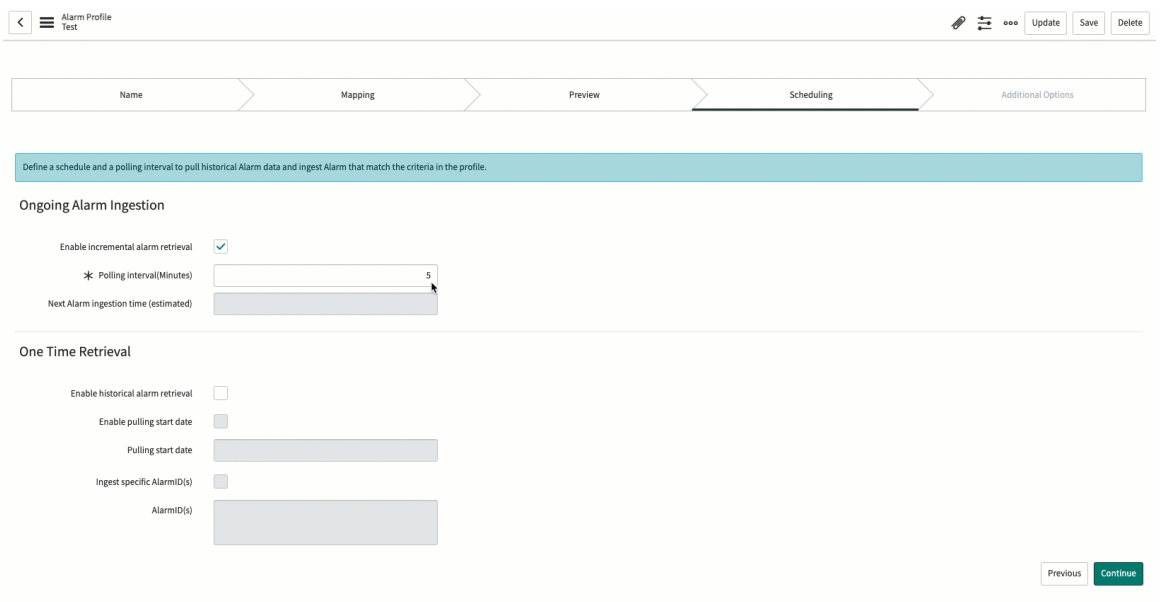
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	from the date and time you enter to the current date. **Ingest specific alarm Alarm ID(s)** Default is cleared. Select this option to ingest specific alarm Alarm IDs. **AlarmID(s)** Enter specific alarm IDs. You pull the specified alarms, and you can enter multiple alarm IDs sep arated by commas. **Note:** After a historical, one-time pull of alarms is completed, this check box is cleared. You will need to select this check box again before you execute an other one-time pull of historical alarms.

3. To edit Historical alarm retrieval, follow these steps to enter a date for alarm retrieval or a specific Alarm ID.

   a. Select **Enable pulling start date**, and then select **Pulling start date**.

   b. In the **Pulling start date** field, click on the calender that is displayed, select the date followed by the green check mark to save your entry.



   The date is displayed.

   c. Alternatively, select **Ingest specific Alarm ID(s)** option, and in the **AlarmID(s)** field, enter the specific Alarm IDs for the historical data to retrieve specific alarm IDs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can enter up to five alarms separated by commas.

d. Click **Update**.

4. Choose one of the following options to continue editing or complete the configuration.

Option	Description
Update	Save your data and remain on the form.
Additional Options (in the progress bar)	To go to the Additional Options step.
Previous	Return to Preview step.
Delete	Delete this alarm profile and the Alarm Profile list is displayed.

What to do next
After you configure the Ongoing Alarm Ingestion and One Time Retrieval details, the next step is to Additional options for LogRhythm alarms.

Additional options for LogRhythm alarms

The LogRhythm Enterprise integration provides you the ability to automatically update or close the LogRhythm alarms based on the security incidents.

Before you begin
Role required: sn_si.analyst

About this task
When you enable the Alarm initial updates option, the alarms are automatically updated in the LogRhythm comments with the initial alarm updates. Similarly, when you enable the Alarm closure updates option, the alarms are automatically closed in LogRhythm along with the SIR Closure Code and and closure comments.

The LogRhythm alarm ID is connected to the ServiceNow AI Platform security incident ID throughout the course of the incident's life cycle. This correlation permits a simultaneous and automated security incident/alarm closure to occur. When the Security Incident Response (SIR) security incident record is closed, there is a comment posted in the alarm on the LogRhythm web console. This comment indicates that the alarm was closed out based on the closure of the ServiceNow AI Platform security incident. The incident number and a URL that links back to the security incident for reference are also included in the comment section in the LogRhythm alarm.

Procedure
1. Click the **Additional Options** step on the progress bar.
2. To use the automated alarm update for SIR Incident creation, choose from the following options to configure your alarm retrieval.

Option	Description
Update LogRhythm alarms upon SIR Incident Creation	Default is cleared. Select this option to automatically update the LogRhythm alarms when the SIR Incident is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Initial comments posted back to Log Rhythm alarm	Indicates the initial comments that are posted for the LogRhythm alarm. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using the format ${field name}$ for any field on the SIR incident form. For example, `The related ServiceNow security incident, ${Number}$ has been created and assigned to ${Assignment group}$. Additional details can be found on the security incident located here - ${URL}$.`

3. To use the automated alarm update for SIR Incident closure, choose from the following options to configure your alarm retrieval.

Option	Description
Close LogRhythm alarms upon SIR Incident Closure	Default is cleared. Select this option to automatically close the LogRhythm alarms when the SIR Incident is closed.
Closure comments posted back to Log Rhythm alarm	Indicates the closure comments that are posted for the LogRhythm alarm. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using the format ${field name}$ for any field on the SIR incident form. For example, `The related ServiceNow security incident, ${Number}$ has been closed by SOC Analyst-${Closed by}$ with the following closure notes - ${Close notes}$. Additional details can be found on the security incident located here - ${URL}$.`

4. Click **Finish** to save the alarm profile.

Trouble?
If you do not see notes indicating the alarm has closed successfully in the security incident, review the work notes for more information about how to proceed to fix the problem. Also, check your server connection. If you confirm the ServiceNow AI Platform security incident has been closed and the server has not timed out, you may have to manually close the alarm on the LogRhythm Web Console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Additional configurations for the LogRhythm integration

Use the LogRhythm Integration Settings to modify the preset system and troubleshooting properties as per you requirements.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **LogRhythm Integration** > **LogRhythm Integration Settings**.
2. Configure the system properties as per your requirements.
3. On the form, fill the fields.

LogRhythm Integration System Properties

Field	Description
This will apply filter before the data is saved into ServiceNow tables.	Option to determine if you want to apply the filter before the data gets stored in the ServiceNow tables. By default, the value is set as Yes.
Max Security Incident can be created in a day	Option to define the maximum number of security incidents that can be created in one day. By default, the value is set as 2000.
LogRhythm periodic ingestion can be 1000+ alarms, hence pagination is used to ingest the alarms. Per page limit allowed to fetch number of alarms per page.	Option to define the maximum number of alarms to be retrieved in a single page. By default, the value is set as 100.
Delete "Source To Task" table records older than specified number of days.	Option to delete Source to Task table records when the specified number of days have been breached. By default, the value is set as 30.

4. Configure the troubleshooting properties as per your requirements.
5. On the form, fill the fields.

LogRhythm Integration Troubleshooting Properties

Field	Description
Debug Scheduled Ingestion: This enables debug level system logs for ingestion done by scheduled job. This will log all the messages/exceptions generated by Scheduled ingestion while pulling Alarms/ Drilldownlogs/Events from LogRhythm.	Option to enable debug level system logs for ingestion performed by the scheduled job. By default, the value is set as No.
Debug Transform Map: This enables debug level system logs for Transform Map. This will	Option to enable debug level system logs for the Transform Map.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
log all the messages generated by transform maps while creating security incident from Alarm Import. This also enabled UI action on Alarm Import table to rerun transform map.	By default, the value is set as No.
Debug Sample Ingestion In Alarm Profile: This enables debug level system logs for Sample Ingestion. This will log all the messages generated while samples are ingested.	Option to enable debug level system logs for Sample Ingestion. By default, the value is set as No.
Debug Preview In Alarm Profile: This enables debug level system logs for Alarm Profile Preview. This will log all the messages generated while preview is rendered for Sample Alarm.	Option to enable debug level system logs for Alarm Profile Preview. By default, the value is set as No.
Debug Outbound REST calls: Enabling this property will allow debug level logging in System Logs table for all REST calls (request and response) going with or without mid server from LogRhythm.	Option to enable debug level logging in System Logs table for all REST calls going with or without MID server from LogRhythm. By default, the value is set as No.

6. Click **Save**.

Use the script editor to format LogRhythm values

In addition to the directly mapped fields from the pulled alarm values, and the alarm values you enter manually, you can use the script editor to format field values on the security incident during the mapping step which is optional.

Before you begin

Role required: sn_si.admin

The script editor changes the values of a LogRhythm alarm so the values that are mapped to the `Priority` and `Category` fields on the security incident are supported.

About this task

In certain cases, if LogRhythm alarm values are mapped to the `Priority` and `Category` fields on the security incident, you may want to edit the mapped values. If you want to translate the value of a LogRhythm alarm to a value that is supported by the `Priority` or `Category` fields on the security incident, use the script editor.

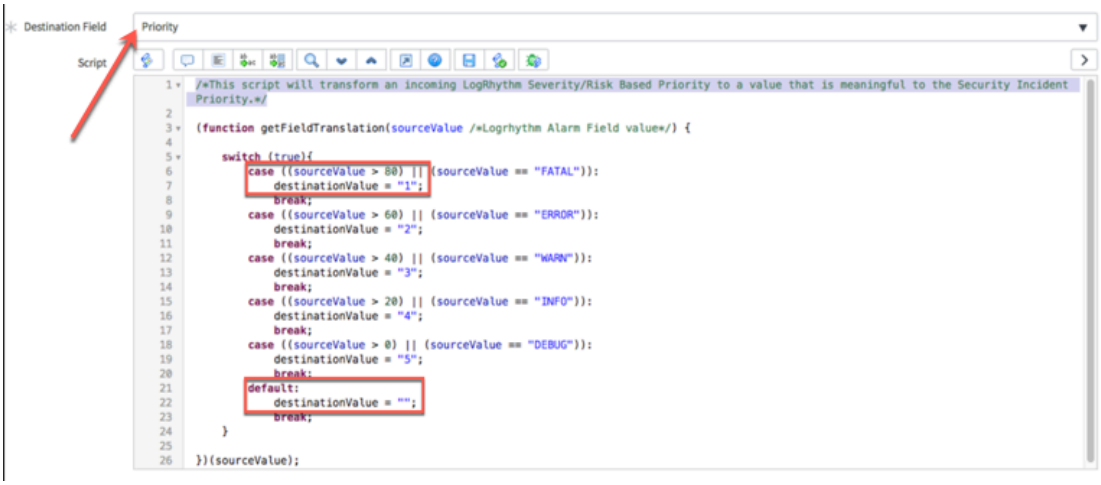
Procedure

1. With the mapping form displayed, in the SIR Incident Field Mapping section, click the bracket icon [{ }] to open the script editor.

   The default values are included for the `Priority` and `Category` fields on the security incident. You can edit these values.

   For this example, in the open editor, verify that **Priority** is displayed in the **Destination Field** choice list, as shown in the following figure. Note that this field is the security incident priority, not the LogRhythm risk-based priority.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

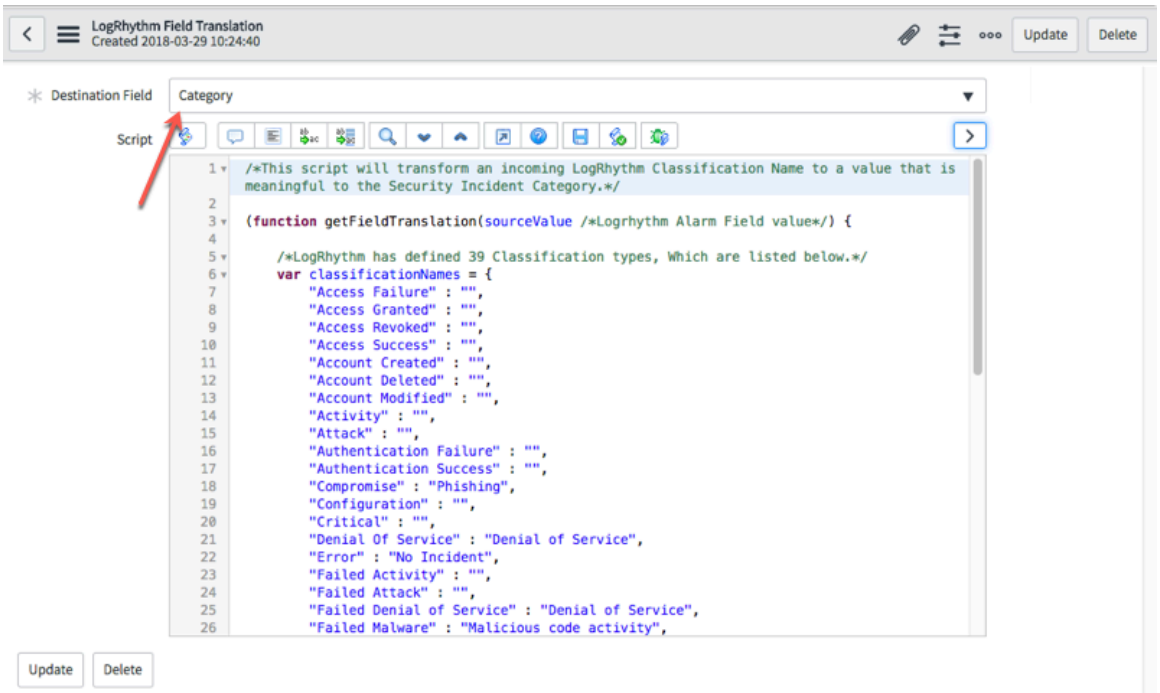


In certain instances, a script include may be appropriate for the `Priority` field. For a LogRhythm alarm, for example, a risk-based priority score is assigned a value between 0-100. However, in the ServiceNow AI Platform, the priority field on a security incident supports values between 1-5. As illustrated in the preceding figure, a script include translates the LogRhythm alarm field values to the appropriate values supported by the field on the security incident in the ServiceNow AI Platform.

In this example for the `Priority` field, if the LogRhythm alarm value is 80 or greater, 1 is displayed in the security incident field (`Priority`). This value translates to a `Critical` priority in the security incident. If there is no value for the alarm, the field on the security incident is set to null.

2. Enter any changes, and click **Update** to save your changes.
   The LogRhythm Field Translations table is displayed.
3. Close the table to return to the Mapping form.

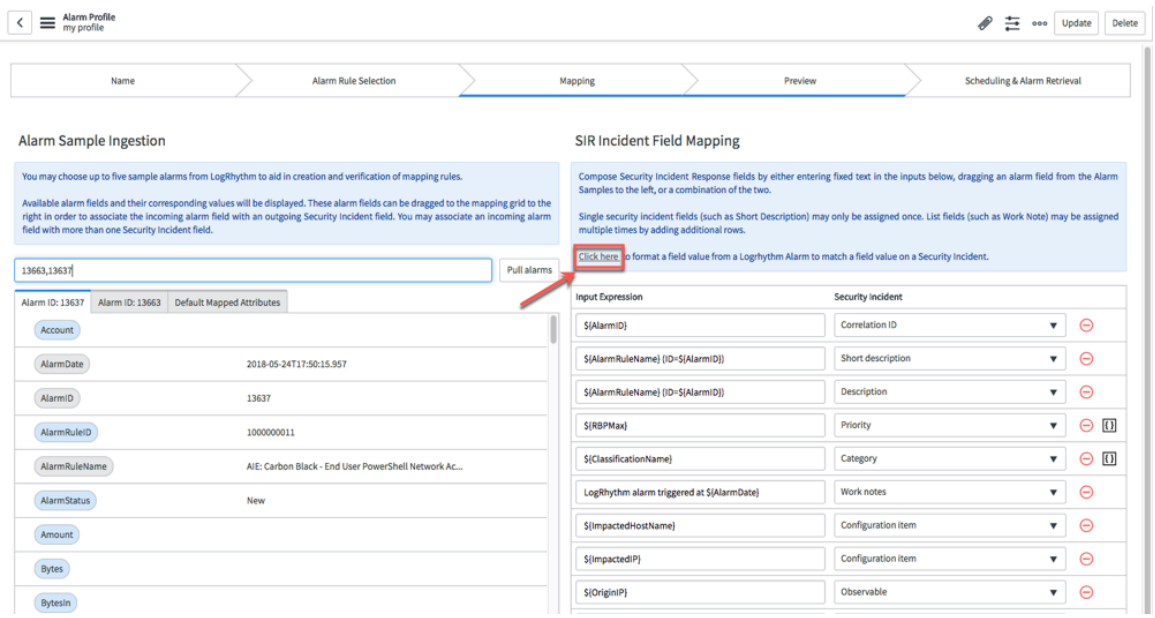
   The following figure shows the script editor with `Category` selected in the Destination Field choice list.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

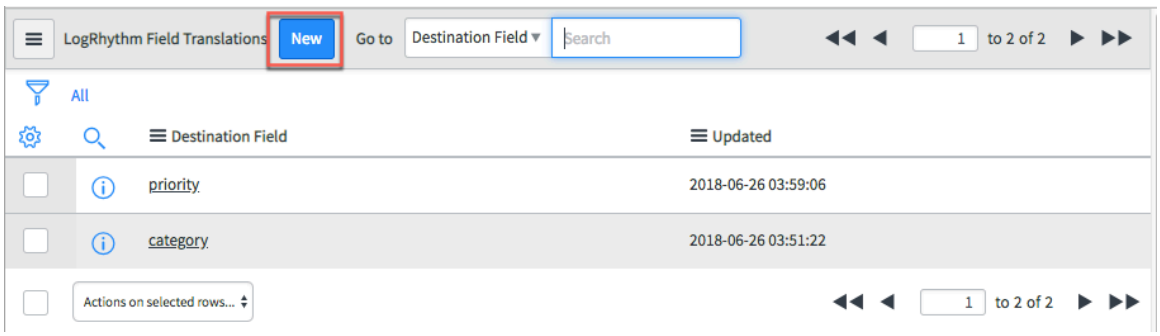
4. If you want to add a new field to the Field Translations list, follow these steps to add a new record.

   a. With the mapping form displayed, in the SIR Incident Field Mapping section, click the **Click here** link.



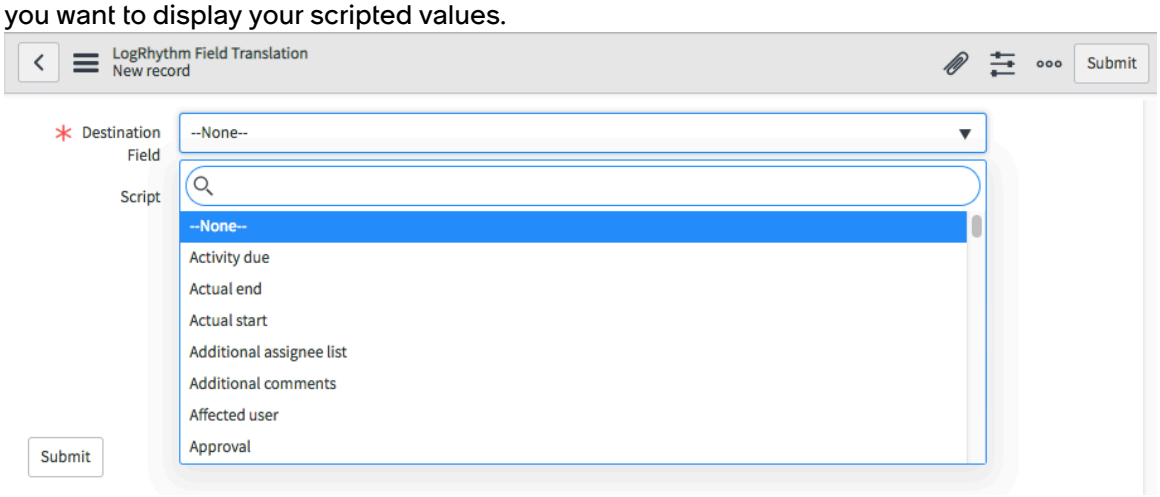
   The LogRhythm Field Translation list with the `priority` and `category` destination fields are displayed.

   b. Click New.



   A new record is displayed.

   c. From the Destination Field choice list, select a destination field on the security incident that you want to display your scripted values.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Click **Submit**.
The script editor is displayed.

e. Enter any changes into the editor, and click **Submit** to save your changes.
The LogRhythm Field Translations table with your new record is displayed.

5. Close the table to return to the Mapping form.

Copy an alarm profile for LogRhythm

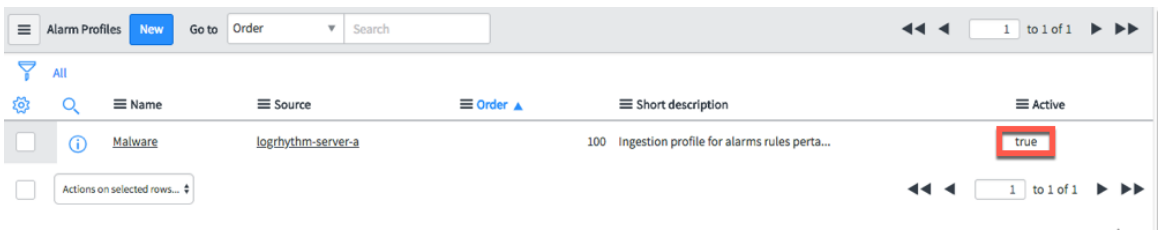
Copy an existing profile and its associated settings instead of creating a new alarm profile. If you are creating multiple alarm profiles for different types of alarms and you want to reuse the settings of an existing profile, you can copy alarm profiles to save time. This process is optional.

Before you begin
Role required: sn_si.admin

About this task
If you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is set to inactive so it is not activated accidentally prior to completing the configuration.

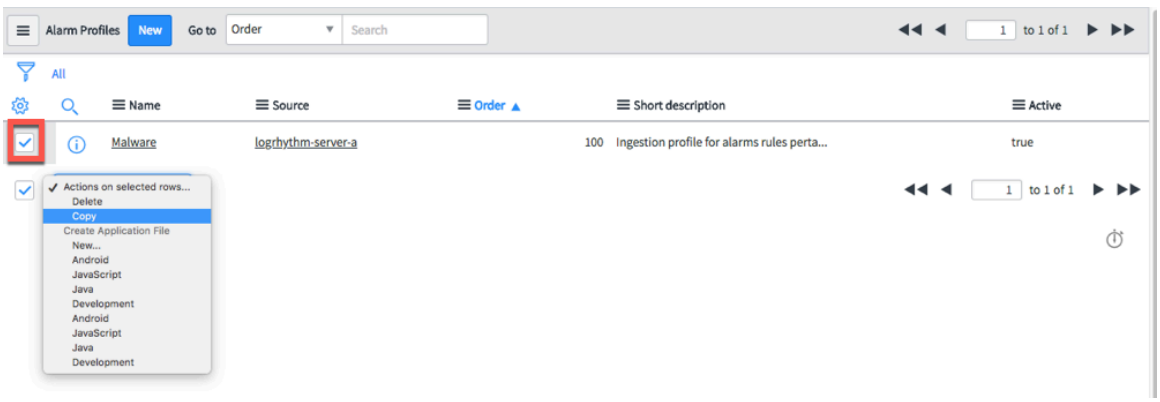
Procedure
1. Navigate to **All** > **LogRhythm Integration** > **LogRhythm Alarm Profiles**.

In the list that is displayed, note the `Active` column indicates if the profile is active (`true`).



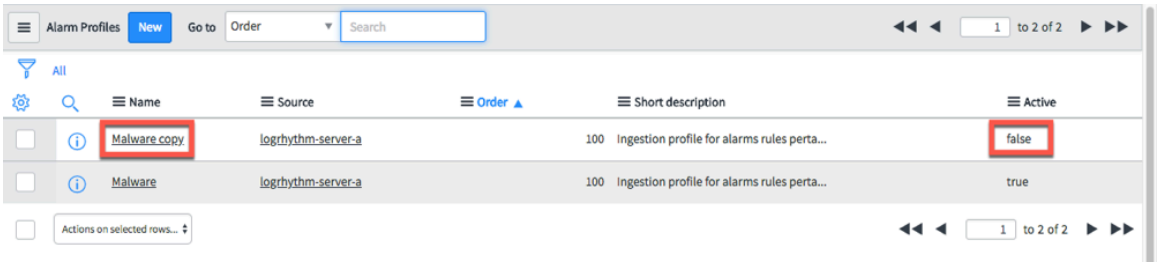
2. In the field to the left of the **Name** column, select the name of the record.

3. From the **Actions on selected rows** choice list, select **Copy**.



In the **Alarm Profiles** list, both the copy and the original profile are displayed. Although the original record is active, the copy is inactive at this point (`false`). After you have configured it, you activate this copied profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can edit values of the copied profile and rename it so alarm rules you pull apply to the new profile. You are prompted to activate the new profile once the configuration steps are completed.

Disable automated alarm closure for LogRhythm

Disable the automated alarm closure capability if you no longer want to view the security incident closure information on the LogRhythm Web Console. Once deactivated, the ServiceNow AI Platform no longer closes alarms within the LogRhythm Web Console. This process is optional.

Before you begin

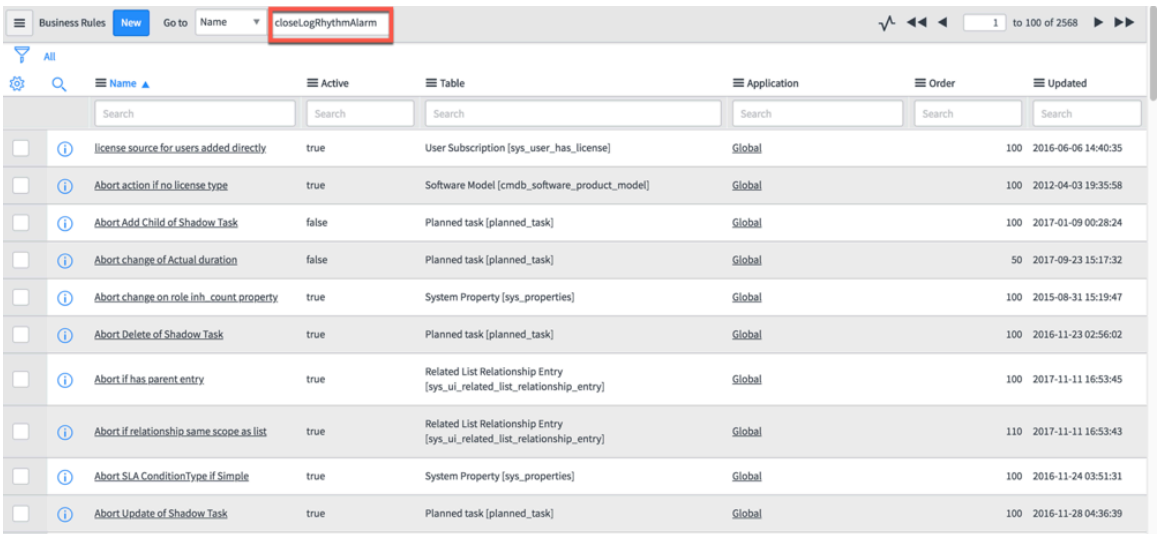
Role required: sn_si.admin

About this task

Once disabled, the status notes and other closure information on the security incident are no longer displayed on the LogRhythm Web Console.

Procedure

1. Navigate to **All** > **System definition** > **Business Rules** and select the **Business Rules** module.
2. If not displayed in the **Business Rules** list, enter **LogRhythm Close Alarm On SI Closure** in the search field and press **Enter**.



3. In the **Name** column, click the **LogRhythm Close Alarm On SI Closure** link to open the record.
4. In the record that is displayed, clear the **Active** check box.
5. Click **Update**.
   The automated alarm closure capability is now disabled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View LogRhythm drilldown events

View the related raw or base events for a LogRhythm alarm in the security incident.

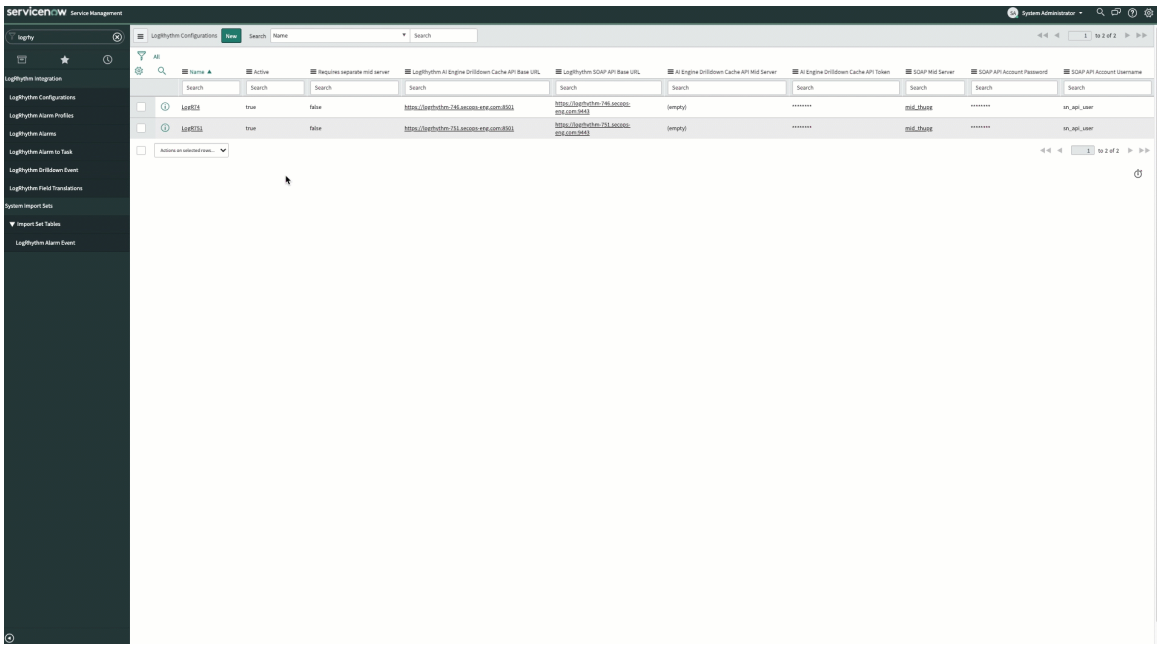
Before you begin
Role required: sn_si.admin

About this task
As a security analyst you can view the related raw or base events for a LogRhythm alarm without having to go back to the LogRhythm console. You can do this by going to a related list that contains all the drill-down events on the SIR incident.

Procedure

Navigate to **All** > **LogRhythm Integration** > **LogRhythm Drilldown Events**.

The following illustration shows how to navigate to the **LogRhythm Drilldown Events** module, sort the list of events by **Group By Alarm ID**, and click the associated security incident. In the security incident, you can find the **LogRhythm Drilldown Events** tab in the related links.



Troubleshooting the LogRhythm integration

Troubleshoot connectivity and alarm ingestion issues.

Refer to the following topics for troubleshooting:

- Verify connectivity for LogRhythm
- Script execution and system log for LogRhythm

Verify connectivity for LogRhythm

Verify your connection to the LogRhythm Client Console by sending curl requests to test the LogRhythm REST API. The verification process is optional.

Before you begin
Role required: sn_si.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

To verify the connection to the LogRhythm Client Console is working properly after you set up the LogRhythm REST APIs, send two curl requests from the computer hosting the MID Server you configured in Install the plugin and configure LogRhythm.

The LogRhythm REST API uses WSSE for authentication, which requires some outside scripting to work with Curl and Postman.

The LogRhythm REST API uses a token for authentication, so you can make the actual validation call that the integration uses. The "0" at the end of the URL is a LogRhythm Alarm ID. The LogRhythm REST API with a default configuration requires port 8501. This port number should be included in the URL that you plan to use for the test.

Procedure

Update the URL **<LogRhythm REST url>** and token **<api token>** in the following curl request and send it to validate the LogRhythm REST API: `curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Authorization: Bearer <api token>" "https://<cache drilldown url>/lr-drilldown-cache-api/drilldown/0"`
For a successful connection to the LogRhythm REST API, you should receive an HTTP 404, but the response body contains `Alarm ID: 0 not found`.

Script execution and system log for LogRhythm

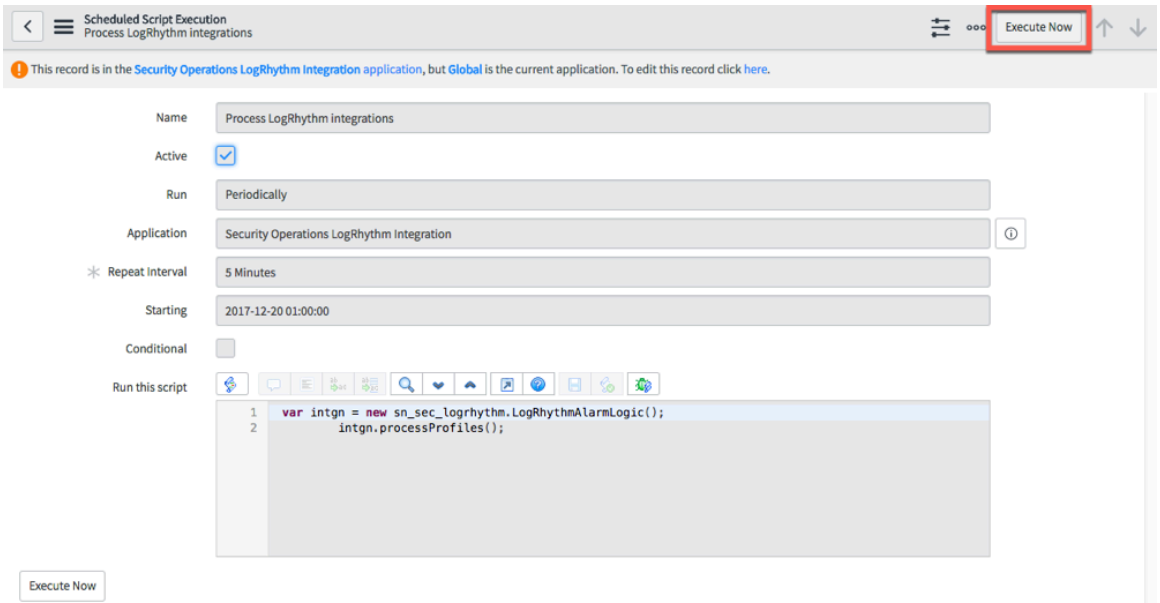
If you are troubleshooting an alarm ingestion issue, you can override the default five-minute polling interval to view results immediately. In this scenario, call the script execution manually to execute polling. This execution is optional.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Scheduled job** > **Scheduled Jobs** and select the **Scheduled Jobs** module.
2. Click the Process LogRhythm integrations job record.
3. In the Scheduled Script Execution record that is displayed, click **Execute Now**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you require more troubleshooting help, you can access the system log for the LogRhythm queries.

4. For other general troubleshooting issues, follow these steps to access the system logs.

   a. Navigate to **System log** > **All** and select **All**.

   b. Set the filter (`Go to`) to **Source** and enter `sn_sec_logrhythm`.

   c. Press **Enter**.
   Any messages generated by the integration are displayed in this table. The messages listed can provide insight into the running processes of the integration, and they may assist you with further troubleshooting.

McAfee ePO integration

The McAfee ePO integration endpoint detection and response (EDR) capability that helps Security Operations Center (SOC) analysts identify cyberthreats and repair the damage caused by malicious files.

Overview

There are two sets of McAfee ePO capabilities used in this integration, the capabilities that invoke actions, such as isolating a host and initiating a malware scan, and the capabilities that run queries to gather system details and threat events. Both types of capabilities, the actions and the queries, are invoked from your ServiceNow AI Platform® instance. You can group these capabilities together so that they automatically run when a specific type of security event occurs, or, you can invoke them manually from a ServiceNow AI Platform® security incident.

The following McAfee ePO capabilities are available for this integration.

Get system details

Gather system details that include operating system details.

Initiate malware scan

Based on scan configuration and scheduling, initiate a scan of an impacted endpoint.

Isolate/Unisolate host

Remove a system from network access for investigation and restore access to the network.

List threat events

Gather compliance status and the most current threat events.

Key features

This integration includes the following key features.

- Supports automated triggering of McAfee ePO queries that are based on incident conditions.
- Supports launching McAfee ePO capabilities manually from ServiceNow AI Platform® Security Incident Response (SIR) security incidents that perform on-demand actions.
- The flexibility to create multiple profiles for triggering different types of McAfee ePO and ServiceNow AI Platform® Security Operations capabilities. These profiles gather threat event information or perform actions based on the conditions of specific incident categories such as malware.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Validate your profile configuration with a preview of the McAfee ePO results on SIR security incidents.
- If tagging is enabled, security tags identify which McAfee ePO capabilities are initially launched by a workflow and when the queries or actions are successfully completed.
- A complete audit trail of the McAfee ePO queries and actions is posted in the work notes on SIR security incidents, and commands from the ServiceNow AI Platform® are logged in the McAfee ePO console.
- Supports multiple McAfee ePO consoles.

ServiceNow Plugins

The com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response
5. Security Incident Response Workspace

For more information on setting up your ServiceNow AI Platform instance for the integration, see Set up your ServiceNow AI Platform instance for the McAfee ePO integration.

The ServiceNow extension plugin

The ServiceNow Security Operations Extension for McAfee ePO# extension plugin is required for this integration. You install this ServiceNow plugin in your McAfee ePO console. For more information, see Set up your ServiceNow AI Platform instance for the McAfee ePO integration.

MID Server

This integration requires an installed and configured MID Server in your ServiceNow AI Platform® instance to connect to the McAfee ePO server (console). See the ServiceNow Product Documentation website for more information about MID Servers.

Supported versions of McAfee

The integration supports version 5.9.1 & 5.10 of McAfee ePO. It supports McAfee Agent: MA 5.5.1.388 For more information about McAfee products and the ePolicy Orchestrator, see the McAfee product website.

The integration supports the version 10.5 of the McAfee Endpoint Security Threat Prevention product. If you are not running version 10.5, consult with your McAfee ePO administrator to see if your version can support on-demand scans via tag actions.

McAfee ePO security tags are used in this integration. You are required to create these tags in your McAfee ePO console. For more information on these tags, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

References

Reference	Document Identifier	Document Title
1	McAfee product website	McAfee product website
2	McAfee Business Product Documentation for ePolicy Orchestrator Cloud	McAfee Product Documentation
3	ServiceNow Product documentation website	ServiceNow Product Documentation website

For a checklist to track your progress with setting up, installing, and verifying results for the integration, see Checklist for the McAfee ePO integration.

For a smooth installation of the application and to help you verify expected results, follow the topics in the order they are presented.

Related topics

Integration architecture for McAfee ePO

Integration architecture for McAfee ePO

The following topic is an overview of the system architecture and lists key features of the integration. This section also provides information about the setup steps that you are required to complete in your ServiceNow AI Platform instance and in the McAfee ePolicy Orchestrator (McAfee ePO) console prior to installing the application from the ServiceNow Store.

Key terms for the McAfee ePO integration

The following terms are used throughout the installation and configuration documentation for the integration.

ServiceNow AI Platform

An enterprise ServiceNow product. The ServiceNow AI Platform is the base upon which individual components, such as Security Incident Response (SIR), IT Service Management, (ITSM), and other products are built.

Security Incident Response (SIR)

A ServiceNow AI Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

Plugin

Plugins are software components that provide specific features and functionalities within your ServiceNow AI Platform instance. For more information on the installation and configuration of the integration plugins, see Install the application and configure a server for the McAfee ePO integration.

ePolicy Orchestrator (McAfee ePO)

The user console where you manage the McAfee services, products and settings.

McAfee extension plugin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This ServiceNow extension plugin is required for this integration. This plugin resides on your McAfee ePO console and connects your McAfee ePO console to your ServiceNow AI Platform instance.

Capability

An automatic activity initiated from your ServiceNow AI Platform instance that is run in the McAfee ePO console to conduct enrichment queries and perform actions on your assets.

Profile

Settings for McAfee ePO capabilities that you configure to specify when and under what conditions capabilities conduct enrichment queries and perform actions on your assets.

MID server

An application that facilitates communication and the movement of data between the ServiceNow AI Platform and external applications, data sources, and services.

ServiceNow administrator (admin)

A user with this role downloads and installs the SIR and McAfee ePO plugins to your ServiceNow AI Platform instance. A user with this role also assigns the security incident administrator role as required.

ServiceNow Security incident administrator (sn_si.admin)

A user with this role performs the configuration of the McAfee ePO integration with the Security Incident Response (SIR) product in your ServiceNow AI Platform instance as required. A user with this role also assigns the security incident analyst role as required.

ServiceNow security incident analyst (sn_si.analyst)

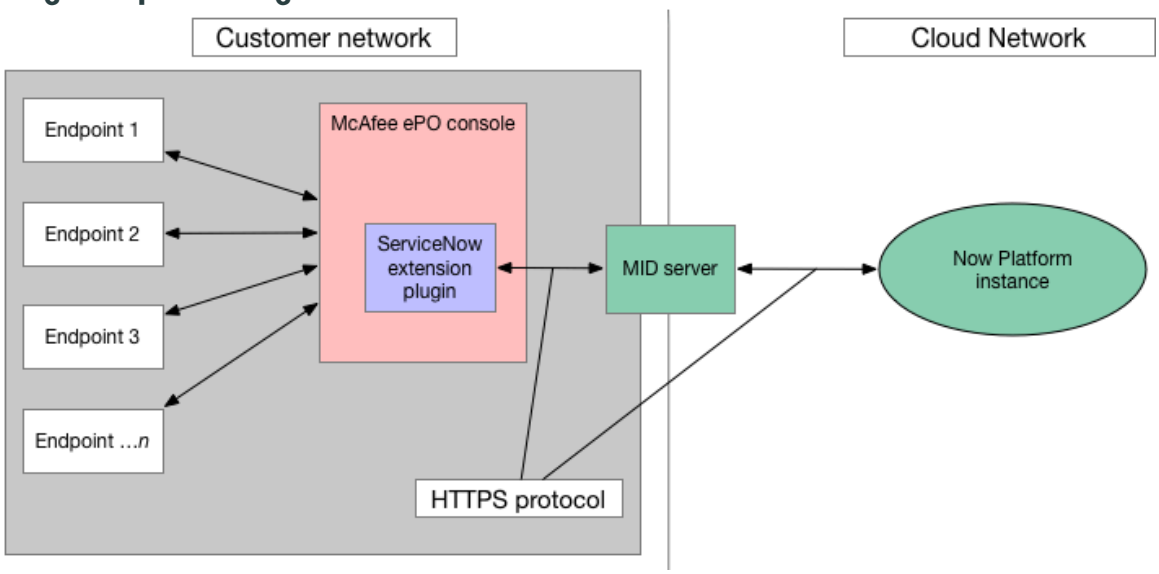
A user with this role interacts with and analyzes security incidents in the SIR product.

System connection and data flow

The following figure is an example of a customer environment. A ServiceNow AI Platform MID server is required so that your ServiceNow AI Platform instance can connect to a McAfee ePO server (console) via a ServiceNow extension plugin. After you are connected, you invoke capabilities from your ServiceNow AI Platform to initiate malware scans, isolate host machines and restore them to your network, retrieve last scan results, and gather system details on your assets. When these capabilities return results from your assets that match your search criteria, data is pulled via the MID server into your ServiceNow AI Platform instance. Data is displayed on the related lists of a ServiceNow AI Platform Security Incident Response (SIR) security incident. The following figure illustrates the data flow for one group of endpoints managed by one McAfee ePO console.

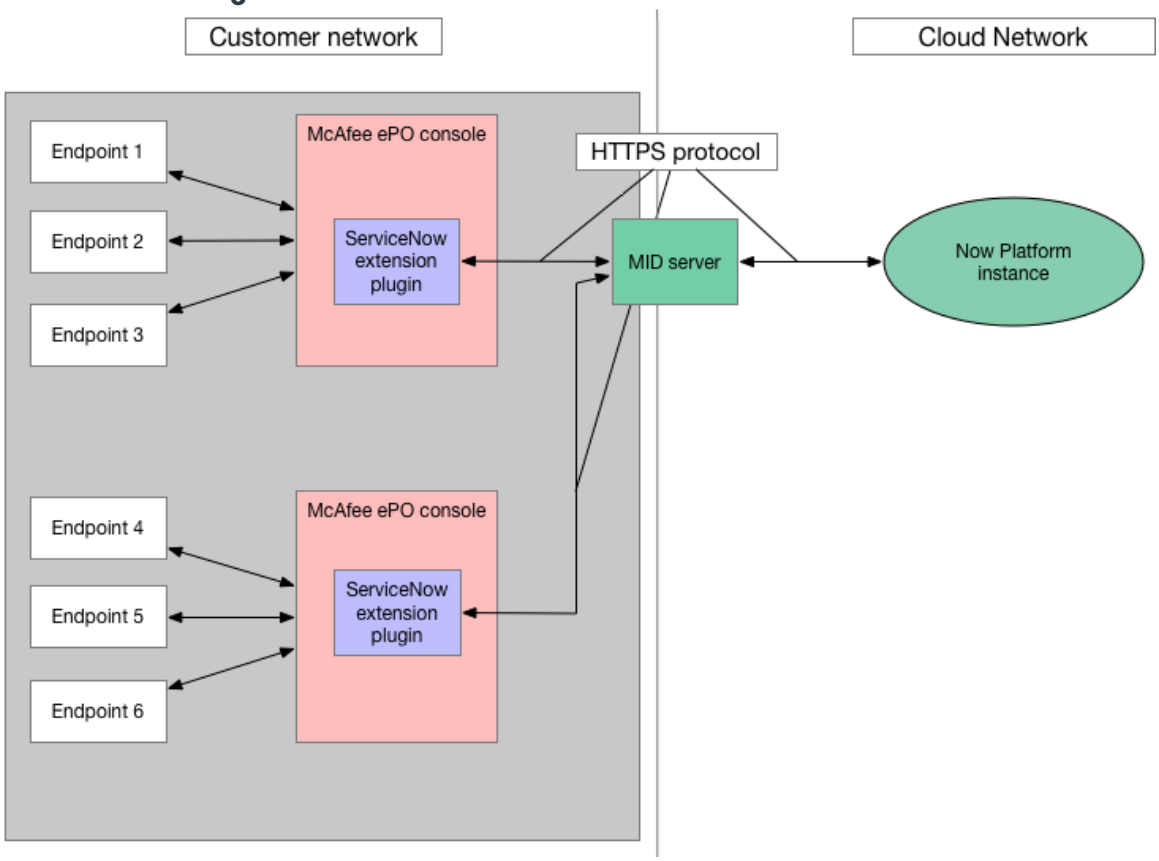
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Single endpoint configuration



As shown in the following figure, this integration can support more than one McAfee ePO console. You can have one group of endpoints managed by one McAfee ePO console, and another group of endpoints managed by another McAfee ePO console. Data from multiple McAfee ePO consoles is pulled via a single MID server. However, you also may prefer to configure multiple MID servers if required by your organization.

MID servers configuration



Workflows for the McAfee ePO integration

This integration includes the following workflows. These workflows are pre-configured and are designed specifically for this integration. You can edit these workflows to meet the needs of your

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

organization as required. For more general information about workflows and using the workflow editor, see Getting started with workflows.

- Security Operations McAfee EPO integration - Get Host Details
- Security Operations McAfee EPO integration - Initiate Malware Scan
- Security Operations McAfee EPO integration - Isolate Host
- Security Operations McAfee EPO integration - List Threat Events
- Security Operations McAfee EPO integration - Remove Isolation

External systems connection

The integration requires that the MID server communicates via HTTPS protocol connection to the McAfee ePO console.

Checklist for the McAfee ePO integration

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

Before you begin

Role required: Roles are listed for each step.

About this task

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.

Procedure

Follow the steps in the table in the order that they are presented.

Checklist

Item	Description
☐	As a user with the ServiceNow AI Platform® administrator role, set up your ServiceNow AI Platform® instance. **a.** Assign ServiceNow AI Platform® and Security Incident Response roles. **b.** Verify that any ServiceNow Security Incident Response and other plugins that support the integration are installed and activated for your release of the ServiceNow AI Platform. **c.** Install and configure a MID server in your ServiceNow AI Platform® instance. **d.** Create an approval group if you want to process requests submitted from the security incident analyst for the isolate host and initiate malware scan actions. For more information, see Set up your ServiceNow AI Platform instance for the McAfee ePO integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
☐	As McAfee ePO administrator, set up your McAfee ePO console. **a.** Verify that you are using version 5.9 of McAfee ePO. **b.** Install the ServiceNow extension plugin in your McAfee ePO console. **c.** Verify you have created security tags in your McAfee ePO console for the isolate host and initiate malware scan actions. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR). For more information and to obtain the extension plugin file, in your ServiceNow AI Platform instance, navigate to **Knowledge** > **Articles** > **All** and, in the Search field, enter, `ServiceNow Security Operations Extension for McAfee ePO`.
☐	As a user with the ServiceNow AI Platform administrator role, install the McAfee ePO application from the ServiceNow Store, configure a server, and connect to the McAfee ePO console. For more information, see Install the application and configure a server for the McAfee ePO integration.
☐	As a user with the ServiceNow AI Platform security incident administrator role, edit the security tag names in your ServiceNow AI Platform® instance so that they match the tag names that you created in your McAfee ePO console. For more information, see Edit security tags in the ServiceNow AI Platform for the McAfee ePO integration.
☐	As a user with the security incident administrator role, create a profile for McAfee ePO capabilities. For information about profiles, see McAfee ePO integration capability profiles. For the steps required to create a profile, see Create a capability profile for the McAfee ePO integration.
☐	As a user with the security incident administrator role, configure a profile and test security incidents. **a.** Review the information about triggering conditions and settings. **b.** Configure a profile. **c.** Test and preview security incidents. **d.** Locate search results and other details on the related lists on the security incident. **e.** Create and Configure different types of profiles and test security incidents for each type. For information about triggering conditions and the alternate CI field, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile. For the steps required to configure a profile, test, and preview security incidents and examples of profile types, see the examples that follow Configuring profiles for the McAfee ePO integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Item	Description
☐	As a user with the ServiceNow AI Platform security incident analyst role, submit additional requests for Malware scans and List threat events. For more information, see Trigger McAfee ePO profile manually from a security incident In the ServiceNow AI Platform, as a user with an approval role, or, as a member of an approval group, approve requests for isolate host isolation and remove isolation. For more information on processing approval requests, see Create an approval group.

You have successfully completed the set up steps, installed and configured the application, and verified expected results for the integration.

Set up your ServiceNow AI Platform® instance for the McAfee ePO integration

The following section lists the setup tasks that you're required to complete in your ServiceNow AI Platform® instance prior to installing the application for the McAfee ePO integration.

Set up requirements

Role required: ServiceNow AI Platform administrator (admin). Review the following information before your ServiceNow AI Platform® instance for the McAfee ePO integration.

The following table is a list of setup requirements for the application. Verify that you've completed these tasks before you install the application for the integration from the ServiceNow Store.

Set up task	Description
Verify that you've assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.	The following roles are required: • A user with the system administrator (admin) role to install the application. • A user with the security incident administrator (sn_si.admin) role configures the application, and creates, activates, and removes profiles. • A user with the security incident analyst (sn_si.analyst) role works with security incidents. Tasks include manually launching profiles from security incidents. If the approval option is selected in a profile during the configuration step, users with this role also submit requests for isolating hosts and returning them to the network.
Verify that you are using version 5.9 of McAfee ePO.	The integration supports version 10.4.3 of the McAfee ePolicy Orchestrator.
Verify that you have installed the ServiceNow extension plugin in your McAfee ePO console.	Install the ServiceNow plugin in your McAfee ePO console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up task	Description
	For more information and to obtain the plugin file, in your ServiceNow AI Platform instance, navigate to **Knowledge** > **Articles** > **All** and, in the Search field, enter, ServiceNow Security Operations Extension for McAfee ePO .
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Incident Response Workspace **3.** Security Integration Framework **4.** Security Support Common **5.** Security Support Orchestration For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.
Verify that you have installed and configured a MID Server.	An installed and configured MID Server is required in your ServiceNow AI Platform® instance. See the ServiceNow Product Documentation website for more information about MID Servers.
If you want to enable the approval process for profiles, verify that you have created an approval group to process requests.	There is an optional approval process available for isolating host machines and restoring them to the network. If this option is enabled, prior approval is required before host machines are isolated and restored to your network. If your organization wants an extra level of control over these actions, enable the **Require approval** option during the configuration step for a profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up task	Description
	By default, approval authority is assigned to the ServiceNow AI Platform® security incident administrator (sn_si.admin). This authority can be reassigned to an approval group. Within the group, any member has permission to approve or reject requests. You select an active approval group during the configuration step of your profile setup. For more information, see Create an approval group.

Set up your McAfee ePO console to integrate with Security Incident Response (SIR)

The following section lists the setup steps that you are required to complete in your McAfee ePO console prior to installing the application from the ServiceNow Store for the integration.

Before you begin

Role required: McAfee ePO administrator

As a user with the McAfee ePO administrator permission, verify that you have installed the `Servicenow.zip` extension plugin in your McAfee ePO console. This extension plugin is required for the integration. For more information and to obtain the plugin, in your ServiceNow AI Platform instance, navigate to **Knowledge** > **Articles** > **All**. In the Search field, enter, ServiceNow Security Operations Extension for McAfee ePO.

About this task

The ServiceNow extension plugin connects your ServiceNow AI Platform instance to your McAfee ePO console. This connection allows you to reference the security tags you that create in your McAfee ePO console for the isolate host and initiate malware scan actions to the capability profiles in your ServiceNow AI Platform instance.

The security tags in your McAfee ePO console must match the security tags in the capability records in your ServiceNow AI Platform instance.

The following steps show you how to install the extension plugin, create a security tag in your McAfee ePO console, and assign an action to the tag. For more information about the security tags in the McAfee ePO console, see the McAfee Product Documentation website.

Note: The figures in the following section are from the McAfee ePO console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. If you have not installed the ServiceNow extension plugin on your McAfee ePO console, follow these steps to install it.

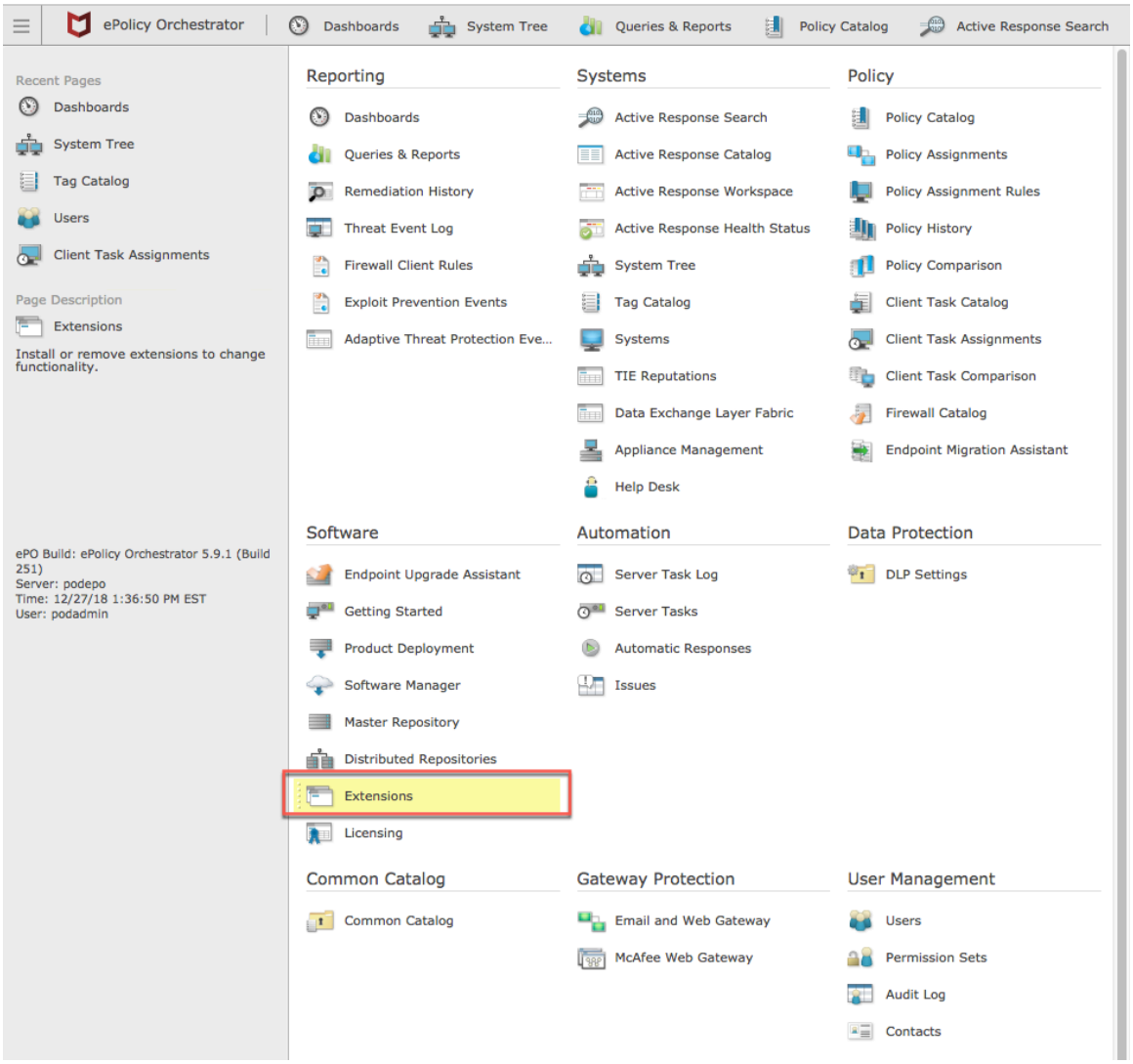
   a. Log in to your McAfee ePO console with your McAfee user name and password.



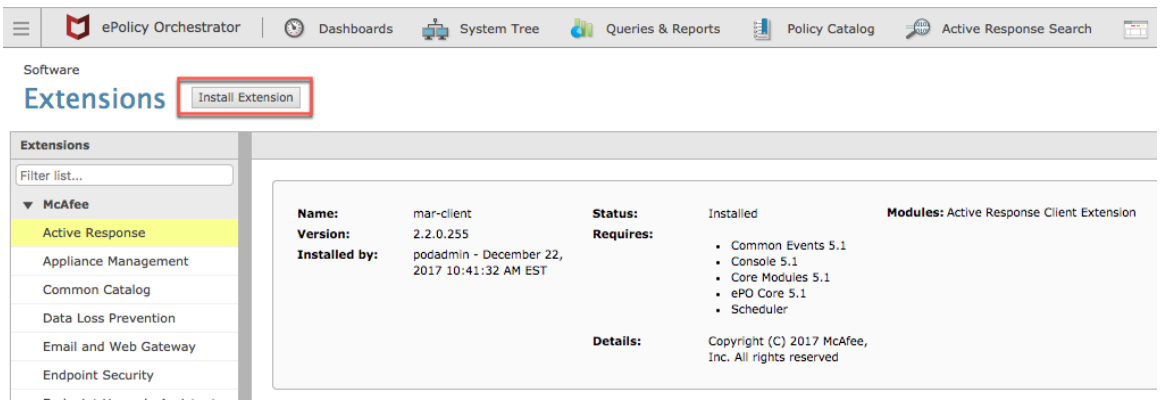
2. If the page shown in the following figure is not displayed, in the top left of banner of the home page, click the menu icon to display it.

3. In the Software section, click the **Extensions** link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

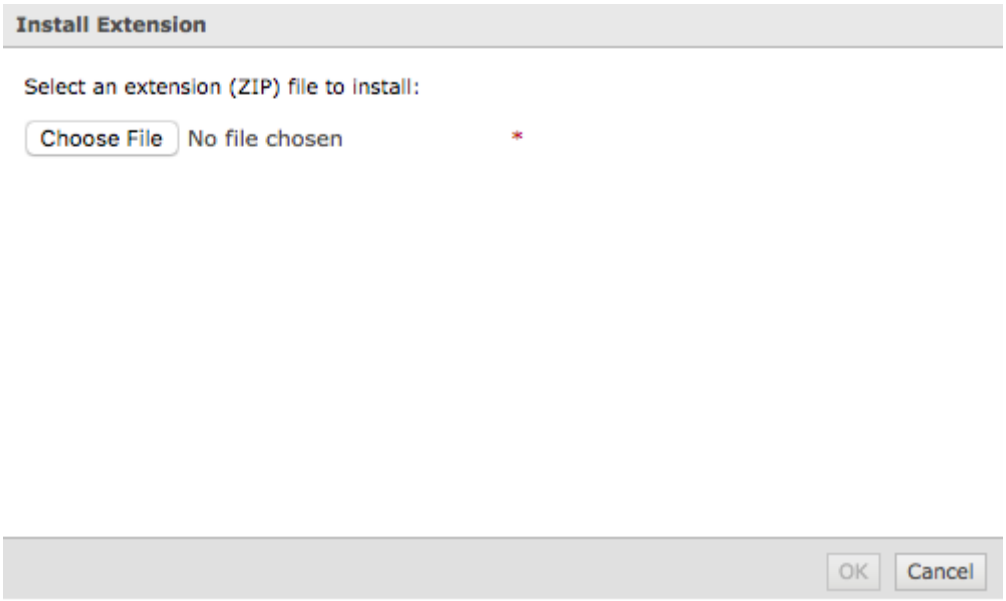


4. On the Extensions page that is displayed, click **Install Extension**.

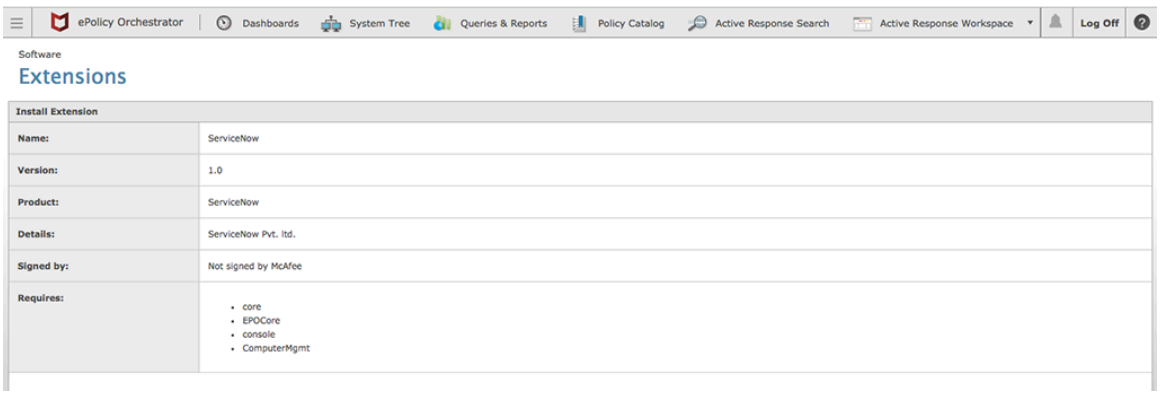


5. In the Install Extension dialog, click **Choose File**, navigate to the `Servicenow.zip` file on your system, and click **OK** to download it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



After the download is completed, the Software Extensions page is displayed with the ServiceNow Extension plugin listed.

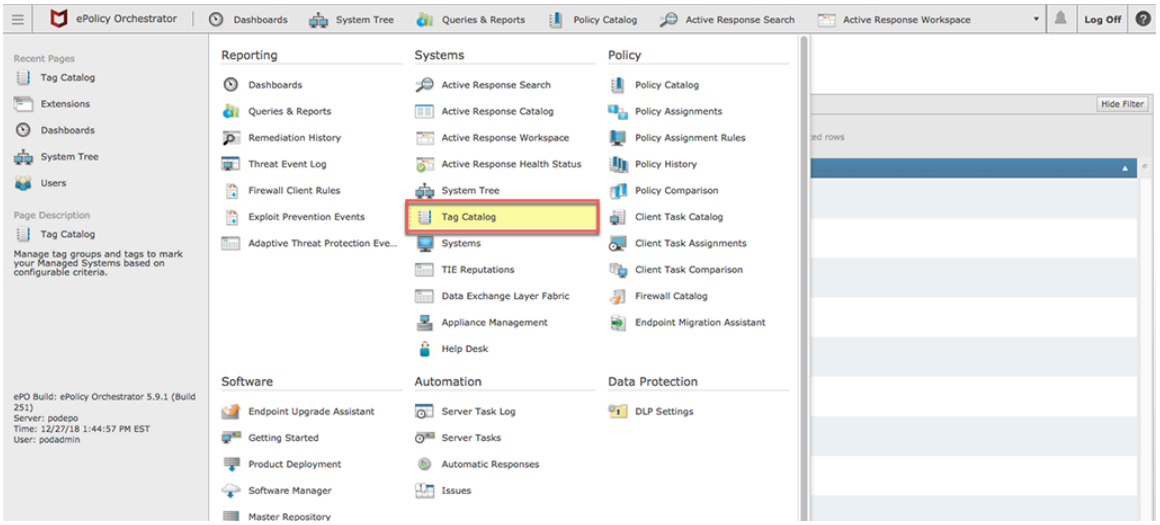


You have successfully installed the ServiceNow plugin Extension on your McAfee ePO console.

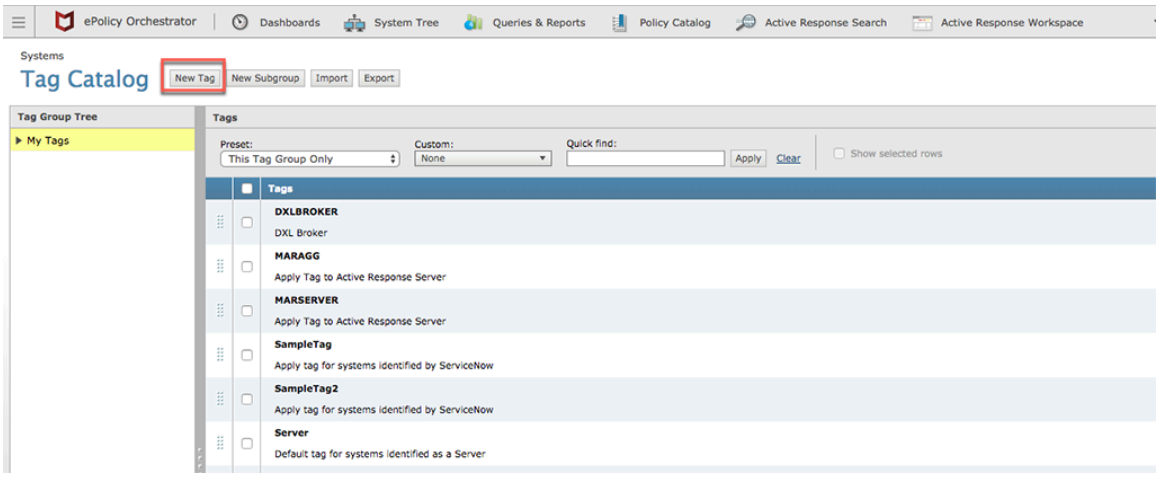
6. If you have not created security tags in McAfee ePO console for the initiate malware scan and isolate host actions, follow these steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to the home page and click the **Tag Catalog** link.

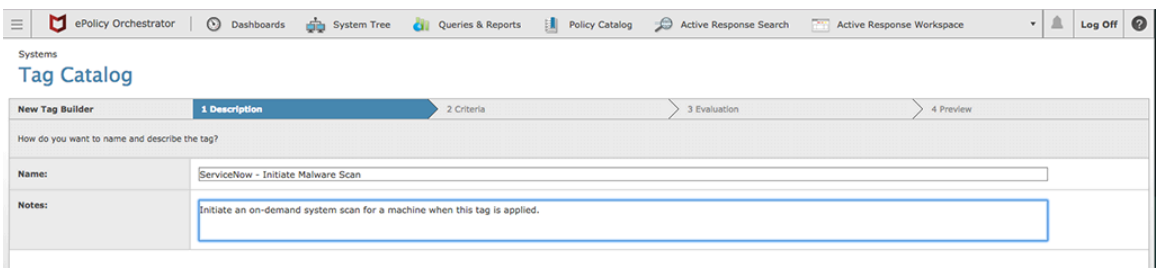


b. On the Tag Catalog page that is displayed, click **New Tag**.



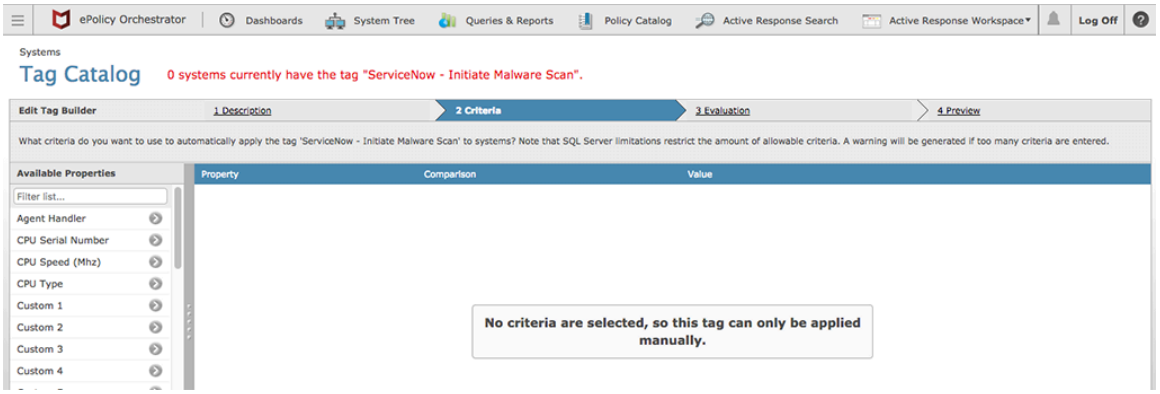
c. With the Description step selected in the progress bar that is displayed, enter a name and description for the tag.

For this example, a tag with a name and description for the Initiate Malware Scan capability is displayed. This tag name is what is matched and referenced in your ServiceNow AI Platform instance.

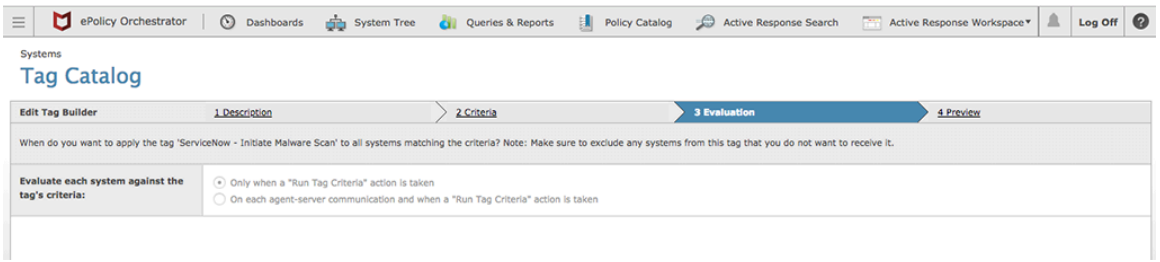


d. To advance to the Criteria step, click **Criteria** in the progress bar.
The messages that are displayed indicate that no actions are currently assigned to this tag, and that the tag can only be applied manually.

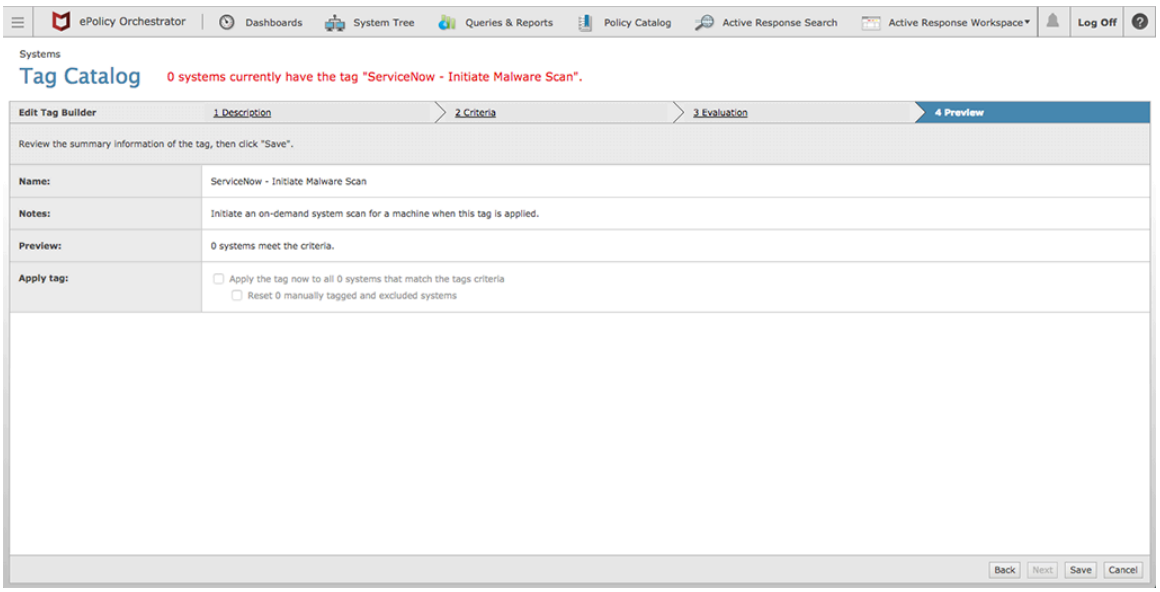
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



e. Click **Evaluation** in the progress bar to continue.



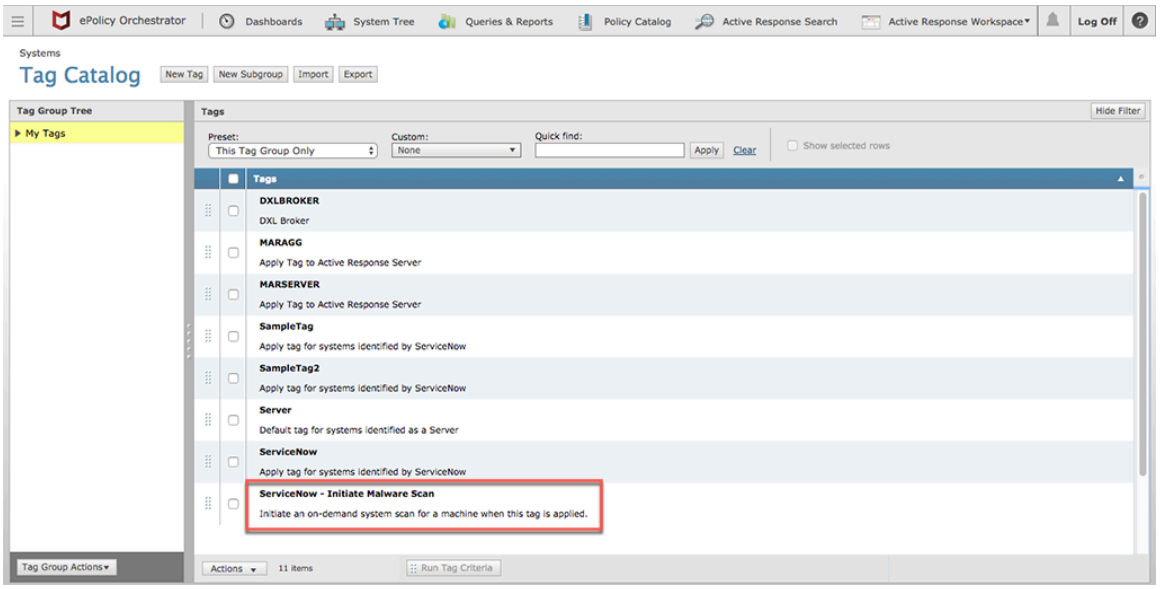
f. With the Tag Catalog page of the Evaluation step displayed, leave the settings on this page in their defaults, and, in the progress bar, click **Preview**.



g. With the Preview page displayed, in the lower right of the page, click **Save** to save the record.

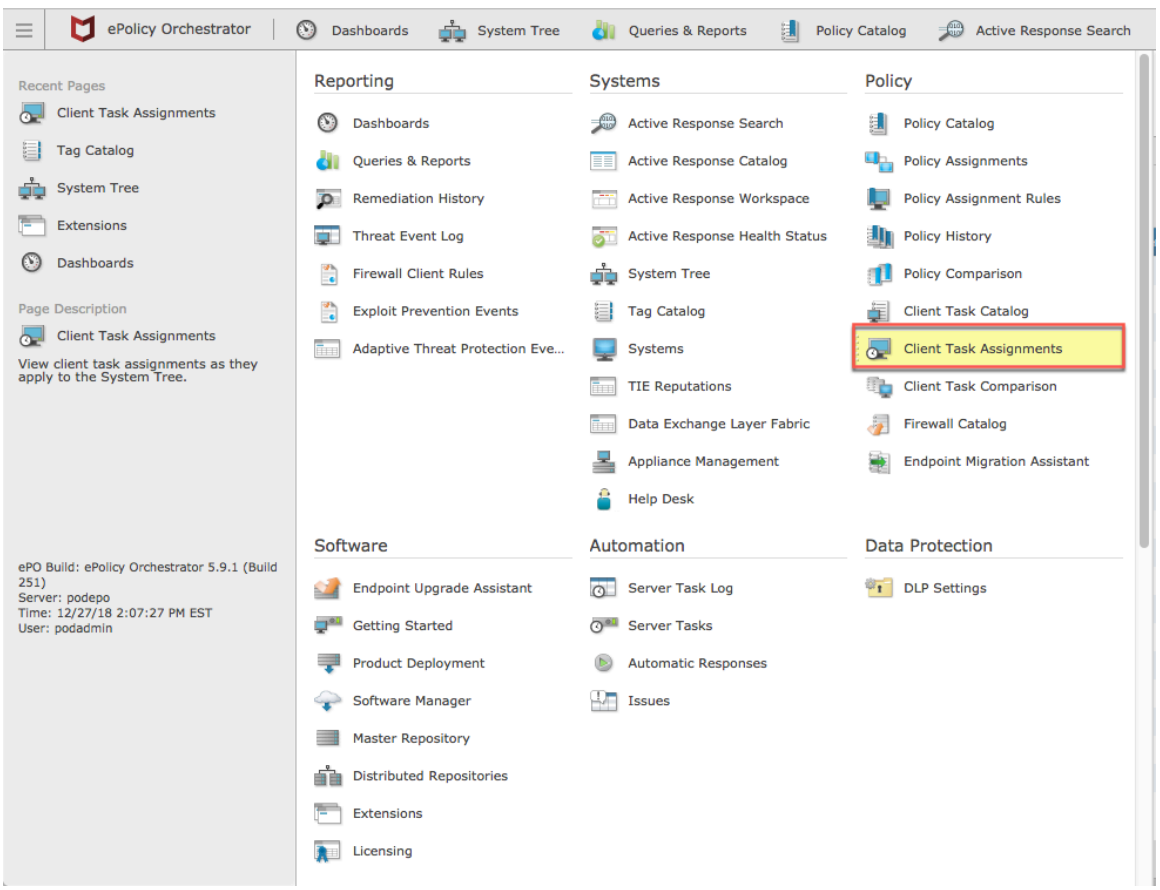
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The new tag is displayed in the Tag catalog as shown in the following figure.



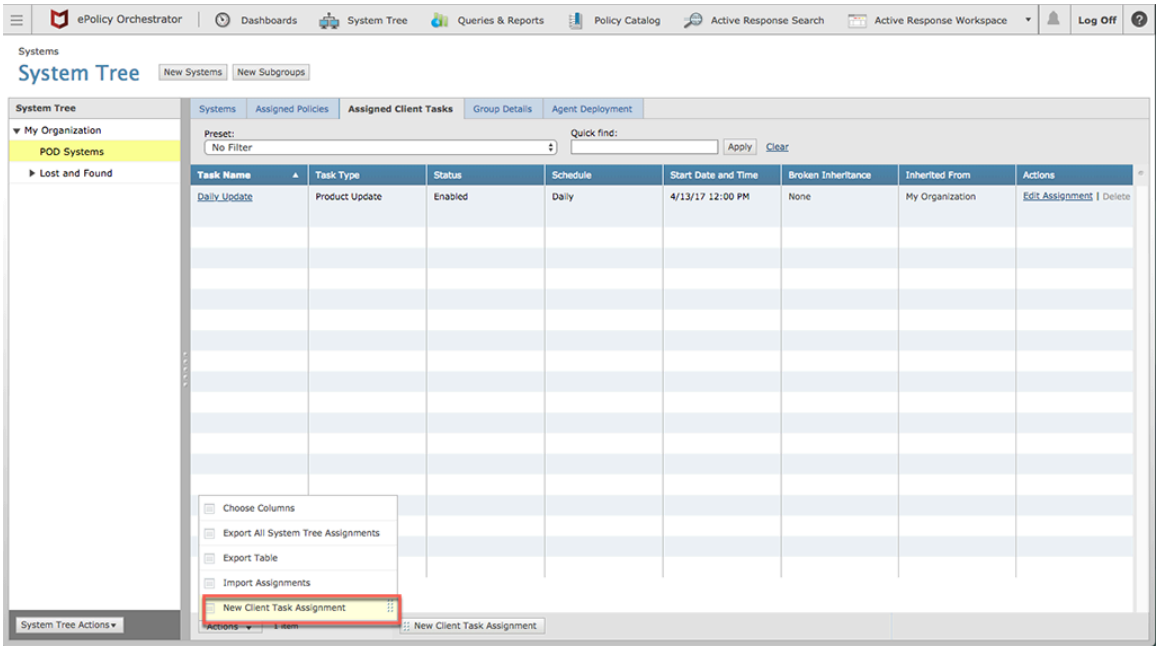
7. Create a security tag for the host isolation action by repeating the previous steps. After you have created both tags, you are ready to assign actions to the new tags.
8. To add an action to your new tag, follow these steps.

   a. Navigate to the home page and in the Policy section, click the **Client Task Assignments** link.

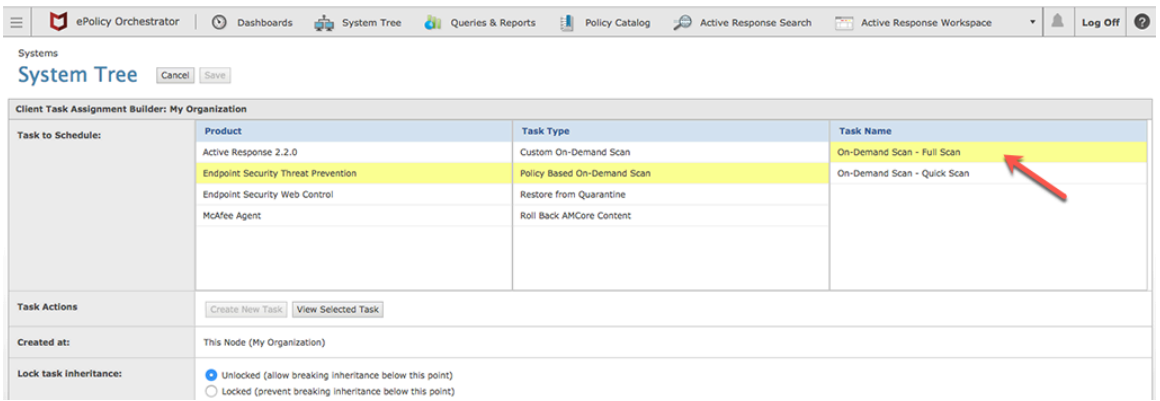


   b. In the System Tree page that is displayed, at the bottom of the page, expand the **Actions** menu and select **New Client Task Assignment**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

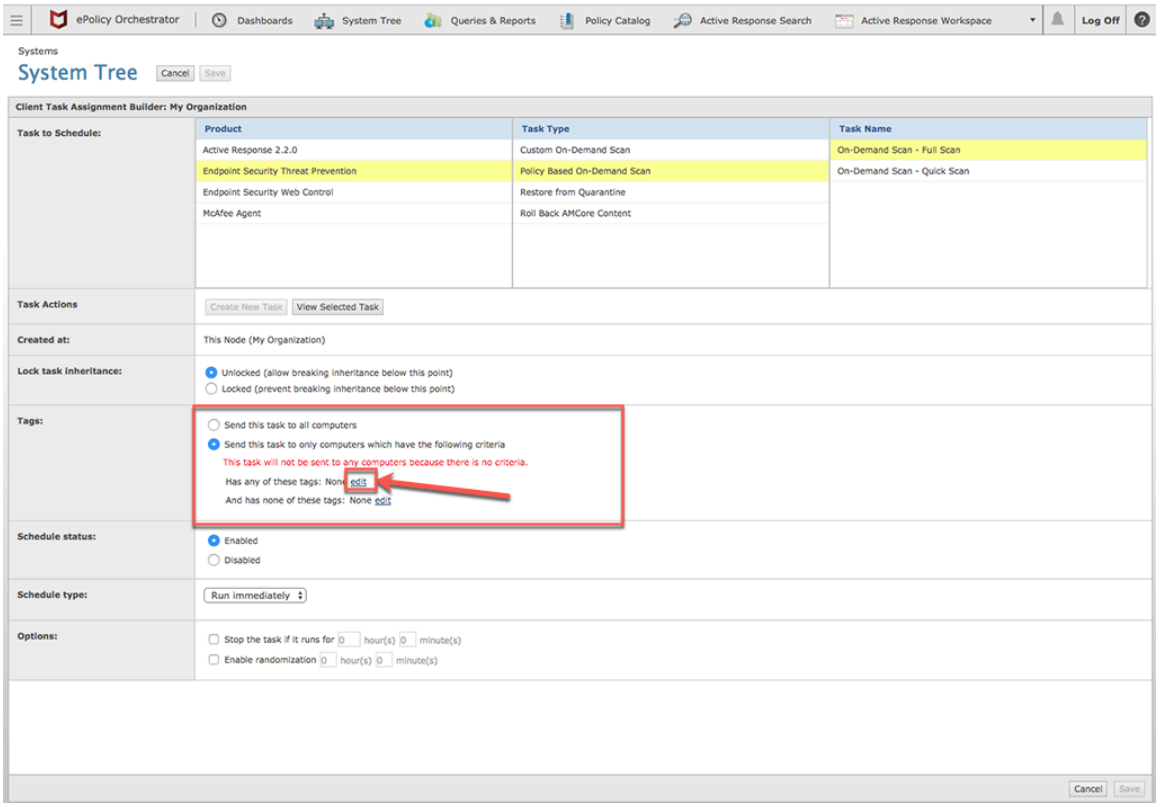


c. On the page that is displayed, navigate to **Endpoint Security Threat Prevention** > **Policy Based On-Demand Scan** > **On-Demand Scan - Full Scan** by selecting the path as shown in the following figure.

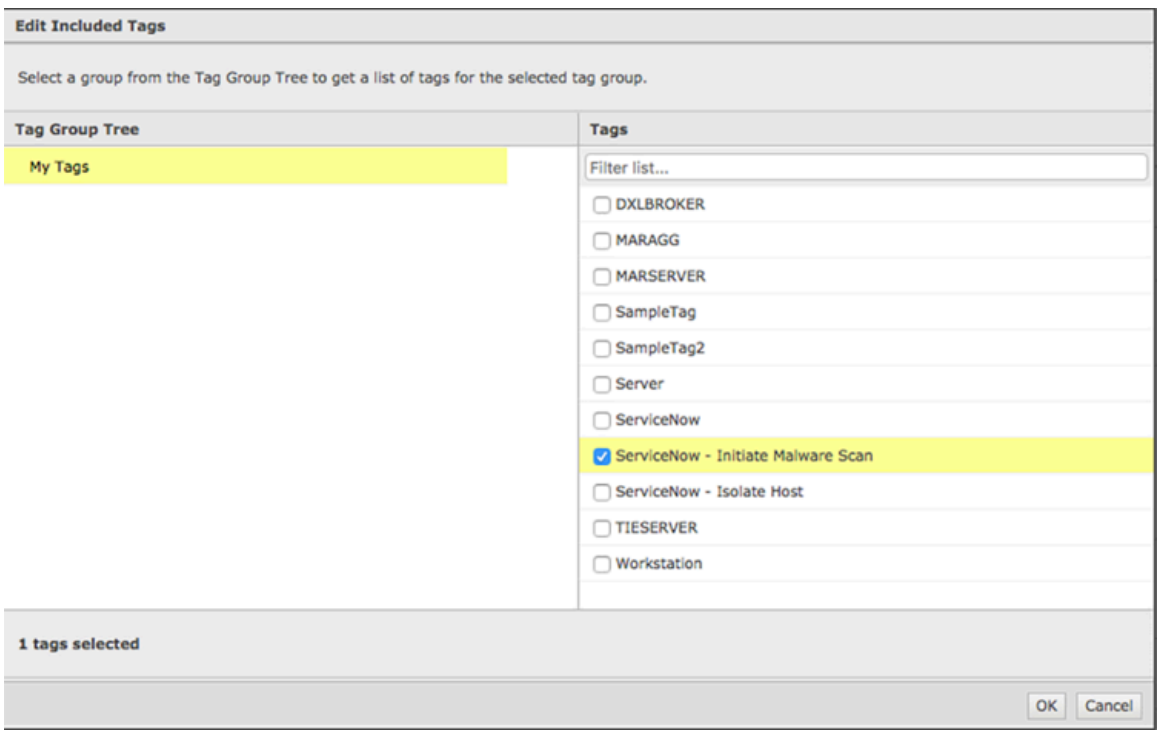


d. In the Tags section, under the radio button and next to `Has any of these tags:`, click the **edit** link to edit the criteria for the tag.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



e. In the dialog that is displayed, select the Initiate Malware Scan ServiceNow tag that you created in the preceding steps and click **OK**.

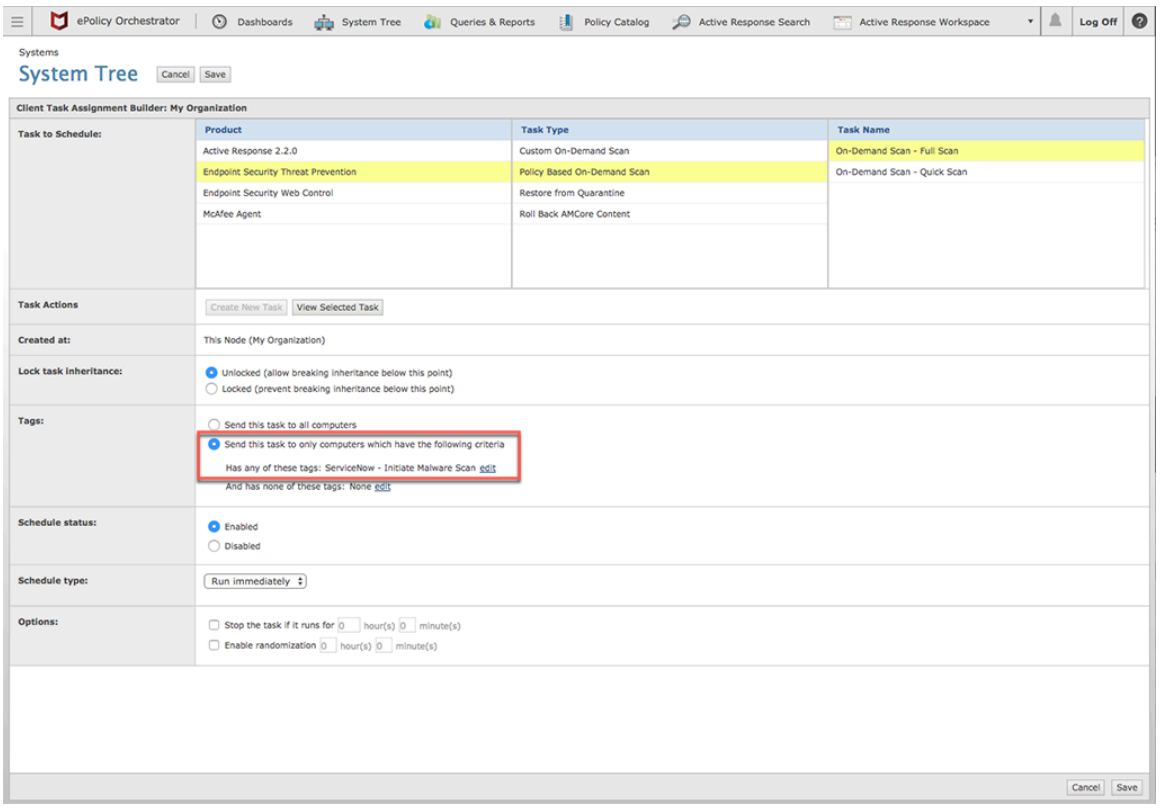


The ServiceNow Initiate Malware Scan tag you created is assigned to the On-Demand Scan action.

f. Click **OK**.

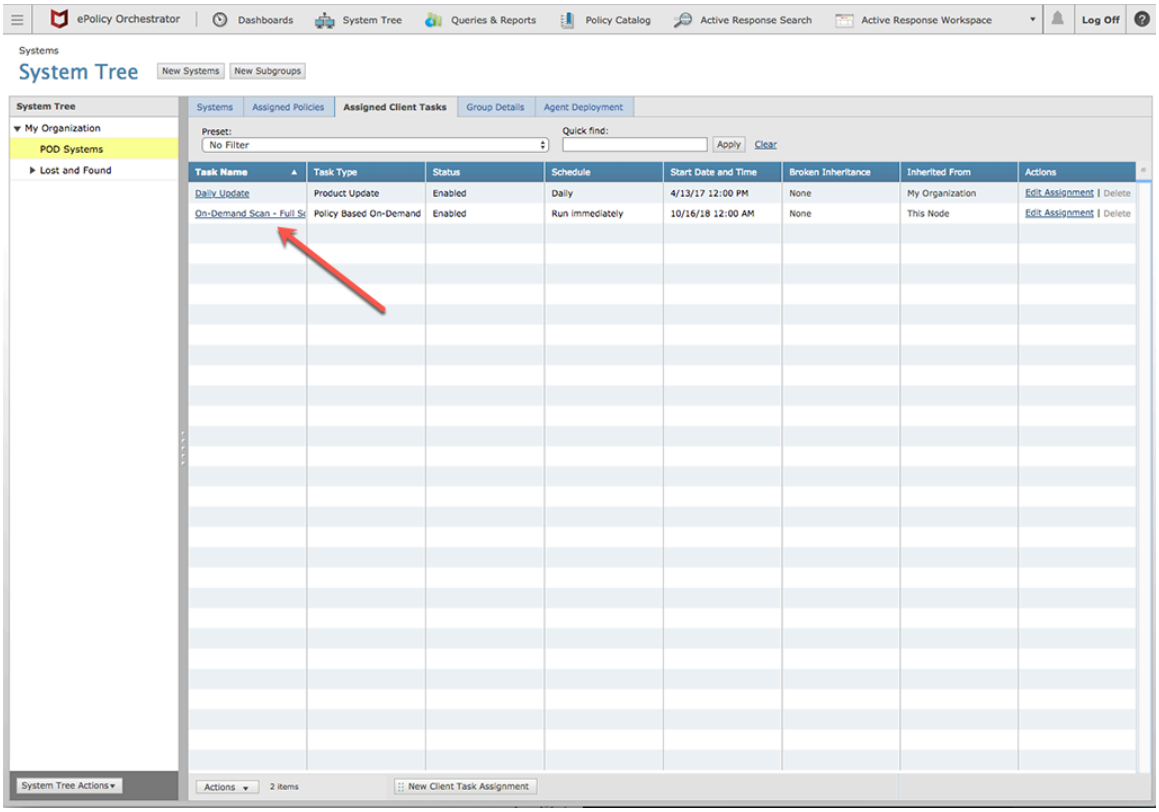
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the Tags section, under the radio button and next to `Has any of these tags:`, the Initiate Malware Scan tag is displayed.



g. Click **Save**.
On the System Tree page, the task is displayed on the Assigned Client Tasks list (tab).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



h. If you have not assigned an action to the Isolate Host action, repeat the previous steps to assign it.

You have successfully installed the extension plugin, created security tags, and assigned tasks to your tags. You have completed the setup for the integration in your McAfee ePO console. The next step is to configure a server in your ServiceNow AI Platform instance.

Install the application and configure a server for the McAfee ePO integration

Before you invoke the workflows for the integration, install and configure the McAfee ePO application from the ServiceNow Store on your ServiceNow AI Platform instance. The configuration is required to connect to the McAfee ePO console.

Before you begin

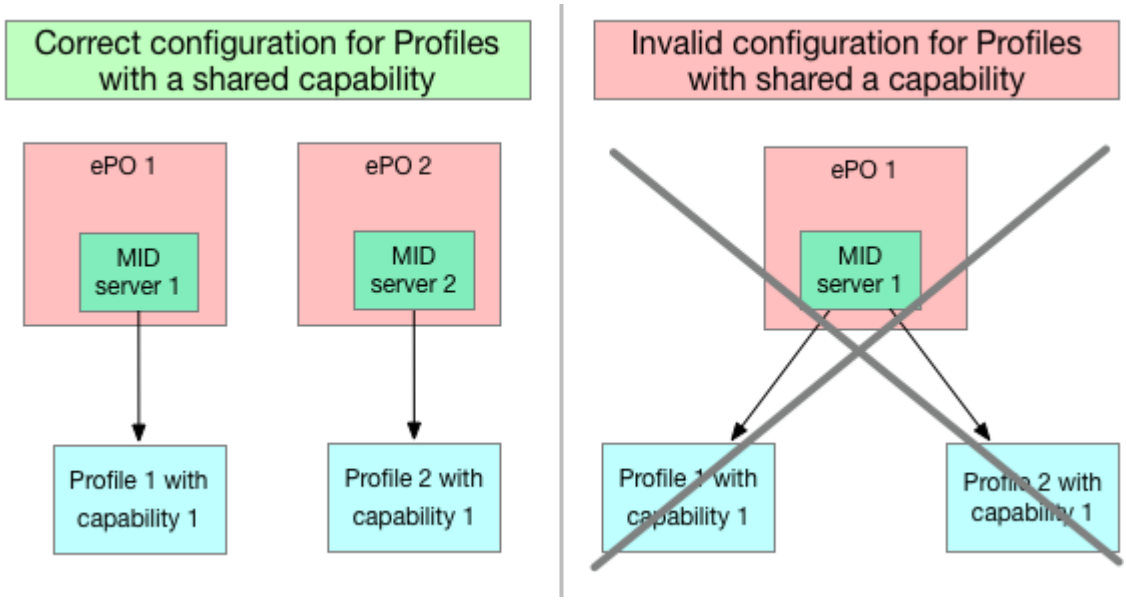
Role required: ServiceNow AI Platform administrator (admin)

About this task

The integration supports multiple servers, however, to avoid conflicts in profiles that share the same triggering conditions, you cannot share a McAfee ePO capability with multiple profiles that use the same McAfee ePO server. For example, as shown in the following figure, you can have capability 1 in more than one profile as long as each McAfee ePO server is mapped to a unique profile that has capability 1.

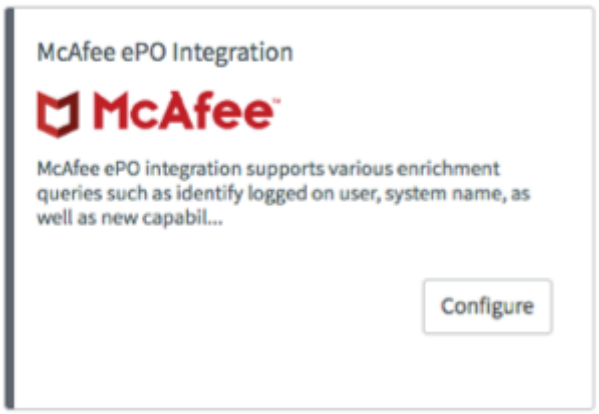
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

McAfee Shared Profile limitations



Procedure

1. Download the McAfee ePO for Security Operations from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the McAfee ePO for Security Operations integration tile, and click **Configure**.



4. On the form, fill in the fields.

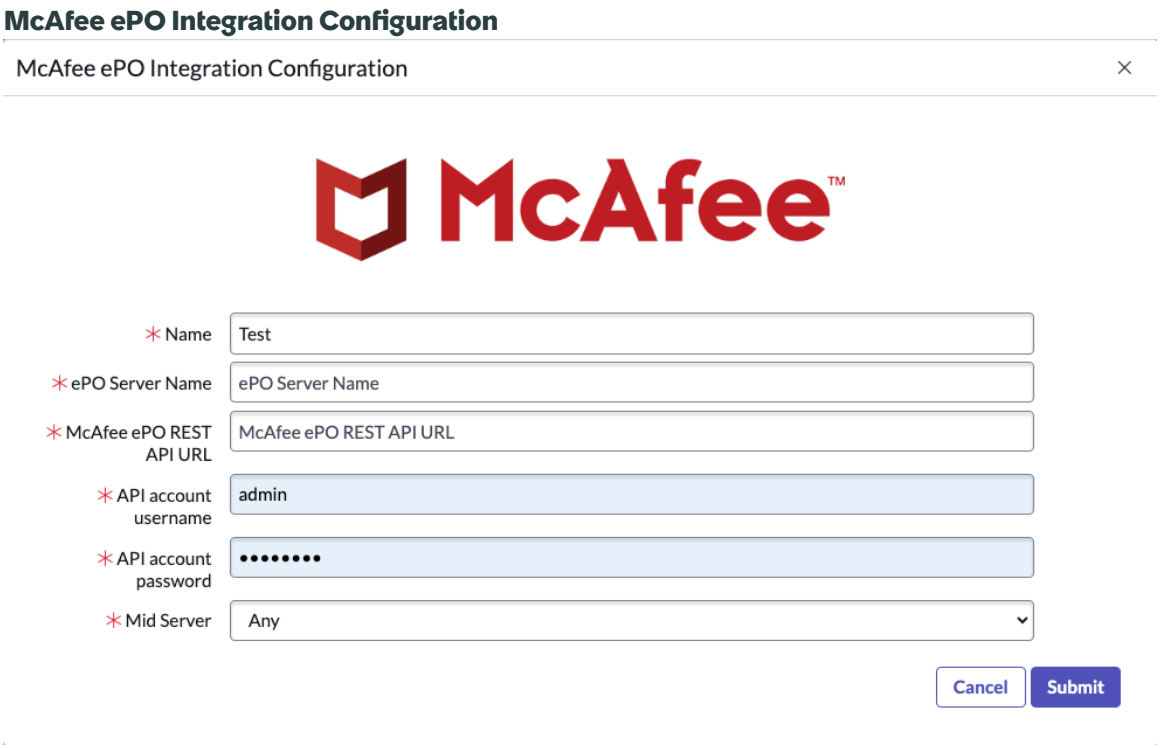
McAfee ePO Integration Configuration

Field	Description
Name	Name of the integration, for example, `demo - 1`.
ePO Server Name	Name for the McAfee ePO server. If you use one server, an example is, `McAfee HQ` (McAfee Head Quarters). This name is how the server and related credentials are recognized.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If your organization requires support for multiple servers, enter the name for each server and repeat the process.
McAfee ePO REST API URL	Base URL hosting the McAfee ePO REST API. Enter the URL with the https:// protocol, for example, `https://corp.epo_server:8443`.
API account username	Unique account username, for example, `ServiceNow API`.
API account password	Unique password for the API account.
MID Server	Select the name of the MID Server that you configured during the setup of your ServiceNow AI Platform instance. You can select a specific MID Server from the list or select **Any** to enable an auto-selection of a valid MID Server from the list for this integration. **Note:** ○ The MID Server selected during this configuration time applies throughout this integration. ○ Only MID Servers that are active and validated are displayed on this list. By default, the value is set to **Any**. An example name is, `secops_local_midserver`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.
   The McAfee ePO Configurations list is displayed with your new configuration record. You have successfully completed the configuration for a McAfee ePO server.

Note: If your organization requires support for multiple servers, then repeat the steps.

Edit security tags in the ServiceNow AI Platform for the McAfee ePO integration

As part of the setup for the integration, edit the security tag names that you created in your McAfee ePO console in your ServiceNow AI Platform instance. Edit the tag names in your ServiceNow AI Platform instance so that they match the names of the tags in your McAfee ePO console.

Before you begin

Role required: ServiceNow AI Platform security incident administrator (sn_si.admin)

About this task

The security tag names in your McAfee ePO console for the initiate malware scan and isolate host actions must match the security tag names in the records for these capabilities of your ServiceNow AI Platform instance.

Before you create a capability profile to run your capabilities, view the list of available McAfee ePO capabilities and edit the security tags in your ServiceNow AI Platform instance so that they match the security tag names in your McAfee ePO console.

For more information about creating the security tag names in your McAfee ePO console, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).

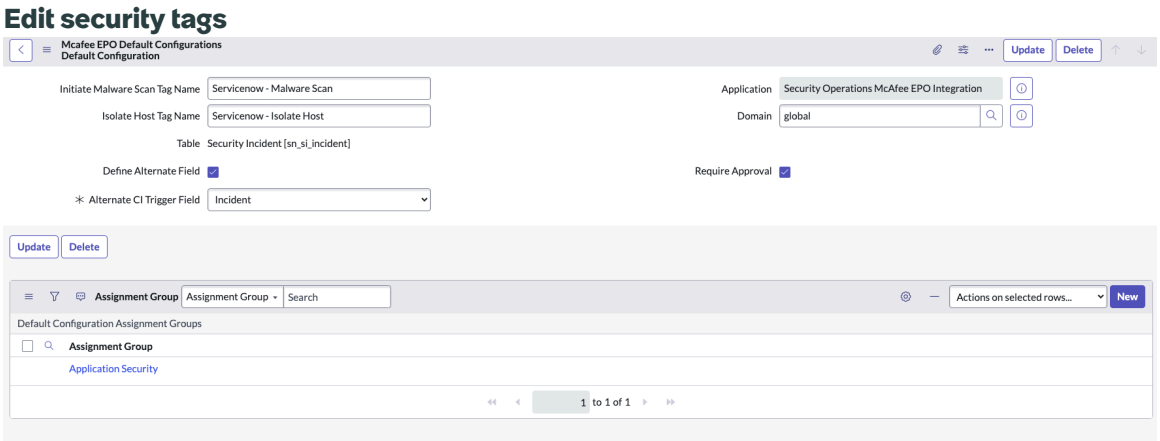
Procedure

1. Navigate to **All** > **McAfee ePO Integration** > **Default Settings**.
2. To edit the security tag name of the McAfee ePO integration, click **Default Configuration**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Makes sure you perform this configuration after you install the McAfee ePO integration.

3. In the Initiate Malware Scan Tag Name field, enter the name of the security tag that you created in your McAfee ePO console for the initiate scan action.
   For example, ServiceNow - Malware Scan
4. In the Isolate Host Tag Name field, enter the name of the security tag that you created in your McAfee ePO console for the isolate host action.
   For example, ServiceNow - Isolate Host
5. If you want to do not wish to use the CI trigger field upon incident creation, select the **Define Alternate field** check box.
   When this option is enabled, the Alternate CI trigger field choice list is displayed.



6. Choose an alternate field from the choice list to check for your CI search criteria.
   For this example, as a user with the sn_si.admin role, you believe that the CI field will not be populated on the security incident upon incident creation. Alternatively, you think CI information for a FQDN, host name, or IP address will be populated in the `Identified CI` field on the security incident, and you select the Identified CI field as an alternate. The Identified CI is selected for this example, but you can use any field on the security incident for the alternate CI.
7. In the Domain field, select a domain or group for this configuration using the search option.
   For example, global.
8. In the Require Approval field, select the **Require Approval** check box if you are using Isolate Host and Remove isolation capabilities.

   Note: The Initiate Malware Scan, List Threat Events, and Get System Details capabilities do not need approval.

9. Click **Update**.
   The EPO Tag Name is updated and displayed on the McAfee ePO Default Configurations list. The security tag name for the malware scan action in your ServiceNow AI Platform instance matches the name for the scan in your McAfee ePO console.

   You have successfully edited the EPO Tag Names for the malware scan and the isolate host capabilities in your ServiceNow AI Platform instance. The next step is to create a profile for your capabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

McAfee Product Documentation

Create an approval group

Create an approval group for the McAfee ePO for Security Operations integration that can approve requests for isolating host machines, restoring them to the network.

Before you begin

You can't reassign the approval authority to a group, unless an approval group is available in your instance.

Note: The approvals option in the Configuring profiles for the McAfee ePO integration appears only for Isolate Host and Remove Host Isolation capabilities.

Role required: ServiceNow AI Platform® Security incident administrator (sn_si.admin)

About this task

Approval requests submitted by the security incident analyst to isolate host machines and remove isolation are assigned to the user with the sn_si.admin role by default. As a user with this role, you can reassign this approval authority during the configuration step for a profile. Before you can reassign authority to an approval group, an approval group must be available on the `Groups` list in your ServiceNow AI Platform instance.

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. In the groups list, click **New**.
3. On the form, fill in the fields.

Approval group form

Field	Description
Name	Name of the group that is displayed when an approval request is submitted, for example, `Approvers McAfee host isolation`.
Group email	Group email distribution list or the email address of the point of contact, such as the group manager, `McAfeeapproval@servicenow`.com
Manager	Name of group manager. Click the search icon to view the list.
Parent	(Optional) Other group of which this group is a member, if this group has a parent.
Description	Additional information about this group.
Include members	Option to include members to this group.
Default assignee	Option to choose a user as default assignee for this group. Use the Search option to open the list of users.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Roles	Option to select the roles for this group. Use the Add and Remove option to add and remove roles.
Type	Option to choose a category for this group. Use the Search option to open the list of group types.
Vendors	Option to choose a vendor for this group. Use the Search option to open the list of vendors.

4. Click **Submit**.
   The new group is displayed in the Groups list.

   This group is available to process requests when you enable the **Require approval** option during the configuration of this profile.

   To monitor and process requests submitted by users with the sn_si.analyst role, each member of the approval group navigates to **My Approvals** tab in the ServiceNow AI Platform.

McAfee ePO integration capability profiles

As a user with the security incident administrator (sn_si.admin) role, you create profiles for the McAfee ePO capabilities in your ServiceNow AI Platform® instance. You group queries or actions in profiles and determine which McAfee ePO capabilities you want to run when a new security incident is created.

Capability profiles

You create profiles™ so you can group McAfee ePO capabilities and configure the settings for these capabilities from your ServiceNow AI Platform® instance. You have the flexibility to create multiple profiles for these capabilities, which allows you to determine which actions or queries are invoked when a Security Incident Response (SIR) incident is created. To fit the needs of your organization, you can create a single profile that runs queries for system details, initiates malware scans, and isolates host machines, for example, or, you can create multiple profiles, each with its own, single McAfee ePO capability.

Profile types and required McAfee ePO capabilities

Primary purpose of your profile	Set up requirements	McAfee ePO capabilities required for this profile type
Gather system details	None	**Get Host Details**
Isolate a host	Verify with your McAfee ePO administrator that you have created the security tags for the isolate host action in your McAfee ePO console. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).	**Isolate Host**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Profile types and required McAfee ePO capabilities (continued)

Primary purpose of your profile	Set up requirements	McAfee ePO capabilities required for this profile type
Scan and search for threats on your host	Verify with your McAfee ePO administrator that you have created the security tags for the initiate malware scan action in your McAfee ePO console. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).	**Initiate Malware Scan** **Note:** As part of the McAfee ePO malware scan, the List Threat Events capability is invoked automatically. However, you are not required to add the List Threat Events capability to the profile with the malware scan capability. Results of the malware scan are displayed on the Threat Event Details tab on the security incident.
Remove isolation for a host	Verify with your McAfee ePO administrator that you have created the security tags for the isolate host action in your McAfee ePO console. For more information, see Set up your McAfee ePO console to integrate with Security Incident Response (SIR).	**Remove Isolation**
Gather threat enrichment data.	None	**List Threat Events**

Create a capability profile for the McAfee ePO integration

Create a profile and select the McAfee ePO capabilities that you want the profile to run.

Before you begin

Role required: ServiceNow AI Platform® Security incident administrator (sn_si.admin)

About this task

For this step of the configuration, you create a profile for the McAfee ePO capabilities. When you create profiles, consider the intention of the profile before you add McAfee ePO capabilities to it. Refer to the following table when you create profiles.

The following table lists the capabilities that you are required to add to a profile if you want the profile perform certain queries or actions. Create a single profile that runs queries for host details, initiates malware scans, remove isolation, and isolates host machines, or, create multiple profiles, each with its own, single capability.

Procedure

1. Navigate to **McAfee ePO Integration** > **McAfee ePO Capability Profiles**.
   The McAfee ePO Capability Profiles list is displayed.

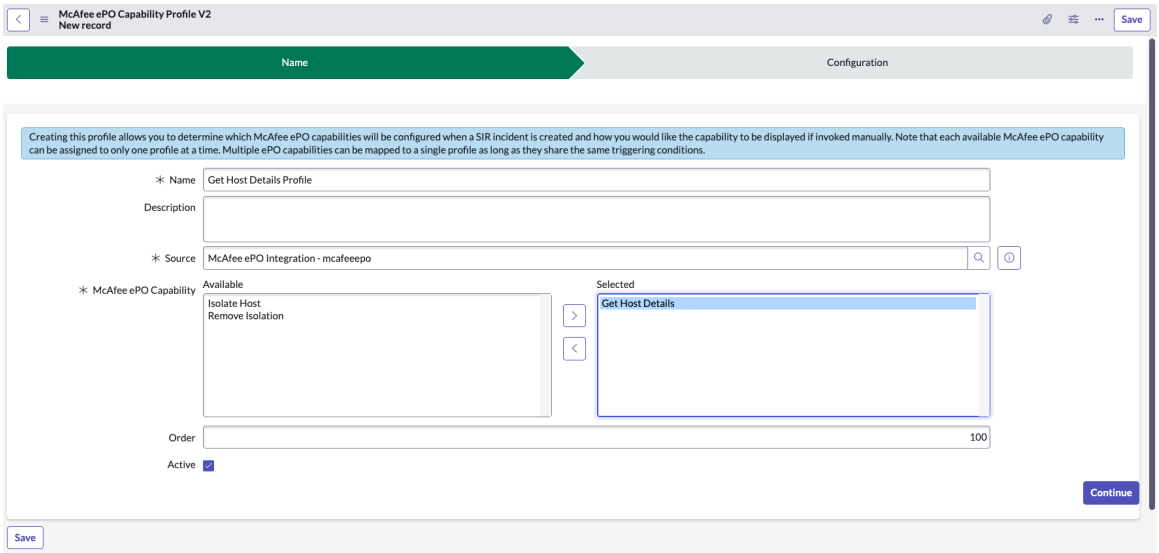
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Click **New**.
3. On the form, fill the fields.

Field	Description
Name	Name for the McAfee ePO capability profile. This name helps you identify the profile type and describe it. An example for a profile that runs queries is, Host and Threat Details. This name is also the name for the security tag for this profile by default.
Description	Additional information about the profile that further describes the activities of the profile. An example description for a profile that runs queries is, Threat enrichment for system de tails and a list of threat events. An example de scription for a profile that runs actions is, Iso late host machine.
Source	Name of the McAfee ePO server. Only config ured servers are available from the choice list.
McAfee ePO Capability	Capabilities of the McAfee ePO profile. McAfee ePO supports the following capabili ties: ○ Get Host Details ○ Isolate Host Profile ○ Initiate Malware Scan ○ Remove Isolation ○ List Threat Events Select the capabilities you want for this profile from the **Available** column and move them to the **Selected** column. You can't add Get Host Details, Initiate Mal ware Scan and List Threat Events in the same profile, and you can't add Remove Isolation and Isolate Host on the same profile.
Order	Workflow priority. Default is 100. The value of this field indicates the order that workflows are executed when two or more profiles share triggering conditions. The workflow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400.
Active	The check box is selected by default to indi cate that the profile is active. When selected, the profile is active and trig gers automatically when a security incident is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	created that matches the filtering conditions that you specify during the configuration step. When inactive, the profile will not run, and it is not available to invoke from a list.



4. To save and validate the profile, click **Continue**.
   If validation is successful, the page reloads and the **Configuration** form is displayed.

What to do next

The next step is to configure your profile. Before you configure the settings for the profile, you may prefer to review the concepts for configuring profiles and triggering conditions. See Set up your McAfee ePO console to integrate with Security Incident Response (SIR) and Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile for more information.

Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile

After you create a profile and select the McAfee ePO capabilities that you want the profile to run, you configure the settings of the profile so that it runs only when a set of specific conditions are met.

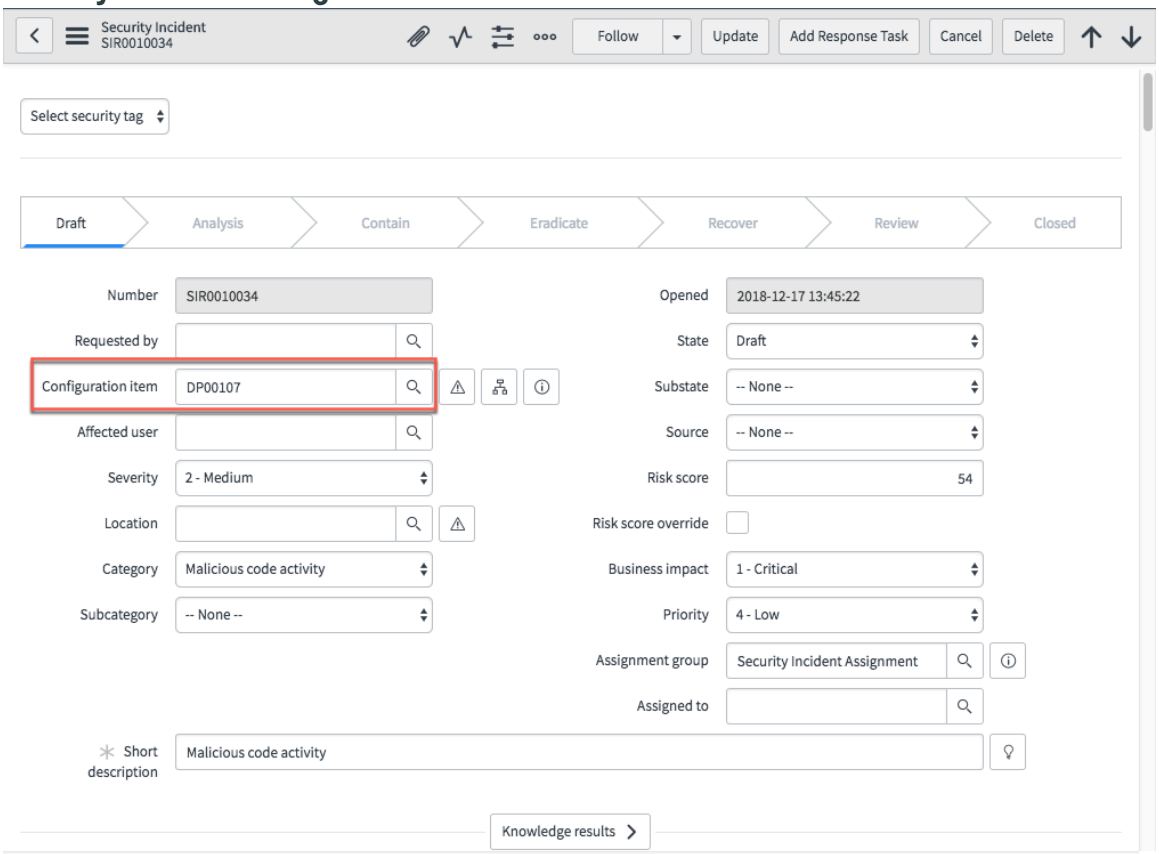
You have the flexibility to set these triggering conditions so the profile runs automatically based on the default field values that are matched on a ServiceNow AI Platform® Security Incident Response security incident. Alternatively, you can set up a profile so it searches for matches on field values you specifically identify on the security incident.

One of the keys to the functionality of the integration and how a profile works is the Configuration Item (CI) field on the ServiceNow AI Platform® Security Incident Response (SIR) security incident. The value of this field is the principle value on a security incident. This value is used to match the IDs of your assets with the information stored in the ServiceNow AI Platform® database. When a SIR security incident is created by a security event, and a profile is activated, your assets are scanned for a matching value for a Fully Qualified Domain Name (FQDN), a host name, or an IP address based on the value of the Configuration Item field.

In an ideal case, a matching value is found in the database, and data can be gathered from the McAfee ePO console for the matching asset, pulled into your ServiceNow AI Platform® instance, and displayed on the related lists of a security incident. The following figure shows an example of the Configuration Item field populated with a host name on a SIR security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident - Configuration item

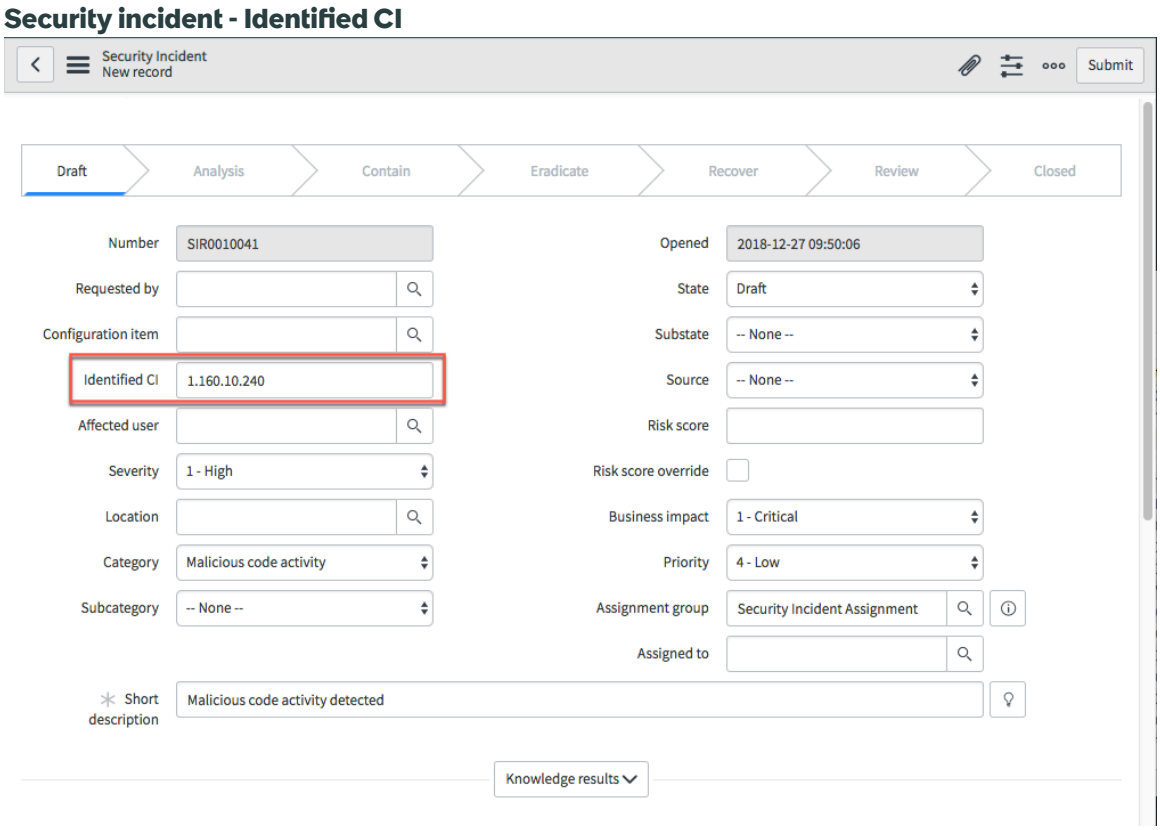


In cases when the Configuration item (CI) field is not populated on the security incident, or a match cannot be found for a FQDN, a host name, or an IP address that matches the database, you can select an alternate field on the security incident to display any matching CI enrichment data found during the scan of your assets.

During the configuration step of the profile setup, you can select an alternate CI trigger field for endpoint identification to ensure that the CI enrichment data from the McAfee ePO lookup is populated on the associated security incident. You can select any field on the security incident as an alternate CI trigger field including custom fields that you create. By selecting this alternate CI field as a backup, you ensure that your profiles run even if the CI field is not populated on the associated security incident upon incident creation.

As an example, as a security operations center (SOC) analyst, you create a custom field for a security incident called, IP Address on my security incident. If you do not think that the value of this custom field will be displayed in the Configuration Item field on the security incident upon incident creation, you can set up the profile so it scans for this IP address. If matched, the IP address is displayed on the security incident in the field of your choice. In the following figure, the `Identified CI` field is selected as the alternate field for the IP Address for this example.

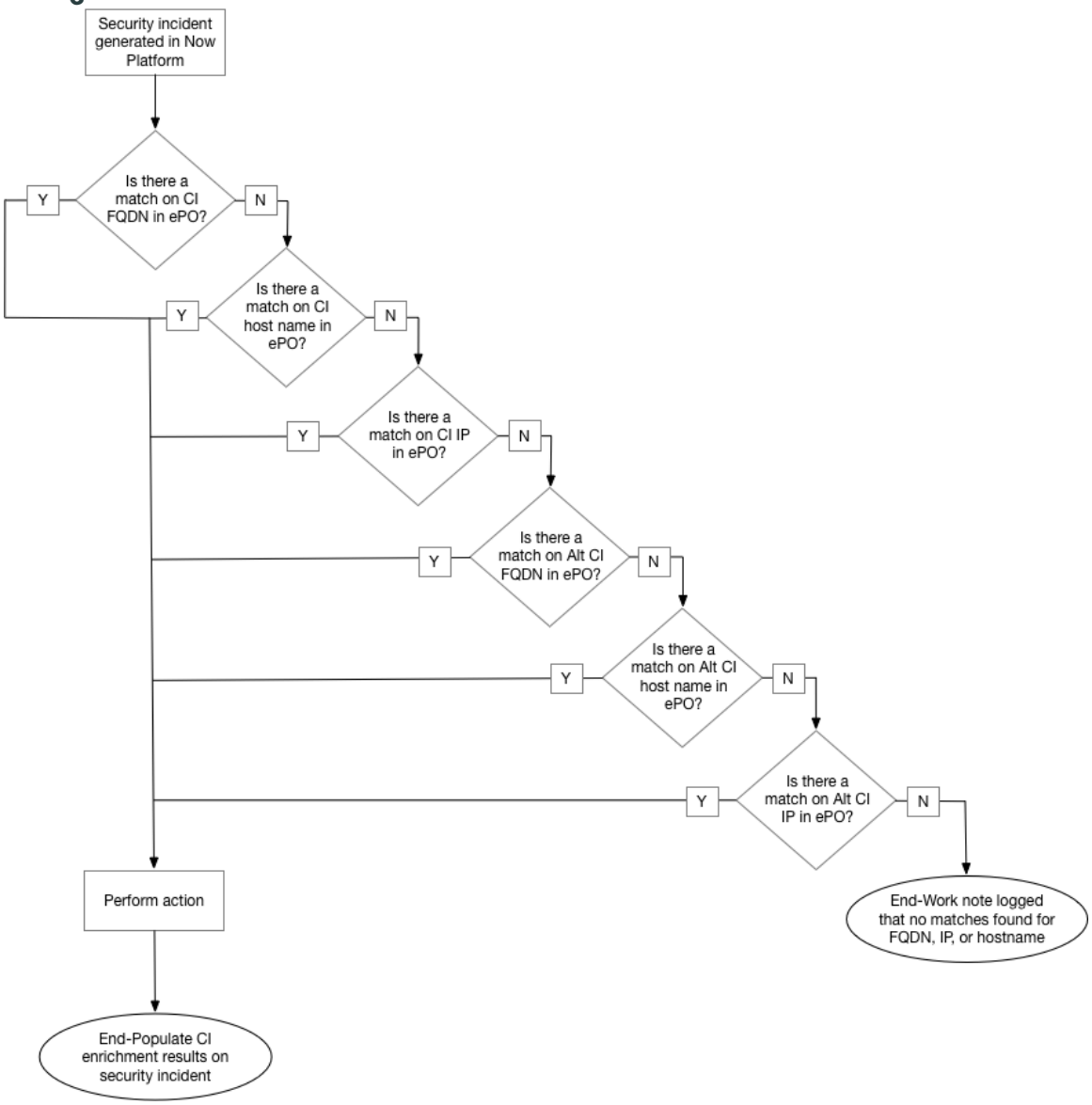
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The following figure illustrates how the first search of the workflow scans for matches for Configuration Items. If the Alternate CI trigger field is enabled, the second search scans for matches for alternate values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration items workflow



If matching IDs are not found for the CI field or the alternate CI field, a work note is logged and a message is displayed on the security incident. When no matches are found, no enrichment data are populated on the security incidents related to the event.

You enable the alternate CI trigger field and select the field you want to display the matching ID during the configuration step for a profile. This step for enabling the alternate CI field is described along with the other profile configuration requirements in Configuring profiles for the McAfee ePO integration.

Configuring profiles for the McAfee ePO integration

After you create a profile and select the McAfee ePO capabilities that you want the profile to run, configure the settings so that the profile is invoked only under the specific conditions that you define.

Configuring a profile

In this step, you configure a capability profile so that it runs only when the conditions you specify are fulfilled. You define which conditions on security incidents automatically trigger the McAfee ePO capabilities that you selected for the profile. You also have the option to select an alternate input field for the Configuration Item (CI) field and set filtering conditions so that only those

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

security incidents that are related to your triggering event automatically launch the profile. The configuration step includes the following settings on the configuration form for the profile.

Alternate configuration item (CI) trigger field

In cases when the Configuration item (CI) field on the ServiceNow AI Platform® Security Incident Response (SIR) security incident is not populated with a value, or a match cannot be found in the database, you can select an alternate field on the security incident to display any matching CI enrichment data found during the scan of your assets. For more information about the Configuration item and the Alternate configuration item fields on a security incident, see Defining triggering conditions with a Configuration item (CI) field for a McAfee ePO profile.

Security tags

To help you track the status of isolated host machines and when malware scans are initiated, an optional tagging feature is available. By default, this option is disabled on the configuration form for profiles. If this option is enabled during the configuration step, security tag names are displayed on the configuration form. These are the names of the tags that are displayed on related security incidents. These tags inform you when a host isolation action is successfully initiated and when it is approved. After a host is successfully returned to the network, the security tag is automatically removed from the security incident. For malware scans, a tag is displayed on the related security incident when a scan is scheduled. After the scan is finished, the scheduled tag is automatically replaced by a tag that indicates that the scan is successfully completed.

Auto-trigger based on incident

When the Auto-trigger based on incident option is enabled, the filter condition builder is available, and you are required to set filtering conditions that specify when the profile runs automatically. A common filter is Category is malicious code activity™ and Business impact is 1 - Critical™. With these filters, only security incidents that are related to malicious code and that have a critical business impact launch the profile. Using the Auto-trigger option can reduce the number of security incidents that automatically invoke the profile.

Approvals

If your organization wants an extra level of control over actions such as isolating host machines and initiating malware scans, you can enable the Require approval option during the configuration step for a profile.

For example, if both the approval and tagging features are enabled for a profile, after a request to isolate a host machine or to return it to the network is submitted for approval, the associated security incident is tagged automatically that the action is initiated. Requests are sent for approval to a user with the sn_si.admin role by default, but this approval can be reassigned to another individual or an approval group to fit the needs of your organization. Approvers process requests in **My Approvals** in their ServiceNow AI Platform® instances. Security tags are displayed on related security incidents. All workflow activities are also logged in work notes to create an audit trail.

ServiceNow audit log in the McAfee ePO console

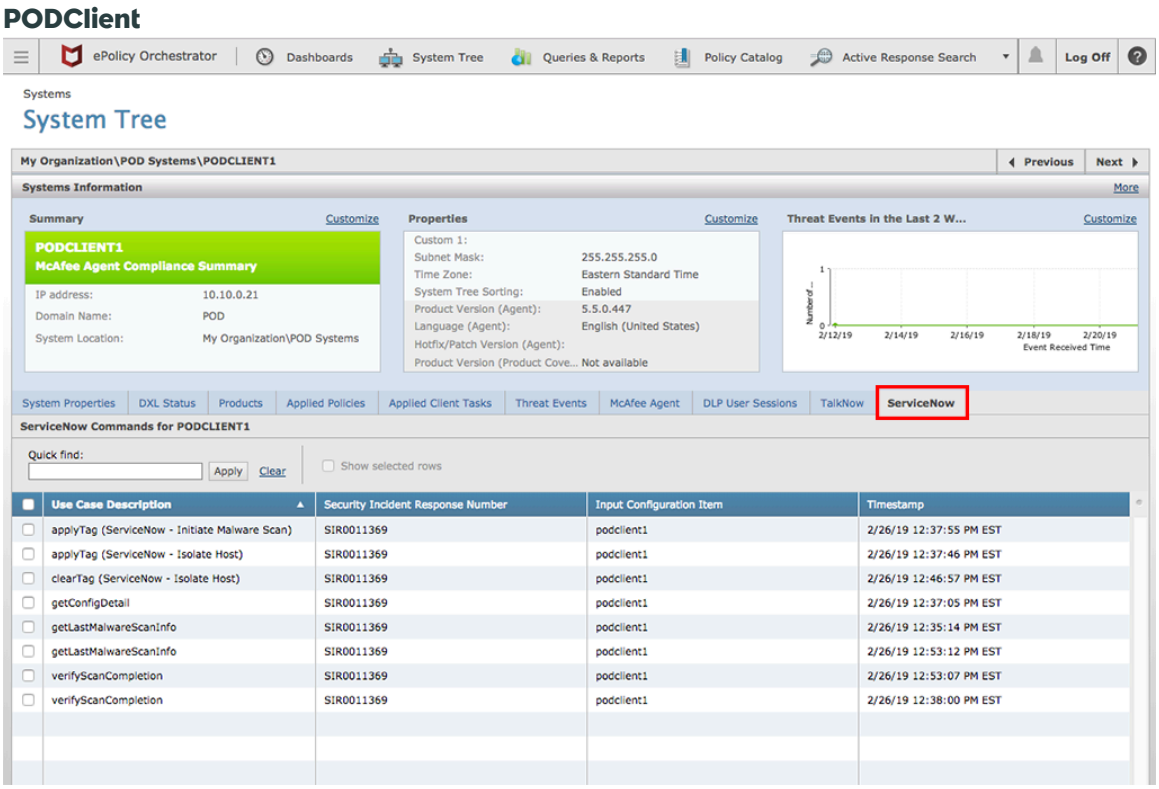
In version 5.10.0 of McAfee ePO, a ServiceNow tab is displayed with a log of commands that are initiated from your ServiceNow AI Platform® instance. After an action or a query is invoked from a profile in your ServiceNow AI Platform® instance on a host machine (endpoint) in the McAfee ePO console, an audit log of ServiceNow commands is created in the McAfee ePO console. This log is displayed in the System tree in the McAfee ePO console and helps you audit the times of

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the commands that are sent to specific endpoints. To view logged ServiceNow events on specific machines in a McAfee ePO console, follow these steps.

1. Navigate to the System tree in your McAfee ePO console and locate the ServiceNow tab.
2. Click the tab to open a list of host machines.
3. In the Name column, click a host name to open the audit log.

In the following image, an example of a log for a host (PODCLIENT1) is displayed.



The events initiated from the profiles in your ServiceNow AI Platform® instance are recorded and displayed in the log. Verify by checking the status of the host machine that the events listed in the log are successfully completed on the host.

Example profiles

The following topics include examples for how to configure profiles and test security incidents. These examples include profiles for all of the McAfee ePO capabilities that are available for this integration.

Configure profiles and security incidents for system enrichment queries for the McAfee ePO integration

Configure your profile settings so that the profile triggers only under the conditions that you set.

Before you begin

Role required: ServiceNow AI Platform® security incident administrator (sn_si.admin)

About this task

Define the conditions that automatically trigger the McAfee ePO capabilities that you selected for the profile. You can also select an alternate input field for the Configuration Item (CI) field. In this alternate field, you can set filtering conditions so that only those security incidents that are related to your triggering event automatically trigger the profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

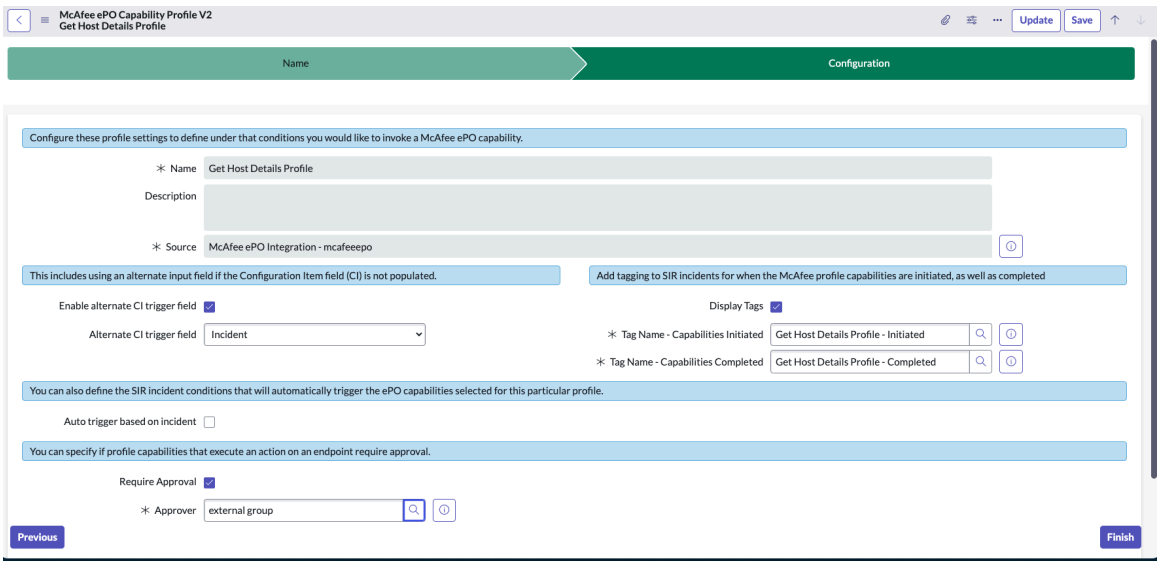
Procedure

1. If the Configuration page is not displayed, click **Configuration** on the progress bar.
2. On the form, fill the fields

Option	Description
Enable alternate CI trigger field	Alternate configuration item (CI) trigger field. Default is cleared. When this check box is cleared, and the alter nate CI trigger field option is disabled, an al ternate for the CI field is not identified. If dis abled, a value for the CI field must be populat ed on a SIR security incident, and the value in the field must be recognized by the McAfee ePO console before the profile gathers enrich ment data. Select this check box if you believe the CI field will not be populated upon incident cre ation, but CI information will be populated in another field on the security incident. When this option is enabled, the Alternate CI trig ger field choice list is displayed. Choose an al ternate field from the choice list to check for your CI search criteria. For more information on the alternate CI trigger field, see Defining triggering condi tions with a Configuration item (CI) field for a McAfee ePO profile.
Display Tags	Security tags are displayed on security inci dents. Default is cleared. When this check box is cleared, and the tag ging option is disabled, no security tag names are displayed on the configuration form, and tags are not displayed on related security inci dents. For this example, the security tags op tion is disabled.
Auto trigger based on incident	Filter conditions. Default is cleared. When the check box is cleared, and the op tion is disabled, the profile must be invoked manually from a security incident. When this option is enabled, the Filter condi tion builder is displayed. You are required to set the filtering conditions to specify when the profile runs automatically upon incident creation. A common example of a filter for a profile that runs enrichment queries is `Category is Malicious code activity` and `Busi`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	`ness impact is 1-Critical`. These filter conditions help you locate the incidents that are related to specific types of security events, and they help you limit the number of security incidents you have to review. These filter settings remain saved until you change them, and they are available for edit ing during the preview and test incident step of the configuration.
Require approval	Request approval option. Default is cleared. This approval option is available for any pro file. Usually, approvals are used for capabili ties that invoke actions such as host isolation and malware scans. When the check box is cleared, and this op tion is disabled, no approval requests are sub mitted. For this example, no prior permission is required for system enrichment queries.



3. To enable the alternate CI field option and set the filtering conditions that automatically invoke this profile, follow these steps.

   a. Select the **Enable alternate CI trigger field** check box.
   The Alternate CI trigger field is displayed. For this example, as a user with the sn_si.admin role, you believe that the CI field will not be populated on the security incident upon incident creation. Alternatively, you think CI information for a FQDN, host name, or IP address will be populated in the `Identified CI` field on the security incident, and you select the Identified CI field as an alternate. The Identified CI is selected for this example, but you can use any field on the security incident for the alternate CI.

   b. From the **Alternate CI trigger** field choice list that is displayed, select the **Identified CI** field.

   All the available fields on the security incident are displayed in the list including any custom fields. In the Alternate CI trigger field, `Identified CI` is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When this profile is invoked, and the CI field is not populated on the associated security incident upon the initial event trigger, the profile alternatively uses the value from the Identified CI field in the search.

c. Select the **Auto trigger based on incident** check box.
The filter conditions builder is displayed. With this option, set filtering conditions and specify when the profile is invoked automatically upon creation of a security incident.

d. Define the SIR incident conditions that will automatically trigger the ePO capabilities selected for this particular profile.

e. If the profile capabilities that execute an action on an endpoint require approval, select the **Require Approval** check box.

f. Select an approve using the search icon.

4. Click **Finish**.
You have successfully configured the profile so it is triggered automatically upon incident creation, and an alternate field is used to populate matching CI results.

Trigger McAfee ePO profile manually from a security incident

Trigger a capability profile manually from a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Before you begin
Role required: sn_si.admin

Note: The approvals option in the Configuring profiles for the McAfee ePO integration appears only for Isolate Host and Remove Host Isolation capabilities.

About this task
You can invoke a request to Get Host Details, Isolate Host machine, or Remove Isolation of a machine automatically if the triggering conditions you specify in the profile match the conditions on security incidents. Alternatively, if you want to submit a request manually, submit the request directly from a security incident.

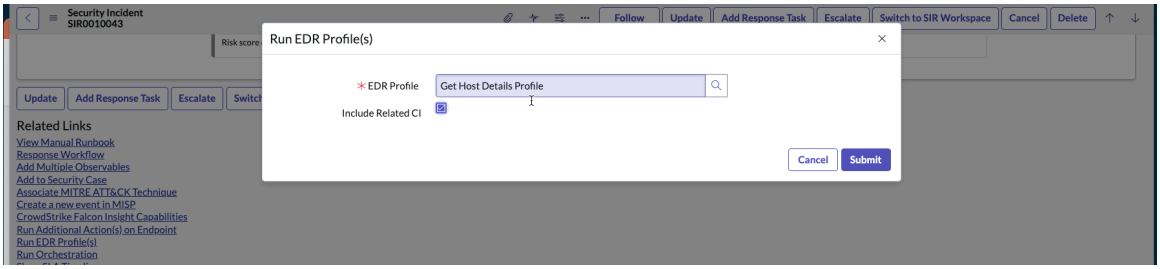
Once you activate the profile, based on the configured trigger conditions, you can view the query results in the ServiceNow AI Platform security incidents. McAfee ePO integrations also enables you to run individual capabilities on Configuration Items (CIs) without using a profile.

Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the McAfee ePO information.
3. In the related lists section, select **Run EDR Profile(s)**.

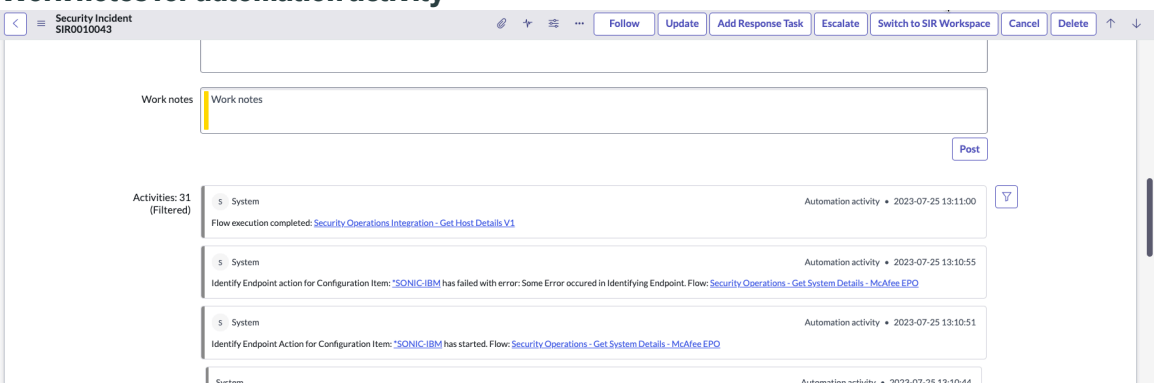
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

McAfee Run EDR Profile



4. Browse and select a profile from the list of available profiles.
   The list of available profiles are Get Host Details, Isolate Host machine, and Remove Isolation. For example, let's select Get Host Details.
5. Select **Include Related CI** to run this profile on all the related CIs of the profile.
   For example, if there are five CIs associated with the security incident, then the selected profile runs on all the five CIs.
6. Click **Submit**.
   The selected profile is triggered manually. You can review the work notes and activities section and the profile-initiated and profile-completed tags in the work notes section.

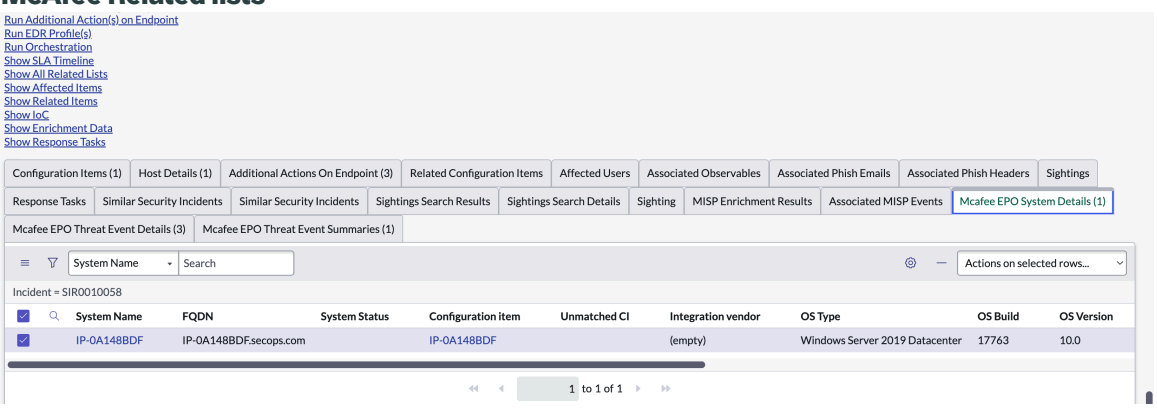
Work notes for automation activity



The results appear in the form of related lists such as Get Host Details, Isolate Host machine, or Remove Isolation.

Note: All the related list tables extend the base tables. In this example, the McAfee EPO System Details is an extended table of the Host Details base table.

McAfee Related lists



7. To run individual capabilities on a Configuration Item (CI), perform the following steps:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In the Configuration Items related list, select the required CI.

b. Click the **Actions on selected rows...** drop-down list, and select the required capability that you want to run for the selected CI.
For example, Isolate Host.

c. Click **Isolate Host** to run it on the selected CI.
The select CI gets isolated from the network.

Trigger additional actions in McAfee ePO integration

The List Threat Events and Initiate Malware Scan capabilities can be triggered from Run Additional Actions.

Before you begin

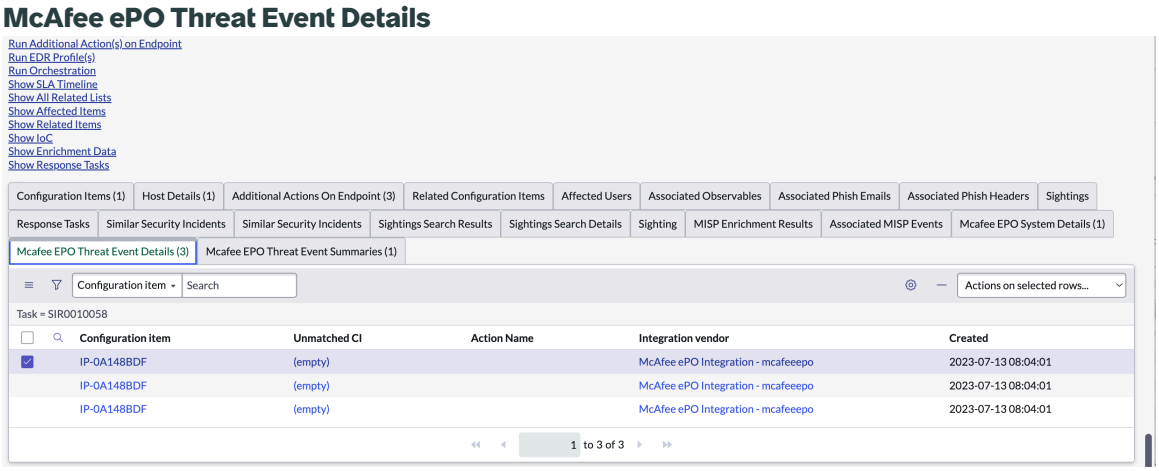
Role required: sn_si.admin

About this task

You can configure and trigger additional actions in the McAfee ePO integration enables by using **Run Additional Actions on Endpoint**, which include the McAfee ePO List Threat Events and McAfee ePO Initiate Malware Scan capabilities.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident on which you want to run the additional actions.
3. In the Related Links section, click **Run Additional Action(s) on Endpoint**.
4. Browse and select the capability implementation that you want to trigger from the list of additional actions.
   For example, McAfee ePO List Threat Events.
5. Select **Include Related CI** to run this additional action on all the related CIs of the profile.
   For example, if there are five CIs associated with the security incident, then the selected profile runs on all the five CIs.
6. Click **Run Additional Actions**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: All the related list tables extend the base tables. In this example, the McAfee EPO Threat Event Details table is an extended table of the Additional Actions on Endpoint base table.

7. View and validate the McAfee ePO Threat Event Details on the related lists.

Using McAfee ePO integration in Analyst Workspace

Use the McAfee ePO integration to leverage the McAfee ePO capabilities on the SIR Analyst workspace.

Before you begin

Role required: sn_si.admin

Before you use McAfee ePO integration on the Security Incident Response workspace, you must download it from the ServiceNow Store and configure it. For more information, see Set up your ServiceNow AI Platform instance for the McAfee ePO integration.

About this task

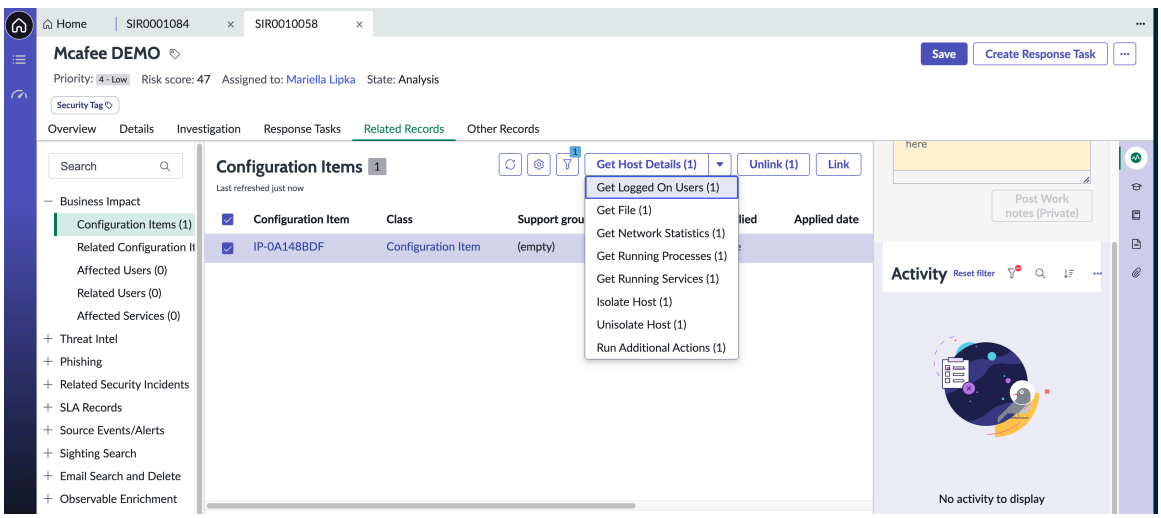
You can use the McAfee ePO integration to make remediation actions on the endpoints in real time, use profiles to gather details about the host, and make specific queries or actions on the endpoint using the Security Incident Response workspace.

The McAfee ePO integration enables analysts to use the following McAfee ePO capabilities on the Security Incident Response Analyst workspace:

- **Get Host Details**
- **Isolate Host**
- **Remove Isolation**
- **Run Additional Action(s) on Endpoint**

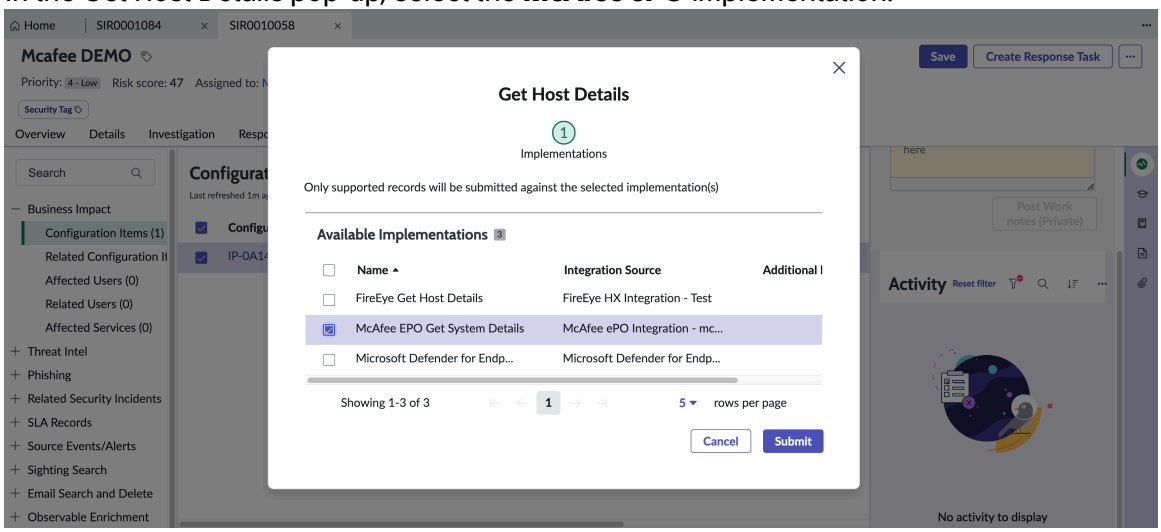
Procedure

1. To open the security incident in the SIR workspace, click **Switch to SIR Workspace** on the security incident.
2. In the SIR workspace, select the **Related Records** tab.
3. Select any **Configuration Item**, and choose a McAfee ePO capability to trigger from the related list drop down action.
   For example, Get Host Details.

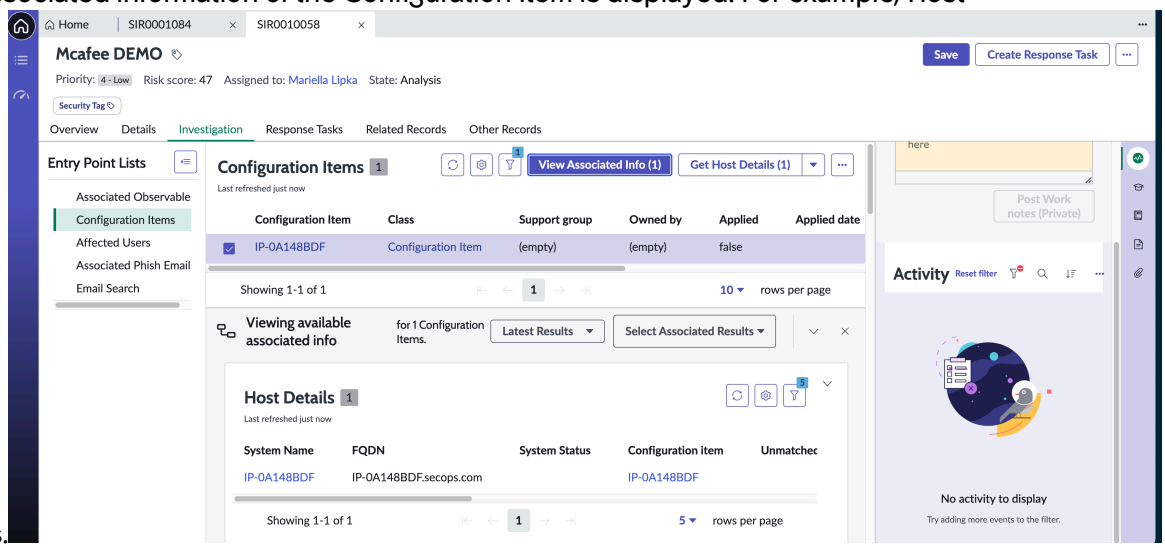


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the Get Host Details pop-up, select the **McAfee ePO** implementation.



5. Click **Submit**.
   The Get Host Details capability is invoked on the CI. You can view the worknotes for the results and findings.
6. To view the data for the triggered capability, select the **Investigation** tab.
7. Select the **Configuration Item**, and click the **View Associated Info** action.
   The Associated information of the Configuration Item is displayed. For example, Host Details.



8. Click the **Configuration Item** to view the host details.
   Similarly, you can try using the other McAfee ePO capability for you security incidents on the SIR Analyst Workspace.
9. You can use the McAfee ePO capabilities on the **Endpoint Detection and Reponse (EDR)** related list for analysis.
10. Browse and select a profile from the list of available profiles.
    The list of available profiles are Get Host Details, Isolate Host machine, and Remove Isolation. For example, let's select Get Host Details.
11. Select the **McAfee ePO** implementation, and click **Submit**.

McAfee ESM - Email Parser integration

The ESM - Email Parser integration is supported by an email parser that consumes email notifications from ESM to create security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure McAfee ESM - Email Parser integration

McAfee ESM - Email Parser integration uses email notifications from ESM to drive enrichment, and response workflows.

Before you begin

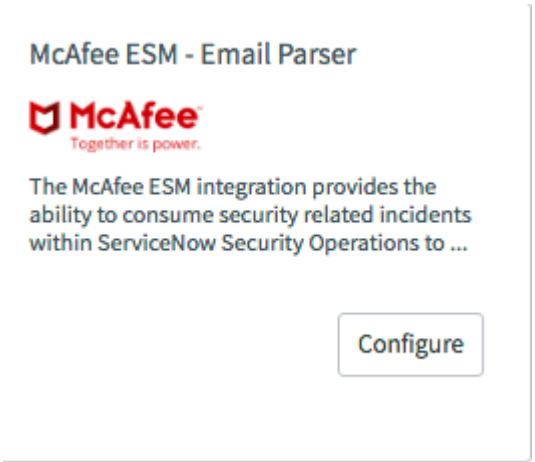
Role required: sn_si_admin

About this task

A McAfee ESM email parser template is provided to use for the integration. It must be configured and activated before the integration takes place. Updating the parser activates it.

Procedure

1. Navigate to **All** > **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.



2. In the McAfee ESM - Email Parser card, click **Configure**.
3. In the **McAfee ESM - Email Parser Configuration** dialog box, click the **Configure Email Parser** link.
4. Click the **McAfee ESM** link to edit the settings in the template email parser provided.
   At a minimum, fill in the `Email is from` field. To create you own email parser, see Create email parsers in Security Operations.
5. Check the **Active** box.
6. Click **Update** in the **Email Parser** form.
   The email parser is active. You do not need to return to **Integration Configurations**.

McAfee ESM - Incident Enrichment Integration

McAfee ESM - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

Explore **Set up**

Security Incident Response integrations

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Get started with the McAfee ESM - Incident Enrichment integration
- Create sightings search configuration records

Use

- Run a Sightings Search
- Security Operations Integration - Sightings Search Flow
- Security Operations - McAfee ESM Sightings Search Flow
- View Sightings Search Details
- View Sightings Search Results

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Get started with the McAfee ESM - Incident Enrichment integration

McAfee ESM protects endpoints against viruses, spyware, Trojan horses, and other malware threats and integrates easily with Security Operations. Before you can use the McAfee ESM - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.

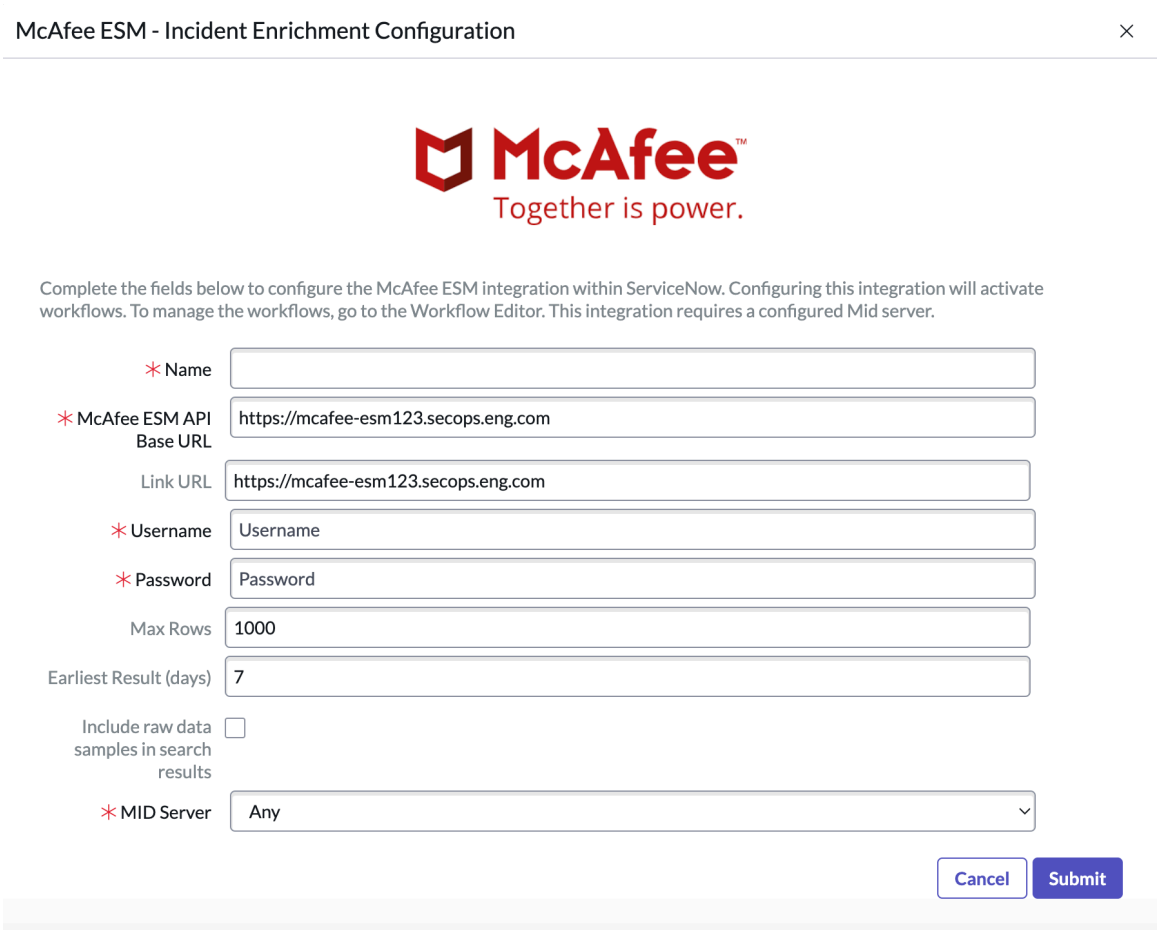
Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations** > **Integrations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
3. In the McAfee ESM - Incident Enrichment card, click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.
McAfee ESM API Base URL	The base URL you acquired from the McAfee ESM site.
Link URL	[Optional] The Link URL that links to an McAfee ESM instance, when available. **Note:** If you're getting an error, please use the McAfee ESM API Base URL.
Username	Your McAfee ESM username.
Password	Your McAfee ESM password.
Max Rows	The maximum number of rows you want to search.
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

5. Click **Submit**.
   The integration configuration card displays.
6. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Microsoft Azure Sentinel integration

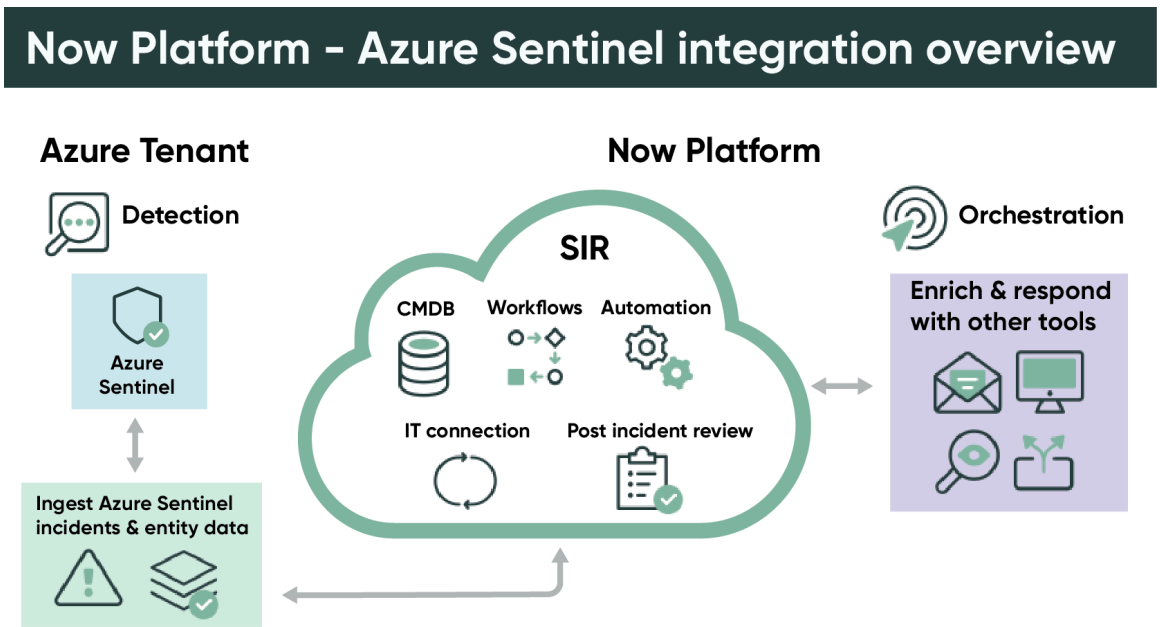
Microsoft Azure Sentinel is a cloud-based Security Information Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution. You can use the Microsoft Azure Sentinel integration to ingest Azure Sentinel incidents and automatically create security incidents in Security Incident Response.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview of Microsoft Azure Sentinel integration

See the following diagram to learn how Microsoft Azure Sentinel integrates with the ServiceNow AI Platform Security Operations applications.



Key features

Use the key features of this integration to do the following actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Discover Microsoft Azure Sentinel incidents that are candidates for security incidents and automate the creation of these security incidents.
- Map Microsoft Azure Sentinel incident and entity fields to SIR security incident fields.
- Filter Microsoft Azure Sentinel incidents.
- Aggregate incidents to existing open security incidents so that you don't have to create duplicate security incidents.
- Automate Microsoft Azure Sentinel incident status updates for Security Incident Response so that you can create and close security incidents.

> **Note:** ServiceNow updates the status of Microsoft Azure Sentinel incidents based on the security incident creation or closure. This update also includes comments of aggregated incidents and new incidents.

- Schedule incident ingestion to create security incidents periodically.
- Synchronize Microsoft Azure Sentinel incident comments with SIR Work notes.

Learn about this integration

Document identifier	Document title
Microsoft product documentation website	Microsoft Product Documentation website
ServiceNow product documentation website	ServiceNow Product Documentation website

Get started with Microsoft Azure Sentinel integration

Activate and set up the Microsoft Azure Sentinel - Incident Ingestion for Security Operation plug-in to interface with your ServiceNow AI Platform instance and Security Incident Response product.

Before you can use the Microsoft Azure Sentinel integration, you must download it from the ServiceNow Store.

Role required: Microsoft Azure application developer, Microsoft Azure tenant administrator.

Review the following setup checklist and verify that you've completed all the tasks for a smooth integration.

Checklist

Setup task	Description

Assign and verify the required ServiceNow AI Platform and Security Incident Response roles.	The following roles are required for configuration and verification of the expected results:
	• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.ingestion_profile_admin role.
	• The sn_si.ingestion_profile_admin role performs the following tasks:
	  ○ Configures the integration.
	  ○ Creates incident profiles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	○ Maps the Microsoft Azure Sentinel incident data fields to the security incident fields. ○ Schedules on-going incident ingestion. ○ Enables incident updates when a Security Incident Response incident is created or closed. ○ Assigns the security incident analyst (sn_si.analyst) role.
Assign the Microsoft Azure required roles.	The following roles are required in Microsoft Azure to register and configure your application: • Application developer for registering the application. • Tenant administrator for giving permissions to the application by calling the admin consent endpoint.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration.	The ServiceNow Integration Hub Starter Pack Installer [com.glide.hub.integrations] plugin is required. The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications that are required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications aren't already installed, you must install, and activate each application one at a time in the following order to ensure a smooth installation: **1.** Security Incident Response **2.** Security Incident Response UI **3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
Register and configure your application in the Microsoft Azure portal.	Register your application in the Microsoft Azure portal and grant your users with read and write access to the application.

Register and configure the Microsoft Azure portal

Register your application in the Microsoft Azure portal and grant your users with read and write access to the application.

Before you begin

Role required: Microsoft Azure application developer, Microsoft Azure tenant administrator

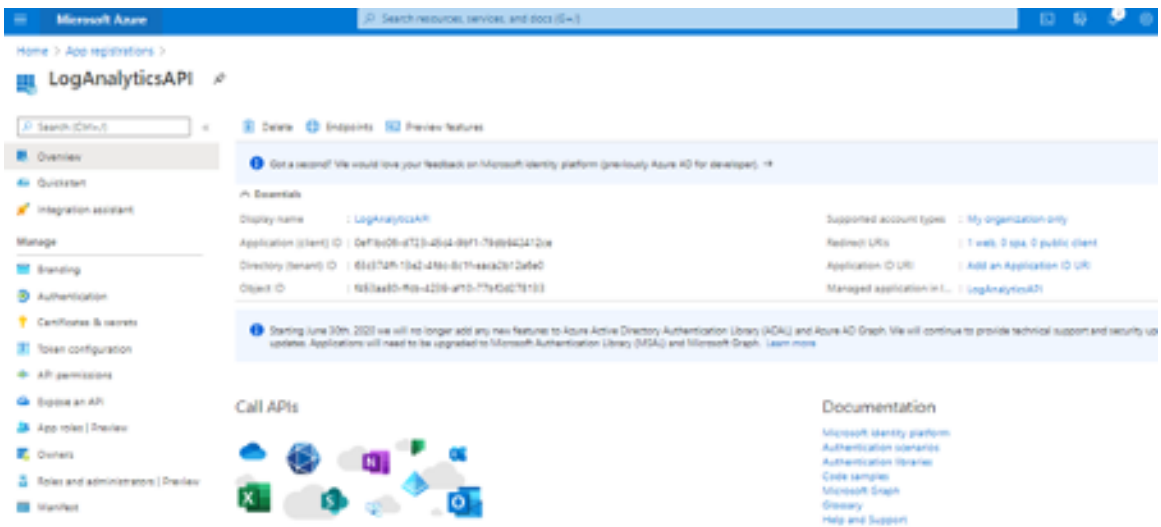
Procedure

1. Sign in to the Microsoft Azure portal.
2. Search for and select **App registrations**.
3. Click **New registration**.
4. On the form, fill in the fields.

Register an application form

Field	Description
Name	User-facing display name for the application. For example, LogAnalyticsAPI.
Supported account types	Account type that can use this application or access the API.
Redirect URI	Redirect URI. The authentication response is directed to this URI after successfully authenticating a user.

5. Click **Register**.
   After you successfully register the application, you see the Overview page.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Navigate to **Manage** > **Certificates & secrets**.
7. In the Client secrets section, click **New client secret**.
   You can't view the client secret later, so make sure that you copy and save the client secret now at this step. If you forget the client secret, you can generate a new one by following the instructions in steps 4 and 5.
8. Navigate to **Manage** > **API permissions**.
9. Click **Add a permission**.
10. In the Request API permissions window, click the **APIs my organization uses** tab.
11. Search and select **Log Analytics API** app name.
12. In the Log Analytics API permissions, select **Application permissions**.
    Enabling this permission ensures that the application runs as a background service or daemon without a signed-in user.
13. Under the Data section, select **Data.Read**
14. Click **Add Permissions**.
    The permissions are updated.
15. Enable the **Grant admin consent for Default Directory** option for the Data.Read API permission that you enabled in step 13.
16. Search for and select **Log Analytics workspaces**.
17. Select your Sentinel Log Analytics workspace.
    You now see the Sentinel Log Analytics workspace Overview page.
18. Navigate to **Access control (IAM)** > **Role assignments**.
19. Click **Add**, and select **Add role assignment**.
20. On the form, fill in the fields.

Add role assignment form

Field	Description
Role	Account type that can use this application. Select **Azure Sentinel Responder**.
Assign access to	Permissions scope that you define. Select **User**, **group**, or **service principal**.
Select	Application that you created earlier in step 4. For example, LogAnalyticsAPI.

21. Click **Save**.

Install and configure the Microsoft Azure Sentinel integration

Install and configure the Microsoft Azure Sentinel integration from the ServiceNow Store on your ServiceNow AI Platform instance to start ingesting Azure Sentinel incidents.

Before you begin
Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Download the Microsoft Azure Sentinel integration from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the Microsoft Azure Sentinel tile and click **Configure**.
4. On the form, fill in the fields.

Microsoft Azure Sentinel - Incident Ingestion Configuration form

Field	Description
Name	Name for the Microsoft Azure Cloud instance configuration.
Identity URL	Identity URL for the Microsoft Azure Cloud tenant. For example, `login.microsoftonline.com`. For additional information, see Microsoft Azure documentation.
Azure Resource Manager	Azure Resource Manager Endpoint for Microsoft Azure Cloud tenant. For example, `management.azure.com`. For additional information, see Microsoft Azure documentation.
Tenant ID	Microsoft Azure Sentinel Tenant ID. This is the instance from which all the incidents in the Microsoft Azure portal are retrieved.
Client ID	Client ID for the application that you've registered in the Microsoft Azure portal.
Client Secret	Client secret for your registered application.
Subscription ID	Subscription ID for your registered application.
Resource Group Name	Resource group name for your registered application.
Workspace Name	Workspace name for your registered application.

5. Click **Submit**.

Result

After you successfully validate and submit the configuration, each incident ingestion server configuration is saved on the Security Integrations page as a tile.

Create a profile for Microsoft Azure Sentinel

Create an incident profile in your ServiceNow AI Platform instance and determine the Microsoft Azure Sentinel incidents that are suitable for creating security incidents.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The integration enables you to create different types of incidents, such as unauthorized access attempts and malware. These incidents are created based on the profiles that you configure in the ServiceNow AI Platform instance. All incidents are initially created for a configured incident type in a profile. Created incidents can then be further filtered to specify which incidents create security incidents.

All incidents that meet the selection criteria in your Microsoft Azure tenant, and are available over the Microsoft Azure Sentinel API, are initially ingested into your ServiceNow AI Platform instance.

Procedure

1. Navigate to **All** > **Microsoft Azure Sentinel Integration** > **Azure Sentinel Incident Profile**.
2. Click **New**.
3. On the form, fill in the fields.

Microsoft Azure Sentinel - Incident Ingestion Configuration form

Field	Description
Name	Name for the profile. This name helps you to identify the profile type and is also the default name for the security tag that is associated with this profile.
Active	Indicator that the profile is active. When the profile is active, it implies that the ServiceNow AI Platform is actively polling Azure Sentinel incidents and that corresponding security incidents are created in SIR when the filtering conditions are matched.
Source	Microsoft Azure tenant that you configured to ingest incidents. If you have multiple tenants configured, select the appropriate tenant for the incident types that you are planning to ingest for the profile.
Order	Flow priority. The value for this field indicates the order that flows are executed when two or more profiles share triggering conditions. The flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400. The default is 100.
Description	Extra text to help you distinguish this profile from other profiles.

4. To move to the Mapping section, click **Continue**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Map individual Microsoft Azure Sentinel incident fields to the fields on the ServiceNow AI Platform SIR security incident.

Map the Microsoft Azure Sentinel incident fields

Map the individual Microsoft Azure Sentinel incident fields to the fields on the SIR security incident so that you can create incidents with the mapped data.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

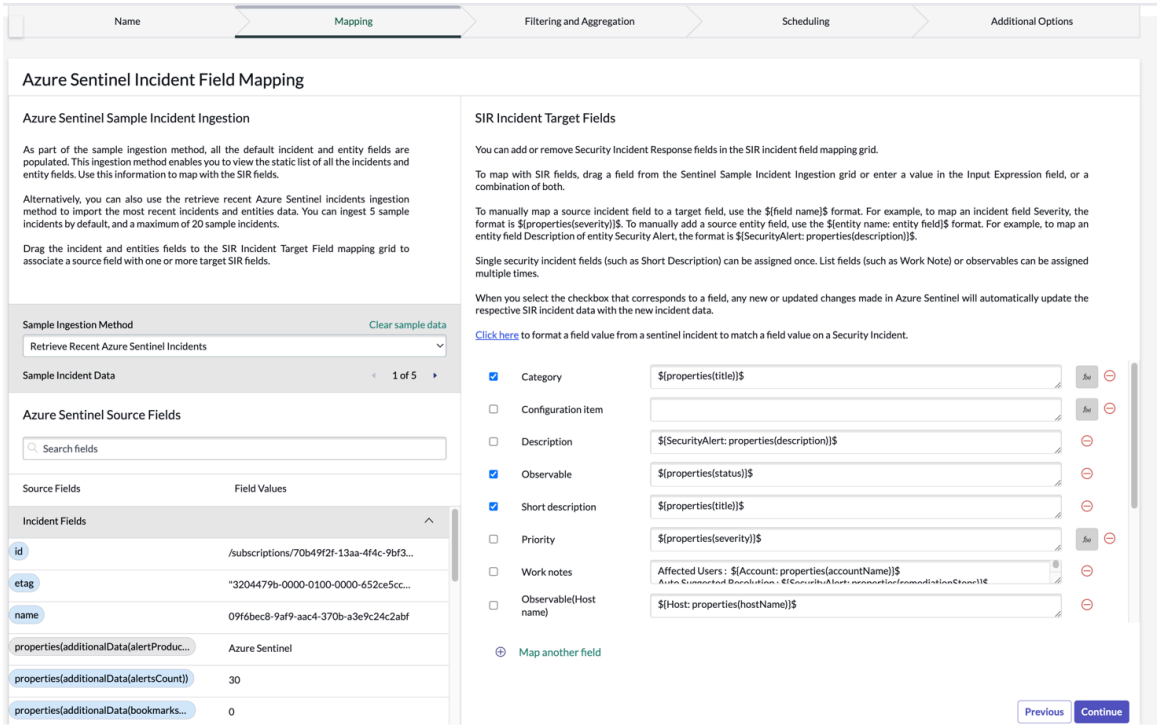
1. On the mapping page, in the Azure Sentinel Field Mapping section, select one of the Sample Ingestion Methods.

Sample Ingestion Methods

Field	Description
All default Incident and entity fields	Use this ingestion method to view the static list of all the incidents and entity fields. This method contains only default field names without any values. You can use this information to map with the SIR fields.
Retrieve Recent Azure Sentinel incidents	Use this ingestion method to import the most recent incidents and entities data. If the Azure Sentinel incident contains the entity data, then the entity data is retrieved and it is available for mapping in the Azure Sentinel Source Fields section. Sometimes the Azure Sentinel incident may not contain the entity data, and hence the entity fields are not available for mapping in such a scenario. If the Azure Sentinel incident contains multiple alerts, the earliest alert that is part of the incident is shown in the mapping section. During ingestion as well the earliest security alert field values will be used. You can ingest 5 sample incidents by default and a maximum of 20 sample incidents. The sample incident field values populate when the profile ingests the sample incidents. You can map these incidents to the **SIR Incident Target Fields**. The incident fields and values appear as individual tabs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Import Sample Data	Click **Import Sample Data** to import sample incidents from Azure Sentinel. This button appears when you select the Retrieve Recent Azure Sentinel incidents ingestion method. Retrieving sample incidents from Microsoft Azure Sentinel server may take a moment. Map these retrieved incidents to the **SIR Incident Target Fields**. The incident fields and values appear as individual tabs.



2. To add fields to the default fields that are displayed on the security incident, do the following actions:

   a. On the SIR Incident Target Fields section, click the 

   Map another field button.
   It shows a list of SIR fields, from which you can select a field for a new field to be displayed.

   b. In the Security Incident column, expand the list that is displayed and then select a field.

   Note: Multiple observables can be displayed on the same security incident. For example, the **Observable** field can be mapped multiple times with different values. Similarly, the **Configuration Item** and **Work notes fields** support multiple values. If you try to map two values to a field that can't support multiple values, you see an error message that this field does not support multiple values. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field does not populate on the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. From the Azure Sentinel Source Fields section, drag and drop your field to map it to your new field.

d. When you select the checkbox that corresponds to a field, any new or updated changes made in Azure Sentinel will automatically update the respective SIR incident data with the new incident data.

Note: In the base system, the system property sn_sec_sentinel.incident_updates is by default set to True to receive the Microsoft Azure Sentinel updates related to new alerts that are linked to SIR.

- By default, the Affected Users, Configuration items, and Observables fields are checked. This means that whenever there are new observables or associated configuration items, or affected users that gets added to the incident then that information is automatically extracted and populated in the respective related lists in the Security Incident Response (SIR) during that polling interval.
- For any other fields, you must select the checkbox that corresponds to a field for any new or updated changes made in the Azure Sentinel incident record within Azure Sentinel. This will automatically update the respective SIR incident data with the new incident data.

Important: Due diligence is required to be done before selecting this functionality as overriding the existing data may result in unstable data for the analyst to work with and any other automation that is set even by the field values of security incident may also get affected. So, it is very important to do the due diligence before you select any override functionality.

3. To remove a field, use the Remove item button next to the input expression field in the SIR Incident Target Fields section.
4. To map a field value from the Azure Sentinel Source Fields section to a field on the SIR Incident Target Fields section, use one of the following actions:

a. Drag the field name (for example, id) and drop it next to a field name in the SIR Incident Target Fields column.

You can match any value from the Azure Sentinel Source Fields section to a field on the SIR Incident Target Fields section. Fields are color-coded so that you do not overlook or duplicate incident fields in the mapping process. Light blue fields indicate that an incident field is not yet selected and mapped on the security incident. You may prefer to associate an incoming incident field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This way, you can visualize which field values have been added to the security incident and if any remaining important incident information remains unmapped.

b. You can add a combination of text and field.
For example, `Incident name is ${name}$`. Here `Incident name is` can be manually entered while `${name}$` is mapped from the Azure Sentinel Source Fields section.

c. You can directly manually enter and map a source incident or entity field to a target field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To manually map a source incident field use the ${field name}$ format. For example, to map an incident field Severity, the format is`${properties(severity)}$`.
- To manually add a source entity field, use the `${entity name: entity field}$` format. For example, to map an entity field Description of entity Security Alert, the format is `${SecurityAlert: properties(description)}$`.

This integration classifies certain observable sub-types. When you map an Azure Sentinel field with the SIR observable field, the ServiceNow AI Platform auto-classifies the observable. If you want to generically map the incoming Azure Sentinel observable to the observable type in SIR, then drag and drop the Azure Sentinel field in the Observable field. However, if you aware of the observable type for the incoming Azure Sentinel observable in SIR, then map specifically to the SIR Observable type field. Some examples of specific observable types in SIR include Observable(Domain name), Observable(Email address), Observable(IP address (V4)), and Observable(Host name).

If your incoming Azure Sentinel fields contain any MITRE-ATT&CK information, then map it to the MITRE-ATT&CK Technique field. Ensure that the incoming Azure Sentinel field contains the MITRE-ATT&CK technique ID or technique name.

Sometimes, incident field values in Microsoft Azure Sentinel may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

5. To format a field translation for a new field from an Azure sentinel incident to match a field value on a Security Incident, click the **Click here** link in the **SIR Incident Target Fields** header.
6. To modify the fields which support field translation, click the  script format field translation icon.
   The fields that support field translation are **Category**, **Configuration Item**, and **Priority**. For example, click on  icon next to the Category. The Azure Sentinel Field Translation script editor opens.
7. Enter any changes to the script and click **Update** to save the changes and return to the Mapping page.
   For example, for Category define the following in the script editor:

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to
    assign to the Security Incident>".
   ```

   This mapping ensures that a profile uses only configured categories.
8. Continue your mapping by adding or removing field values.
   You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming incident must satisfy to create a security incident.
9. To move to the Filtering and Aggregation section, click **Continue**.

What to do next

Define and set filter conditions so that you can specify which incidents should create security incidents. You can use the same field values (defined in the Mapping section) in the Incident Generation Conditions builder (in the Filtering and Aggregation section) to define additional criteria that an incoming incident must satisfy to create a security incident.

Defining filter and aggregation criteria

You can define and set filter conditions so that you can specify which incoming Microsoft Azure Sentinel incidents should create security incidents. You can also define additional incident field

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

criteria that allows an incoming incident to be appended to an open security incident instead of creating an incident.

Set the filtering conditions for security incidents

Set the filtering conditions so that security incidents are created only when the filtering conditions match.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

This type of filtering helps you to isolate security incidents and limits the number of security incidents that you create. If you set additional filtering criteria, only the required incidents are ingested without having to change the query or the triggered incident configuration.

Procedure

1. To define the criteria that an incoming Microsoft Azure Sentinel incident must satisfy so that a security incident is created, select **Filter based on conditions**.

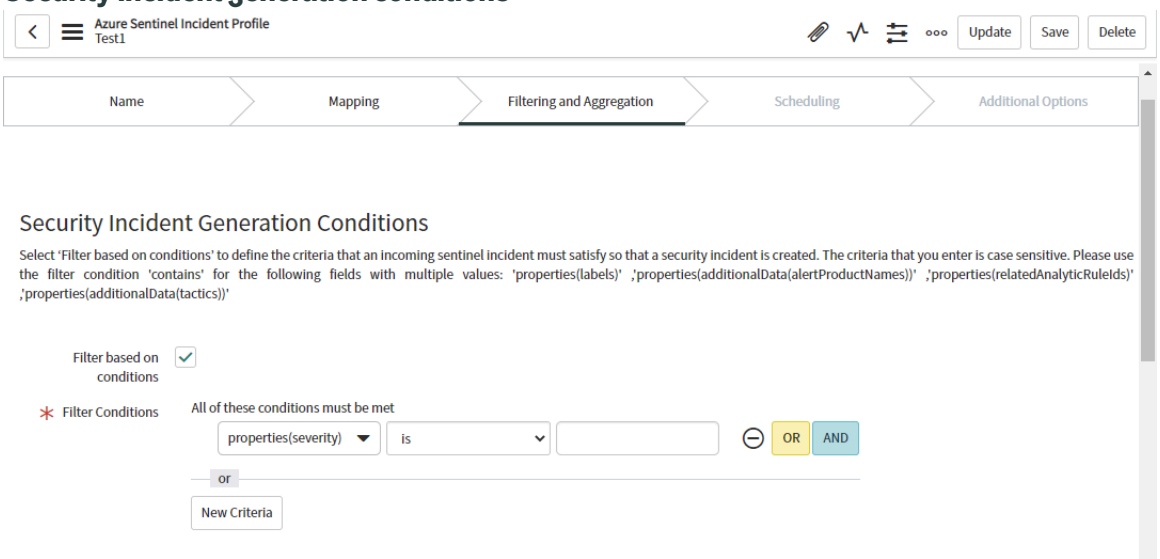
   The options in the first field in the Filter Conditions match the fields that are displayed on the Azure Sentinel Sample Incident Ingestion section for the incident that you ingested. These fields are dynamic and change depending on the incident that you ingest. The criteria that you enter is case-sensitive. Verify that the criteria that you define matches the values of the incident.

   Use the filter condition *`contains`* for the following fields with multiple values:

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   Because the filter condition can retrieve only strings, you must use the *`contains`* filter condition for the above fields to ensure that the data is filtered correctly.

Security incident generation conditions



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Using the lists and fields of the conditions builder, set the filters for the first row.
3. To add more conditions, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
4. To set a second filter condition, click **New Criteria**.

Define aggregation conditions

Define additional incident aggregation criteria that aggregates an incoming incident to an existing SIR security incident instead of creating similar, potentially duplicate incidents. When you use field matching value criteria for each profile, this additional aggregation can reduce the number of active, overlapping security incidents by placing all related incidents data on a single security incident.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

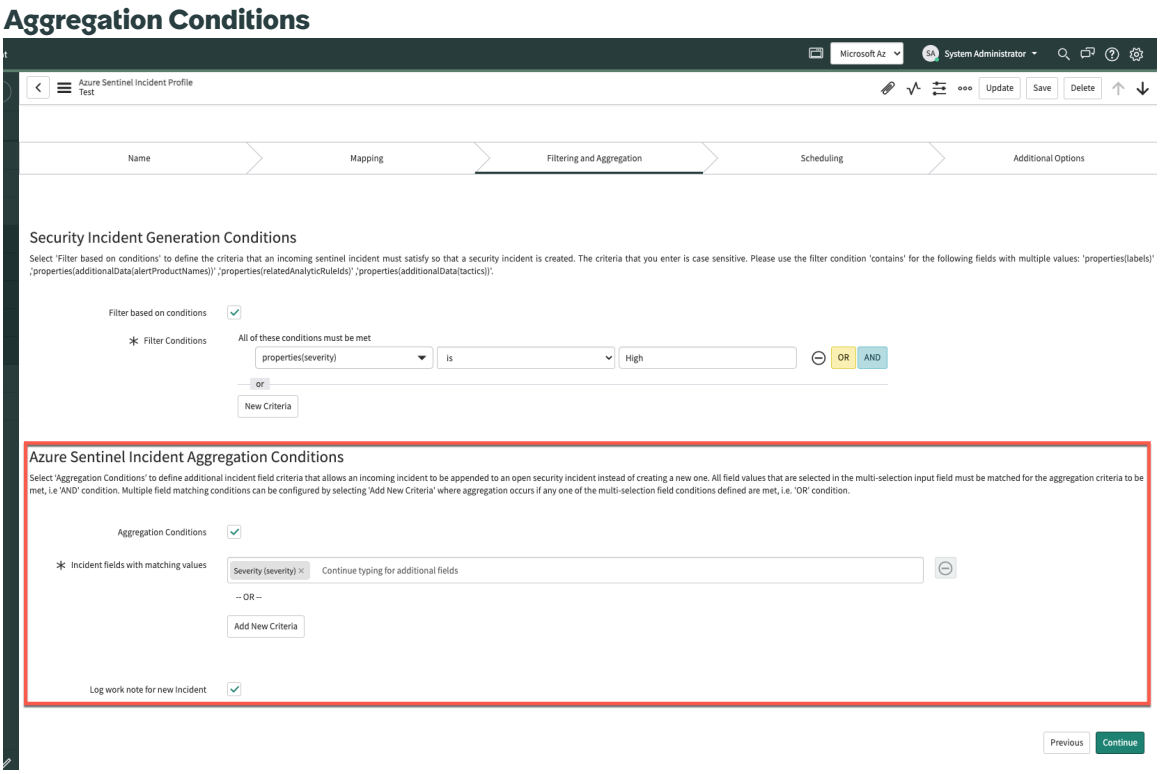
About this task

If a new incident matches all the values that are selected in the aggregation field conditions in the mapping step, the incident is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate incidents on a related list on a security incident. All the aggregated incidents on a security incident are displayed on the Azure Sentinel Aggregated Incidents related list. This list details the associated timestamps and aggregated field values. This information helps you understand why incidents are added to the existing security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To define additional incident field criteria that allows an incoming Microsoft Azure Sentinel incident to be appended to an open security incident instead of creating a new incident, select the **Aggregation Conditions** option as shown in the following figure.



2. In the **Incident fields with matching values** field, enter the field values that you want to match on existing security incidents in your ServiceNow AI Platform instance.
   All field values that you selected in the multi-selection input field must match so that the aggregation criteria is met and that this incoming incident can be appended to an existing security incident. This selection implies it is an *AND* condition where fields, such as Observables and Configuration Items that may have multiple field values, are mapped to them. If only a subset of the values is matched, the Azure Sentinel Incident aggregation conditions are not met and a new security incident is created.
3. To add multiple field matching conditions, click **Add New Criteria**
   The aggregation occurs if any one of the multi-selection field conditions that you define are met. This selection implies the *OR* condition.
4. To update the work note for a new incident when it is added to a security incident, select **Log work note for new Incident**.

   The work note logs that a new incident is added and includes a link to the incident details. The log work note also updates more details that you add to the work note field in your mapping section.

5. To configure the schedule, click **Continue**.

What to do next

Set a schedule to retrieve the incident data and ingested incidents that match the criteria in the profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Schedule the Microsoft Azure Sentinel incident retrieval

Set a schedule to retrieve the incident data and to ingest the Microsoft Azure Sentinel incidents that match the criteria in the profile.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

You can plan how often you want to poll for future Microsoft Azure Sentinel incidents that match the incident profile configuration.

To enable automated incident ingestion, you must configure the scheduling and incident retrieval before you activate the profile. To define a specific date and time for the initial ingestion, enable **set incident ingestion time**. Subsequent ingestion is based on the polling interval period.

The polling interval is configured for each profile individually. The different polling intervals may impact the performance of the Microsoft Azure Sentinel incident integration. When scheduling, plan to balance the system load against the urgency of an incident. A one-minute default value is set for all profiles. You can modify this setting based on the urgency of the incident and the anticipated load on your system.

Any alerts that gets added to the incident in a particular polling interval there will be a process executed and then appended to the Azure Sentinel alerts related lists and worknote is also posted.

Procedure

1. On the scheduling form, fill in the fields.

   Configure the schedule to define how and when you pull incidents from the Microsoft Azure tenant.

   Scheduling form

Field	Description
Ongoing incident ingestion	Ongoing incident ingestion that the ServiceNow AI Platform instance pulls from the Microsoft Azure tenant for new incidents. Security incidents are created if triggered incidents are found and the incident generation filtering criteria matches.
Polling increment (minutes)	Polling frequency that is defined in minutes.
Set incident ingestion time	Incident ingestion that is based on the configured date and time. You can use this option to define a specific date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.
Input incident ingestion time	Date and time that you specify for the incident ingestion.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
One-Time Retrieval	Select this checkbox to allow one-time retrieval of historical Azure Sentinel incidents and then do the reconciliation of the data. When you select this checkox, the application will pull all the open and closed Azure Sentinel incidents for the period upto 6 months approximately. When processing the data both ongoing incidents and historical data both are pulled, but the processing of the ongoing incidents takes precedence over historical pull and otherwise the historical pull may take some time based on the duration as well as the number of incidents that you are ingesting. **Note:** The retrieved historical Azure Sentinel incidents undergo de-duplication checks to prevent any duplicates within the Security Incident Response application.
Since date	The date since when the historical incidents are ingested from Azure Sentinel. **Note:** The incident data is approximately pulled from the past 6months.

The scheduling page enables you to define how and when incidents are pulled from the Microsoft Azure tenant.

2. To navigate to the Additional Options page, click **Continue**.

Automate the incident updates and closures by the SIR incident status

Automate the incident updates and closures by the SIR incident status. The Microsoft Azure Sentinel integration has a bi-directional interface that enables both incidents to create security incidents and to update the incidents after the security incident is created or closed.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

1. On the form, fill in the details.
   Follow the instructions to complete the configuration for updating incidents when you create or close a security incident in SIR.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Automating Incident Updates form

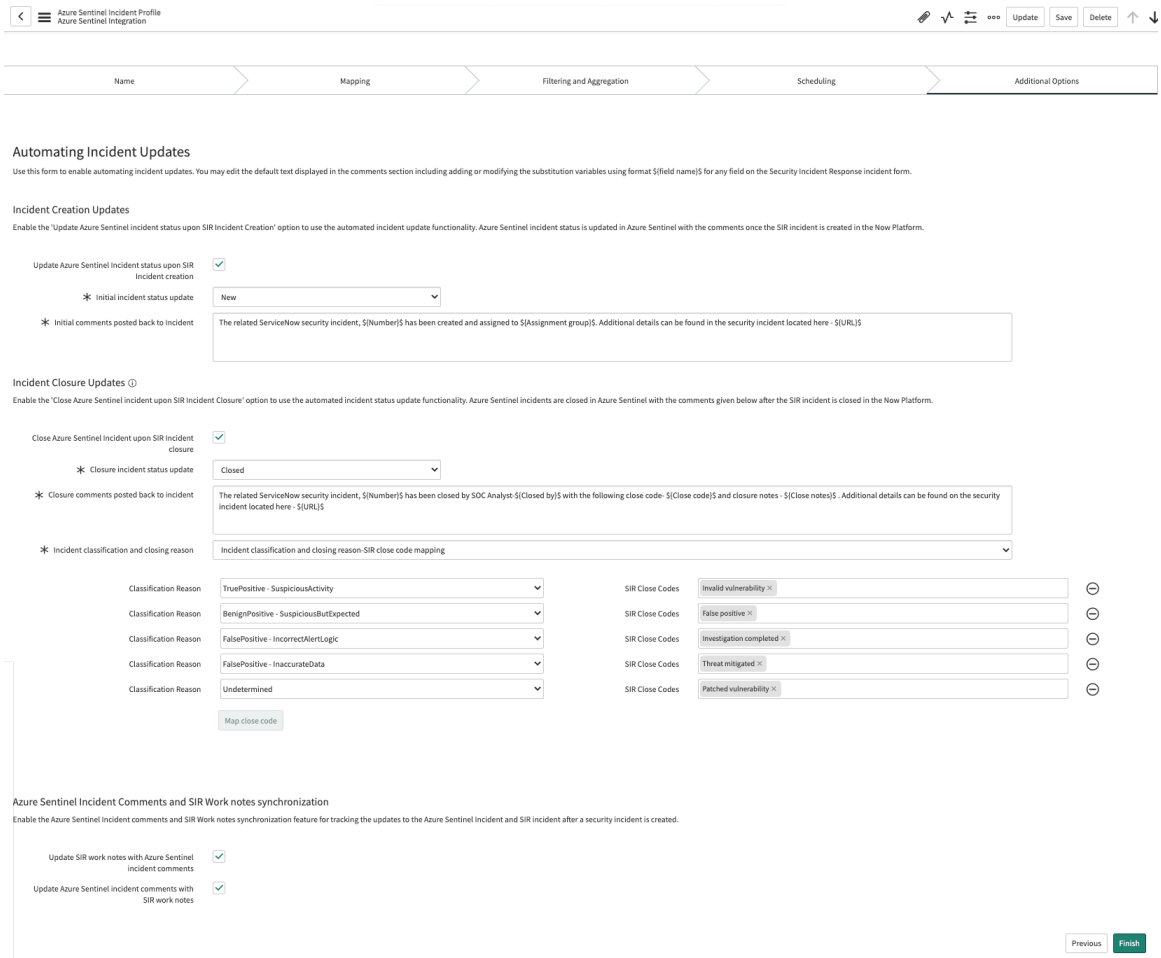
Category	Field	Description
Incident Creation Updates	Update Azure Sentinel Incidents Status upon SIR Incident creation	Option that enables you to use the automated incident update functionality. The Microsoft Azure Sentinel incident status is updated in Microsoft Azure incident with the comments after the SIR incident is created in the ServiceNow AI Platform.
	Initial incident status update	Initial incident status that is updated in the Microsoft Azure Sentinel environment. You can select **New** or **Active** as the status.
	Initial comments posted back to Incident	Initial comments that are posted to the incident in the Microsoft Azure Sentinel environment. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using the format ${field name}$ for any field on the SIR incident form.
Incident Closure Updates	Close Azure Sentinel incidents upon SIR Incident Closure	Option that enables you to use the automated incident status update functionality. Microsoft Azure Sentinel incidents are closed in the Microsoft Azure incident with the comments given after the SIR incident is closed in the ServiceNow AI Platform.
	Closure incident status update	Status update in the Microsoft Azure Sentinel incident when the incident is closed in SIR.
	Closure Comments Posted back to incident	Comments that are posted to the incident in the Microsoft Azure Sentinel incident when the incident is closed in SIR. Edit the default text that is displayed in the comments section by adding or modifying the substitution variables using the format ${field name}$ for any field on the SIR incident form.
	Incident classification and closing reason	Method for the incident classification and closing reason that is used to close the incident

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Category	Field	Description
		in the Microsoft Azure Sentinel environment. Select the **Default incident classification and closing reason** method to close the incident in the Microsoft Azure Sentinel environment. When you select this method, you must define the **Default incident classification and closing reason**. When you close an incident in SIR, the incident status in Azure Sentinel is also closed with the specified **Default incident classification and closing reason**. Select the **Incident classification and closing reason-SIR close code mapping** method to close the incidents and to map the classification reasons with the SIR close codes. You can map multiple SIR close codes to a single classification reason. After you close an incident in SIR using the close code, the incident status in Azure Sentinel is also closed with the mapped incident classification and closing reason. If the classification reason and SIR close codes are not mapped, or a match is not found, then the incident is closed using the default classification reason as 'Undetermined' in the Microsoft Azure Sentinel environment.
Azure Sentinel Incident Comments and SIR Work notes synchronization	Update SIR work notes with Azure Sentinel incident comments	Option that you can select to update your Microsoft Azure Sentinel comments in the SIR work notes. The comment in the SIR work notes appears with the prefix *`Comment from Sentinel`*. The comment also contains the Sentinel ID, Analyst details, and the Time stamp.
	Update Azure Sentinel incident comments with SIR work notes	Option that you can select to update your SIR work notes in the Microsoft Azure Sentinel incident comments. The comment in Microsoft Azure Sentinel appears with the prefix *`Comment from ServiceNow`*.

The following example shows the configuration options that are available for automating incident updates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Click **Finish**.

What to do next

The profile moves to the Waiting state. When the confirmation message shows that the setup and configuration is complete, you can activate the profile.

Copy a Microsoft Azure Sentinel profile

Copy an existing profile and its associated settings instead of creating a profile. When you create multiple profiles, you can reuse the settings of an existing profile by copying these profiles.

Before you begin

Role required: sn_si.ingestion_profile_admin

> **Note:** Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

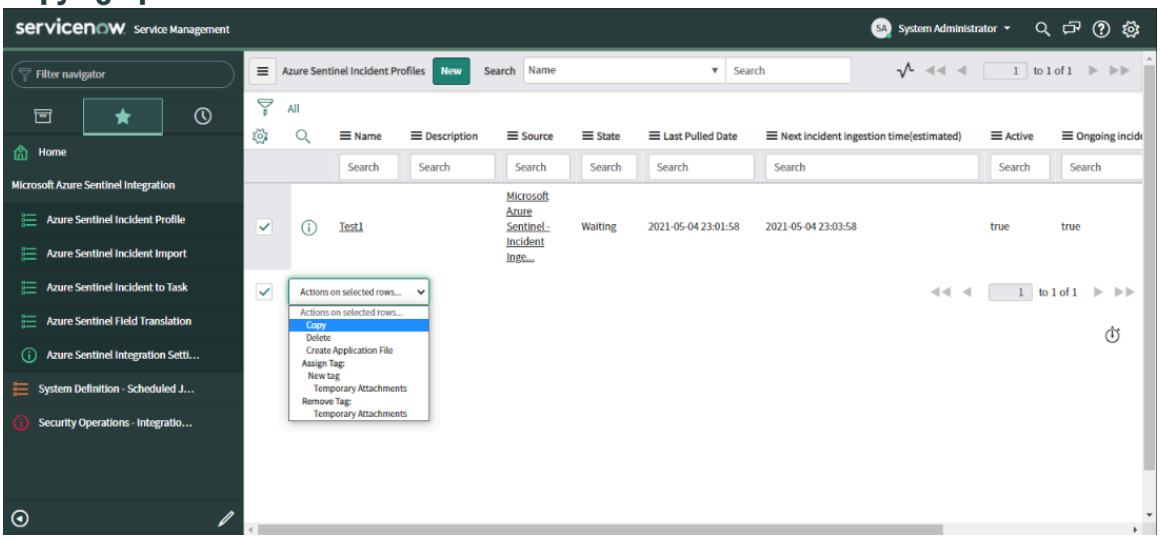
When you copy a profile, the profile name is initially modified to avoid creating duplicate profiles. The copied profile is also turned off (set to false) to ensure that you don't accidentally activate it before you complete the configuration. You can copy the profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure

1. Navigate to **All** > **Microsoft Azure Sentinel Integration** > **Azure Sentinel Profile**.
2. In the Azure Sentinel Profiles list, select a profile that you want to copy, and then from the Actions on selected rows list, click **Copy** as shown in the following example.

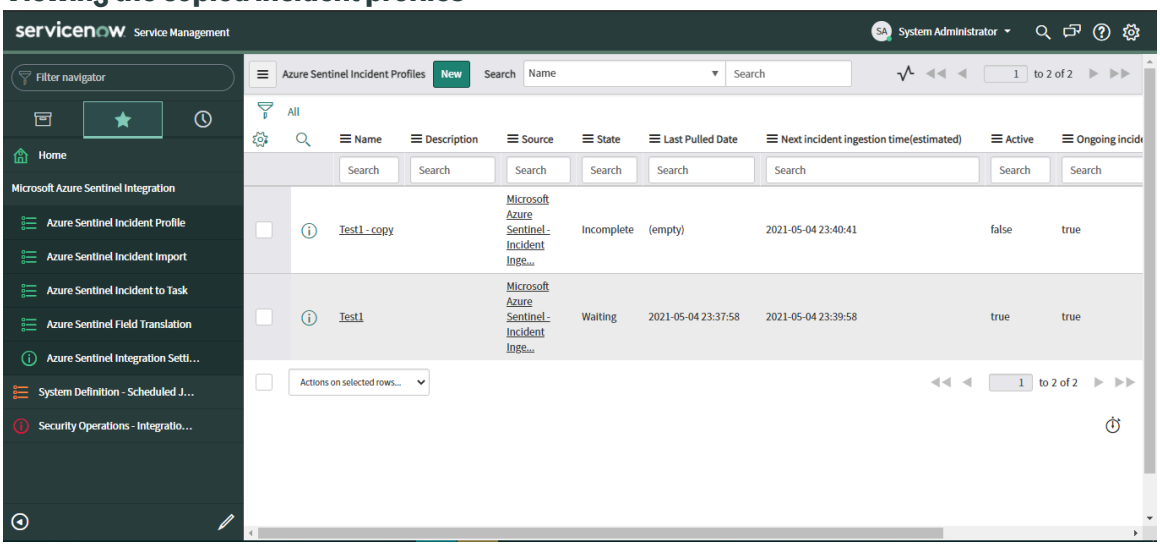
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Copying a profile



The profile is copied and displayed on the list as shown in the following example. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains the word "copy." Although the original profile is enabled (true), the copy is turned off at this point (false). You may prefer to edit values of the copied profile and rename them so that the configuration settings apply to the new profile as required.

Viewing the copied incident profiles



You have successfully copied the settings from an existing profile to a new profile. The Active column status is set to false, which means that the profile must be activated.

SIR form after an incident ingestion

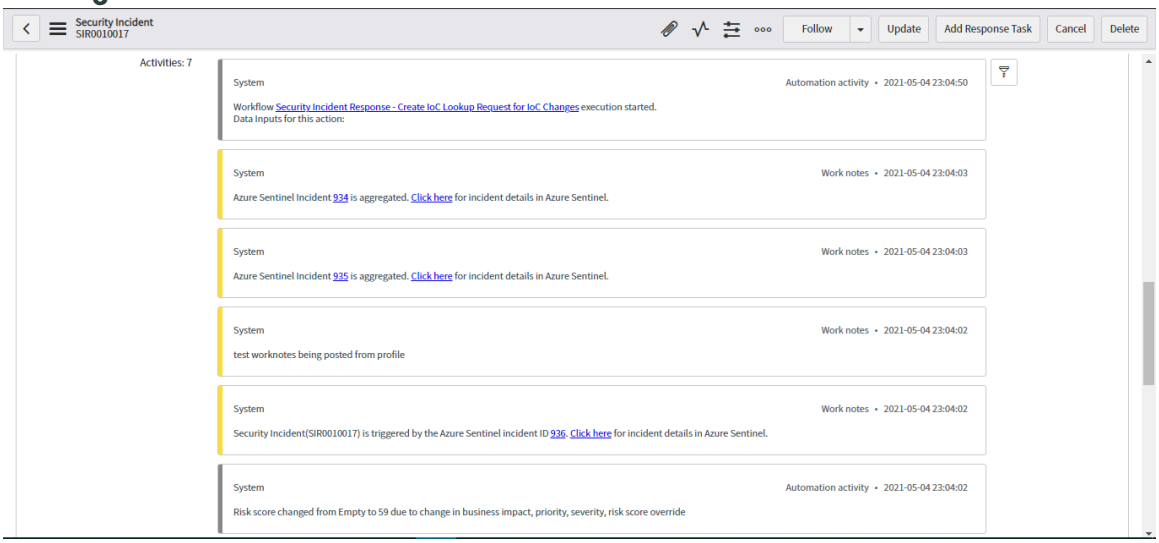
After the ServiceNow AI Platform ingests the Microsoft Azure Sentinel incident, a security incident is created and the updates are made to that security incident record.

Work notes

A work note is posted when an incident is aggregated and if you have configured the **Log work note for new incident** option in the Incident Aggregation Criteria. The following example shows the work notes in SIR.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing work notes in SIR



When you click the incident number, you can view the internal incident import record that contains the raw incident data. The following example shows the raw incident data in SIR.

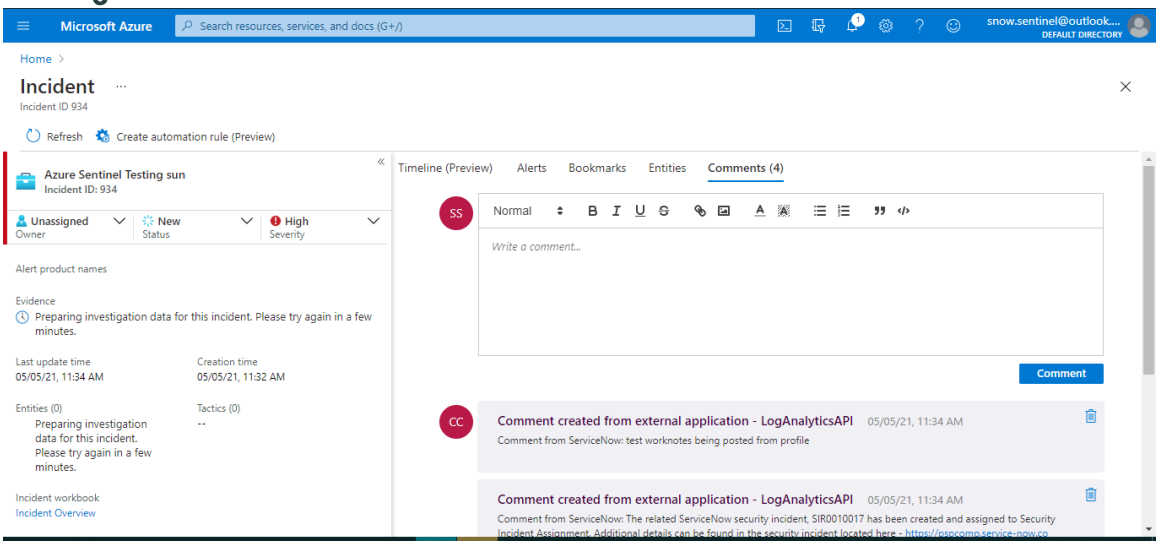
Viewing the incident raw data in SIR



When you click the **Click here** link, you can view the record in the Microsoft Azure Sentinel environment. The following example shows the record in the Microsoft Azure Sentinel environment.

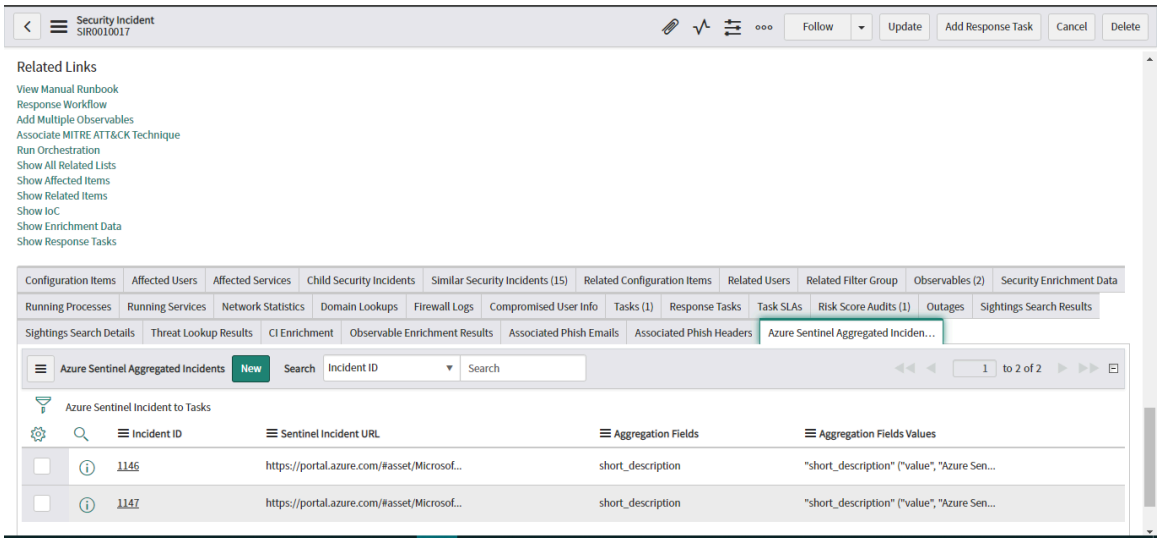
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing the incident record in Azure Sentinel



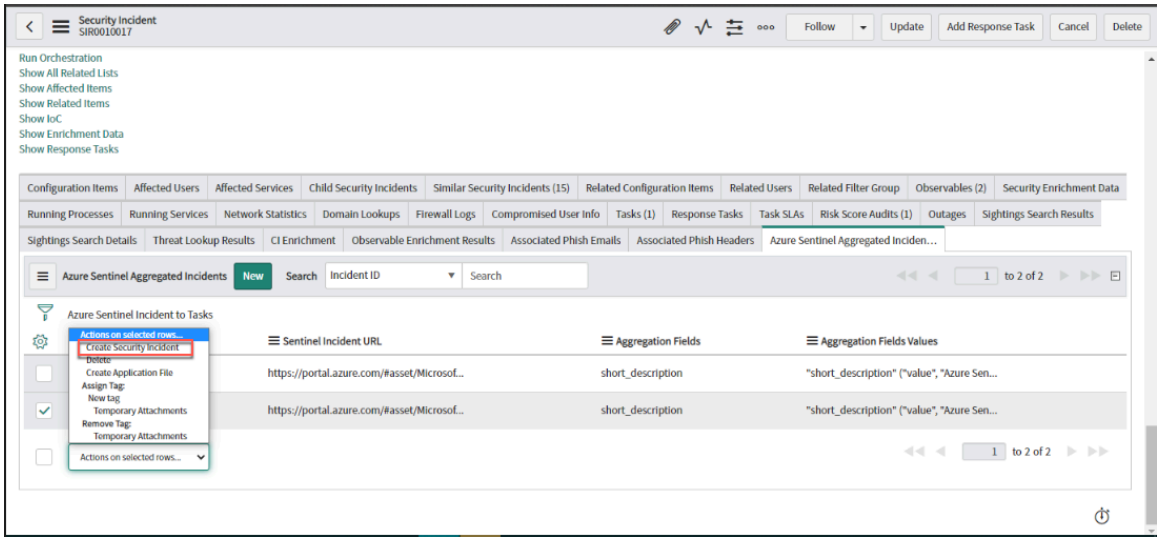
Aggregated Sentinel Incidents

View Aggregated Sentinel Incidents: View the incidents that are aggregated to the security incident. Navigate to **Show All Related Lists** > **Aggregated Microsoft Azure Sentinel incidents**.



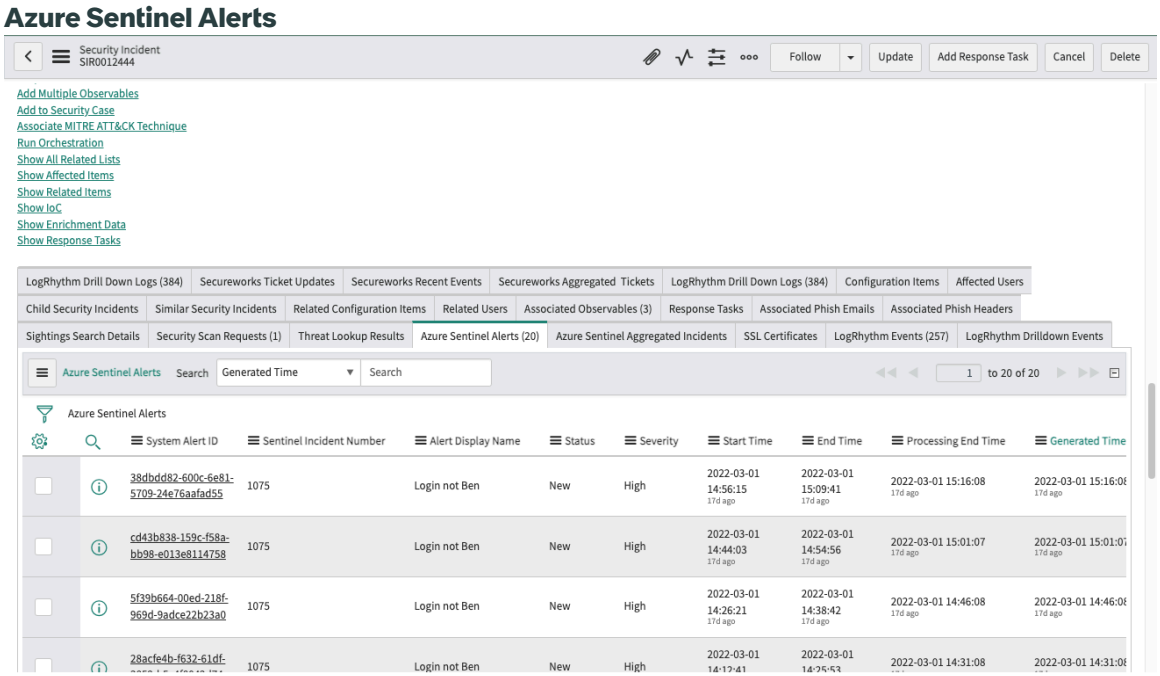
Create security incident: Select an incident from the list, click the **Actions** menu, and then click **Create security incident**. This option creates a new security incident for the incident and this incident is de-aggregated from the parent security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Azure Sentinel Alerts

To view the alerts that are associated with the Sentinel Incident that triggered the security incident, navigate to **Show All Related Lists** > **Azure Sentinel Alerts**.



Review the Microsoft Azure Sentinel integration settings

Review the Microsoft Azure Sentinel integration settings so that you can modify the system properties to suit your environment.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Microsoft Azure Sentinel Integration** > **Azure Sentinel Integration Settings**.
2. Modify the following settings as required.

Microsoft Azure Sentinel Integration Settings

Property Name	Description
Enforce a limit on the number of days for which sample data can be fetched. sn_sec_sentinel.max_num_of_days_for_sample_data	Maximum number of days for which you can fetch sample data from the Microsoft Azure Sentinel environment. Type: integer Default value: 7
Receive updates related to new alerts that are linked to SIR. sn_sec_sentinel.incident_updates	Activate the option to receive incident updates. Type: Boolean Default value: True
The delimiter character to split the values in Microsoft Azure Sentinel field mappings. sn_sec_sentinel.delimiter	The delimiter character to split the values in Microsoft Azure Sentinel field mappings. Type: String Default value: ', ' (comma with space)
Enforce a limit on the number of sample incidents that can be fetched. sn_sec_sentinel.max_num_of_sample_incidents_per_call	Maximum number of sample incidents that you fetch from the Microsoft Azure Sentinel environment for ingestion. Type: integer Default value: 5 Sample maximum value: 20
Enforce a limit on the number of sentinel incidents that can be aggregated to a single incident. sn_sec_sentinel.max_aggregations_per_si	Incident aggregation limit for a security incident. For example, if there are 102 incidents, the first 100 are aggregated to security incident_1 and the remaining 2 to security incident_2. Type: integer Default value: 100
Enforce a limit on the number of security incidents that can be created in a 24-hour period. sn_sec_sentinel.max_si_per_day	Maximum number of security incidents that can be created in a 24-hour period in the ServiceNow AI Platform. Type: integer Default value: 1000

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property Name	Description
Maximum pagination limit for fetching the incident data in one REST call. sn_sec_sentinel.max_page_size	Pagination limit for fetching the incident data in one REST call from the Microsoft Azure Sentinel environment. Type: integer Default value: 100
API version value for Incidents. sn_sec_sentinel.sentinel_security_incident_api_version	The Microsoft API version for retrieving Sentinel incidents. Default value: 2021-10-01
API version value for Alerts. sn_sec_sentinel.sentinel_security_alert_api_version	The Microsoft API version for retrieving Sentinel alerts. Default value: 2021-10-01
API version value for Entities. sn_sec_sentinel.sentinel_security_entities_api_version	The Microsoft API version for retrieving Sentinel entities. Default value: 2021-10-01
sn_sec_sentinel.logging.verbosity	The log verbosity level of the application, meaning the name of the type of information. You can also update the value to the following options: ○ **error** ○ **warn** ○ **info** ○ **debug** Default value: **info**.

3. Click **Save**.
   Your modified integration settings are applied in the next polling interval as defined in the profile.

Domain separation

Domain separation is supported for this application. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

How domain separation works in the Microsoft Azure Sentinel integration

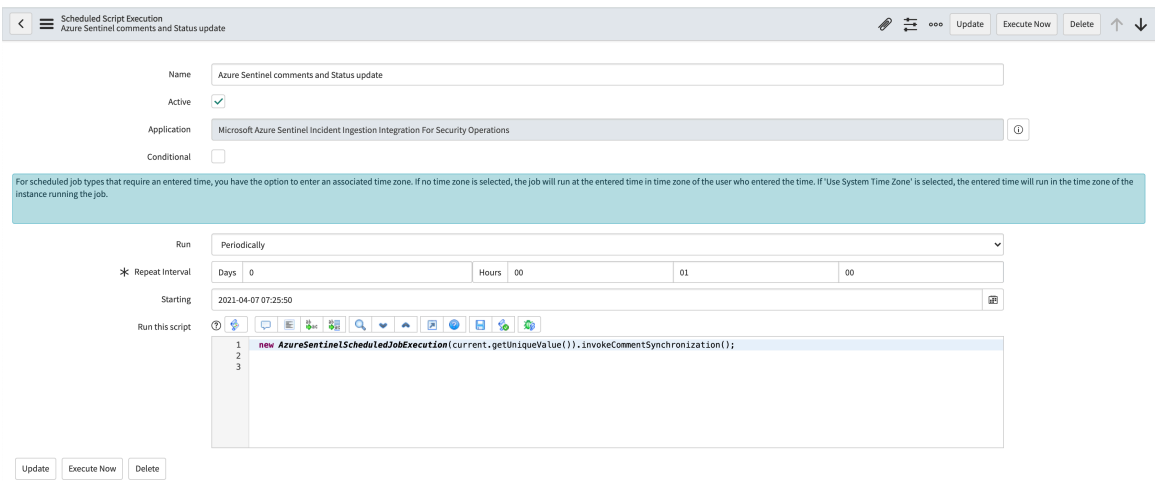
Follow these steps to achieve domain separation:

- Create a user with the sn_si.admin role in the respective domain.

  Note: When you create the profile, use the domain picker to select a domain. Do not create the user in the parent domain and later change the domain of the profile. You should have a user for each domain for your profile with the sn_si.admin role. Use this user to create or modify settings in the profile.

- Disable existing scheduled jobs.
- Replicate the following scheduled jobs for every domain:
  - Azure Sentinel Fetching Alerts & Entities
  - Azure Sentinel Comments Sync
  - Azure Sentinel Status Update
  - Azure Sentinel Profile Process
  - Azure Sentinel Process Raw Data
  - Azure Sentinel Data Cleanup
  - Azure Sentinel Historic Comment Pull
- Change the **Run as** from the system user to the user with the sn_si.admin role in the respective domain and then run the scheduled job.

The following example shows how to replicate the Azure Sentinel comments and Status update job and run the job as a system user.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Domain separation for service providers

Comparing Microsoft Azure Sentinel and Microsoft Graph Security API integrations with SIR

You can view the differences between Microsoft Azure Sentinel and Microsoft Graph Security API integrations and choose the right integration with your ServiceNow AI Platform instance.

Microsoft Azure Sentinel - Incident Ingestion overview

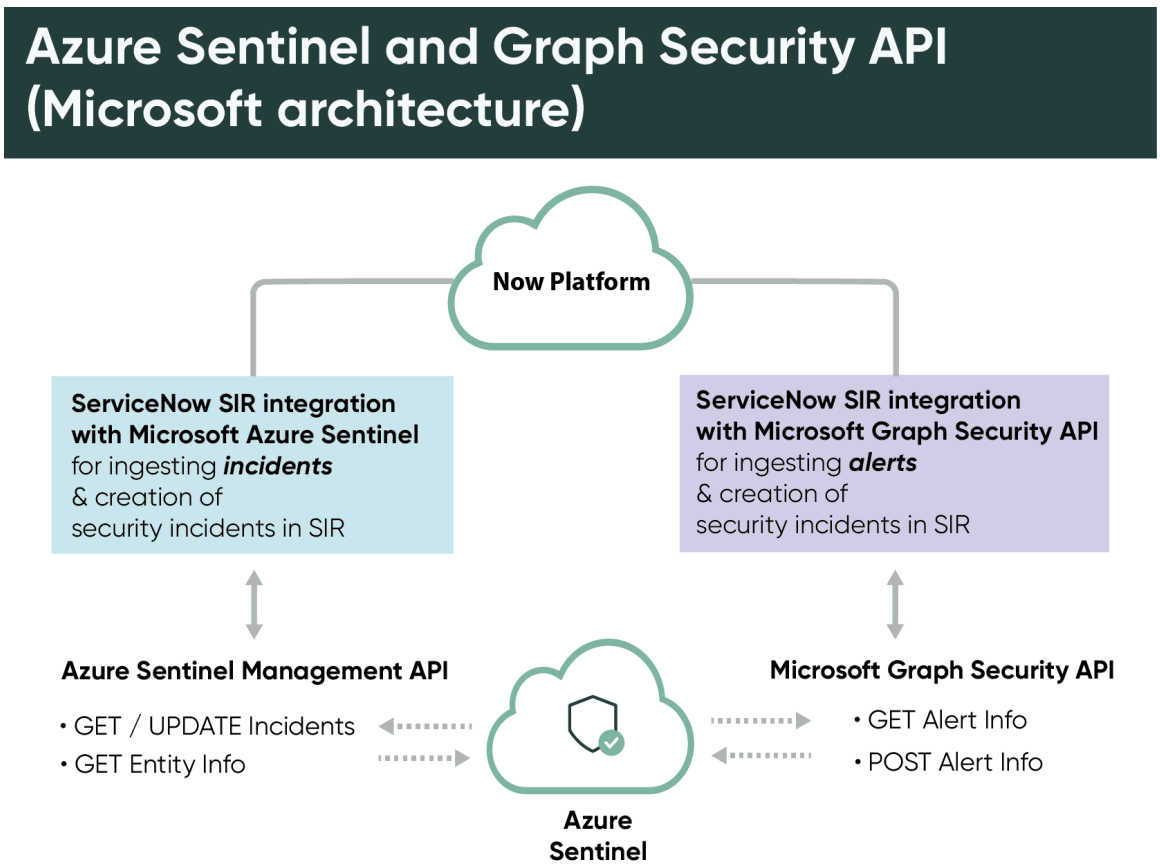
Microsoft Azure Sentinel is a cloud-based security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Microsoft Graph Security API overview

The Microsoft Graph Security API is an intermediary service (or broker) that provides a single programmatic interface for connecting multiple security providers (Native to Microsoft as well as ServiceNow Partners).

The Microsoft Graph Security API integration addresses these issues by using the Microsoft Graph Security API to connect with different Microsoft security technologies like Azure Sentinel, Microsoft Defender Advanced Threat Protection, and Azure Advanced Threat Protection. Alerts from Microsoft Security providers are ingested and security incidents are automatically created in Security Incident Response.

Summary of feature differences



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Microsoft Azure Sentinel vs Microsoft Graph Security API

Microsoft Azure Sentinel	Microsoft Graph Security API
Ingests Microsoft Azure Sentinel incidents along with entity information (when available) and automates security incident creation in SIR.	Ingests alerts from multiple Security providers (including Azure Sentinel) in a standard schema and automates security incident creation in SIR.
Automates Microsoft Azure Sentinel incident status updates for Security Incident Response so that you can create and close security incidents. **Note:** ServiceNow updates the status of Microsoft Azure Sentinel incidents based on the security incident creation or closure.	Supports alert updates (alert status change and alert closure) for selected security providers. **Note:** For more information on the Microsoft Graph Security API supported security providers, view the Microsoft documentation.
Use this integration if your scenario includes the following conditions: • Preliminary incident investigation is in Microsoft Azure Sentinel and subsequent investigation is in SIR • Ingest Microsoft Azure Sentinel incidents to SIR	Use this integration if your scenario includes the following conditions: • Perform incident investigation in SIR. • Ingest Microsoft Azure Sentinel alerts in SIR. • Incidents are not created in Microsoft Azure Sentinel.
Alert is an entity in Microsoft Azure Sentinel. You cannot retrieve standalone or specific alerts using the Microsoft Azure Sentinel Management API. You can only retrieve the alert data associated with an incident. The alert data available using this integration is richer than the alert data available using the Microsoft Graph Security API.	The Microsoft Azure Sentinel normalized alert data is available. The Microsoft Azure Sentinel alert fields that are mapped internally in Microsoft Graph Security API, and are available in Microsoft Graph Security API, are available for use in this integration.
	You cannot update alerts in Microsoft Azure Sentinel using this integration.

Microsoft Defender for Endpoint integration

The Microsoft Defender for Endpoint enables you to proactively inspect, analyze, and contain known and unknown threats on any endpoint.

The Microsoft Defender for Endpoint integration helps Security Analysts efficiently investigate and remediate security incidents without having to navigate between tools.

You can use this integration to create configurations to retrieve the host details, details of logged-in users, related machines details, and other enrichment capabilities. You can request to isolate any machine from accessing the networks or remove the machines from isolation. Requests can be accepted or rejected by the approvers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Key features

Microsoft Defender for Endpoint has the following key features:

- Perform Enterprise Security Search to sight potential malicious observables across endpoints, and take remediation actions.
- Perform response actions such as Isolate host, Remove isolation, Restrict app execution, Run antivirus scan, Remove app restriction, and Stop and quarantine file.
- Create or update indicators.
- Perform observable enrichment and retrieve data related to indicators.

Microsoft Defender for Endpoint

Explore Get started with Microsoft Defender for Endpoint	**Install** Install the application and configure a source for the integration	**Configure** Configure profiles and security incidents for the Microsoft Defender for Endpoint
Capability profile Create a capability profile for the Microsoft Defender for Endpoint integration.	**Additional configurations** Additional configurations that you can perform in the Microsoft Defender for Endpoint	**Miscellaneous** Create and configure a profile for sightings search and indicators with Microsoft Defender for Endpoint.

Register and configure the Microsoft Defender for Endpoint in the Microsoft Azure portal

Register the Microsoft Defender for Endpoint application in the Microsoft Azure portal and grant the read and write access to the application.

Before you begin

Role required: Application developer, Tenant administrator.

Procedure

1. Log in to the Microsoft Azure portal.
2. Enter `App registrations` in the Search box, and click **Click New registration**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Enter a name for your application and the redirect URI, and click **Register**.
   An example name is `Microsoft Defender for Endpoint`. The Redirect URI is used while providing admin consent for the application.
4. In the **App registrations** page, select the application that you registered in Step 3.
5. Under Manage, select **Certificates & secrets**.
6. To create a client secret, select **New client secret**.
7. Copy the client secret and save it.

   In case you forgot the client secret, you can generate a new client secret.
8. Navigate to **Manage** > **API Permissions**.
9. Click **Add a permission**.
10. In the Request API permissions window, click the **APIs my organization uses** tab.
11. Search for and select **WindowsDefenderATP**.
12. In the WindowsDefenderATP permissions, select **Application permissions**.
    Enabling this permission ensures that the application runs as a background service or daemon without a signed-in user.
13. Add the following application level permissions and grant admin consent for the newly added API permissions.

Permission	Permission Display Name
Machine.Read.All	Read all machine profiles
User.Read.All	Read user profiles
Machine.Isolate	Isolate machine
Machine.RestrictExecution	Restrict code execution
Machine.Scan	Scan machine
Machine.StopAndQuarantine	Stop and Quarantine
URL.Read.All	Read URLs
File.Read.All	Read file profiles
Ip.Read.All	Read IP address profiles
Ti.ReadWrite.All	Read and write Indicators

Get started with the Microsoft Defender for Endpoint integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the Microsoft Defender for Endpoint application from the ServiceNow store.

Before you begin

Role required: admin

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform and Security Incident Response (SIR) roles.	The following roles are required: **1.** You must have system administrator (admin) role to install the application for the integration. **2.** You must have security incident administrator (sn_si.admin) role to configure the integration, create, activate, and remove profiles. **3.** You must have security incident analyst (sn_si.analyst) role to work with security incidents. A user with this role can initiate any of the capabilities available in the integration.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, you must install and activate each application one at a time in the following order to ensure a smooth installation: **1.** Security Incident Response **2.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Before you enable the approval option for profiles, verify that you have created an approval group.	An optional approval workflow is available for isolating host machines, restoring them back to the network, and running additional actions on end point. If your organization wants an extra level of control over these actions, enable the Require approval option during the configuration of the profiles. In a scenario where the profile is available, the profile configuration for approval takes precedence. In a scenario where the profile is unavailable, the approvals are handled based on the default settings. As a Security Administrator, you can set up approval while configuring the profiles and the default settings. An approval group must be available on the Groups list in your instance. To monitor and process requests submitted by the users with sn_si.analyst role, each member of the approval group should navigate to My Approvals in the ServiceNow AI Platform®.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	Alternatively, the approvers can find the requests submitted exclusively for Microsoft Defender for Endpoint integration under the Approvals module. For more information on how to create a user group, see Create a user group.

What to do next

You have successfully set up your ServiceNow AI Platform® instance for the Microsoft Defender for Endpoint integration. The next step is to install the Microsoft Defender for Endpoint application from the ServiceNow Store for the integration.

Install the application and configure a source for the integration

Install and configure the Microsoft Defender for Endpoint integration from the ServiceNow Store on your ServiceNow AI Platform instance. Start creating capability profiles using the configurations.

Before you begin

Role required: sn_si.admin

Procedure

1. Download the Microsoft Defender for Endpoint integration from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the Microsoft Defender for Endpoint tile, and click **Configure**.
4. On the form, fill in the following fields.

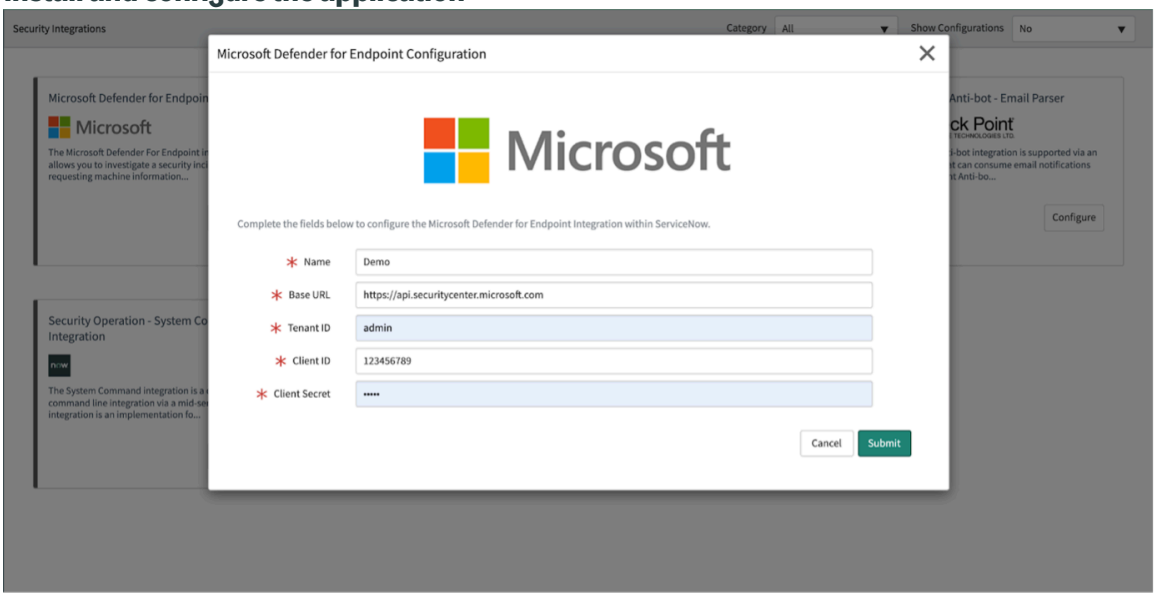
Configure Microsoft Defender for Endpoint

Name	Name for the Microsoft Defender for Endpoint instance configuration.
Base URL	The service base URL for Microsoft Defender for Endpoint
Tenant ID	The Microsoft Defender for Endpoint Tenant ID. All actions would be performed on this instance.
Client ID	Client ID for the application that you have registered in the Microsoft Azure portal.
Client Secret	Client secret for your registered application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Submit**.

Install and configure the application



Result
The Microsoft Defender for Endpoint configurations list is displayed with your new configuration record. You have completed the configuration for the Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint Default Settings

There are additional configuration settings you must perform after you complete the installation.

After you complete the installation, you can find the Default Settings module under the Microsoft Defender for Endpoint application on the left-navigation pane. It contains the default settings for different Microsoft Defender for Endpoint functionalities.

Roles required: sn_si.admin, sn_si.analyst (read-only).

Additional Configurations

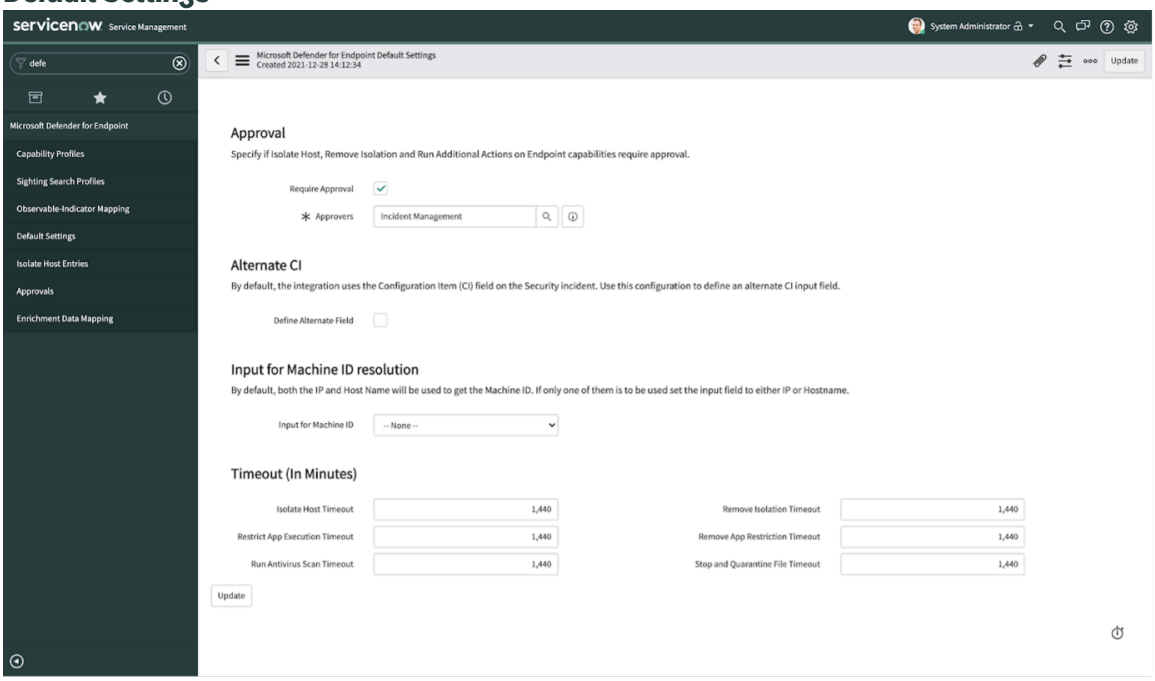
The following are additional configuration settings:

- **Approval**: This approval is specifically for the Isolate Host action, Remove Host Isolation action, and additional actions such as Restrict App Execution, Remove App Restriction and Run Antivirus Scan. You can use this approval only when actions are triggered directly from the Related list, and if there are no any existing profiles. If there are any existing profiles for these capabilities, then the approval configuration in the profile takes precedence.
  - **Require Approval**: When you enable **Require Approval**, the Approvers field is available on the form.
  - **Approvers**: List of approver groups. After you submit a request, approval is required from the group to complete the request.
- **Alternate CI**: Enabling this check box provides the list of fields available to pass an alternate CI to the capability. By default, the integration uses the Configuration Item (CI) field on the Security incident. This configuration is applicable only for the Run Additional Actions on Endpoint capability. Use this configuration to define an alternate CI input field for the only Run Additional Actions on Endpoint capability. For the other capabilities, use the configuration in the profile section. If the profiles do not define an alternate CI, then the capabilities would take the CI field from the Security Incident form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Input for Agent ID resolution**: By default, IP and Host Name is used to get the Agent ID. If you're going to use only one of them, then set the input field to either IP or Host Name.
- **Timeout**:
  - **Isolate Host Timeout (in minutes):** Indicates the execution threshold for the Isolate Host capabilities.
  - **Remove Isolation Timeout (in minutes):** Indicates the execution threshold for the Remove Isolation Timeout capability.
  - **Restrict App Execution Timeout (in minutes):** Indicates the execution threshold for the Restrict App Execution capability.
  - **Remove App Restriction Timeout (in minutes):** Indicates the execution threshold for the Remove App Restriction capability.
  - **Run Antivirus Scan Timeout (in minutes):** Indicates the execution threshold for the Run Antivirus Scan capability.
  - **Stop and Quarantine File Timeout (in minutes):** Indicates the execution threshold for the Stop and Quarantine File capability.

Default Settings



Map the Microsoft Defender for Endpoint indicator types

Map the ServiceNow Observable type with the Microsoft Defender for Endpoint indicator type. This mapping would be used in Observable Enrichment and Create Indicator actions in Microsoft Defender.

Before you begin

Role required: sn_si.admin or sn_si.analyst (read-only)

About this task

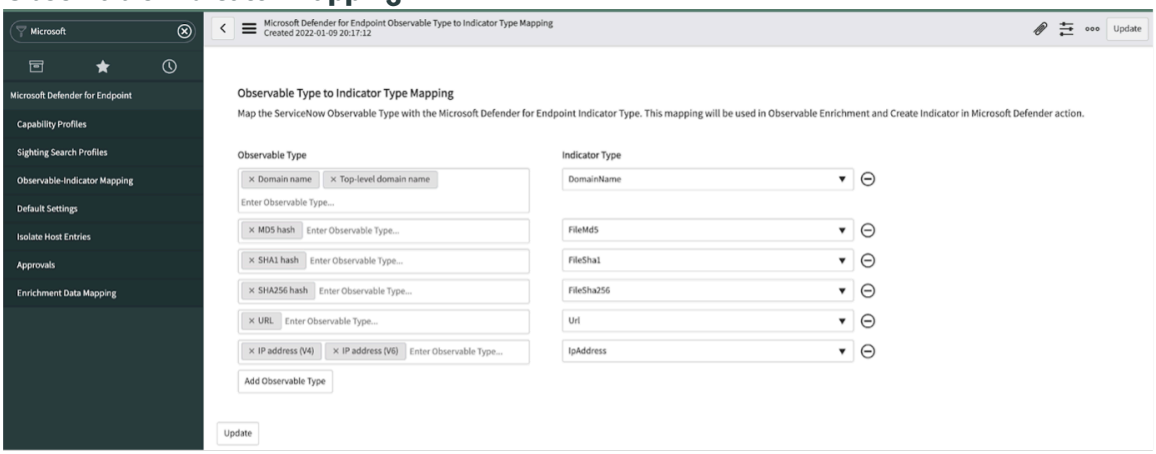
In a scenario where the observable type is not mapped to an indicator type, such observables are not eligible for Observable enrichment and indicator creation in Microsoft Defender for Endpoint.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Microsoft Defender for Endpoint** > **Observable-Indicator Mapping**.

Observable-Indicator Mapping



2. Add or update an Observable type in one of the following ways:
   - To add new mapping, click **Add Observable Type**.
   - To update the Observable to the Indicator type mapping, click any existing row.
3. To save the mapping, click **Update**.

Create a capability profile for the Microsoft Defender for Endpoint integration

Create a profile and select the Microsoft Defender for Endpoint capabilities that you want the profile to run.

Before you begin

Role required: sn_si.admin

About this task

Profiles are created to club or group the capabilities together, which would help Analysts perform the investigation or remediation easily. You can add the following capabilities to the profile:

- Get Host Details
- Get Logged On Users
- Isolate Host
- Remove Isolation

You cannot club Isolate Host and Remove Host Isolation capabilities with other capabilities while creating a profile. Profiles for these capabilities have to be individually created. While on the other hand, the Get Host Details and Get Logged on Users capabilities can be clubbed together. You could create profiles individually or by clubbing them in full or parts as per your requirement.

Note: After a capability is included in a profile, it cannot be included in any other profile from the same source.

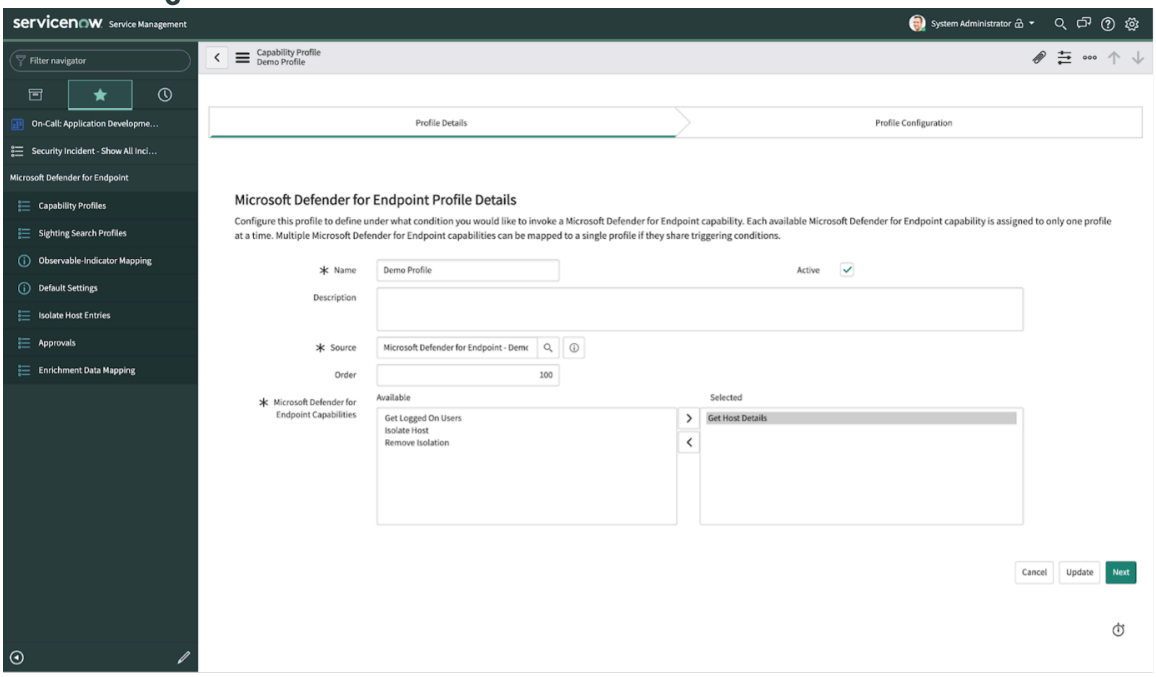
Procedure

1. Navigate to **Microsoft Defender for Endpoint** > **Capability Profiles**.

   The Microsoft Defender for Endpoint capability profiles list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Profile Configuration



2. Click **New**.
3. On the form, fill in the fields.

Capability Profile form

Field	Description
Name	Name for the Microsoft Defender for Endpoint capability profile. This name helps you identify the profile type and describe it.
Description	Additional information about the profile that further describes the profile.
Source	Name of the Microsoft Defender for Endpoint source. Only configured sources are available from the list.
Microsoft Defender for Endpoint capabilities	Capabilities of the Microsoft Defender for Endpoint profile. Select the capabilities you want for this profile from the Available column, and move them to the Selected column.
Order	Flow priority. Default is 100. The value of this field indicates the order that flows are executed when two or more profiles share triggering conditions. The flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	Option to indicate that the profile is active. After the profile is active, the profile is automatically triggered when a security incident is created that matches the filtering conditions that you have specified in the configuration.

4. To continue to Profile Configuration, click **Next**.

What to do next

The next step is to configure your profile. Before you configure the settings for the profile, you may prefer to review the how profiles and configured and triggering conditions. For more information, see Trigger conditions in a configuration item.

Trigger conditions in a configuration item

After you create a profile and select the Microsoft Defender for Endpoint capabilities that you want the profile to run, configure the profile settings so that the profile runs only when a set of specific conditions is met.

How to trigger conditions in a configuration item

You can set trigger conditions so the profile runs automatically whenever a security incident is created that matches the trigger condition. If the trigger condition is not set, these profiles can be manually run by clicking the Run EDR profile(s) form on the security incident, and selecting the profile.

By default, the integration uses the Configuration Item (CI) field on the Security incident. This value is used to match the IDs of your assets with the information stored in the ServiceNow AI Platform Configuration Management Database (CMDB). When a security incident is created, and a profile is run either automatically or manually, the CMDB is searched to retrieve the host name or IP address based on the value of the CI field. The host name or IP is used to resolve the Agent ID on Microsoft Defender for Endpoint to identify the endpoint.

In an ideal scenario, a matching value is found in the database, and data is gathered from the Microsoft Defender for Endpoint console for the matching asset. The data for various capabilities are pulled into your ServiceNow AI Platform Configuration Management Database (CMDB) instance and displayed in the related lists of a security incident. When the Configuration item (CI) field is not populated on the security incident with a host name with or an IP address that matches the database, you can select an alternate field on the security incident that contains either the host name or the IP to perform the Agent ID resolution.

During the configuration step of the profile setup, you can select an alternate CI field for endpoint identification to ensure that you are able to identify the endpoint on Microsoft Defender for Endpoint. You can select any field on the security incident as an alternate CI trigger field, including custom fields that you create. By selecting this alternate CI field as a backup, you ensure that your profiles run even if the CI field is not populated on the associated security incident on incident creation.

Note: The alternate CI fields are considered only for capabilities that could be added to a profile. These capabilities include Get Host Details, Get Logged On Users, Isolate Host, and Remove Isolation. For all the additional actions, the alternate CI must be configured in the Default Settings module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure profiles and security incidents for the Microsoft Defender for Endpoint integration

Create a profile and select the Microsoft Defender for Endpoint capabilities that you want the profile to run. You need to configure the settings so that the profile can be triggered only under the defined conditions.

Before you begin

Role required: sn_si.admin, sn_si.analyst (read-only)

About this task

Configure the profile so that it runs only when the conditions you specify are fulfilled. If required, you can select an alternate input field for the Configuration Item (CI) field, and set filtering conditions so that the profile can be triggered automatically when a security incident meeting the trigger conditions is created.

Note: You can navigate to the Profile Configuration page only after you have entered the Profile Details page.

Procedure

1. Navigate to **Microsoft Defender for Endpoint** > **Capability Profiles**.
2. After completing the Profile details section, click **Next**.
   Review and configure the sections.
3. In the Define Incident Criteria (Automation) section, select the **Define Incident Criteria** option to automatically trigger Microsoft Defender for Endpoint capabilities in the profile.
   Define Incident Criteria (Automation): Define the security incident conditions that would automatically trigger the Microsoft Defender for Endpoint capabilities for the profile. If you do not select the **Define Incident Criteria** option, then the profile and the underlying capabilities can be invoked manually from the Security incident.

   Note: Isolate Host and Remove Host Isolation capabilities cannot be triggered automatically.

   a. In the **Filter Conditions**, select the required field.
   b. Add **New Criteria** and also define the **OR** or the **AND** condition.
4. In the Approvals section, select the **Require Approval** check box to provide an extra level of control.

   If you select this option, then you have more control when using the Microsoft Defender for Endpoint capabilities for isolating host machines, restoring them to the network, getting files.

   The Approvals option in the profile configuration appears only for Isolate Host and Remove Host Isolation capabilities respectively.
5. In the Additional Configuration section, select the **Define Alternative Field** option to define an alternative input field.
   Additional Configuration: When the Configuration item (CI) field is not populated on the security incident with a host name, or an IP address that matches the database, you can select an alternate field on the security incident to query the Microsoft Defender for Endpoint APIs.

   Note: For more information, see Trigger conditions in a configuration item.

   a. Select the **Define Alternative Field** option.
   b. Select the input field from the **Alternate CI Trigger Field**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. In the Tags section, select the **Display Tag** check box to enable tagging security incidents, profile name is prefixed on enabling the tag.

   You can optionally tag security incidents with tags for profile initiated, profile completed, and profile failed tags. By default, this option is turned off for all profiles.

7. Click **Done**.

Verify the Trigger Condition Filters

Validate the profile, and verify that the trigger condition filters that you have configured are working as expected.

Before you begin

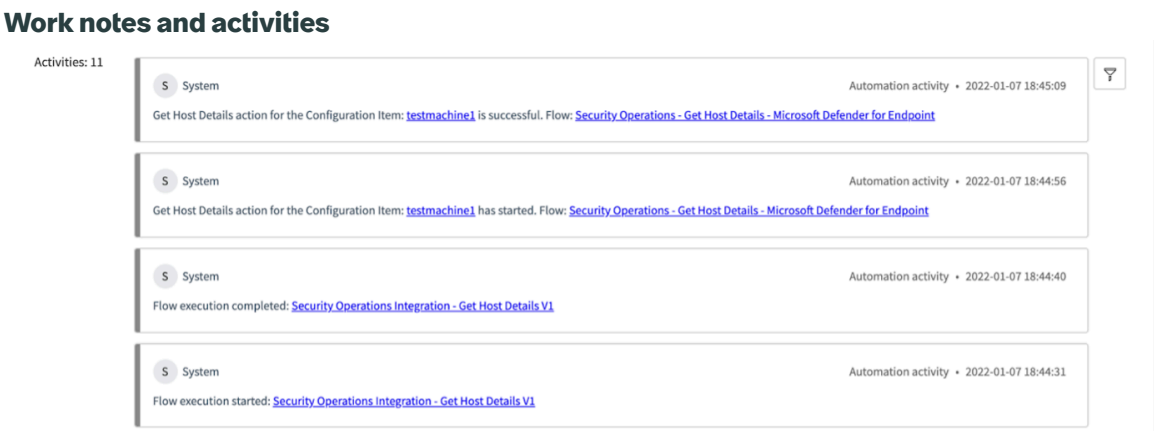
Role required: sn_si.admin or sn_si.analyst

About this task

After you activate the profile, based on the configured trigger conditions you can view the query results in the ServiceNow AI Platform® security incidents.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. To create a new security incident, select **New**.
3. To trigger the respective profile, provide the filter conditions as given in the capability profile.
4. Click **Save**.
5. To validate the work notes and activities section, view and check the records that are tagged with the profile initiated, profile completed, or profile failed tags.



6. To validate all the data in the related lists, click **Show All Related Lists**.
7. Click any **Related List** tab to validate the details.
   For example, Host Details.

Trigger the Microsoft Defender for Endpoint capabilities from Related Links

Trigger a capability profile manually after reviewing a security incident from related links.

Before you begin

Role required: sn_si.admin or sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

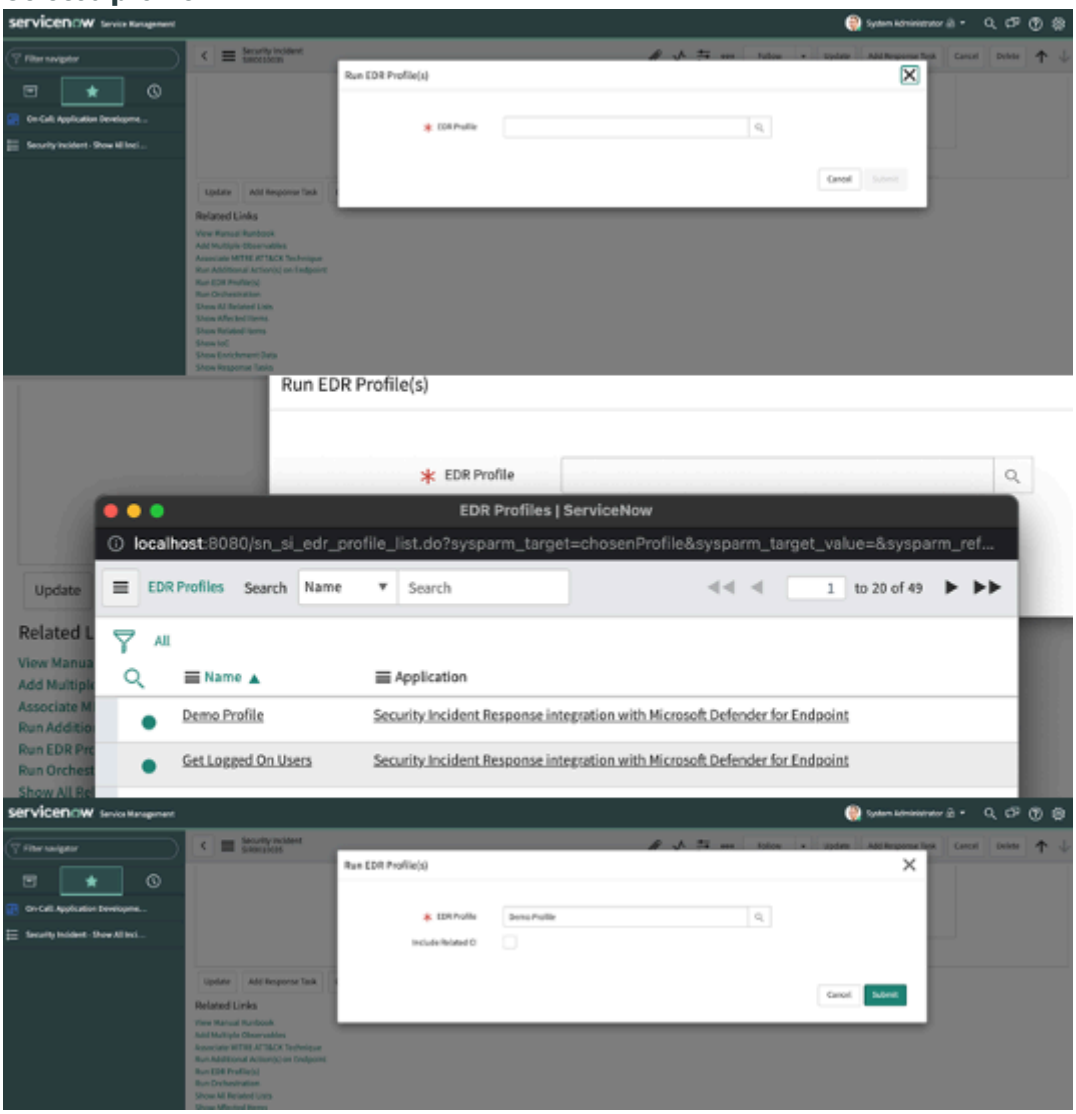
About this task

In addition to running the profile for the CI or the Alternate CI of the security incident, you can also run the profile for CI values present in the Configuration Item related list by selecting **Include Related CI** in the dialog box. This retrieves the data for the CI values present in the related list as well. Alternatively, you could run the profile just for the CI values present in the related list.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. In the Related Links section, click **Run EDR Profile(s)**.
4. Browse and select a profile from the list of available profiles, and click **Submit**.

Select a profile



The selected profile is triggered manually.

5. Validate the work notes and activities section.
6. View the tags, and validate the data in the related lists.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Trigger the Microsoft Defender for Endpoint from Configuration Item related list

Trigger a capability profile manually from the configuration item related list.

Before you begin

Role required: sn_si.admin or sn_si.analyst

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. Click **Show All Related Lists**.
4. Click the Configuration Item related list.
5. Select the added configuration items.
6. From the **Actions** on selected rows, select a capability.
   The selected capability is triggered manually.
7. Validate the work notes and activities section.
8. View the tags, and validate the data in the related lists.

Additional Configurations in Microsoft Defender for Endpoint

The Microsoft Defender for Endpoint integration supports running additional actions beyond the standard actions.

The Microsoft Defender for Endpoint supports the following additional configurations:

Configure Isolate Host capability in Microsoft Defender for Endpoint

Isolate the host from accessing the network in Microsoft Defender for Endpoint based on the severity of the attack. Isolating the host from the network enables you to prevent any other malicious activities or potential attacks on other hosts.

Before you begin

Role required: sn_si.admin or sn_si.analyst

Requirements for Isolate Host capability

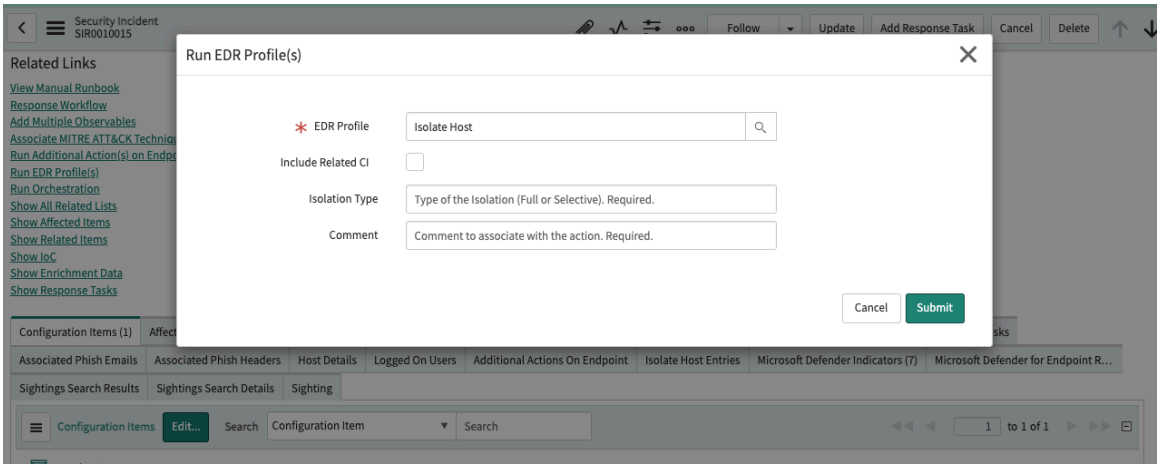
Capability	Required	Description
Isolate Host	Isolation Type	(Required) Type of the Isolation (Full or Selective).
	Comment	(Required) Comment to associate with the action.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. In the Related Links section, click **Run EDR Profile(s)**.
4. Browse and select a profile with **Isolate Host capability** selected from the list of available profiles, and click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Isolate Host



Alternatively, you can perform the following steps:

a. In the related lists section, click **Show All Related Lists**.

b. Click the **Configuration Item** related list.

c. Select **Isolate Host** and select the corresponding capabilities.

5. Validate the automation activity and activities section, and make sure that the data is as expect.
6. View the data, and validate the isolate host details on the related lists.

Configure Remove Host Isolation capability in Microsoft Defender for Endpoint

If needed, remove the isolation of a host that was previously isolated from the network in Microsoft Defender for Endpoint. You can prevent any other malicious activities or potential attacks on other hosts.

Before you begin

Requirements for Remove Isolation capability

Capability	Required Input	Description
Remove Isolation	Comment	(Required) Comment to associate with the action.

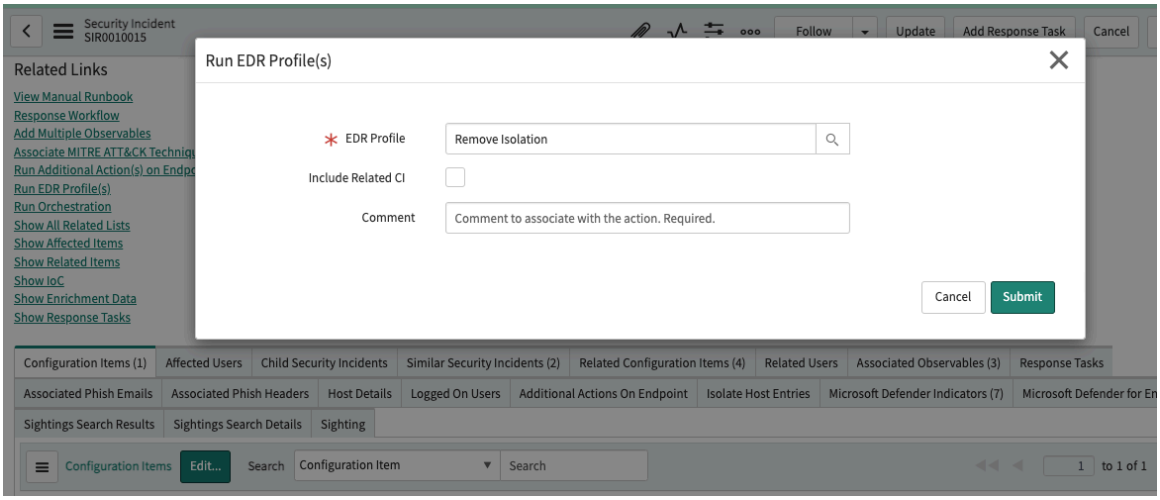
Role required: sn_si.admin or sn_si.analyst

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. In the Related Links section, click **Run EDR Profile(s)**.
4. Browse and select a profile with **Remove Isolation capability** selected from the list of available profiles, and click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remove Isolation



Alternatively, you can perform the following steps:

a. Click **Show All Related Lists** in the related lists section.

b. Click the **Configuration Item** related list.

c. Select **Remove Isolation** and select the corresponding capabilities.

5. Validate the automation activity and activities section.

6. View the data, and validate the isolate host details on the related lists.

7. Validate the automation activities of the execution.

Configure Run Antivirus Scan capability in Microsoft Defender for Endpoint

Remotely initiate an antivirus scan to help identify and remediate malware that might be present on a compromised device. Run the scan as part of the investigation or response process.

Before you begin

Role required: sn_si.admin or sn_si.analyst

Requirements for Run Antivirus Scan capability

Input	Description
Scan Type	(Required) Type of the Scan (Full or Quick).
Comment	(Required) Comment to associate with the action.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.

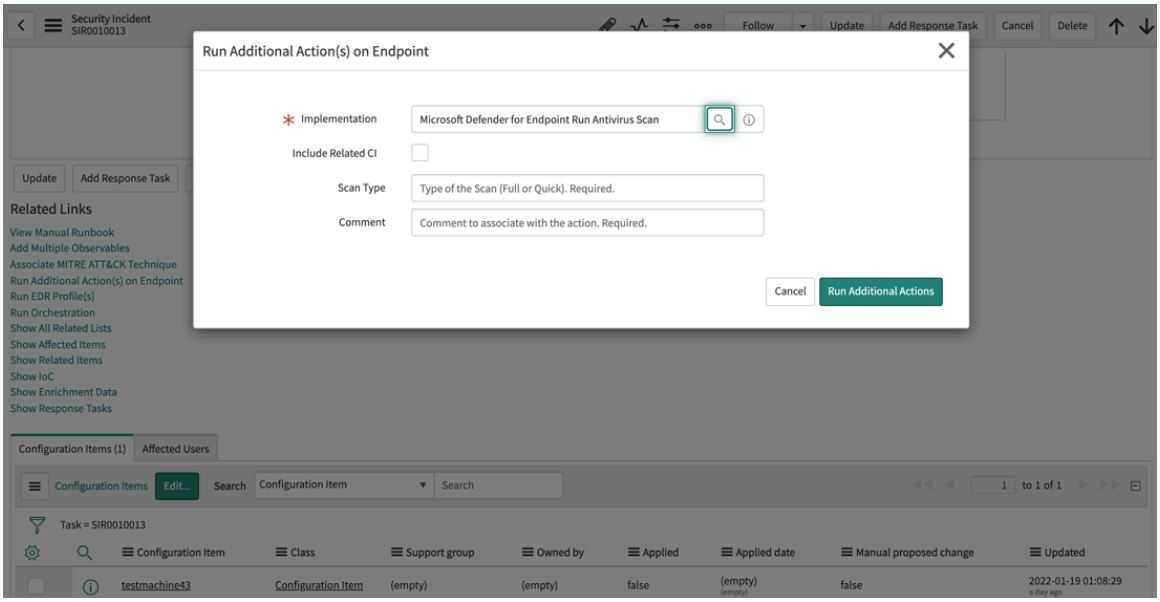
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.

a. In the related links section, click **Run Additional Actions on Endpoint**.

b. Browse and select the required capability.
For example, click **Run Antivirus Scan** capability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run Antivirus Scan



Alternatively, you can perform the following steps:

a. In the related lists section, click **Show All Related Lists**.

b. Click the **Configuration Item** related list.

c. Select the added configuration items, and from the Actions on selected rows, select **Run Additional Actions on Endpoint**.

After you select the **Run Antivirus Scan** capability implementation, the **Additional Scan Type** and **Comment input** fields are displayed.

3. Select the **Scan type** that you want to run (Quick or Full), and add a comment before executing the scan.
4. To initiate the antivirus scan, click **Run Additional Action**.
5. View the automation activities of the execution, and validate them.
6. Validate the status of the action on the Additional Actions on Endpoint related lists.

Configure Restrict App Execution capability in Microsoft Defender for Endpoint

To contain an attack, restrict or lock a device and prevent subsequent attempts of potentially malicious programs from running.

Before you begin

Requirements for Restrict App Execution capability

Input	Description
Comment	(Required) Comment to associate with the action)

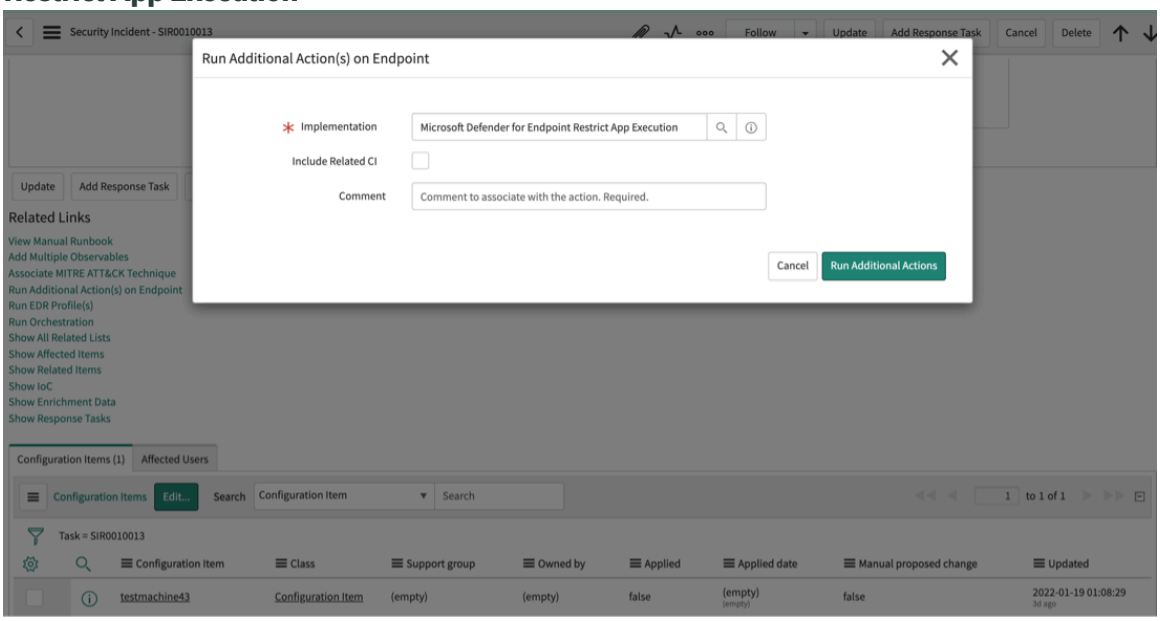
Role required: sn_si.admin or sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
   a. In the related links section, click **Run Additional Actions on Endpoint**.
   b. Browse and select the **Restrict App Execution** capability.

Restrict App Execution



Alternatively, you can perform the following steps:

   a. In the related lists section, click **Show All Related Lists**.
   b. Click the **Configuration Item** related list.
   c. Select the added configuration items.
   d. From the Actions on selected rows, select **Run Additional Actions on Endpoint**.
3. To enable Restrict App Execution on the machine, click **Run Additional Action**.
4. View the automation activities of the execution, and validate them.
5. Validate the status of the action on the Additional Actions on Endpoint related lists.

Configure Remove App Restriction capability in Microsoft Defender for Endpoint

If needed, remove the restrictions of any application on the device.

Before you begin

Role required: sn_si.admin or sn_si.analyst

Requirements for Remove App Restriction capability

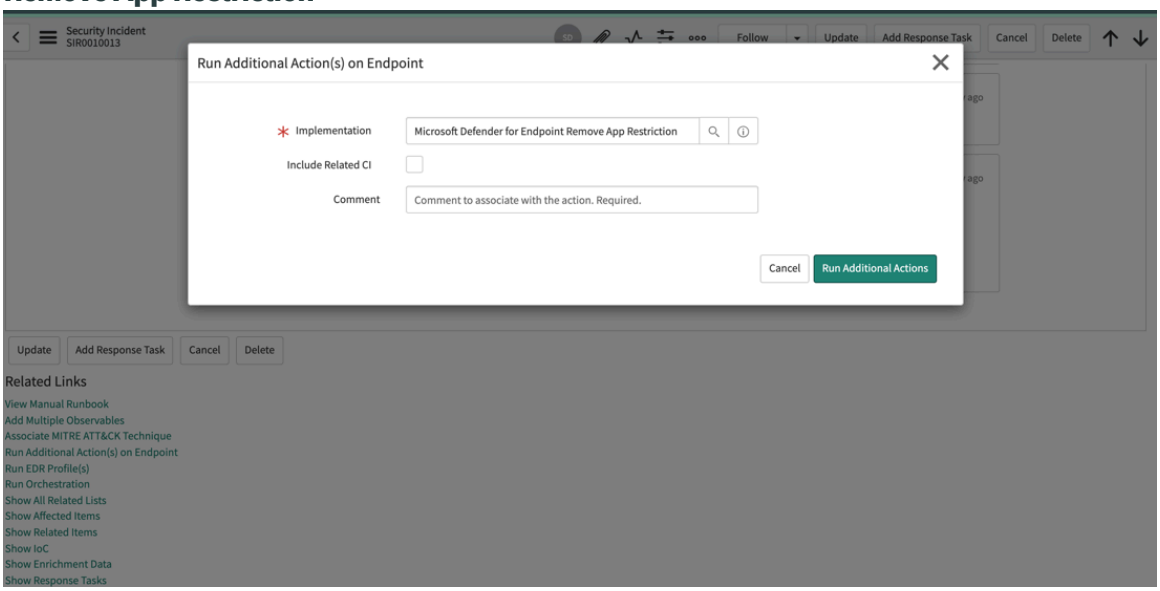
Input	Description
Comment	(Required) Comment to associate with the action)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
   a. In the related links section, click **Run Additional Actions on Endpoint**.
   b. Browse and select the **Remove App Restriction** capability.

Remove App Restriction



Alternatively, you can perform the following steps:

   a. In the related lists section, click **Show All Related Lists**.
   b. Click the **Configuration Item** related list.
   c. Select the added configuration items.
   d. Select **Run Additional Actions on Endpoint**.
   The Additional Comment input field is displayed.
3. To remove app restriction, click **Run Additional Action**.
4. View the automation activities of the execution, and validate them.
5. Validate the status of the action on the Additional Actions on Endpoint related lists.

Configure Get Related Machines from Defender Capability in Microsoft Defender for Endpoint

Get the list of related machines of specific observables.

Before you begin

Note: Supported Observable Types are Domain name, SHA1 hash, and Username.

Role required: sn_si.admin or sn_si.analyst

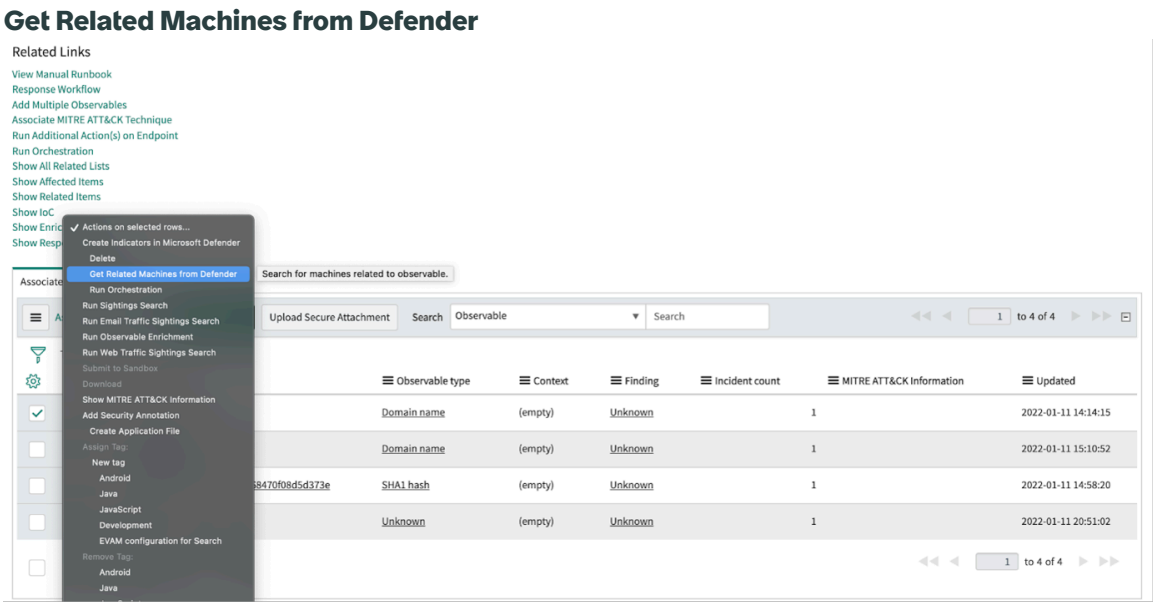
About this task

You can retrieve the list of machines that have accessed the particular observables. You can store the list on the Microsoft Defender for Endpoint Related Machines Details table. You can trigger the Get Related Machines from Defender capability from the Associated Observables related list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.



3. In the Related links section, click **Show IoC**.
4. Click the Associated Observables related list.
5. Select the associated observables.
6. From the Actions list, select the **Get Related Machines from Defender** capability.
7. Validate the automation activity and activities section.
8. View the data, and validate the Microsoft Defender for Endpoint Related Machines details on the related lists.
9. View the automation activities of the execution, and validate them.

Configure Stop and Quarantine File capability in Microsoft Defender for Endpoint

Stop and quarantine files from the Microsoft Defender platform.

Before you begin

Supported Observable Types: SHA1 hash.

Requirements for Stop and Quarantine File capability

Input	Description
Comment	(Required) Comment to associate with the action)

Role required: sn_si.admin or sn_si.analyst

About this task

You can run the Stop and Quarantine File action on the particular observables of type SHA1 only. Store the details on the Additional Actions on Endpoint table. You can trigger the Stop and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Quarantine File capability from the Microsoft Defender for Endpoint Related Machines details related list.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. In the related links section, click **Show All Related Lists**.
4. Click the Microsoft Defender for Endpoint Related Machines Details related list.
5. Select one or more records.
6. From the **Actions** on selected rows, select the **Stop and Quarantine File** capability.
7. Validate the automation activity and activities section.
8. View the data, and validate the data on the related lists.
9. View the automation activities of the execution, and validate them.

Create and configure a profile for sightings search with the Microsoft Defender for Endpoint integration

Create and configure the sightings search profile automatically using the Microsoft Defender for Endpoint.

Before you begin
Role required: sn_si.admin, sn_si.admin

About this task
You can use the Sightings Search workflow to perform the sighting searches. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries that are based on the sighting search configurations, and executes the searches that are based on the configured workflow.

The Microsoft Defender for Endpoint provides a base system sighting search profile that enables you to configure the automatic sighting searches. With this profile, you can access the related observable sighting information of an organization and also see the sightings from other organizations.

Procedure

1. Navigate to **Integrations** > **Sighting Search Configuration**.
2. Click **New**.
3. On the form, fill in the following fields.

Sightings Search Configuration form

Field	Description
Name	Name for the sighting search profile.
Is saved search	Option to save the search configuration. The saved search configuration queries are example queries. You can substitute them with the parameters for your environment and create additional-saved search configurations as required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Sightings search source	The source configured for the sightings search in Microsoft Defender for Endpoint integration.
Search	Native search string that forms a query.
Active	Option to enable the saved search configuration. Only active search configurations can perform a sightings search.
Observable type	Type of observable category. For example, IP address, hash value, URL, and domain name.
Maximum observable per search	Maximum number of observables that you can view from a search query. Set this value to 1 for this integration.
Sightings search parameters	Parameters to define more complex queries that include logic and other operators supported by the specified log store.

4. Click **Submit**.

Perform a manual sighting search in Microsoft Defender for Endpoint

Select individual or multiple observables and perform a manual sighting search in Microsoft Defender for Endpoint to determine the prevalence of a threat over time.

Before you begin
Role required: sn_si.admin, sn_si.analyst

About this task
The supported Observable types are the following:

- Domain name
- IP address (V4)
- IP address (V6)
- MD5 hash
- SHA1 hash
- SHA256 hash

Procedure

1. Navigate to the **Security Incidents**.
2. Open an existing SIR or create a new SIR.
3. In the related links, click **Show IoC**.
4. Click the Associated Observables related lists.
5. Select the observables.
6. From the Actions list, click **Run Observable Enrichment**.
7. Select the observables under **Action** on selected rows, and click **Run Sightings Search**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Sighting search is supported for Domain name, IP address (V4), IP address (V6), MD5 hash, SHA1 hash, and SHA256 hash observables types respectively.

8. Specify the time frame for the search, and click **Search**.

Note: The Microsoft Defender for Endpoint supports sighting search only for the last 30 days. If your range query is earlier than the last 30 days, then sighting search does not retrieve any data. If your range query overlaps with the last 30 days, then the sightings from only the last 30 days get retrieved, and if your range query is within the last 30 days, then the sightings from the defined start time to the current time is retrieved.

9. On completion of the search, validate the results and details in the related lists.
10. Click **Sightings Search Details** to view the sighting search details.
11. Click the **Sighting** tab for details and **Sightings Search Results** tab for search results.

You can view additional information related to the particular sighting in the **Summary** field.

Perform an automatic observable enrichment in Microsoft Defender for Endpoint

Perform an automatic observable enrichment in Microsoft Defender for Endpoint to enrich observables with additional information from various sources.

Before you begin

Verify that you have enabled the **Security Incident Response** system property. This option triggers the observable enrichment capability in SIR, whenever an observable is associated to a Security Incident.

Role required: sn_si.admin, sn_si.analyst

About this task

You can use this capability during incident response investigations to contain an identified threat. When new observables are associated with the security incident, you can enable the observable enrichment in Microsoft Defender for Endpoint capability to run automatically.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. Validate the automation activity once the new observables have been associated with the security incident.
4. View the results the enrichment results in the Indicators related list of the security incident. You can use the following table for more information on the observable enrichment.

Microsoft Defender Indicator

Field	Description
Indicator ID	Identity of the Indicator entity. Click **Open** to view the record in detail in the ServiceNow AI Platform instance
Observable	The observable associated with the result.
Title	Title for the indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Indicator Type	Type of the indicator.
Action	Action performed by the indicator.
Recommended Action	Recommended actions for the indicator.
Integration Vendor	Defender source integration from which the data is retrieved.
Expiration Date	Expiration time for the indicator.
Retrieval Date	Date when the enrichment record is created.

Perform a manual observable enrichment in Microsoft Defender for Endpoint

Select individual or multiple observables and perform a manual observable enrichment to enrich observables with additional information from Microsoft Defender for Endpoint.

Before you begin

Role required: sn_si.analyst

About this task

The Microsoft Defender for Endpoint integration enables observable enrichment for all the observable types that are mapped in the Observable-Indicator Mapping module.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to review with the Microsoft Defender for Endpoint information.
3. Click **Show All related lists**.
4. Click the **Associated Observables** tab.
5. Select the observables.
6. From the Actions list, click **Run Observable Enrichment**.
7. Select a Microsoft Defender for Endpoint **source** and move it to the **Selected** column to specify which implementation you want to use to enrich the selected observables.
8. Click **Submit**.
9. To validate the status of the execution, view the work notes.
10. To view the results, click **Microsoft Defender Indicator** tab.
    You can use the following table for more information on the observable enrichment.

Microsoft Defender Indicator

Field	Description
Indicator ID	Identity of the Indicator entity. Click **Open** to view the record in detail in the ServiceNow AI Platform instance
Observable	The observable associated with the result.
Title	Title for the indicator.
Indicator Type	Type of the indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Action	Action performed by the indicator.
Recommended Action	Recommended actions for the indicator.
Integration Vendor	Defender source integration from which the data is retrieved.
Expiration Date	Expiration time for the indicator.
Retrieval Date	Date when the enrichment record is created.

Create indicators in Microsoft Defender for Endpoint

Create indicators from associated observables of the security incident using the Microsoft Defender for Endpoint.

Before you begin

Role required: sn_si.admin, sn_si.analyst

About this task

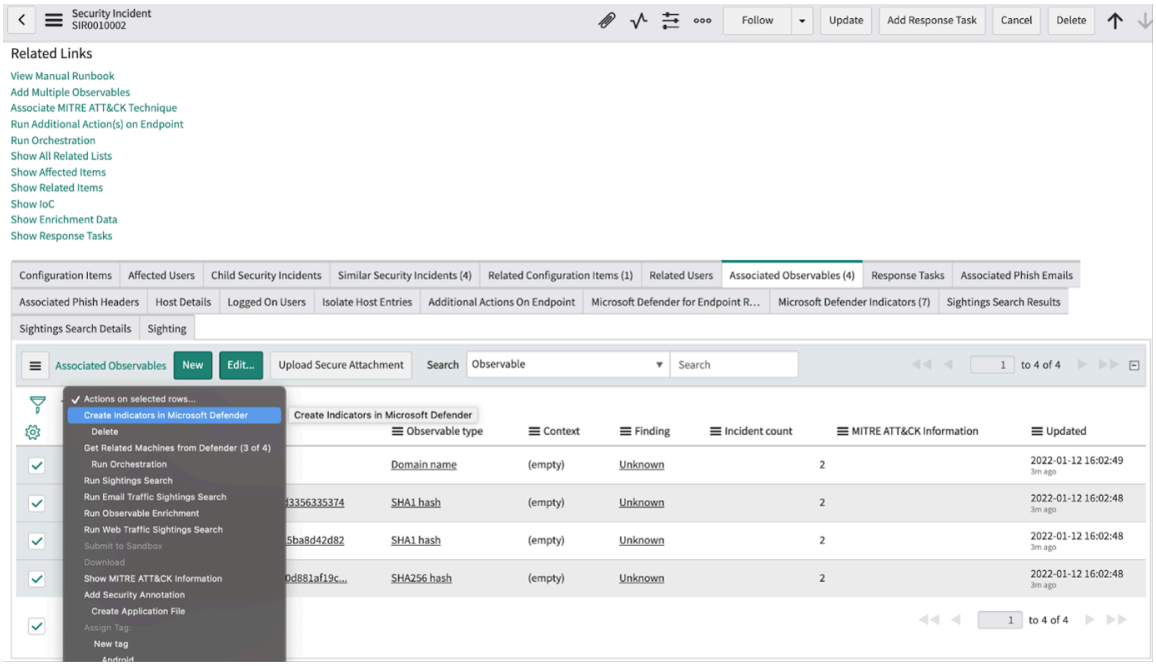
The Microsoft Defender for Endpoint integration allows observable enrichment for all the observable types that are mapped in the Observable-Indicator mapping module.

Create indicators provide you the ability to set a list of indicators for detection, and for blocking prevention and responses. You can create the indicators from associated observable of the security incident.

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Select the security incident that contains the observables for which you want to create indicators in Microsoft Defender for Endpoint.
3. Click the Associated Observables related lists.
4. Add any existing observables or create new observables.
5. Select the observables.
6. From the **Actions** on selected rows, click **Create Indicator in Microsoft Defender**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. On the form, fill in the fields.

Field	Description
Selected Observables	Observables that are affected. This action can be used to create indicators for multiple observables. If you want to deselect an observable, you can do that by deselecting the observables from the list. **Note:** If the supported observable types are not mapped, then the indicators are not created in the Microsoft Defender for such observables.
Title	Title for the indicator.
Description	Description for the indicator.
Expiration Time	Expiration time for the indicator.
Recommended Actions	Recommended actions that must be performed for the indicator.
Source	Integration configuration to create the indicator.
Action	Actions that will be performed if the Indicator is discovered in the organization. The possible values are as follows: ○ **Warn** ○ **Block** ○ **Audit**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **'BlockAndRemediate** ○ **Allowed**
Application	The Microsoft Defender for Endpoint application that is associated with the indicator. This field is applicable only for a new indicator and cannot be used for an existing indicator.
Severity	Severity of the Indicator. The possible values are as follows: ○ **Low** ○ **Medium** ○ **High**
RBAC Group Names	RBAC group names that the indicator would be applied to. The names are in a comma-separated list.

8. Click **Create Indicator**
9. Validate the activity and UI messages.
10. Click the **Microsoft Defender Indicator** tab to view the results.

Update indicators in Microsoft Defender for Endpoint

Update the existing indicators in Microsoft Defender for Endpoint from the list context-menu or from the form view of the Microsoft Defender Indicator respectively.

Before you begin

Role required: sn_si.admin, sn_si.analyst

Procedure

1. Navigate to **Security Incidents** > **Show All Incidents**.
2. Click **Show All Related Lists** and then click the **Microsoft Defender Indicators** tab.

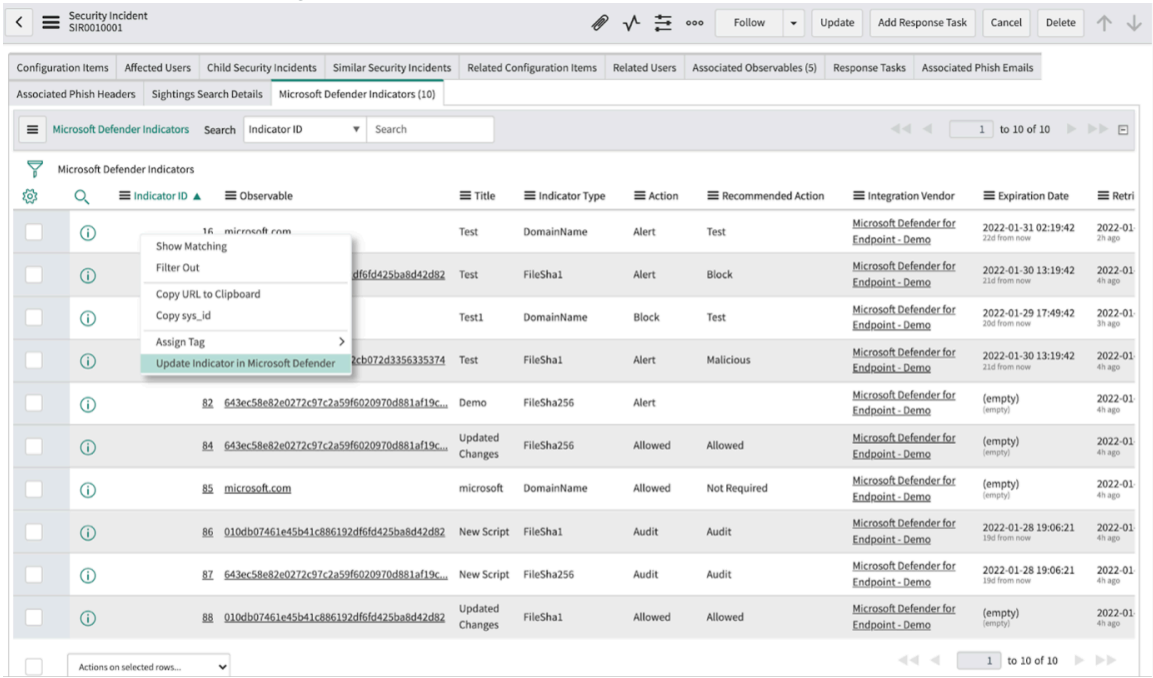
> **Note:**
>
> You must configure the related list for the Microsoft Defender Indicators, which would appear in the Security Incident related lists. For more information, see Form UI actions.

3. Update the Microsoft Defender for Endpoint indicators in one of the following ways:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

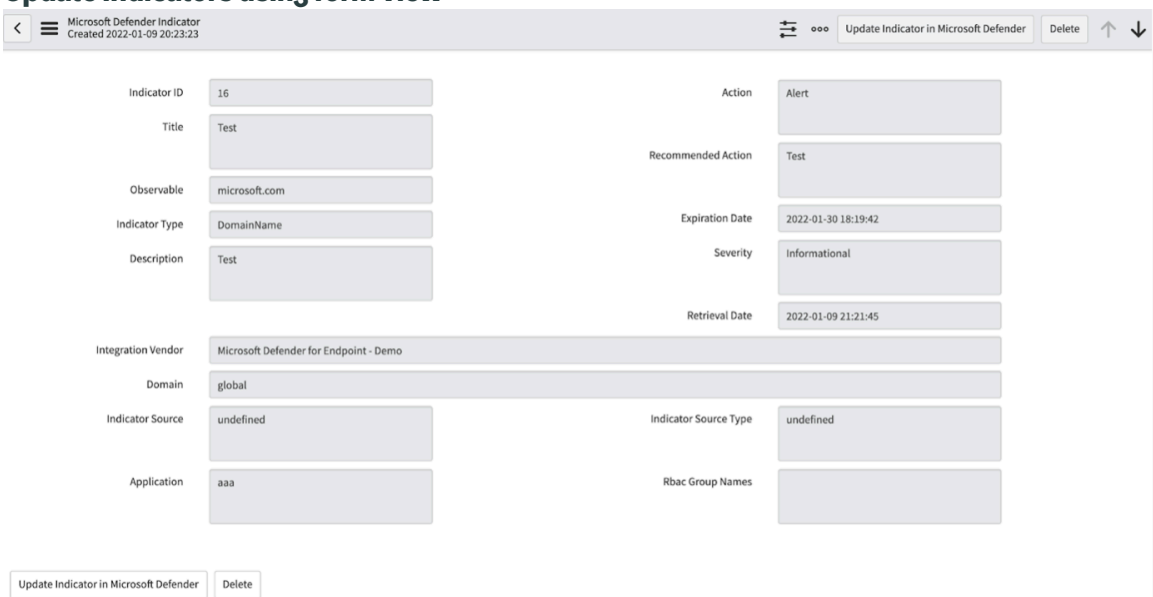
- To update the indicators from the list context-menu, select the row of the indicator that you want to update and click **Update Indicator in the Microsoft Defender** option.

Update Indicators using list context-menu



- To update the indicators from the form view, click **Update Indicator in Microsoft Defender** in the form view.

Update Indicators using form view



4. On the form, fill in the fields.

Microsoft Defender Indicator form

Field	Description
Title	Title for the indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Description for the indicator.
Expiration Time	Expiration time for the indicator.
Recommended Actions	Recommended actions to be performed for the indicator.
Source	Integration configuration to create the indicator.
Action	Actions that are performed if the indicator is discovered in the organization. The possible values are as follows: ○ **Warn** ○ **Block** ○ **Audit** ○ **BlockAndRemediate** ○ **Allowed**
Application	The Microsoft Defender for Endpoint application that is associated with the indicator. This field is applicable only for a new indicator and cannot be used for an existing indicator.
Severity	Severity of the Indicator. Possible values are as follows: ○ **Low** ○ **Medium** ○ **High**
RBAC Group Names	RBAC group names that the indicator is applied to. The names are in a comma-separated list.

5. Click **Update Indicator**.
6. Validate the activity and UI messages.

Domain separation in Microsoft Defender for Endpoint integration

Domain separation is supported in Microsoft Defender for Endpoint integration. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic

Use the following steps for domain separation:

1. Create a user with the sn_si.admin role in the respective domain.
2. Perform the Microsoft Defender for Endpoint integration procedures in the appropriate domain.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Rate limit configuration in Microsoft Defender for Endpoint integration

Configure the rate limit of the API and timeout for the rate limit for Microsoft Defender for Endpoint integration.

Before you begin

Role required: sn_si.admin, sn_si.analyst (read-only)

Procedure

1. In the navigation filter, enter `sys.properties.list`.
   The entire list of properties in the System Properties [sys_properties] table appears.
2. Search and modify the following properties as per your requirements.

Property Name	Description
sn_sec_defender_ep.rate_limit_timeout_in_minutes	If a request does not execute within the specified time frame, the execution gets halted and an appropriate error message is displayed. Default value: 75.
sn_sec_defender_ep.request_per_hour_limit	If the configured API call is made on the same Endpoint within one hour, the request gets queued until the threshold is reached or the configured timeout. Default value: 1500.
sn_sec_defender_ep.request_per_minute_limit	If the configured API call is made on the same Endpoint within one minute, the request gets queued until the threshold is reached or the configured timeout. Default value: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	If the configured API call is made on the endpoint within one minute, the request gets queued until the threshold is reached or the configured timeout. Default value: 30.

Microsoft Exchange Online integration

For the Microsoft Exchange Online integration application by ServiceNow, the ServiceNow AI Platform® Security Incident Response (SIR) product is integrated with the Microsoft Exchange Online service, one of the cloud-based services in the Microsoft Office 365 suite of products. Your Security Operation Center (SOC) analyst can search your corporate email environment for security-related threats and remove and remediate phishing emails with email search and delete capabilities.

Overview of Microsoft Exchange Online integration

As the security incident analyst, you execute the integration from the security analyst interface, and the workflow returns email message details that match search criteria. Email searches are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

based on criteria that include subject lines as well as sender and recipient email addresses. After the email search is complete, you can delete suspicious emails from the Microsoft Exchange Online service, and, an optional approval process can be configured to request approval prior to deleting emails.

This email search and delete integration can be used with a broader phishing response incident workflow or runbook. After a corporate user or employee receives a suspicious email and reports it to the company's phishing response team or inbox, the reported email is forwarded to the ServiceNow AI Platform and categorized as a security incident. After you have verified that an email is a phishing attack, as the analyst responsible for investigating phishing incidents, you can initiate an email search to determine if other corporate users have received this phishing email. The search allows you to locate related emails from the same phishing campaign and identify other potential victims who may have received the email, read it, and also potentially clicked a malicious URL or opened an attachment.

Key features

The integration includes the following key features:

- Configure search criteria for phishing threats in Security Incident Response based on combinations of the sender, recipient, and subject fields on email messages.
- For large and lengthy email searches, the security incident analyst is notified via email when the search has successfully completed, along with the number of matched messages.
- Status for individual messages informs you if recipients have read or deleted suspicious emails.
- If configured, optional approval processes ensure that suspicious emails are not deleted without prior approval.
- A complete audit trail for delete requests that includes the number of deleted emails is logged in the work notes of security incidents.
- If tagging is configured, security tags record when email search and delete workflows are initiated and successfully completed on security incidents.

Supported Microsoft Exchange Online versions

This integration supports Microsoft Exchange Online services, which are part of the Microsoft Office 365 suite. The integration does not support hosted Microsoft Exchange environments. Microsoft runs Microsoft Exchange Online services on the Exchange 2016 version.

Prerequisites

The com.snc.si_dep plugin is required for any ServiceNow AI Platform version. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up your Microsoft Azure account

Complete the following setup tasks in your Microsoft Azure portal prior to installing the ServiceNow application for this integration. This account permits access to the Microsoft Exchange Online tenant for email message details.

Before you begin

Role required: Microsoft Azure portal administrator

This account is required to access the Microsoft Exchange Online tenant to gather additional email message details and to delete email messages. This account is set up in the Microsoft Azure portal.

The images in the following tasks are privileged and proprietary and are used with permission from Microsoft. This content is subject to updates by Microsoft. To verify that you have access to the most current content, see the Microsoft doc website.

In the following images, `ServiceNow Inc.` is displayed for the account name in the examples for the Azure portal. In your Azure portal account, the company name for your account in the Azure portal is displayed.

Procedure

If you have not created an application ID for OAUTH authentication in the Microsoft Azure portal, follow these steps.

a. Log in to the Microsoft Azure portal using your Azure portal administrator credentials.

b. Select **Microsoft Entra ID**.

c. In the Overview pane that is displayed, select **App registrations**.

d. In the App registrations pane that is displayed, select **New registration**.

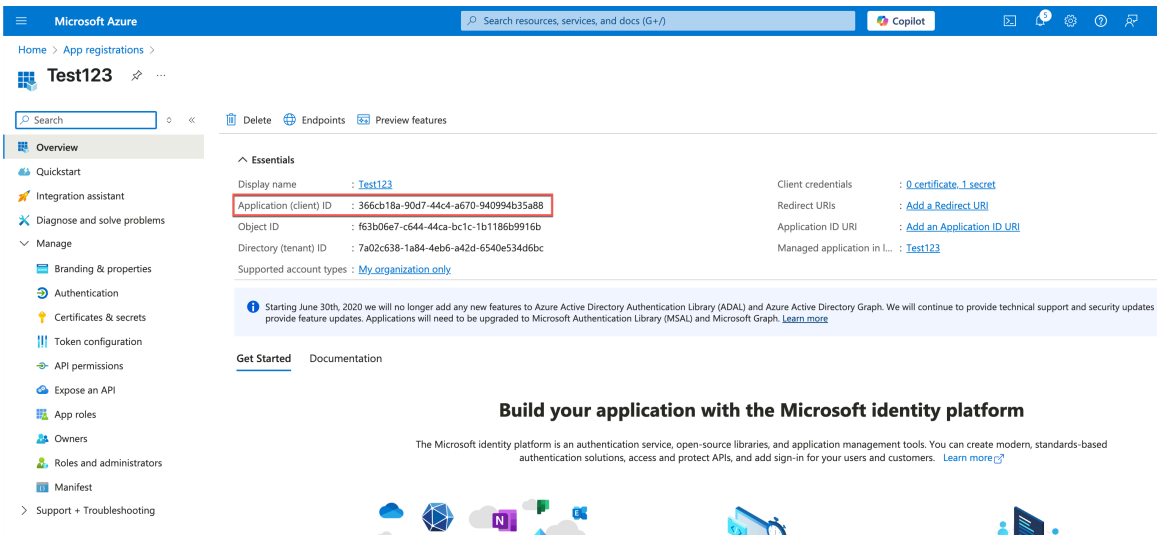
e. Fill in the Register an application form that is displayed.

Field	Description
Name	Name for the application. In this example, `ServiceNow Exchange Online Integration` is entered.
Supported account types	For this account, in Supported account types, select **Accounts in this organizational directory only (your organization name)**. This domain is used for the email searches.
Redirect URL (optional)	If you enter a value for this field, it is not used by the integration.

f. Select **Register**.
An Application ID is created. This ID is similar to a user name. You enter this value on the configuration page in the **OAUTH Application ID** field during the configuration step in your ServiceNow AI Platform instance that is described in Configure the Microsoft Exchange Online integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

g. With the Application (client) ID displayed in the ServiceNow Exchange Online Integration pane, select **API permissions**.



h. In the ServiceNow Exchange Online Integration - API permissions pane that is displayed, select **Add a Permission**.

i. In the Request API permissions pane that is displayed, select **Microsoft Graph**.

j. In the Request API permissions pane that is displayed, select **Application permissions**.

k. In the Select Permissions field that is displayed, enter **Mail.ReadWrite** and select the **Mail.ReadWrite** check box.

l. Select **Add Permissions**.

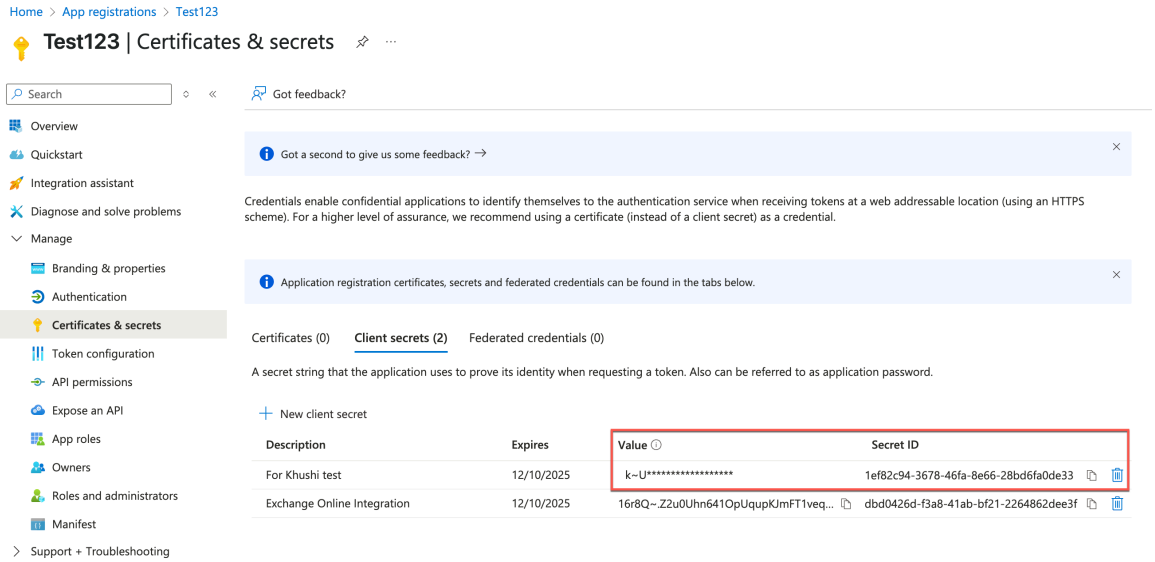
m. In the ServiceNow Exchange Online Integration - API permissions pane that is displayed, click **Grant Admin Consent for <your organization name>**.

n. To confirm the previous API selection (Microsoft Graph API) that you entered, click **Confirm**.

o. In the ServiceNow Exchange Online Integration - Certificates & Secrets pane, select **Certificates & secrets** followed by **New Client secret** (password).

p. In the form that is displayed on the ServiceNow Exchange Online Integration - Certificates & Secrets pane, enter the name for the application in the `Description` field, click an option for expiration, and select **Add**.
In the Certificates & Secrets pane that is displayed, in the **Client secrets** section, under `Value`, the row is populated with the new client secret (password). Save this password in a secure location. After you leave this page, this password value is no longer visible. You enter this password in the **OAUTH Client Secret** field on the configuration page during the configuration step for the integration in your ServiceNow AI Platform instance. The configuration steps for the integration are described in Configure the Microsoft Exchange Online integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You have successfully created an application ID for OAuth authentication in the Microsoft Azure portal.

What to do next

You are ready to set up your ServiceNow AI Platform® instance for the integration.

Install Microsoft Exchange Online application

Before you run the integration on your instance, install the Microsoft Exchange Online application for the integration from the ServiceNow Store.

Before you begin

Before you install the application from the ServiceNow Store on your ServiceNow AI Platform instance, complete all the tasks listed in the prerequisite checklists.

Role required: admin

Procedure

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you've installed the application from the ServiceNow Store, configure it to connect to your ServiceNow AI Platform instance.

Configure the Microsoft Exchange Online integration

After you've installed the application from the ServiceNow Store, configure it to connect to your ServiceNow AI Platform instance. This activation activates the search and delete workflows.

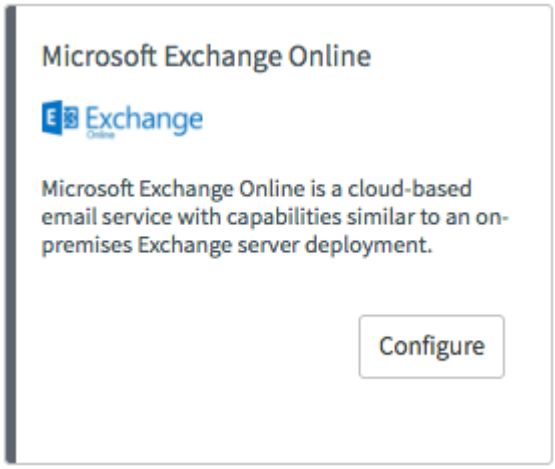
Before you begin

Role required: sn_si.admin

Procedure

1. In your ServiceNow AI Platform instance, navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
2. Locate the Microsoft Exchange Online tile.
3. Click **Configure**.

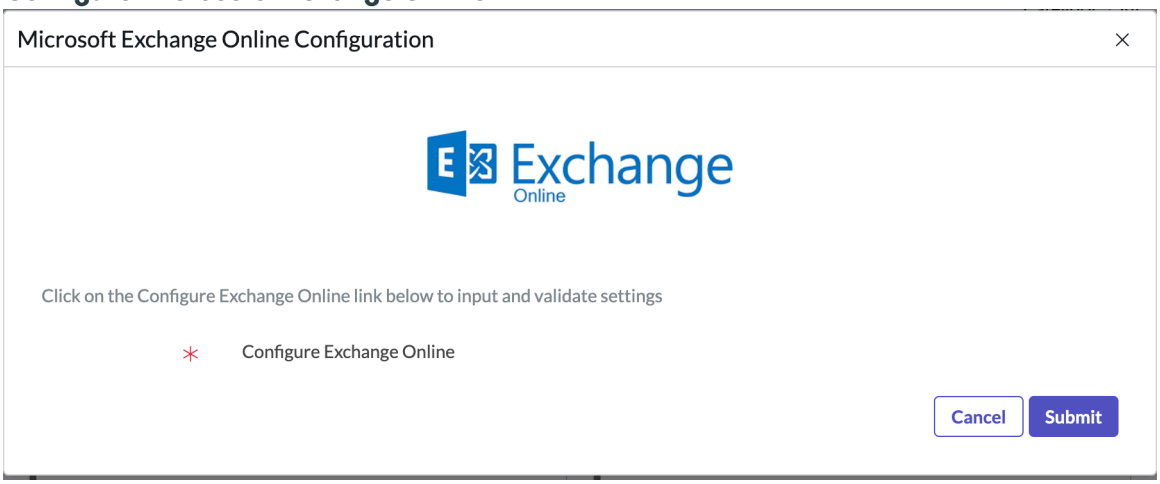
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In the Microsoft Exchange Online Configuration dialog that is displayed, click **Configure Exchange Online**.

   An example of a completed and validated form follows the table.

Configure Microsoft Exchange Online



Option	Description
Connection Settings tab	
Tenant	The Microsoft Exchange Online tenant that you want to perform searches on. This text is the unique name that appears after @ for email addresses for your organization. For this example, `snowsecops.onmicrosoft.com` is the tenant (domain).
Certificate Thumbprint	A certificate thumbprint is a hash of a certificate, computed over all certificate data and its signature. Thumbprints are used as unique identifiers for certificates, in applications when making trust decisions, in configuration files, and displayed in interfaces.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
OAuth Application ID	The Application (client) ID that was generated for the account that you created in the Microsoft Azure portal. For more information, see Set up your Microsoft Azure account.
OAuth Client Secret	Password (client secret) for the account that you created in the Microsoft Azure portal. For more information, see Set up your Microsoft Azure account.
Additional Settings tab	
Email Search Window (days)	The email search history range in number of days. The integration searches for email messages that have been sent or received in the Microsoft Exchange Online server for the number of calendar days that you enter. You're required to enter a value between 1-30. 30 days is the default and the maximum number of days you can enter for a search. Entering a low number of days in the search window range improves response time, but you may not capture all matched messages as a result. This global setting is for all searches. Prior to executing the email search, there are no parameters that permit you to change this value for individual searches.
Maximum Search Duration	Use this option to set the search timeout threshold. If the timeout threshold is reached, the search ends and no results are displayed. You can specify a default value of 90 minutes and a maximum value of 240 minutes. By setting this threshold, you can avoid endless search loops that could cause performance issues on the Microsoft Exchange Online tenant and the ServiceNow instance.
Tagging	Security tag. Default is selected. When enabled, security tags are automatically applied to related security incidents when search and delete capabilities are initiated and successfully completed. The default tag names are displayed, but tag names and colors can be edited. For more information, see Edit security tags for the Microsoft Exchange Online integration.

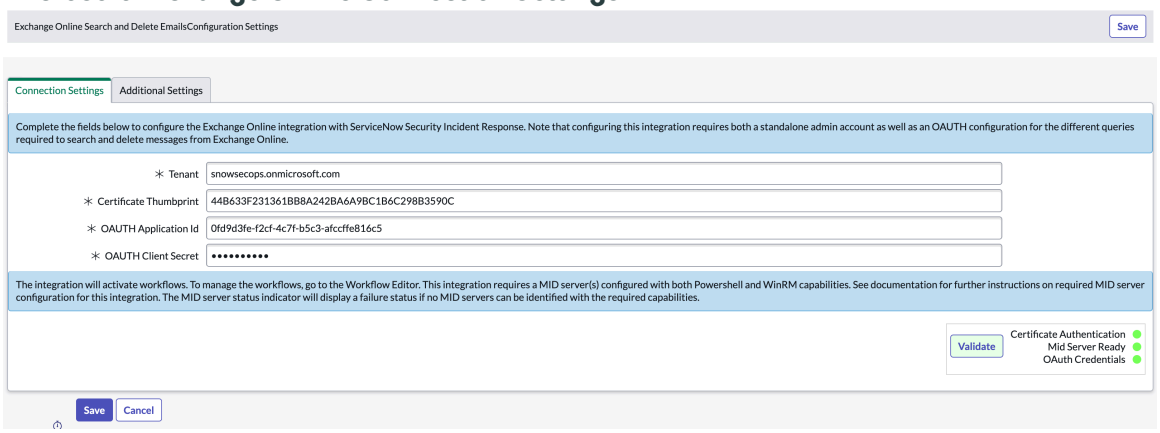
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Recover Deleted Emails	Default is selected. This item only applies to emails that you have deleted using this integration. If you don't want users in your organization to have access to the emails that you've deleted, verify that this check box is cleared. If the check box is cleared, the emails that you delete using the workflow of this integration are permanently deleted and placed in the Purges folder. This folder is a sub folder within the Recoverable Items folder on Microsoft Exchange Online that a user normally can't access. If you want users to recover the emails you delete, select this check box. If this check box is selected, depending on how the user's account is configured in Microsoft Exchange Online, the emails you delete using the workflow of this integration are placed in the Deleted Items folder in the mailbox of the user. If an account is configured so that the user can view the Deleted Items folder in their mailbox, the user can recover the emails you delete from their Microsoft Exchange Online account. For more information, see Recover deleted items or
Search Completion Notification	Select this option to enable notifications when the search is completed. If the **Enable** check box is selected, you'll receive notifications if any matching emails are found. If the check box is cleared, search completion notifications aren't sent.
Approvals	Request approval to delete emails. Default is cleared. When the check box is cleared, the optional approval process for requesting prior permission before deleting emails from the Microsoft Exchange Online service is disabled. Verify that this check box is cleared if you want to grant your security incident analyst permission to delete emails without requesting prior permission. If enabled, a request is submitted via email to each member of an approval group. From the list, select an approval group from the list.

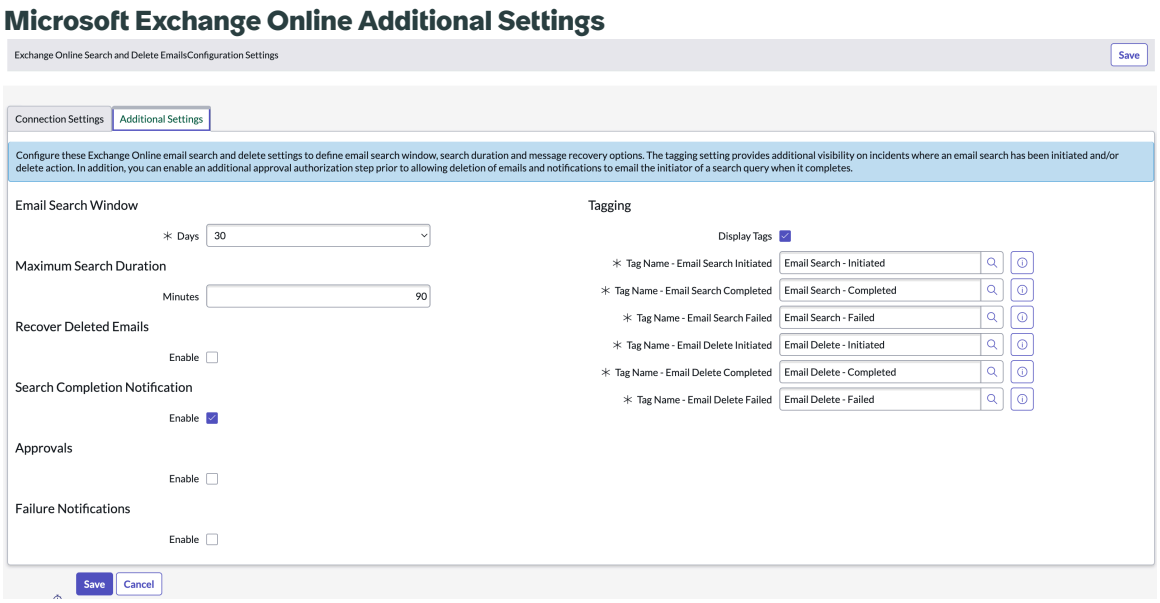
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	After a request is submitted to an approval group, only one approval is required from the group to complete the request. Any member of the approval group has approval authority. Having a group with more than one person with approval permission ensures that these requests are processed in a timely way.
Failure Notifications	Select the check box to enable failure notifi cations when the search or delete action fails due to invalid OAuth credentials. If Enabled, failure notifications are sent through email to each member of the failure notifications group when OAuth credentials are invalid. If the check box is cleared, no failure notifica tions are sent.
Email Result Threshold	From version 10.3 or later, you can specify an email delete threshold for approvals. If the number of emails being deleted is greater than or equal to the value specified here, the Delete request must be approved before the Delete action is invoked. If the threshold val ue is set to 1, every Delete request must be ap proved.

Microsoft Exchange Online Connection Settings



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Choose one to continue.

Option	Description
Save	Save your edits. This action doesn't verify your connection.
On the Connection Settings tab, click Validate.	This action validates your Certificate authentication, your MID server connection, and OAuth credentials. If your credentials are valid, the **Validate** button and both indicators are green.

Trouble?
If an error message is displayed, or one or more of the indicators to the right of the Validate button are red, verify that the user account credentials you entered are valid. Enter your credentials and click **Save** again.



Refer to the following table for more information about the **Validate** button and the colored icons.

State of Validate button and indicators	Description
Validate button is green and all the small colored indicators are green.	Indicates that the MID Server connection and the credentials are valid.
Validate button is light red with a blue border and one or all the small colored indicators are orange.	The validation is in process. Validation may take a few more moments to complete.
Validate button is light red and one or all of the small colored indicators are red.	• Exchange Online certificate-based authentication or OAuth credentials button is red: Indicates that the Exchange Online certificate-based authentication or OAuth credentials are invalid.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State of Validate button and indicators	Description
	• Exchange Online certificate-based authentication and MID Server Ready buttons are red: Indicates that the MID Server isn't reachable and therefore, Exchange Online certificate-based authentication through the MID Server has failed. • Exchange Online certificate-based authentication indicator is red but MID Server Ready button is green: Indicates that the MID Server is active and configured correctly, but the Exchange Online certificate-based authentication are incorrect.

Define email search criteria and request a search on the Microsoft Exchange Online service

As a user with the sn_si.analyst role, define search criteria and submit an email search request based on incident details on a security incident record.

Before you begin

Role required: sn_si.analyst

The figures in this procedure are shown with **Tabbed forms** selected in System Settings. For more information about selecting and clearing tabbed forms, see the section titled, Display tabbed forms in Configuring the form layout on the ServiceNow Product Documentation website.

Role required: sn_si.analyst

About this task

The status of individual messages that match the search query and the results of the search are reported on the security incident record. If email notifications are enabled, you can view the search results from an email message.

Search criteria may include message sender addresses, recipient addresses, or subject names. The following combinations of message Subject, Sender, and Recipient search parameters are often used for finding phishing-related email messages that may be part of a single phish campaign:

- Find all original emails sent by a phishing account: Search by sender.
- Find all original emails for a single phishing campaign: Search by subject and sender.
- Find all emails received for a single phishing campaign (original and forwarded, any sender): Search by subject.
- Find all forwarded emails for a single phishing email from a single user: Search by recipient + subject.
- Find all phishing-related emails sent to a single user: Search by sender + recipient.

Note: Searches are conducted on emails sent or received within last 30 calendar days, unless a shorter search window is configured during the initial setup. A successful email search is required before you can delete emails.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows you how to initiate a search from a ServiceNow AI Platform security incident. A security incident is created based on the original email of a suspected phishing attack in the Microsoft Exchange Online server of your organization. For this example, the search criteria is Sender (From) plus Subject, where From is `phisher@cbazyx.com`, and the Subject is `log in to your account`.

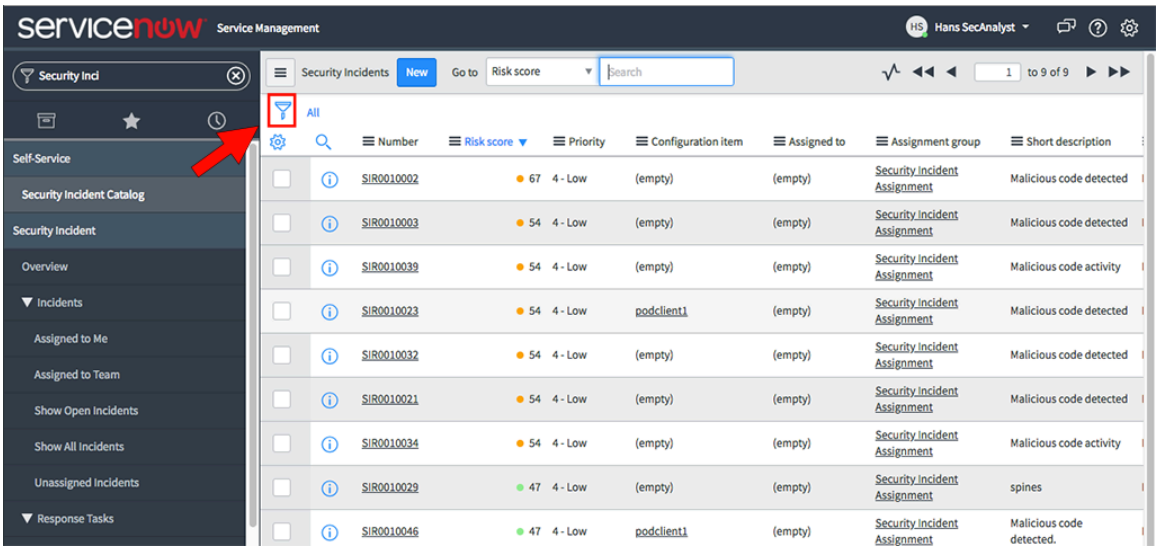
Results for searches on subjects are returned when the search finds text strings that contain key words that match the entered search criteria. In this example, the subject is `log in to your account`. Use the **AND** operator to separate the From and Subject search conditions to return results for all the email messages that contain these given search criteria. The following steps describe how to set up a search that finds only emails that contain subject line text sent by a specific phishing account.

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents** and locate the security incident that you are working with.
2. Alternatively, follow these steps to set and run a filter so that only security incidents created by phishing events are displayed.

   a. Navigate to **Security Incident** > **Show All Incidents** to open the Security Incidents list.

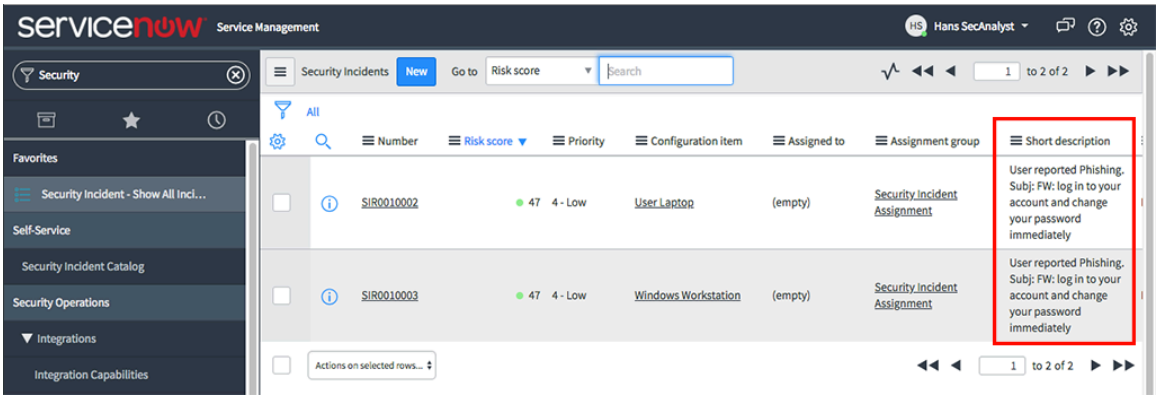
   b. In the upper-left corner of the list that is displayed, click the filter icon.



   c. In the fields that are displayed, select **Short description** > **contains** from the choice lists, then enter **user reported phishing** and click **Run**.

      The phishing-related security incidents are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

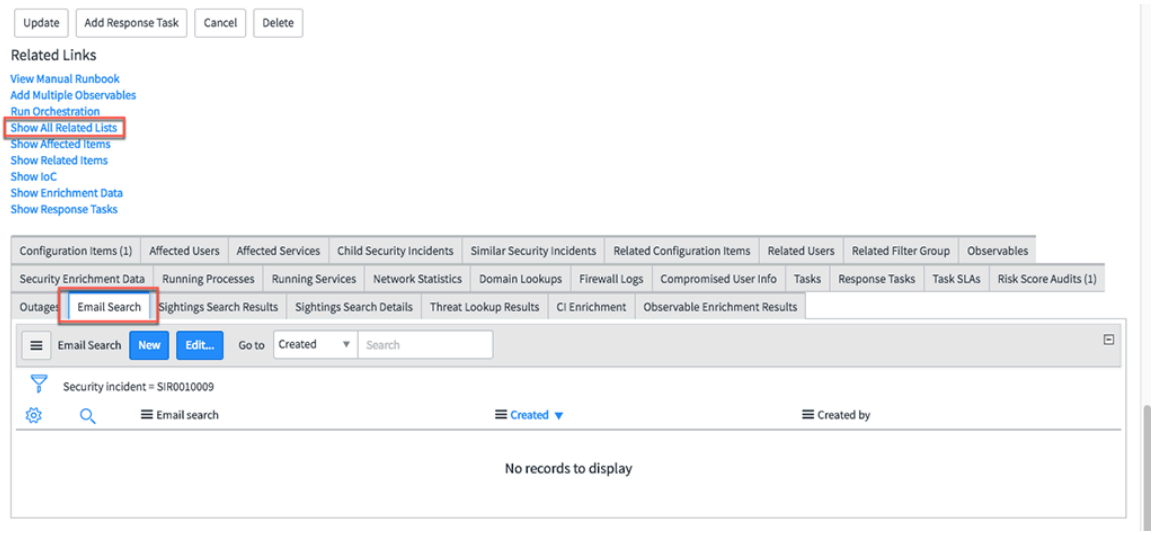


d. Use the text in the Short description column to help you locate the security incident that you are working with.

e. In the Number column, click a security incident to open a record.

3. Scroll to the bottom of the Security Incident record and click the Email Search related list.

If the Email Search related list is not displayed, click the **Show All Related Lists** related link to display this related list.



4. In the Email Search related list, click **New** to create a new email search record.
The Email Search form is displayed. If you determine that you want to rerun this search query for the same phishing-related incident with minor modifications, you can use this search query record again. However, it is unlikely that you would use this search for a different phishing-related incident, because phishing campaigns are dynamic and the sender and message fields often change.

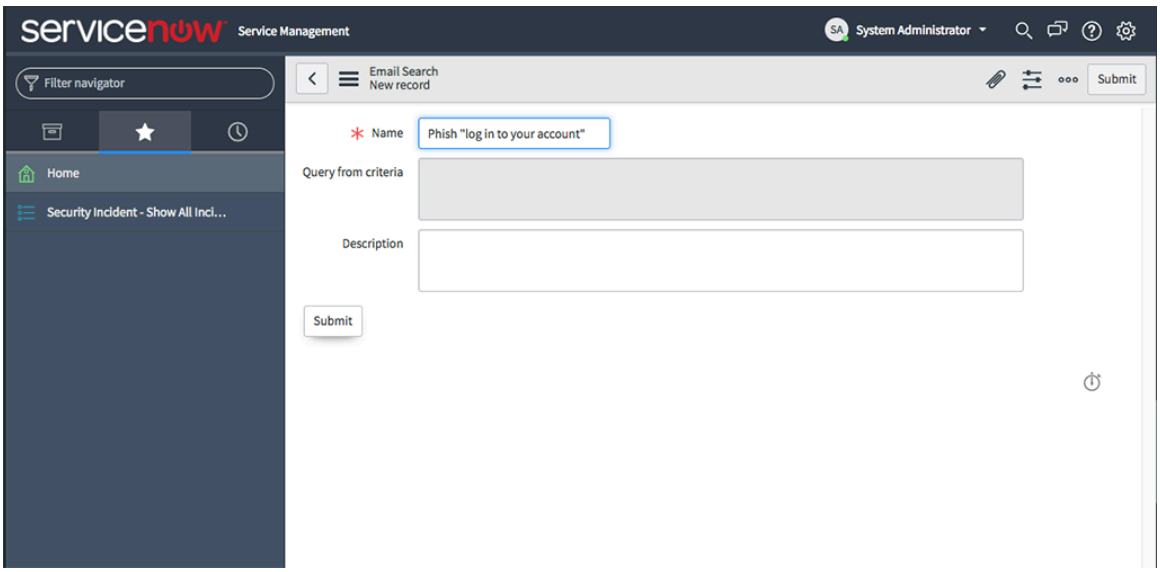
5. Optional: To edit an existing search query record, click **Edit**.

6. On the Email Search form, fill in the fields.

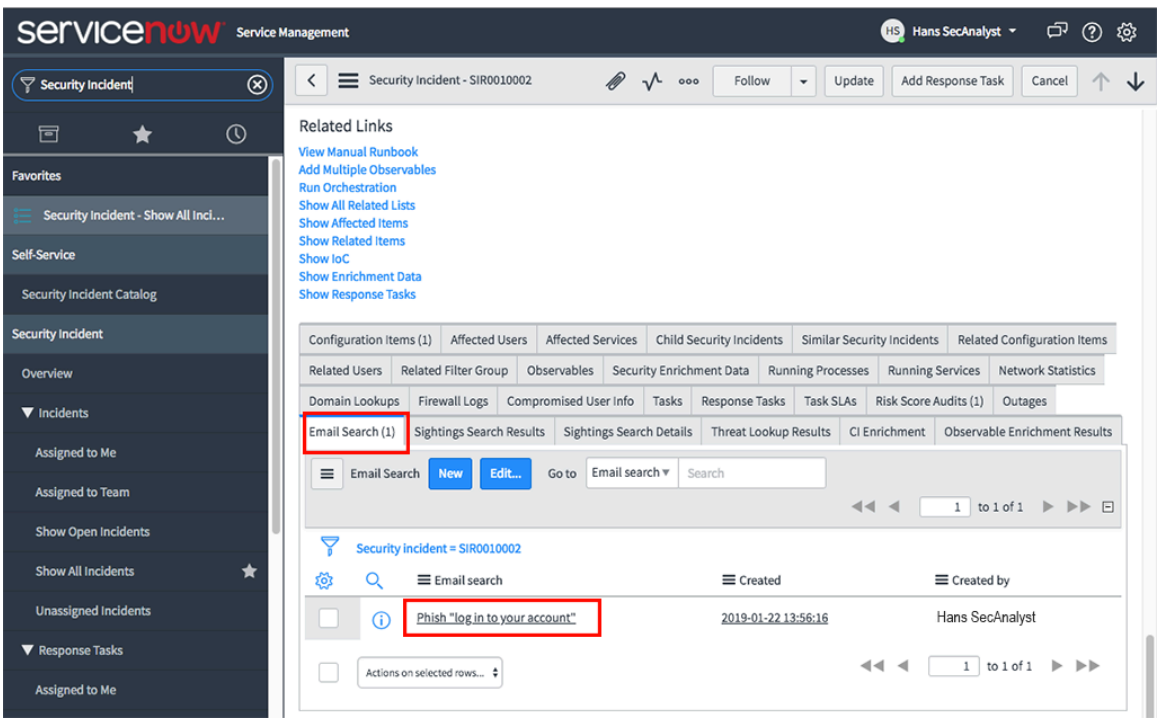
Field	Description
Name	Information to describe the type of search. For this example, a name for a From + Subject

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	search is `Phish "log in to your account"`.
Description	Information about the search in the email server. An example for this search is `From=phisher@cbazyx.com + Subject=log in to your account`.

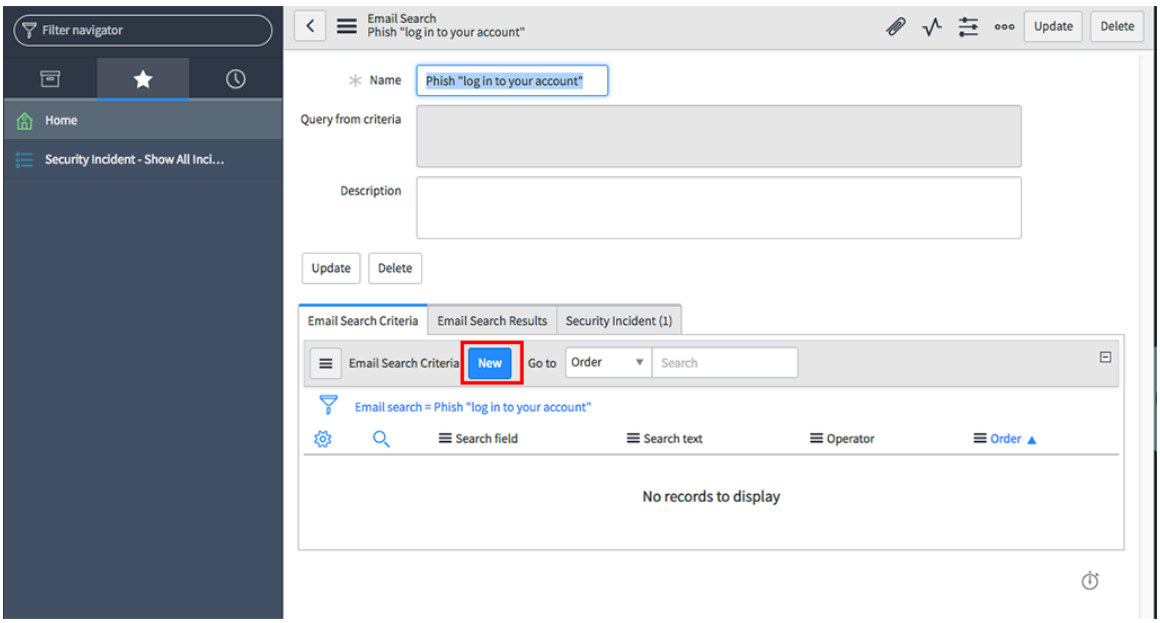


7. Click **Submit**.
   The security incident is displayed and the name of the email search is displayed in the Email search column in the Email Search related list. Before you can use this new search query, search criteria must be defined for the search record.
8. To define search criteria, with the Email Search related list selected, in the Email search column, click **Phish "log in to your account"**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. On the Email search record that is displayed, click the Email Search Criteria related list, and click **New**.



10. On the Email Search Criteria form, fill in the fields.

    An example of a completed form follows the table.

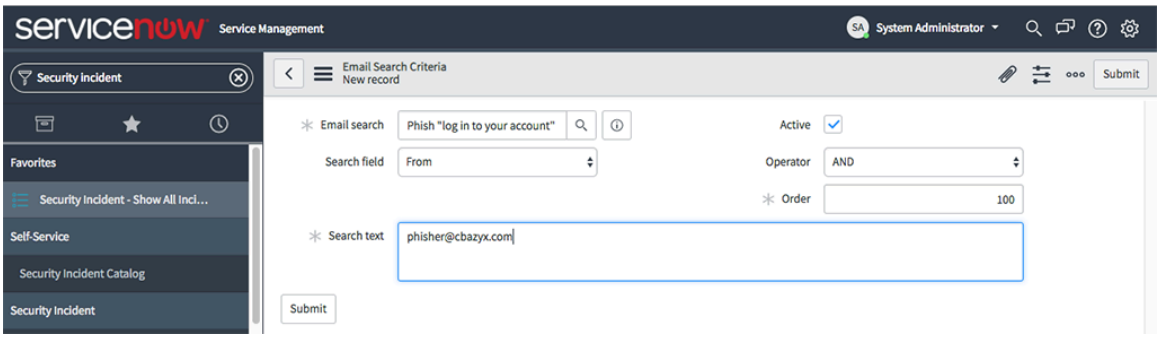
Field	Description
Email search	Field is populated automatically with the name that you entered for the Email Search record.
Search icon	Lookup using list. A list of saved searches. Click the icon to open a list of saved email searches. Click an item in this list to remove the current search and select a previously saved email search.
Information icon	Icon used to view the Email Search record. Click the icon to view the email search record.
Search field	Search criterion (**Subject**, **From**, or **Recipient**). Select the search criterion from the choice list and define a value that you want to search for in the text field. For this example, start with From `phisher@cbazyx.com` (the email address of the sender of the phishing email).
Active	Option for activating the search. The search is activated by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

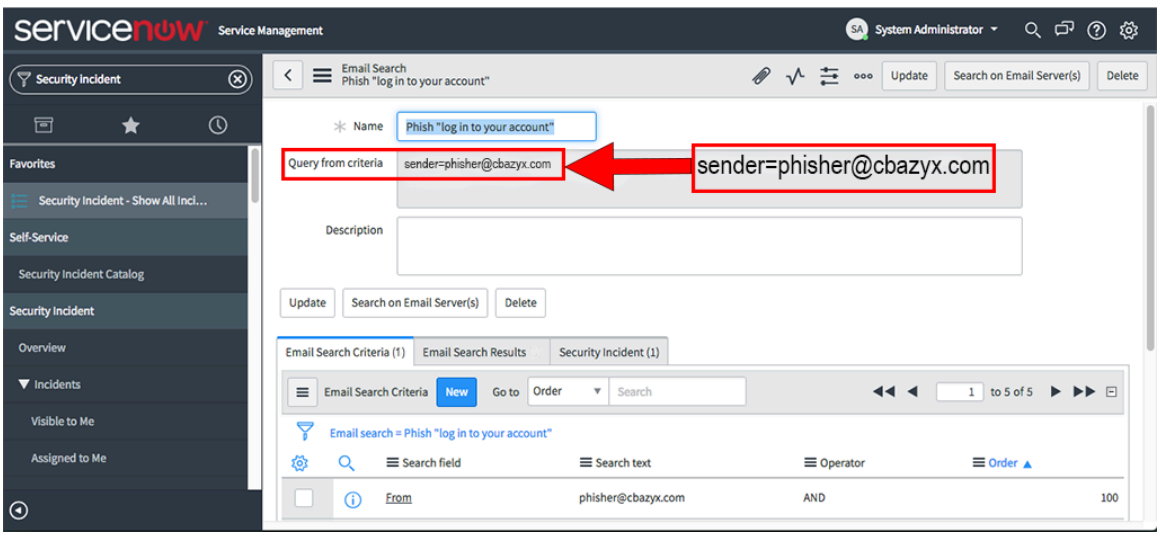
Field	Description
	If you clear this option, this record is not included in a search.
Operator	Operators (**AND**, **OR**) to further define your search. **AND**: The system searches for the conditions separated by **AND** and returns results only if all the conditions are met. For the sender-plus-subject search, use the **AND** operator so that both search conditions are met during the email search. For this example, use the **AND** operator so that the query is From (Sender) = `phisher@cbazyx.com` **AND** Subject = `log in to your account`. **OR**: The system searches and returns results if any of the conditions separated by **OR** are met. An example is From (Sender) = `phisher@cbazyx.com` **OR** From (Sender) = `phisher-2@cbazyx.com`.
Order	If you enter more than two search conditions, use Order to prioritize the conditions. 100 is the default. Enter a value between 1 and 100 for each condition, for example, 100, 95, 90, 80. The condition with the lowest number assigned has the highest search priority within a group of conditions.
Search text	The text values (key words) for the search (email addresses or subject lines). The search field contains the text used in the search, for example, `phisher@cbazyx.com`. For the search to return results accurately for Sender (From) and recipient searches, the search strings must match exactly. For subject searches, the search string can contain key words that are part of a larger string. For example, a subject may contain the exact search string that is matched in a forwarded or a response message header such as `FW: log in to your account and change your password immediately`. For example, `Log in to your account` are exact key words in the string `log in to your account and change your password immediately`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	No wildcard (*) designation is required to support a contains type of search. Currently, no filtering method exists for matching an exact search string that is not part of a larger text string.



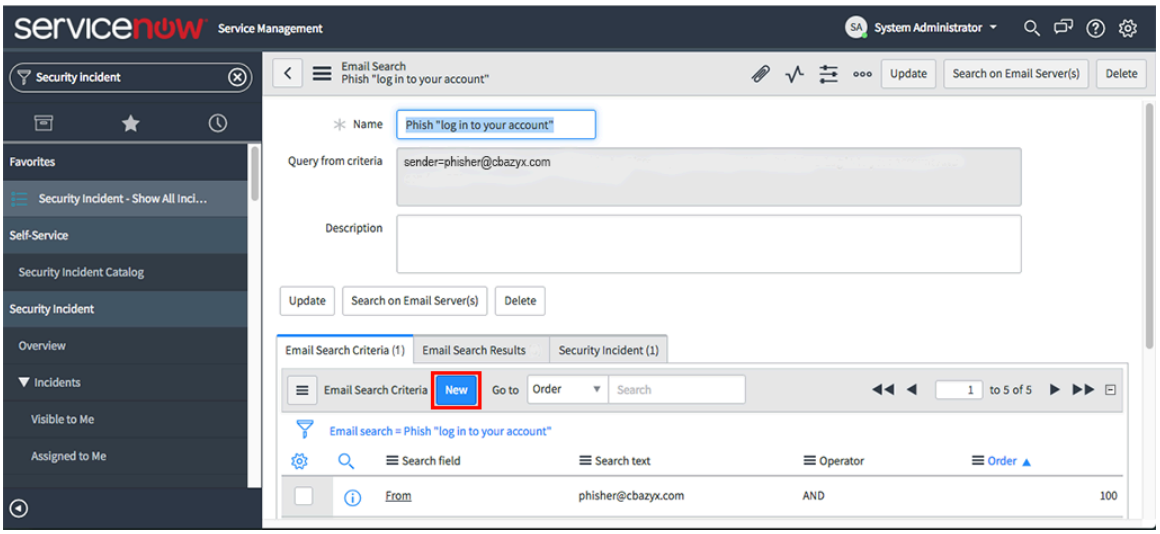
11. Click **Submit**.
The Email Search record is displayed. In the **Query from criteria** field, the search criteria you added for the Sender (From) is displayed.



12. To update this email search criteria with more information so that the query includes the subject-plus-sender condition that you want, follow the steps to add another search condition.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

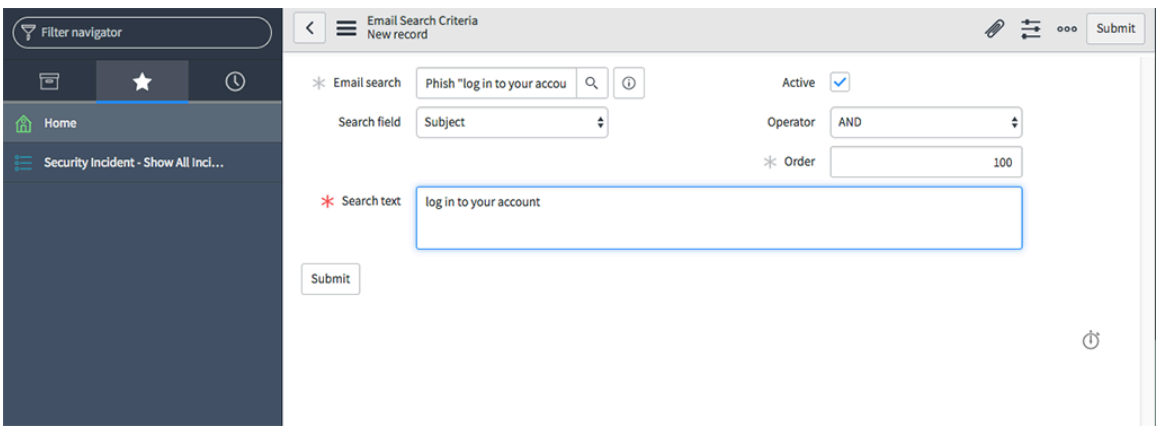
a. In the Email Search Criteria related list, click **New**.



b. From the **Search field**list on the Email Search Criteria record that is displayed, select **Subject**.

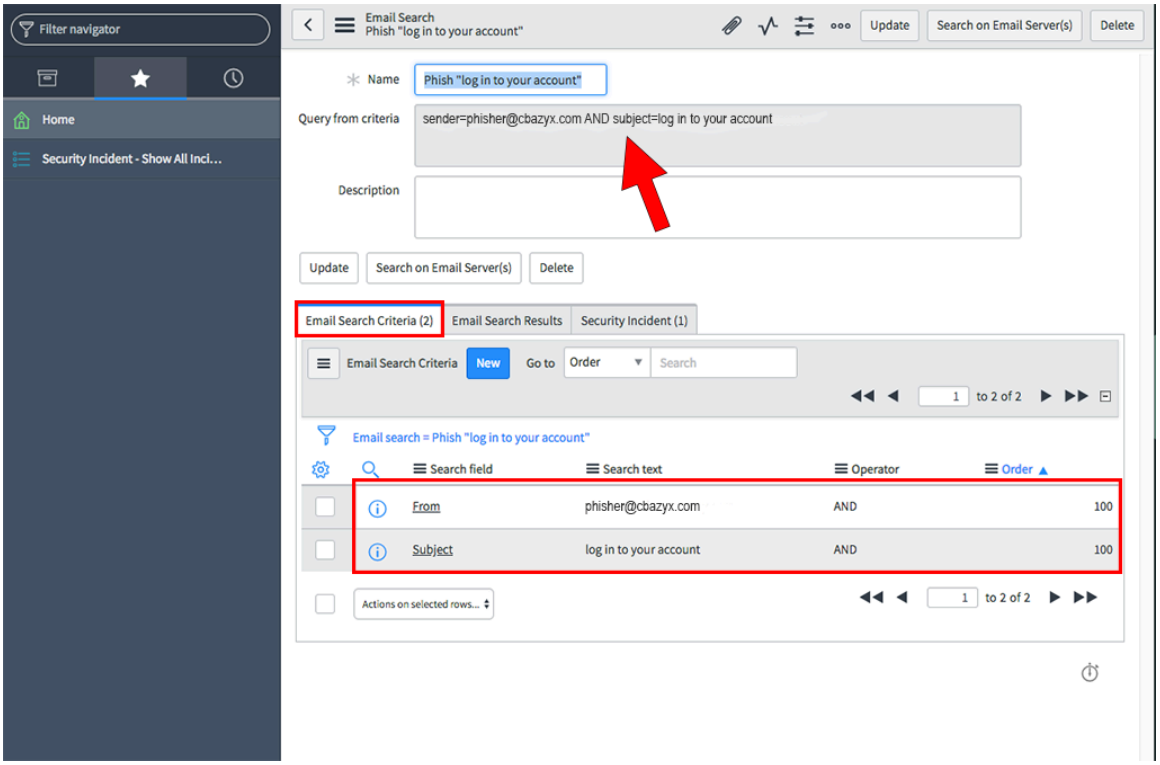
c. From the Operator list, select**AND** or **OR**.
If you select **OR**, the search returns results if either key words in the subject line text string are matched, or the email address condition is matched. **AND** is selected for this example so that the search returns results only for emails that contain the key words of the subject text string and that match the email address of the sender.

d. In the **Search text** field, enter the value for subject line text, `log in to your account`.



e. Click **Submit**.
The new condition is displayed in the Email Search Criteria related list, and both conditions are displayed in the **Query from criteria** field separated by the **AND** operator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



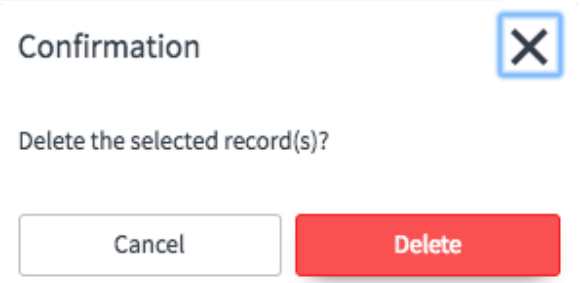
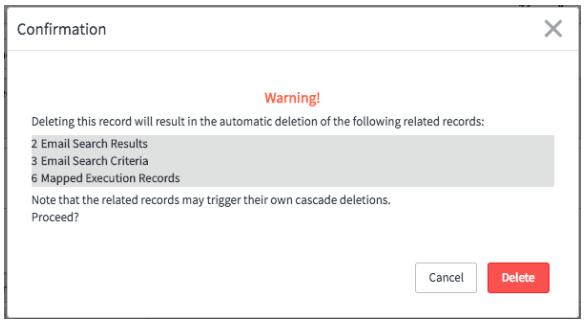
f. Optional: If you have more than two search conditions, and you select **AND** to separate each condition, set the order value to prioritize them.

g. Continue to add, modify, or remove search criteria as desired and click **Update** to save your changes to the record.

13. Choose one option to continue.

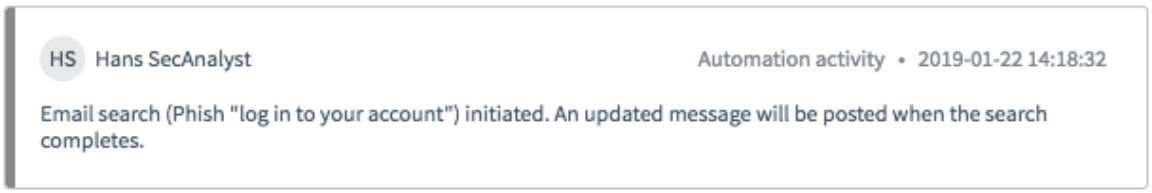
Option	Description
Update	Update and save your changes to the record.
Search on Email Server(s)	Initiate a search on the servers with the crite ria that you saved on the Email Search Crite ria record.
Delete	Delete this Email Search record from your ServiceNow AI Platform instance. This action does not delete the actual email messages. It only deletes the search record used for find ing messages. A dialog box is displayed. If you click **Delete**, the email search results and email search cri teria for this search record are deleted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	 If a record has search results, the following warning is displayed. 

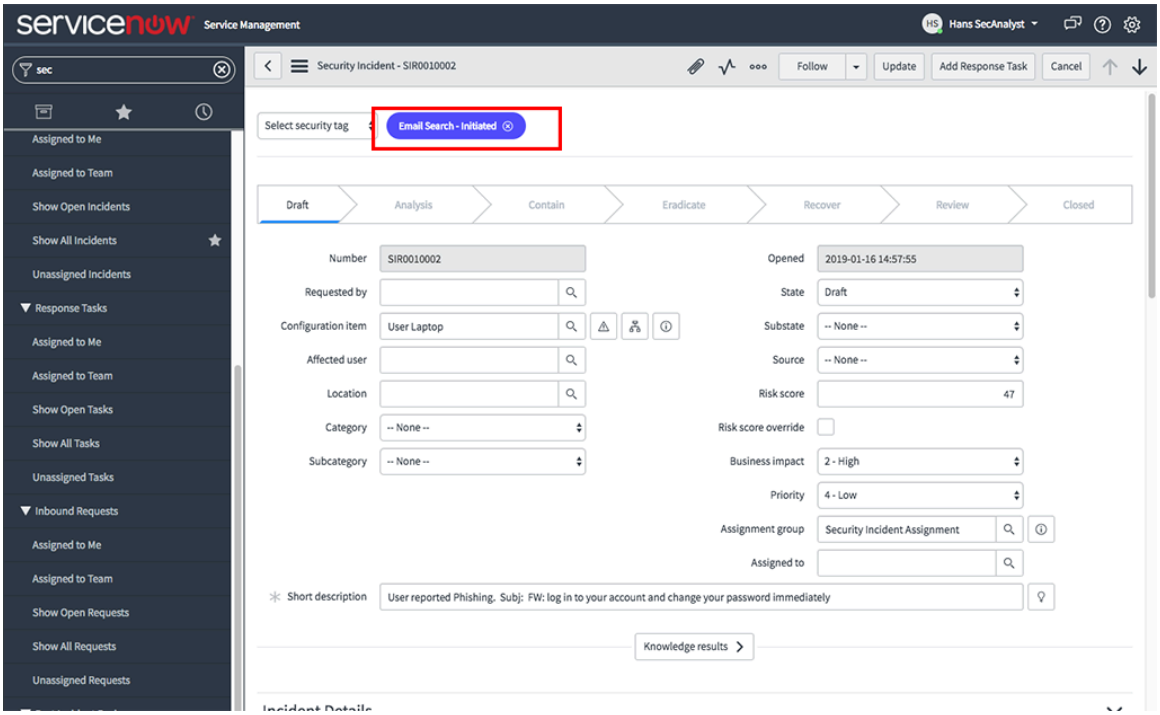
14. To initiate an email search, on the email search record, click **Search on Email Servers(s)**.
    A message is displayed that indicates the search request is submitted.

    On the Security Incident record, a work note is displayed indicating that a search has been initiated.

    If tagging is enabled, at the top of the Security Incident record, the `Email Search - Initiated` security tag is displayed.

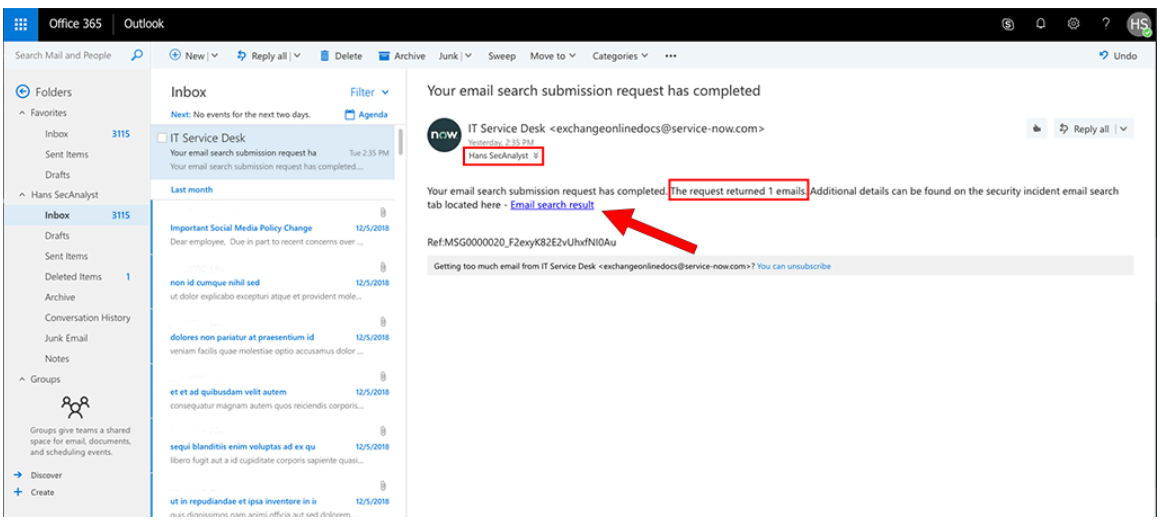
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



After the search is successfully completed, if email notifications are enabled, an email is sent to the email address of the individual who initiated the search.

In this example, the user with the sn_si.analyst role, `Hans SecAnalyst`, submitted this search. The following image shows that this notification is sent to an account in Microsoft Exchange Online. However, these notifications can be sent to a different email service, as required.

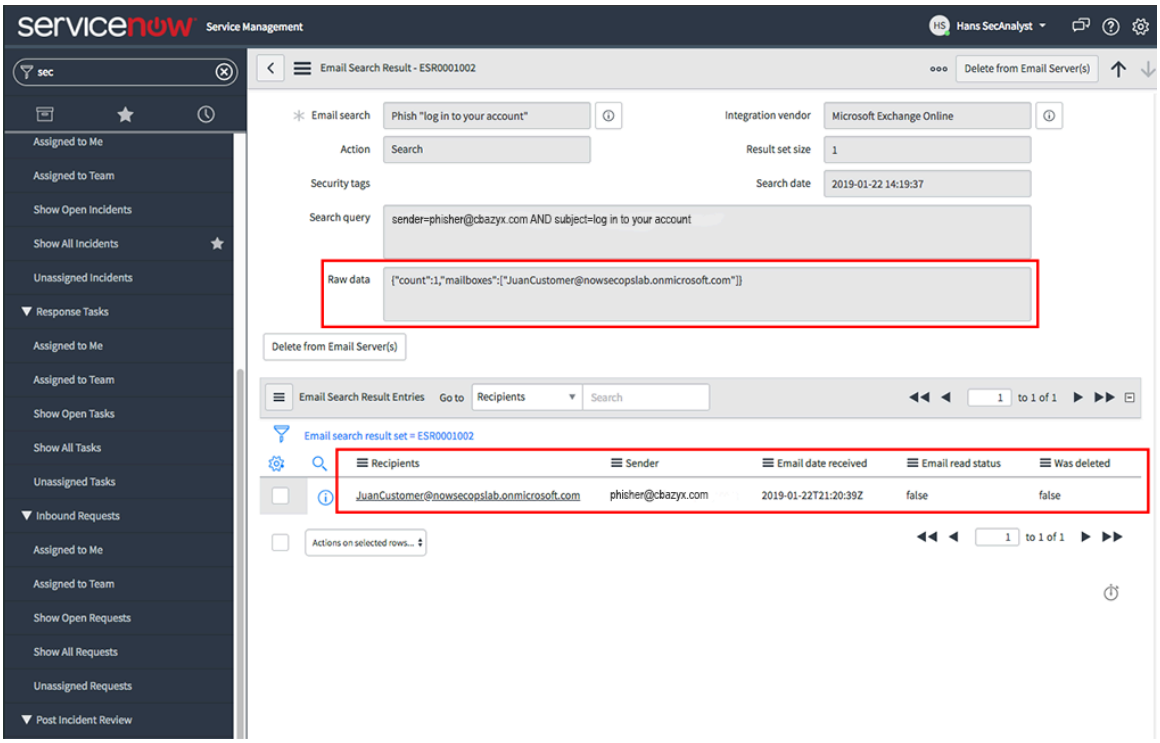
This notification lets you view any matched results that require follow-up and deletion. The following example shows that there is one email that matched the search criteria. An Email search result link to the email search result record in your ServiceNow AI Platform instance is also provided. If you want to view the search record, click this link.



15. From this email, to view the search results, click the **Email search result** link.
    The email search result record is displayed. On this record, you can verify and review the following data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

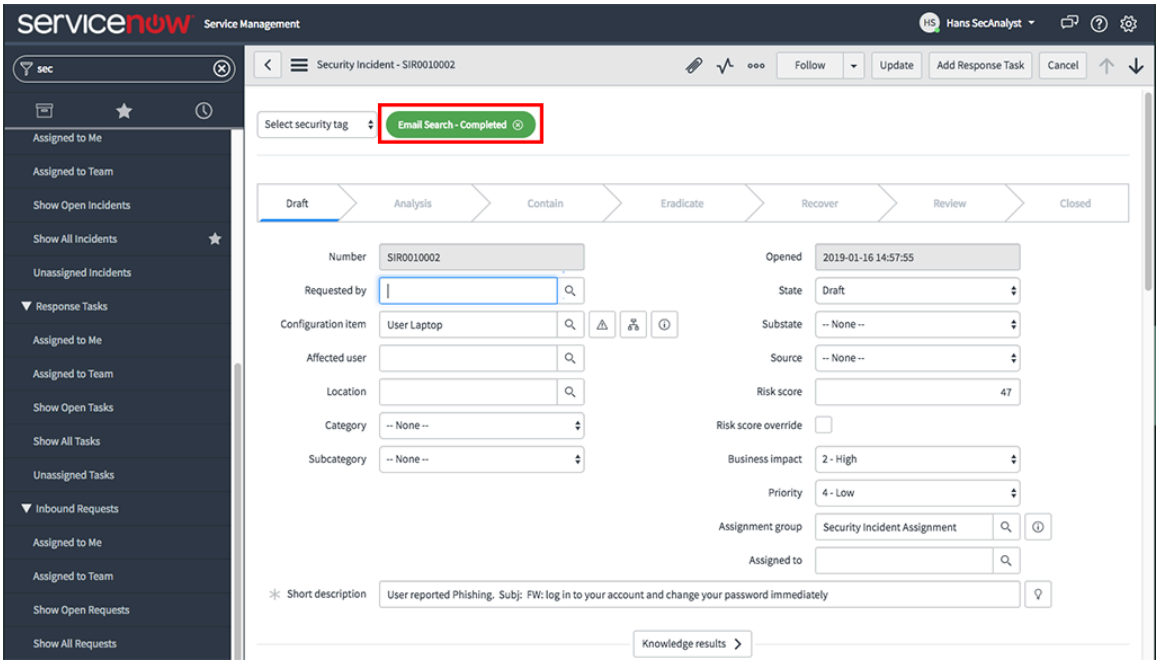
- In the **Raw data** field, the email count for the number of emails that matched the search criteria `{"count":1}`, and the mailbox addresses where the emails were found are displayed `["JuanCustomer@nowsecopslab.onmicrosoft.com"]`.
- In the Recipients column, the recipient is (`JuanCustomer@nowsecopslab.onmicrosoft.com`).
- In the `Sender` column, the source of the email is displayed.
- In the `Email date received` column, the date and time the email was received is displayed to help you track phishing campaign time lines.
- In the `Email read status` column, the email in this example has not been read (`false`). If an email has been read, `true` is displayed.
- In the `Was deleted` column, the email in this example has not been deleted. If an email has been deleted, `true` is displayed.



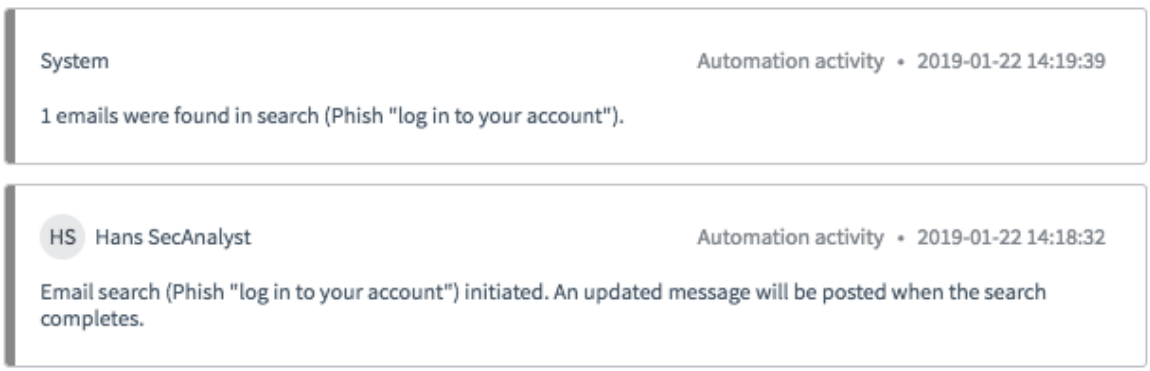
16. Alternatively, to view the search results from the security incident, follow these steps.

a. Navigate to **Security Incident** > **Incidents** and open the security incident that you are working with.
At the top of the record, when the search is successfully completed, the `Email Search - Completed` security tag replaces the `Email Search - Initiated` security tag.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



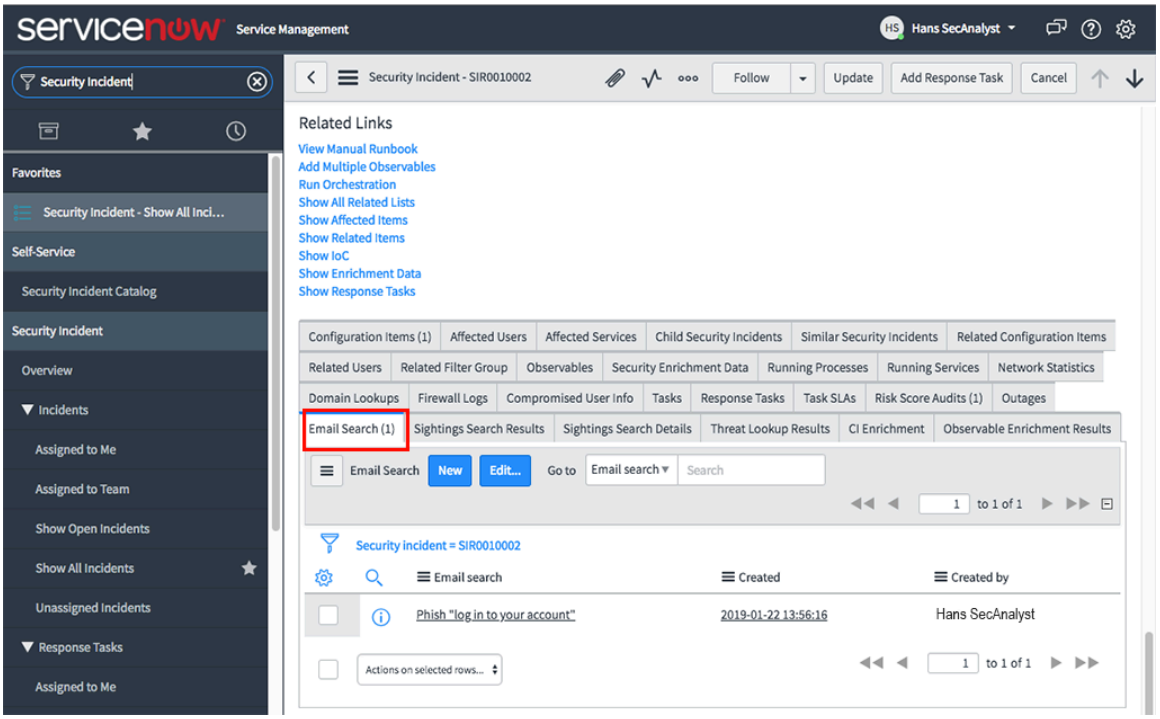
Work notes are displayed that the search is successfully completed and that one matching email was found.



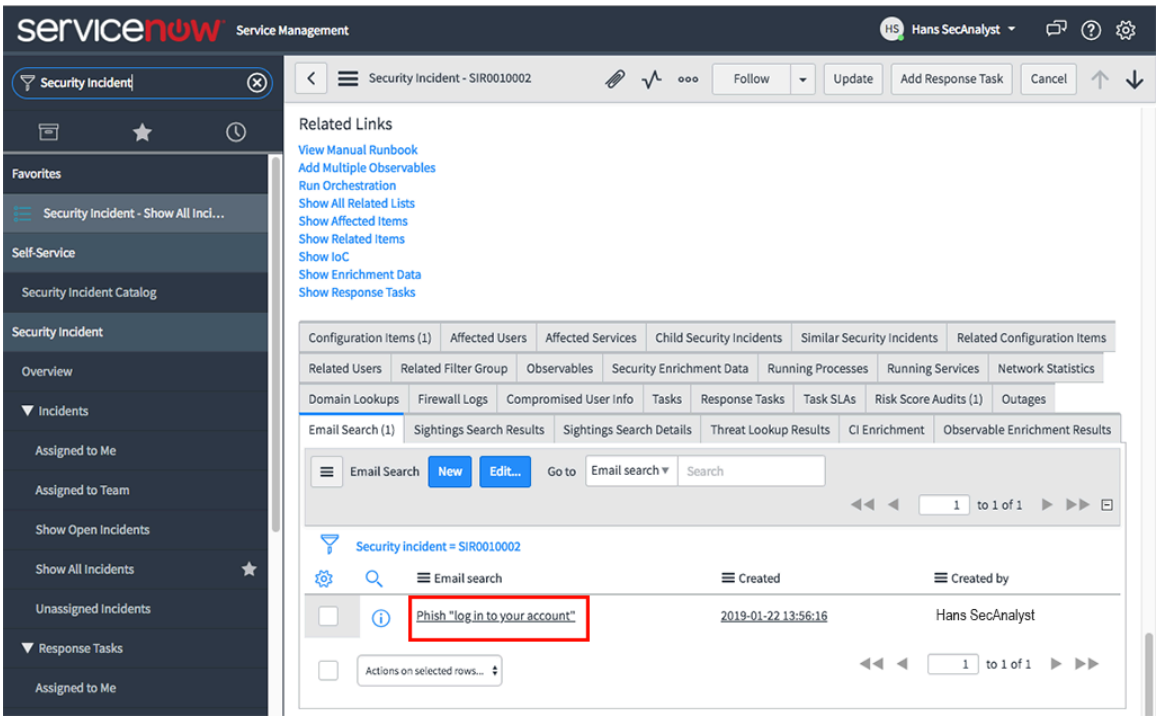
b. Scroll to the bottom of the Security Incident record and click the Email Search related list.

If the Email Search related list is not displayed, click the**Show All Related Lists** related link to display this related list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. With the Email Search related list selected, in the Email search column, click the name of your search.

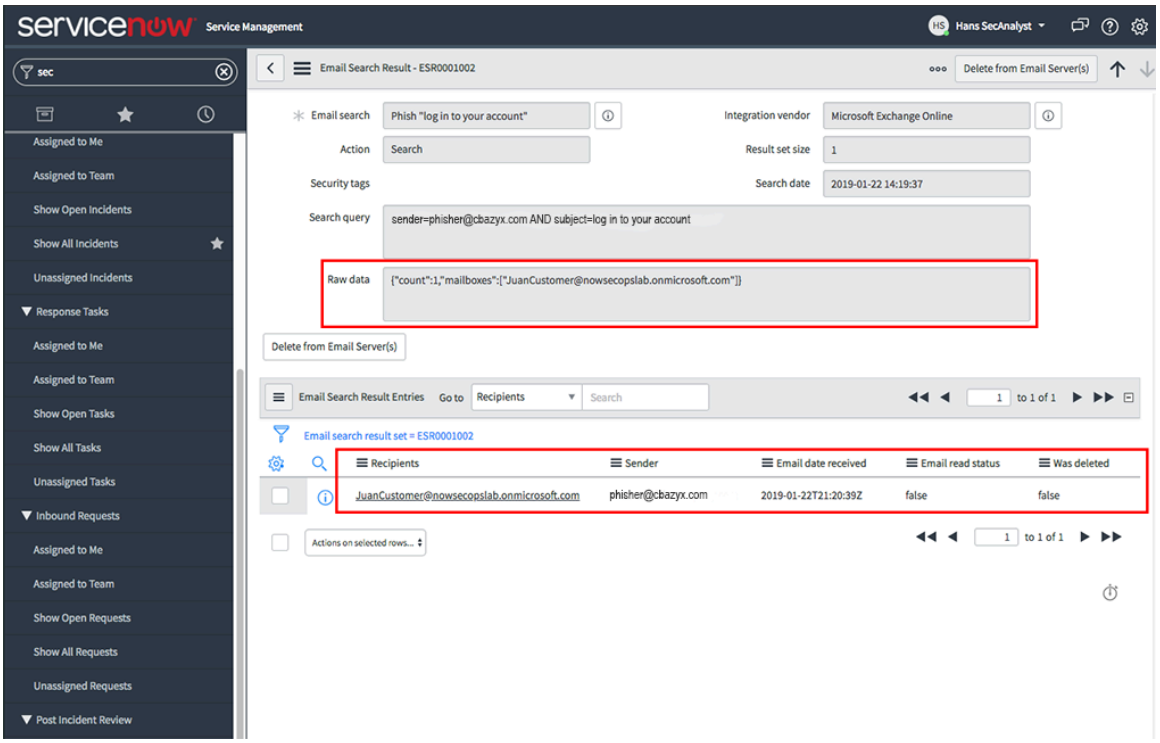


d. In the Email Search record, click the Email Search Results related list.

e. In the Search date column, click the date of your search to display the data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The email search result record is displayed.



After an email search is successfully completed, evaluate the results. If you determine that emails require remediation, you are now ready to delete emails, or request delete approval.

Request delete approval for emails on Microsoft Exchange online service

After an email search is successfully completed and matching messages are identified, you can permanently delete all the suspicious emails from the Microsoft exchange online service that are related to the security incident and phishing campaign.

Before you begin

Role required: sn_si.analyst

The system performs deletions on your latest successful search results.

About this task

If the approvals and email notifications are enabled, send a request to delete emails to an approval group prior to email removal.

Email search results are displayed with any messages that have been received. To ensure that phishing emails are successfully deleted, the delete results are posted to the work notes of the associated security incident. If tagging is enabled, a security tag is also displayed on the related security incident. If the email is not successfully deleted, you are also notified in the work notes.

Depending on your organizational policies, you may need to request approval prior to deleting phishing emails. The delete approval process requires information on the number of emails to be deleted and, potentially, access to other message details. For processing the delete request, in an email notification, an approver is provided with the matching email message count, the security incident link for access to complete message details, and approve or reject links. The links in this email permit an approver to accept or reject the delete request from the email notification. A full audit trail with a time stamp is also available that tracks when the approval status changed in work notes. If an approval group is assigned, one user in the group may process the request for the entire group. Each member of the approval group receives an email notification for the request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

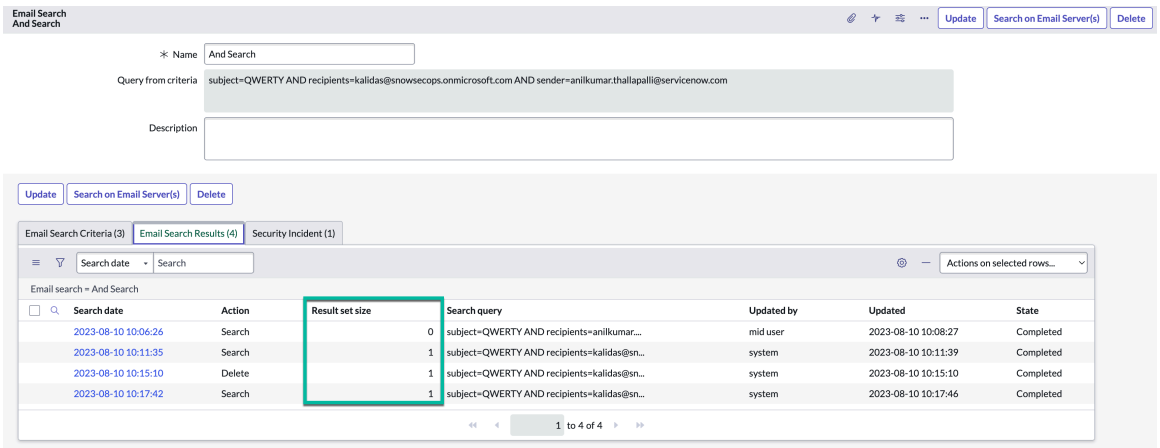
As a user with the sn_si.analyst role, if you determine that emails require remediation, follow the required steps to delete emails. If approvals are enabled, request approval to delete emails from the Microsoft Exchange Online service.

Procedure

1. Navigate to **All** > **Security Incident > Show All Incidents**.
2. Click the **Email Search** related list.
3. With the Email Search related list selected, in the Email search column, click the name of your search.
   The search results are displayed in the Email Search Results related list.

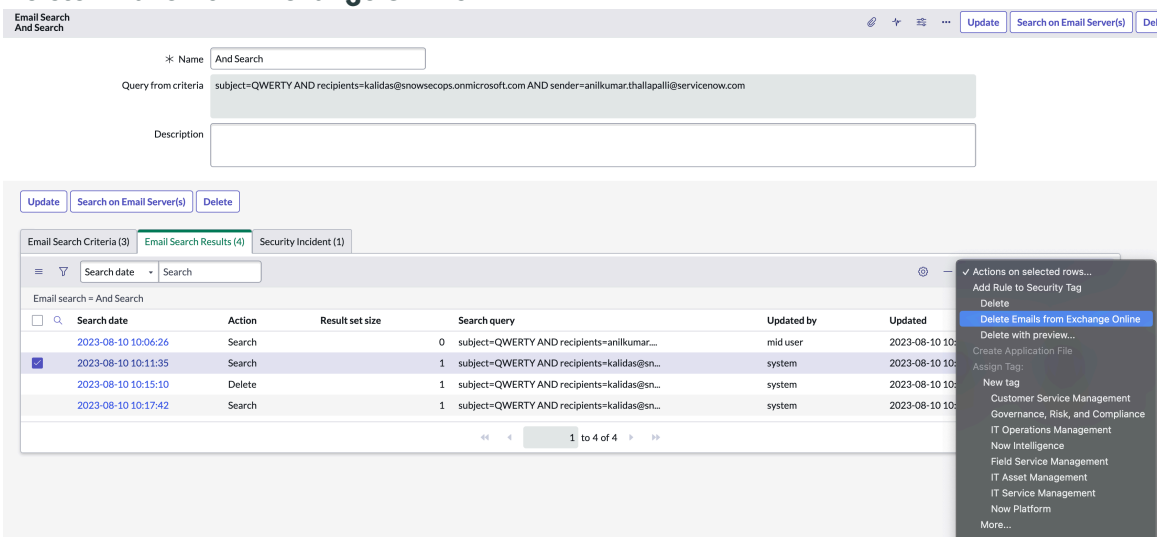
   For this example, this search has found emails that match your search criteria. There are two search actions listed on the record. One search has no matches (0), and the other search has one matching email (1).

Email Search Result set size



4. To delete email items associated with a search, to the left of the Search Date column, select the check box of a search result set.
   You can select a single result set, or multiple result sets from the list.
5. Select the result sets that you want to delete.

Delete Emails from Exchange Online

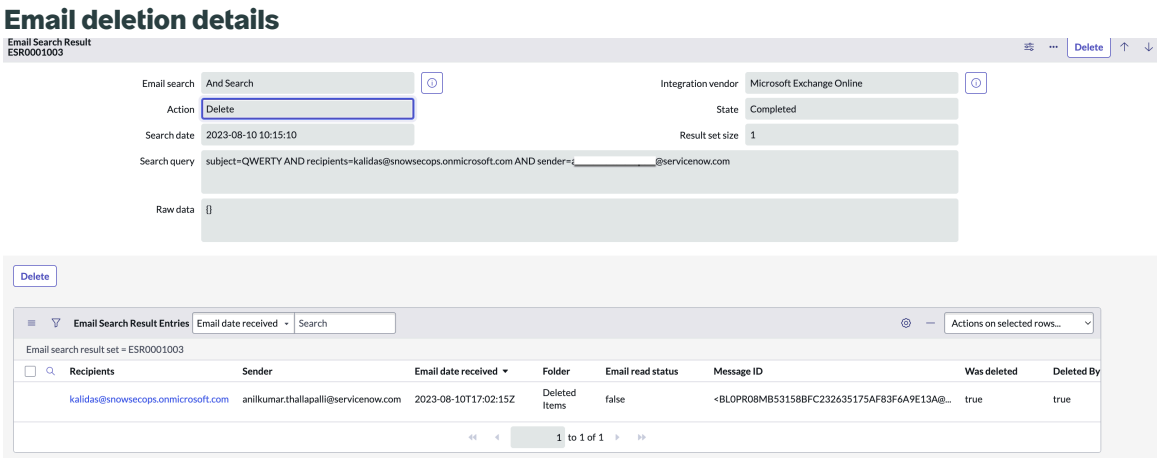


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. At the bottom of the Email Search Results related list, from the Actions on selected rows list, select **Delete Emails from Exchange Online** to delete all the email items associated with one or more result sets from the Exchange Online server.
   If a result set contains more than one email, you are not required to open the Email Search Result record and select individual emails to delete them. All emails items with a status of `false` in the Was deleted column in the Email Search Result record are deleted after you select **Delete Emails from Exchange Online**.

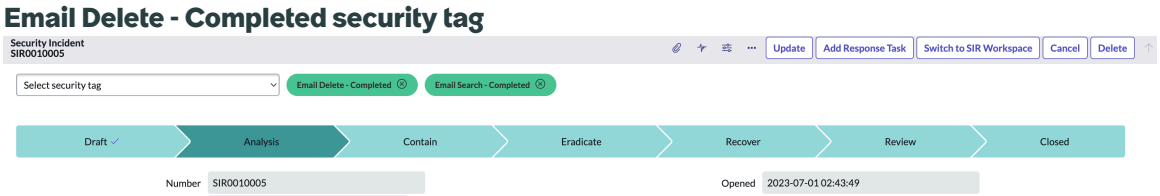
   If an email item in a result set has already been deleted, the status in the Was deleted column in the Email Search Result record is `true`. These items are not deleted again.

   If the approval option is disabled during the configuration step, after you select **Delete Emails from Exchange Online**, the emails associated with the result set are deleted. The result set itself is not deleted. However, the status of all the deleted email items of the result set is updated to `true` in the Was deleted column of the Email Search Result record. For more information on the approval feature, see Configure the Microsoft Exchange Online integration.



   These emails are deleted from the Microsoft Exchange Online tenant that you performed the searches on. A work note is displayed if the emails are successfully deleted.

   On the security incident record, the `Email Delete - Completed` security tag is displayed.



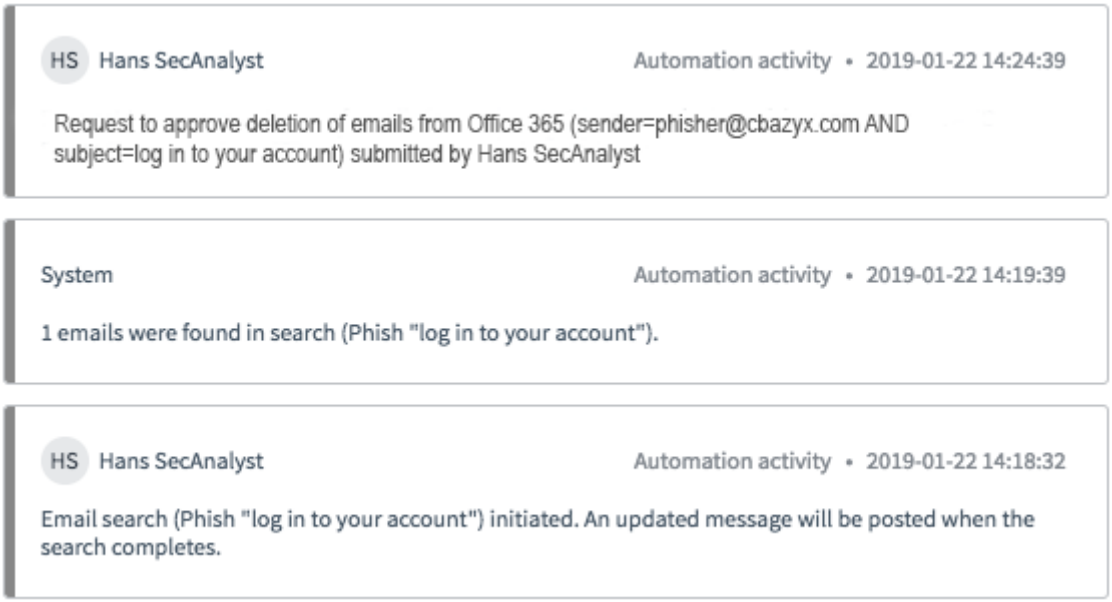
   If approvals are disabled for delete requests, you have successfully deleted emails from the Microsoft Exchange Online tenant.

   If approvals are enabled for delete requests during the configuration step, after you select **Delete Emails from Exchange Online**, an email notification is sent to each member of the approval group that you selected during the configuration step.

   If tagging is enabled during the configuration step, the `Email Delete - Initiated` security tag is displayed on the related security incident record. For more information on tagging, see Configure the Microsoft Exchange Online integration.

   Work notes are displayed that a request to delete emails is submitted by the user with the sn_si.analyst role (`Hans SecAnalyst`).

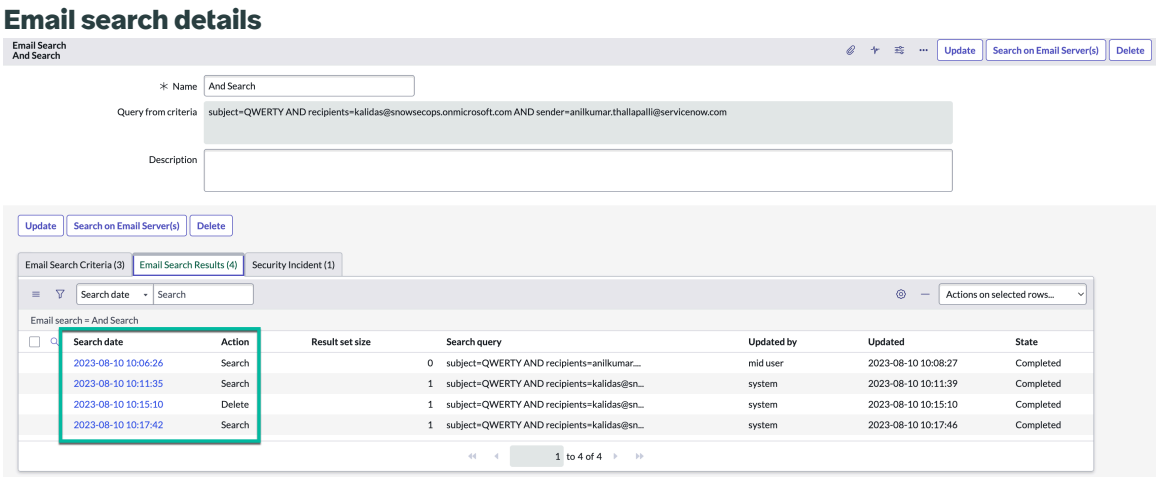
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



If approvals are enabled, the next step is to process the delete request.

7. Alternatively, if you want to view the details and individual email items of a search record prior to deleting it or submitting a delete request, follow these steps.

   a. With the Email Search Results related list selected, in the Search date column, click the date of a search that you want to review.



   The following information about the emails is displayed:

   - Recipients
   - Sender
   - Email date received
   - Email read status (`true` or `false`)
   - Was deleted (`true` or `false`)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Deleted By Integration (`true` or `false`)

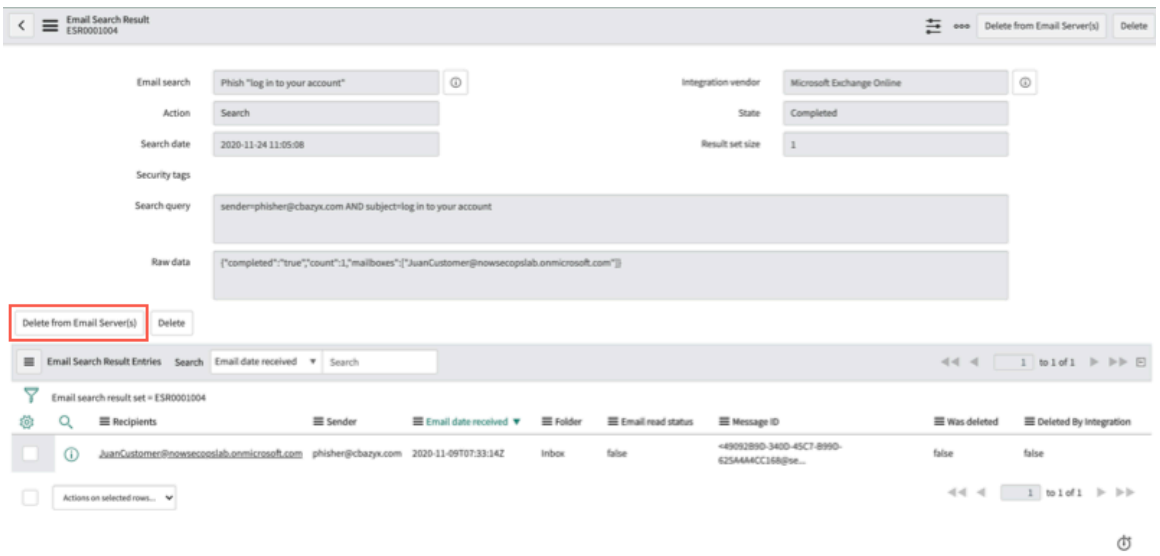
Note:

Value is set to true when the email is deleted when the analyst initiates the Delete from Email Server(s).

The work notes is updated with the total number of deleted records which includes the records deleted by integration and user.

b. After you have reviewed the data, to delete all the emails, or send a request to delete all the emails, click **Delete from Email Server(s)**.

As described in the previous example, if there is more than one email listed on the search result record, you do not need to select the individual emails to remove them. The delete request removes any emails associated with the search when `false` is displayed in the Was deleted column from the latest search results.



If approvals are enabled, you have successfully submitted a request to delete emails. The security tags and work notes are displayed on the related security incident record as described in the previous example. As an approver, the next step is to process the delete request.

Approve delete email requests for the Microsoft Exchange Online integration

If the approval option is enabled in your ServiceNow AI Platform instance, requests to delete emails are sent to each member of the approval group via email. You select the approval group during the configuration step. Approvals provide your organization with an additional level of control over the deletion of emails.

Before you begin

Verify that you have the **Approvals** option selected on the Additional Settings tab of the Exchange Online Search and Delete Emails Configuration Settings form.

Verify that you have enabled the email **Email sending enabled**and **Email receiving enabled** options in your ServiceNow AI Platform instance for approval requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the user with the sn_si.analyst role submits delete email requests, by default, these requests are sent via email to the sn_si.admin. If you have created an approval group, each member of the group receives a notification. Approvers can process email delete requests directly from the email notification. Alternatively, requests can be processed from the email search result records in ServiceNow AI Platform instances. This topic shows both approval methods.

The following information describe the request in the email notification:

Email Search Result record number

Unique number assigned to the search record by the ServiceNow AI Platform as part of the audit trail.

Name of the analyst who submitted the request

Name of the person who submitted the request as part of the audit trail.

Link to the security incident

A link to the security incident related to the phishing event. View the security incident with the work notes, email searches, and email search results directly from the email.

Approve or Reject links

Links to approve or reject the request from the email notification. After you click either link, the system automatically initiates the related workflow and a work note is posted to the security incident record.

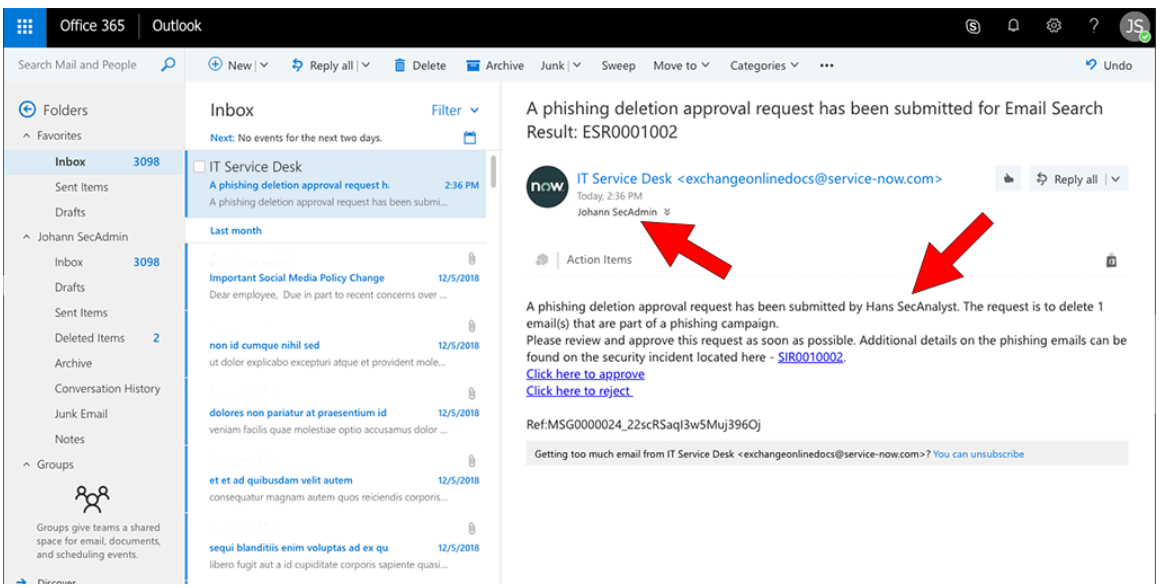
Role required: sn_si.admin or all members of an assigned approval group.

Procedure

1. To process the delete request from the email notification, follow these steps.

a. As an approver, locate the notification email in the email account that you configured in your ServiceNow AI Platform user account.

In this example, the user with the sn_si.analyst role (Hans SecAnalyst) submits a request to delete one email. Johann SecAdmin is a member of the approval group.



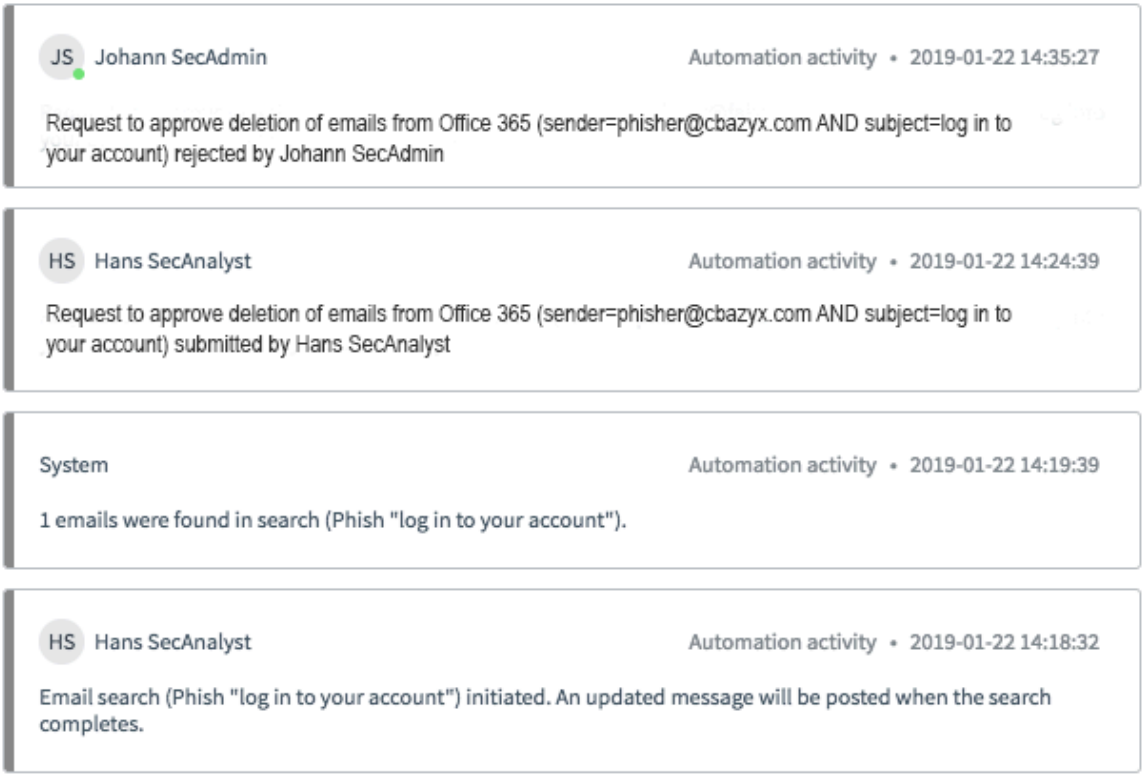
b. In the email notification, choose one option to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Click the Click here to approve Approve link	Approve the delete request. All the email items with a status of `false` in the Was deleted column that are associated with the search result record are automatically deleted from the Microsoft Exchange Online tenant. The status of all the email items of the result set is updated to `true` in the Was deleted col umn of the Email search result record. A work note is posted to the security incident record with the number of successfully delet ed emails. If tagging is enabled, the `Email Delete - Completed` tag replaces the `Email Delete - Initiated` tag.
Click the Click here to reject link	Reject the delete request. A work note is post ed with the name of the person who rejected the request. After a request is rejected, as the user with the sn_si.analyst role, you are required to sub mit a new delete request if you determine that the emails should be deleted.
Click the link to the security incident record (SIR0010002)	Review the related security incident and any related search data prior to processing the re quest.

The following image shows an example of the audit trail created by the work notes on the related security incident record for this example. When the request is rejected from the email notification by an approver, a work note is posted with by the person who rejected the request. Johann SecAdmin rejects this request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



In the ServiceNow AI Platform instance of the person who rejected the request (Johann SecAdmin), in **Self-Service > My Approvals**, `Rejected` is displayed in the State column.

After a request is rejected by any single member of the approval group, as the user with the sn_si.analyst role, you are required to submit a new request to delete these emails if you determine that they should be deleted.

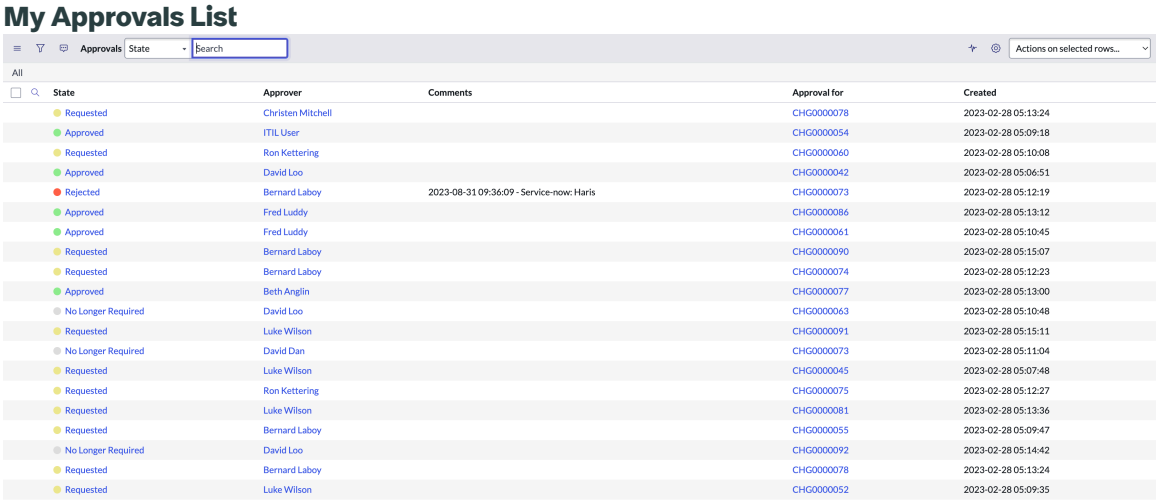
For this example, after the request is rejected, the user with the sn_si.analyst role submits a new request.

Another member of the approval group, John Approver, receives an email similar to the one shown in the preceding example. John Approver can also process this request.

2. Alternatively, approvers can navigate to **Self-Service > My Approvals** in their ServiceNow AI Platform instances to view and process delete requests.
   To process a request from **My Approvals**, follow these steps.

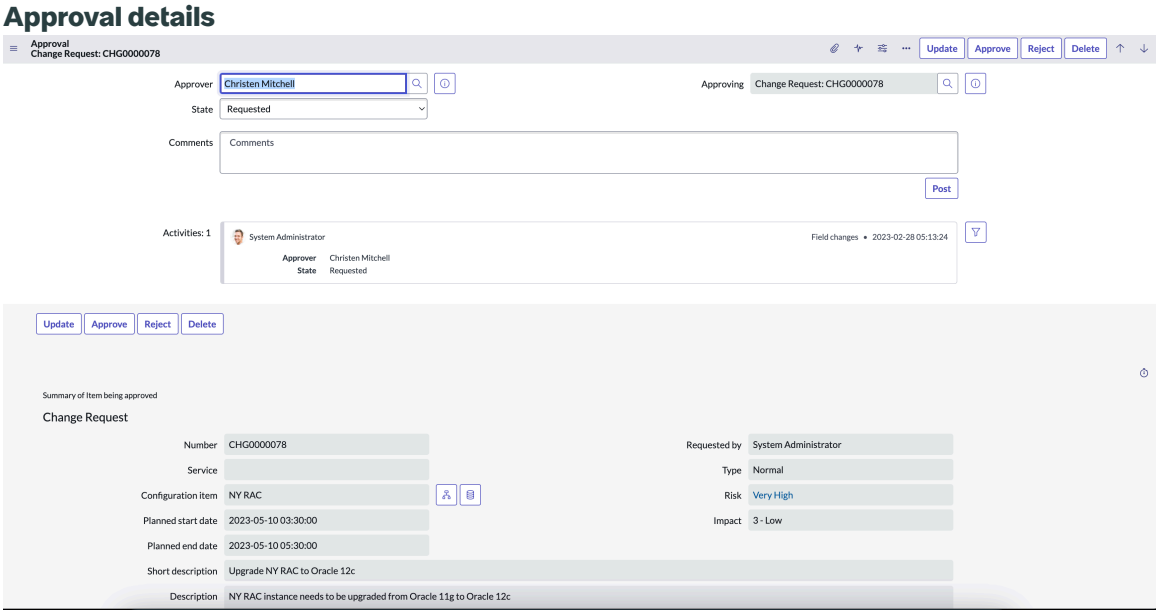
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **Self-Service > My Approvals**.



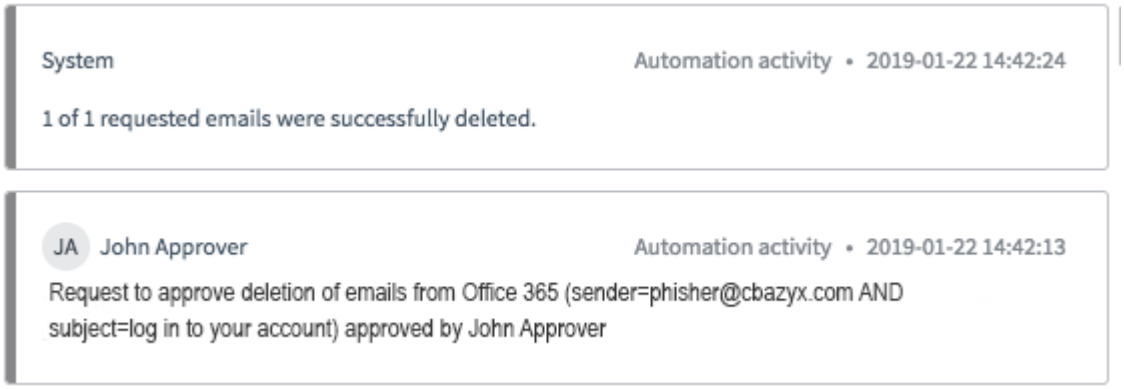
b. In the State column, click the requested item.

In the approval record that is displayed, data about the search, the search request, and the search results are listed.



c. On this record, click **Approve** to approve the request.
After the request is approved, the system initiates the delete workflow to remove the emails. The following image shows an example of the audit trail created by the work notes on the related security incident record for this example. After this delete request is submitted again, it is approved. Regardless of which method is used to approve a request, the number of successfully deleted emails is posted in a work note.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



After the emails are successfully deleted, on the related security incident record, if tagging is enabled, the `Email Delete - Completed` tag replaces the `Email Delete - Initiated` tag.

In **Self-Service > My Approvals** for the approver (John Approver), the state changes from `Requested` to `Approved`.

In **Self-Service > My Approvals** for other members of the approval group, for example, Johann SecAdmin, the state changes to `No Longer Required` after the request is approved.

3. Alternatively, to confirm that emails are deleted in the Email Search Result record on the related security incident record, follow these steps.

   a. Navigate to **Security Incidents > Show All Incidents** and locate the phishing-related security incident.
   At the bottom of the record, the related lists are displayed.

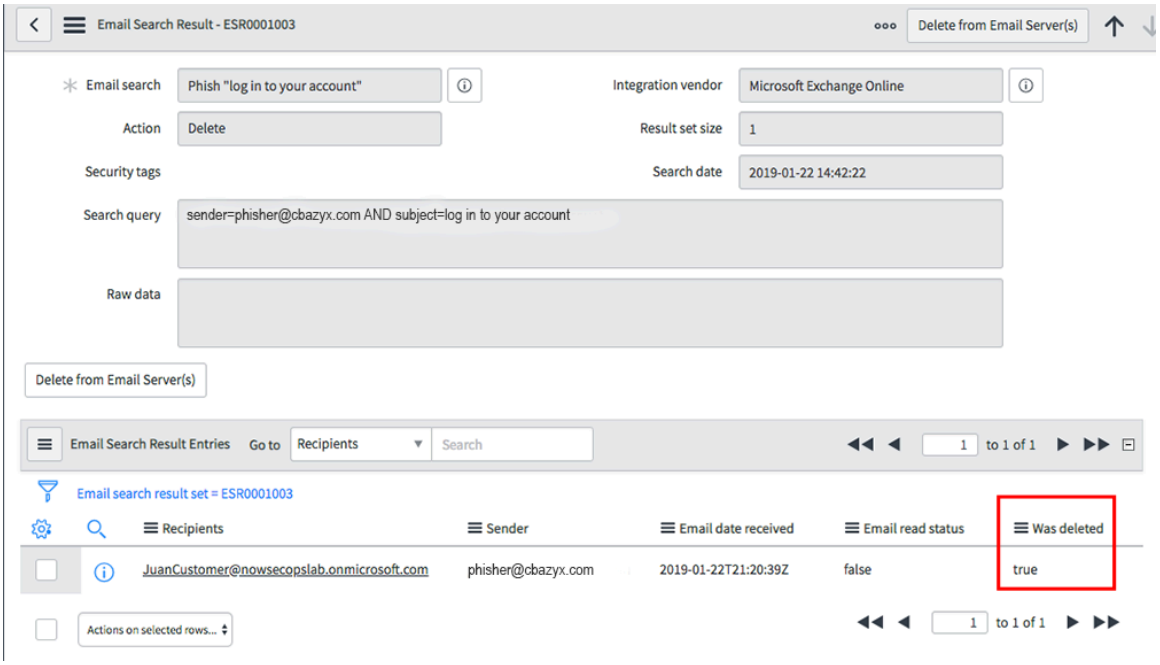
   b. Click the **Email Search** related list.

   c. Click the name of the search in the Email search column (`Phish "log in to your account"`).
   The Email Search record is displayed. If the Email Search related list is not visible, click the **Show All Related Lists**link.

   d. Click the **Email Search Results** related list.
   In the Search date column, the email search and delete actions are displayed with corresponding dates.

   e. In the Search date column, click the item that corresponds to the delete action.
   In the Email Search Result record that is displayed, the Was deleted column status shows that the email is deleted (`true`).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You have successfully approved email delete requests from both an email notification and an approval record and confirmed that emails are deleted. For more information about locating the Email Search Result record, see Define email search criteria and request a search on the Microsoft Exchange Online service.

Recover deleted emails on the Microsoft Exchange Online service

(Optional) As a Microsoft Exchange Administrator, you can recover deleted emails if your incident remediation requires that you to recover the emails deleted by the workflow of this integration.

Before you begin

For more information about how this integration deletes emails, see Configure the Microsoft Exchange Online integration.

For more information about the administrative role in the Microsoft Office 365 product, including information about recovering deleted items in a user mailbox, see About the Exchange Online admin role.

Role required: admin, Microsoft Exchange Administrator

About this task

If you select the **Recover Deleted Emails** option in the Additional Settings tab during the configuration step, you enable the recovery of deleted emails in your Microsoft Exchange Online tenant. Emails deleted using the delete workflow of this integration are placed in the Deleted Items sub folder of the Recoverable items folder in the mailbox of the user on the Microsoft Exchange Online service. If the user's account is configured in Microsoft Exchange Online tenant so that the user can view the Deleted Items folder, the user can recover these emails by using the Microsoft Outlook service on the web. Alternatively, the Microsoft Exchange Online administrator can recover deleted emails from a Deleted Items folder of a user. See Recover deleted items or email in Outlook Web App for more information.

Role required: Microsoft Exchange Online administrator or Microsoft Global administrator to recover deleted emails.

Role required: sn_si.admin in the ServiceNow AI Platform to enable the Recover Deleted Emails option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: sn_si.analyst in the ServiceNow AI Platform for completing a successful search for emails and verifying that emails are successfully deleted prior to recovery.

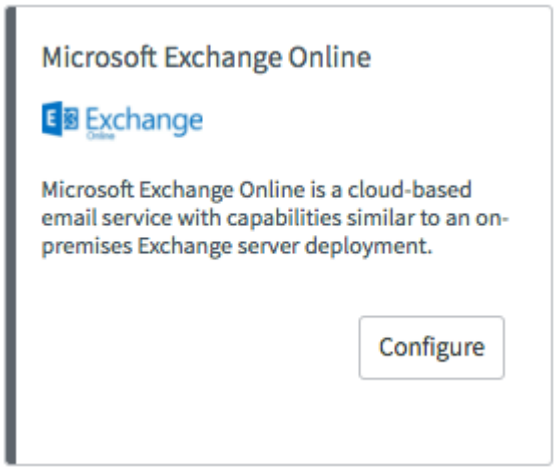
Procedure

To enable the email recovery option, follow these steps.

a. Navigate to **Security Operations** > **Integrations** > **Configurations**.

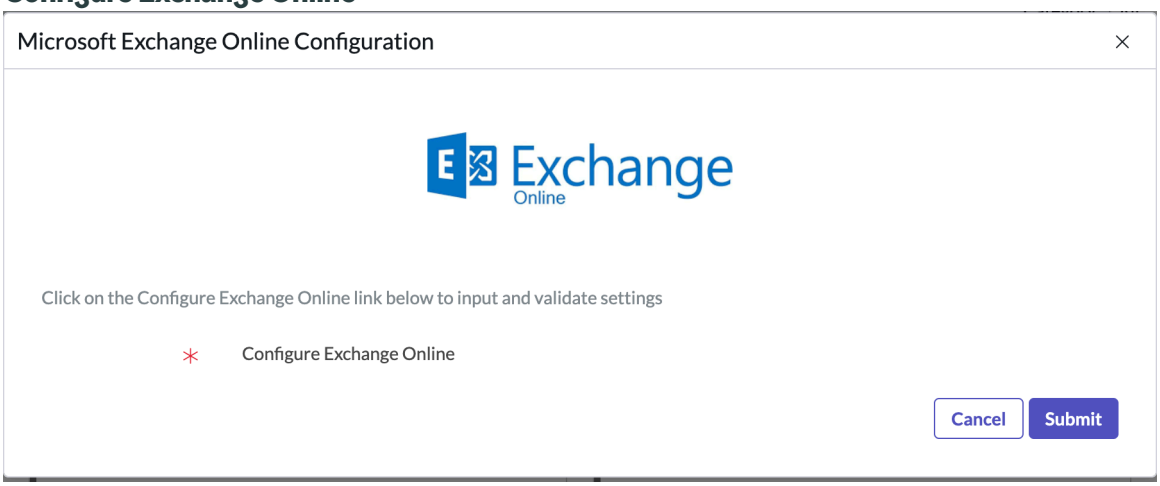
b. Locate the Microsoft Exchange Online tile.

c. Click **Configure**.



d. In the Microsoft Exchange Online Configuration dialog box that is displayed, click **Configure Exchange Online**.

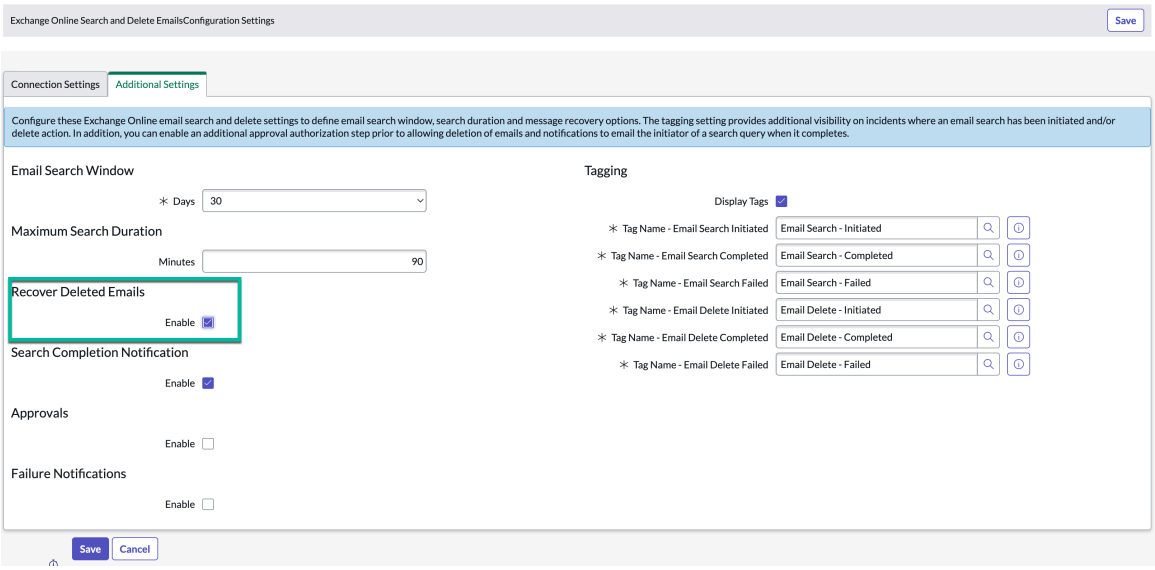
Configure Exchange Online



e. On the `Additional Settings` tab under `Recover Deleted Emails`, select the **Enable** check box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recover Deleted Emails



f. Verify any other settings and click **Submit**.

g. To verify that a search and delete of email messages are successfully completed for the email messages you want to recover, navigate to the security incident that logged the email search and delete workflows.

h. Locate the work notes and verify that the system successfully deleted the messages.



i. As a Microsoft Exchange Online administrator or Global administrator, log in to your Microsoft Office 365 account.

j. Follow the steps described in Recover deleted items or email in Outlook Web App on the Microsoft documentation website.

Edit security tags for the Microsoft Exchange Online integration

You can edit the names and colors of the security tags in your ServiceNow AI Platform® instance for the Microsoft Exchange Online integration. These security tags help you quickly identify when email search either completes or fails. They also identify when requests to delete emails are initiated and when the email items are successfully deleted.

Before you begin

By default, the security tags are enabled in your ServiceNow AI Platform® instance if you select the **Display Tags** option during the configuration step. You can edit tag colors and names, and assign tags to security tag groups to help you organize them in your ServiceNow AI Platform® instance. For example, you can change the colors of tags so that the start tag of a capability is one color, and the completion tag is another color to match the other security tags that are enabled in your ServiceNow AI Platform® instance. These different colors can help you quickly identify when workflows start and are successfully completed. If you decide that you do not need a specific tag, without disabling tagging for the integration, you can also disable a single tag from the tag record. If disabled, this tag is no longer displayed on the related security incidents. For

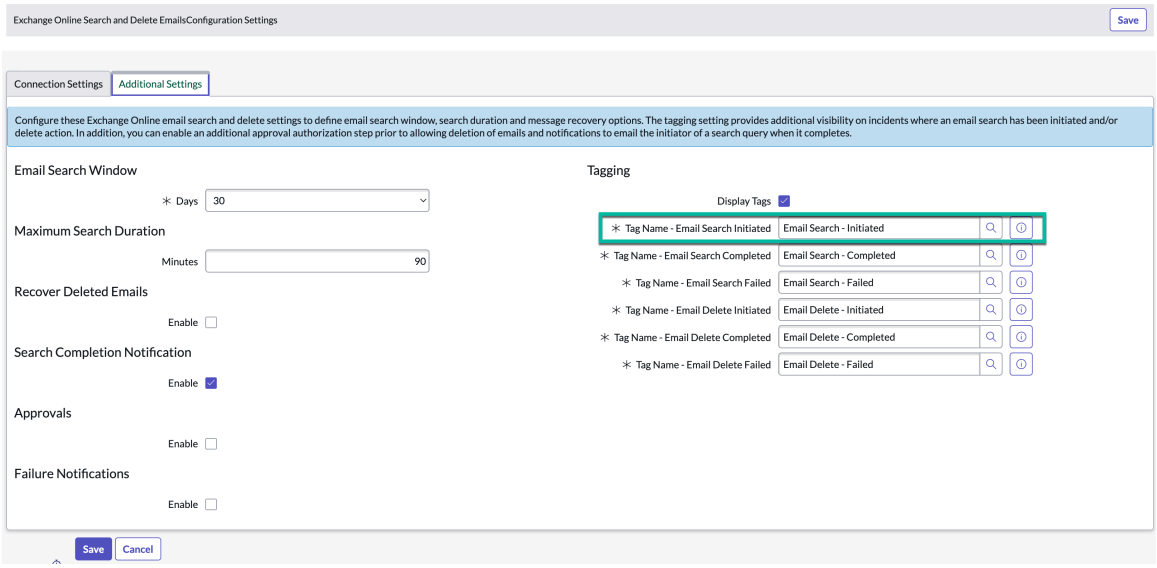
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

more information on how to set up security tag groups and tags, see Set up security tag groups and tags on the Servicenow Product Documentation website.

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Integrations** > **Exchange Online Settings**.
2. Click the **Additional Settings** tab to select it.
3. On the tab that is displayed, if the **Display Tags** option is cleared, select it to display tag names.
4. With the tag names displayed, to the right of a tag, click the information icon.



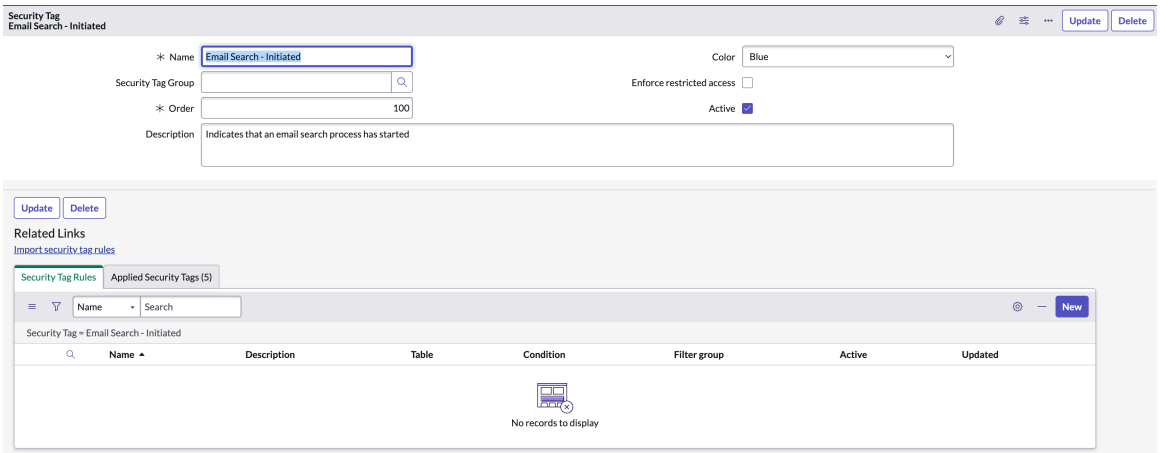
5. In the Security Tag dialog that is displayed, click **Open Record**.
6. In the record that is displayed, edit the fields.

Option	Description
Name	Unique name for the security tag.
Color	Security tag color. Select a color from the choice list.
Security Tag Group	Name of the security tag group. Click the information icon to view the available groups. Default is Metatag group.
Enforce restricted access	Select this option to assign read and write roles needed by users to read or write to records that have this security tag. Default is cleared.
Order	Specify the order the tag appears on forms or within a list. Default is 100. To set the order on the list, enter a value. For example, 100, 200, 300, 400. The tag with the lowest the number is displayed first on the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	list. The profile with the highest number is dis played last.
Active	Turn this tag on or off. Default is selected (ac tive)
Description	Description for the tag.

7. Click **Update** to save your changes.



You have now successfully edited the tag record for a security tag.

Microsoft Exchange On-Premises integration

The Microsoft Exchange On-Premises integration provides tools for security analysts to contain and eradicate phishing and spear phishing email threats in on-premises instances.

Explore

Security Incident Response integrations

Set up

Get started with the Microsoft Exchange On-Premises integration

---

Use

Search for and delete phishing emails

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Get started with the Microsoft Exchange On-Premises integration

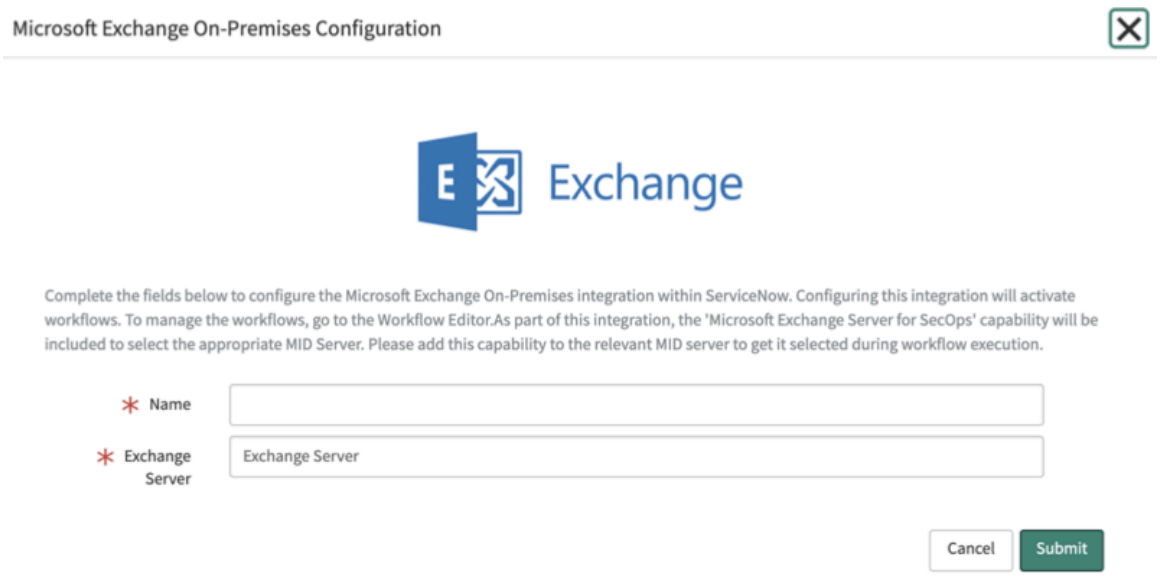
The Microsoft Exchange On-Premises integration provides tools for security analysts to contain and remediate phishing and spear phishing email threats in on-premises instances. Before you can use the Microsoft Exchange On-Premises integration, you must download it from the ServiceNow Store and identify the appropriate Exchange and MID servers.

Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation os complete, navigate to **Security Operations** > **Integrations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
3. Select **Configure**.



4. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Exchange Server	Specify the Exchange server to be used.

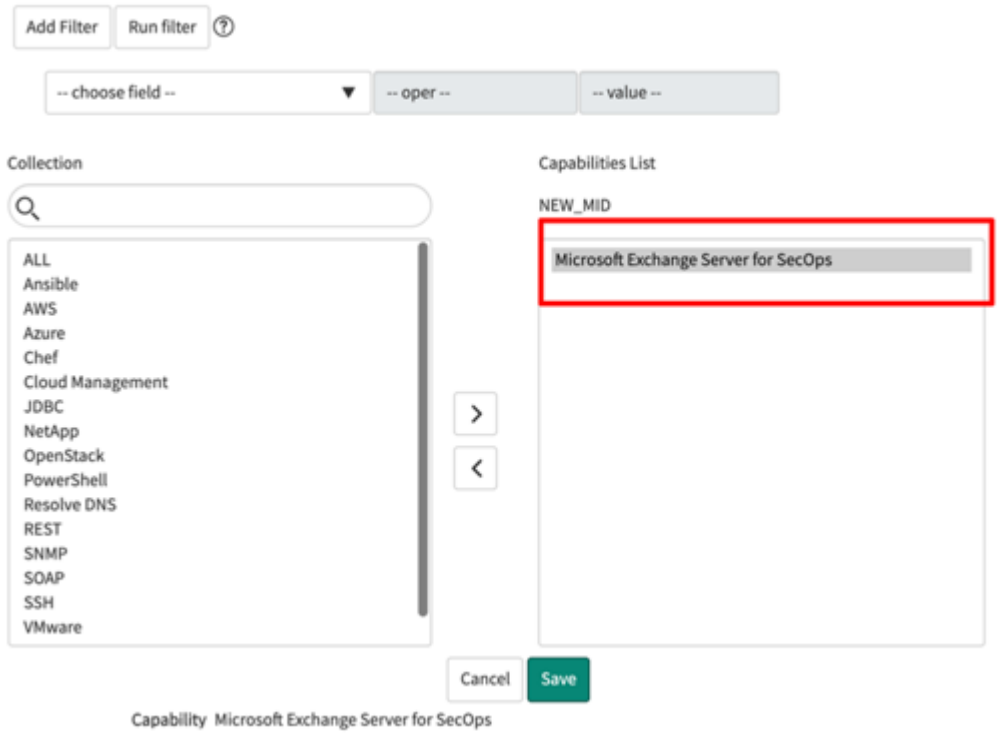
Note: Configuring this integration activates flows. To manage the flows, navigate to the **Workflow Studio/ Flow Designer.**.

5. Click **Submit**.
   The integration configuration card displays.
6. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
7. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.
8. Navigate to **Orchestration** > **MID Servers**.
9. Open the record and verify the status of the MID server which is reachable to the exchange server and its **Status** option is set to **Up** and **Validated** option as **Yes**.
10. Add the MID server capability:
    - Select the respective MID server to add the capability.
    - Click on the **Capabilities** related list and click **Edit**.



    - Remove **All** and add **Microsoft Exchange Server for SecOps**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- Select the **IP Ranges** from the **Related Lists** section and set the value to either **ALL** or any desired value.
- Select the **Supported Applications** from the **Related Lists** section and either set the value to ALL or Orchestration.
- **Save** the record.

11. Validate the connections & credentials.
    - Navigate to Orchestration > Credentials & Connections > Credentials.
    - Select **New** to create credentials for the MID server.
    - Select **Windows Credentials**.
    - Enter **Username** and **Password**.
    - Select **Submit**.
    - Select **Test Credential** in related links.
    - Enter target, port, MID server.
    - Select **OK** and validate your connection and credentials.
12. Once the credentials are validated, the configuration on ServiceNow instance is complete and is ready to perform email search and deletion operations using this integration.

Microsoft Exchange - Perform Email Search and Deletion flow

When the **Microsoft Exchange - Perform Email Search and Deletion** flow is executed, it searches the Exchange server using the search query provided, and returns the details to the on-premises instance.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The **Microsoft Exchange - Perform Email Search and Deletion** flow is executed when email searches are set up and the **Delete from Email Server(s)** or **Search on Email Server(s)** button are pressed.

Actions specific to this integration are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

The flow actions include:

- Create Compliance Search Action
- Check Compliance Search Status Action

Create Compliance Search Preview Action

The Create Compliance Search Preview Action creates a new compliance search action of type preview on the exchange server for the created compliance search.

Input variables

Input variables determine the initial behavior of the action.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Complete	When compliance search action is successfully created.
Error Creating Action	When creation of compliance search action fails due to exception in exchange server.
Error	When exception occurs in flow action.

Check Preview Action Status

The Preview Action Status checks the status of compliance search action of type preview and returns the preview information of the emails found like recipient, sender, subject, email date received.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
response	Contains the status of compliance search action and the preview information of the email found as a part of compliance search.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Preview in Progress	When status of compliance search action is in progress.
No Mail Found	When status of compliance search action is completed, and no emails are found as a part of compliance search.
Preview Complete	When status of compliance search action is completed, and emails are found as a part of compliance search.
Error Checking Status	When status checking fails due to exception in exchange server.
Error	When exception occurs in workflow activity.

Create Compliance Search Delete Action

The Create Compliance Search Delete Action creates a new compliance search action of type purge on the exchange server for the created compliance search.

Input variables

Input variables determine the initial behavior of the action.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Complete	When compliance search action is successfully created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exit Conditions (continued)

Variable	Description
Error Creating Action	When creation of compliance search action fails due to exception in exchange server.
Error	When exception occurs in flow action.

Check Delete Action Status

The Check Delete Action Status checks the status of compliance search action of type purge and performs soft delete operation on the exchange server for the emails found as a part of compliance search.

Input variables

Input variables determine the initial behavior of the action.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
response	Contains the status of compliance search action and count of emails deleted, which were found as a part of compliance search.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Delete in Progress	When status of compliance search action is in progress.
No Mail Found	When status of compliance search action is completed, and no emails are deleted as a part of compliance search.
Delete Complete	When status of compliance search action is completed, and emails are deleted as a part of compliance search.
Error Checking Status	When status checking fails due to exception in exchange server.
Error	When exception occurs in flow action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remove Compliance Search Action

The Remove Compliance Search action removes the created compliance search from exchange server.

Input variables

Input variables determine the initial behavior of the action.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

Microsoft Graph Security API alert ingestion integration

Use the Microsoft Graph Security API integration to ingest alerts from Microsoft Graph security providers and automatically create security incidents.

Overview

The Microsoft Graph Security API is an intermediary service (or broker) that provides a single programmatic interface for connecting multiple security providers (Native to Microsoft as well as ServiceNow Partners).

The Microsoft Graph Security API integration addresses these issues by using the Microsoft Graph Security API to connect with different Microsoft security technologies like Azure Sentinel, Microsoft Defender Advanced Threat Protection, and Azure Advanced Threat Protection. Alerts from Microsoft Security providers are ingested and security incidents are automatically created in Security Incident Response.

Key features

This integration includes the following key features:

- Discovery of Microsoft Graph Security API alerts that are candidates for security incidents and automate the creation of security incidents.
- Mapping of alert fields to security incident fields.
- Aggregation of similar alerts to existing open security incidents instead of creating duplicate security incidents.
- Preview alert field values and validate their mappings in the security incident.
- Automatic alert status update for security incident creation and closure.
- Set up scheduled ingestion of alerts to create security incidents periodically.

Set up your ServiceNow AI Platform instance for the Microsoft Graph Security API integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the application from the ServiceNow Store.

Before you begin

Role required: admin

About this task

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response roles.	The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform® instance. • A user with the ServiceNow AI Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role. • A user with the sn_si.admin role oversees the following tasks in the ServiceNow AI Platform®: ○ Names, creates, and edits alert profiles. ○ Selects and maps Microsoft Graph Security API alert data fields to the security incident fields. ○ Previews security incident details for accuracy prior to finalizing the configuration. ○ Schedules on-going alert ingestion. ○ Enables alert updates when a Security Incident Response incident is created and closed. ○ Assigns the security incident analyst (sn_si.analyst) role. ○ Users with the sn_si.analyst work with security incidents. For more information about roles and assigning roles to users, see Roles on the Servicenow Product Documentation website.
Register your application in the Microsoft Azure portal.	Before you can ingest alerts, you must configure your application in the Microsoft Azure portal. See Configure the Microsoft Azure portal for details.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Event and Alert Ingestion for Security Operations: This application requires:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST **Note:** The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance. For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Configure the Microsoft Azure portal

To retrieve security alerts for an application available in the Microsoft Azure tenant using the Microsoft Graph Security API, you must register the application in the Microsoft Azure portal and grant security event read and write access to the application.

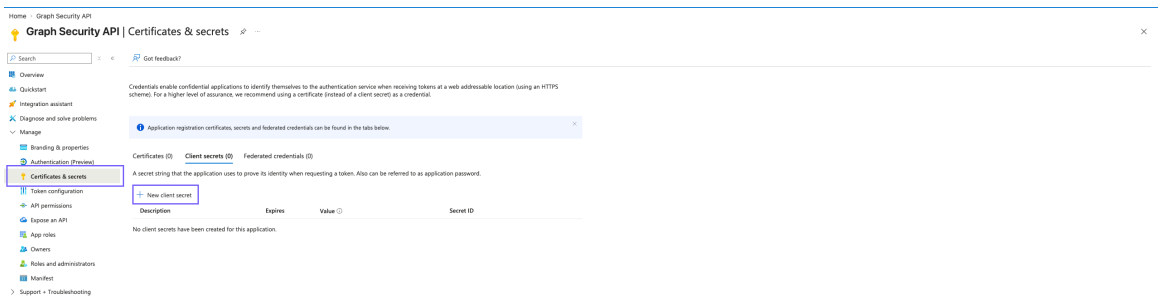
Before you begin

Role required:

- Application Developer: Required for registering the application.
- Tenant Administrator: The Microsoft Azure tenant administrator must grant permissions to the application by making a call to the admin consent endpoint.

Procedure

1. Log in to the Microsoft Azure portal.
2. Enter **App registrations** in the **Search** box.
3. Select **New registration**.
4. Enter a name for your application and the redirect URI, for example http://localhost and click **Register**.
   The Redirect URI is used while providing admin consent for the application.
5. In the App registrations page, select the application you have registered, for example Graph Security Demo.
6. Under **Manage**, select **Certificates & secrets**.

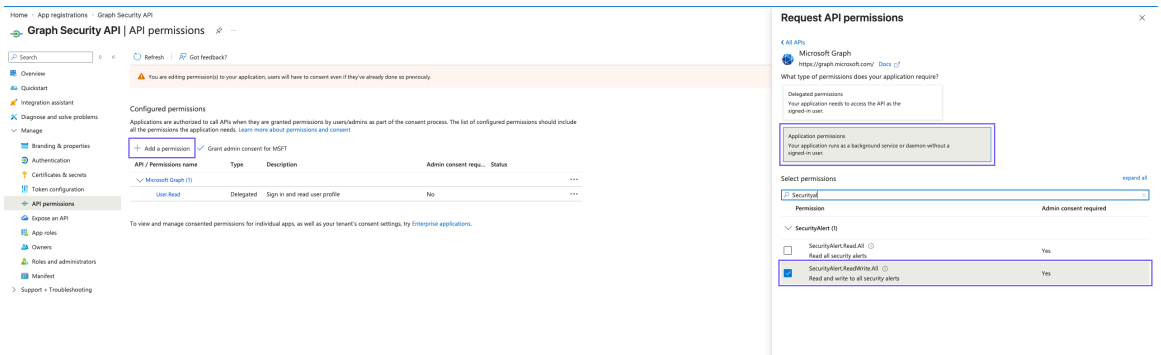


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

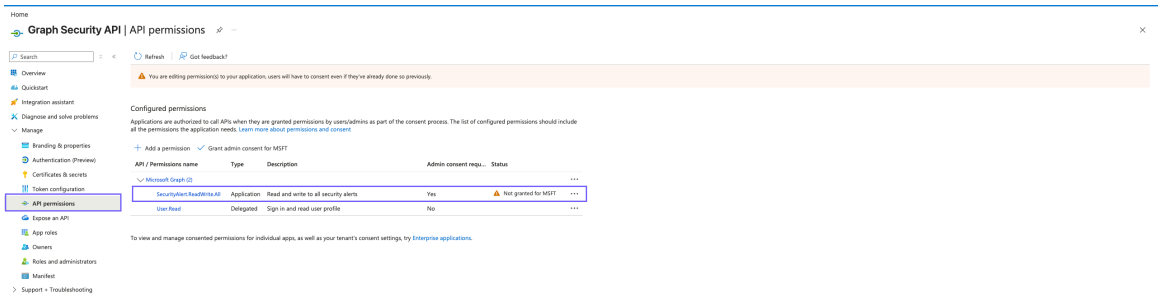
7. Select **New client secret** to create a client secret.
   Copy the client secret and save it as it will not be visible later. In case you forgot the client secret you can generate a new client secret.

   Note: If you forget the client secret, you can generate a new one by following the instructions in steps 4 and 5.

8. Select **View API Permissions** in the Overview page.
9. Add new Application level API permissions for SecurityAlert.ReadWrite.All security events.



10. Grant admin consent for the newly added API permissions.
    For more information, see the Microsoft Graph Permissions reference Microsoft Graph permission model.



11. Log in as a tenant administrator and provide consent for the application.
    The steps are given below:

    a. Navigate to the following URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

       Enter the APPLICATION_ID of the application that you have registered.

12. Select **Accept** to accept permissions requested by the application created above.
    You can then use the application to read security events. See the Microsoft Graph Security Authorization documentation for more details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install and configure the Servicenow application for Microsoft Graph Security API alert ingestion integration

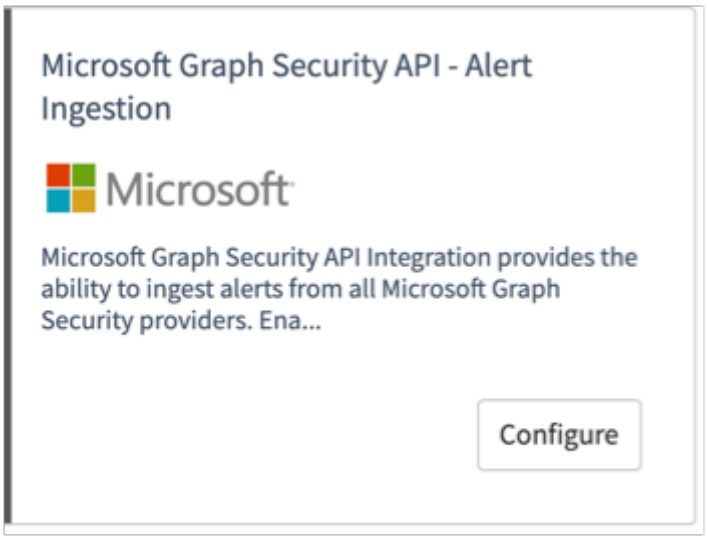
Before you run the integration on your ServiceNow AI Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.admin

Procedure

1. If you have not installed the Microsoft Graph Security API application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **Integrations** > **Integrations Configurations** and locate the Microsoft Graph Security API - Alert Ingestion tile.



3. To configure the application, click **Configure**.
4. In the Alert Ingestions Configuration dialog that is displayed, fill in the fields.

Field	Description
Name	Name of the Microsoft Azure Cloud instance. You can enter only alphanumeric values and hyphens (-) in this field.
Tenant ID	The Microsoft Azure Tenant ID. This is the instance from which all the alerts in the Mi crosoft Azure portal are retrieved.
Client ID	The Client ID for the application that you have registered in the Microsoft Azure portal. See Configure the Microsoft Azure portal for details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Client Secret	The password for your registered application.

5. Click **Submit**.
   After it is successfully validated and submitted, each alert ingestions server configuration is saved on the Security Integrations page as a tile. If your saved configuration tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.

What to do next
You have successfully installed and configured the application. The next step is to create an alert profile.

Create a profile for the Microsoft Graph Security API alert ingestion integration

As a user with the sn_si.admin role, you create an alert profile in your ServiceNow AI Platform instance and determine which alerts create security incidents. Before security incidents are created from ingested alerts, the field values from alerts are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident will be displayed.

Before you begin
Role required: sn_si.admin

About this task
The integration allows you to ingest different types of alerts such as unauthorized access attempts and malware, for example. These alerts are ingested based on the profiles that you configure in the Security Operations environment of your instance. All alerts are initially ingested for a configured alert type in a profile. Ingested alerts can then be further filtered to specify which alerts create security incidents.

For example, you may prefer filters that create security incidents only for alerts that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested alerts, individual field values on the filtered alerts are mapped to corresponding fields on a layout of security incident for a preview. All alerts that meet the selection criteria in your Microsoft Azure tenant and are available over the Microsoft Graph Security API are initially ingested into your ServiceNow AI Platform instance.

Identify the source for the profile

Specify the name and source for the profile.

Before you begin
Role required: sn_si.admin

Procedure

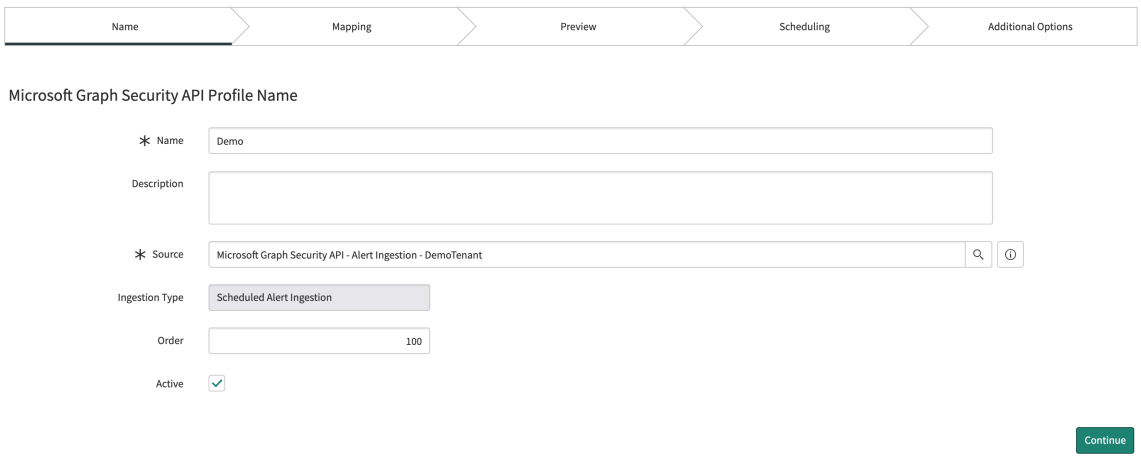
1. To create a profile for an alert in your ServiceNow AI Platform instance, navigate to **Microsoft Graph Security API Integration** > **Microsoft Graph Security API Profile**.
2. Click **New**.
3. Fill in the fields.

   An example of a completed form follows the table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Active	Check box is cleared by default. If this option is disabled, the profile is not active. **Note:** You should complete all sections in the profile before making it active.
Source	The Microsoft Azure tenant that you configured to ingest alerts. If you have multiple tenants configured, select the appropriate tenant for the alert types that you are planning to ingest for the profile. You are required to enter a value.
Order	Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The lower the order value, higher the priority.
(Optional) Description	Additional text to help you distinguish this profile from other profiles.

The following figure is an example of a completed form.



What to do next

The next step is to map the alert fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mapping of alert fields for Microsoft Graph Security API alert ingestion integration

After you identify the sources for scheduled alert ingestion, the next step is to map individual alert fields to the fields on a ServiceNow AI Platform SIR security incident.

For the mapping step, you must first ingest sample alerts from the Microsoft Azure tenant. Then you must ensure that all relevant alert field data is mapped to the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

Mapping of the sample alert fields involves the following:

- Ingest sample Microsoft Graph Security API alerts
- Mapping alerts to security incident response fields

Ingest sample Microsoft Graph Security API alerts

Ingest sample alerts from your Microsoft Azure tenant.

Before you begin

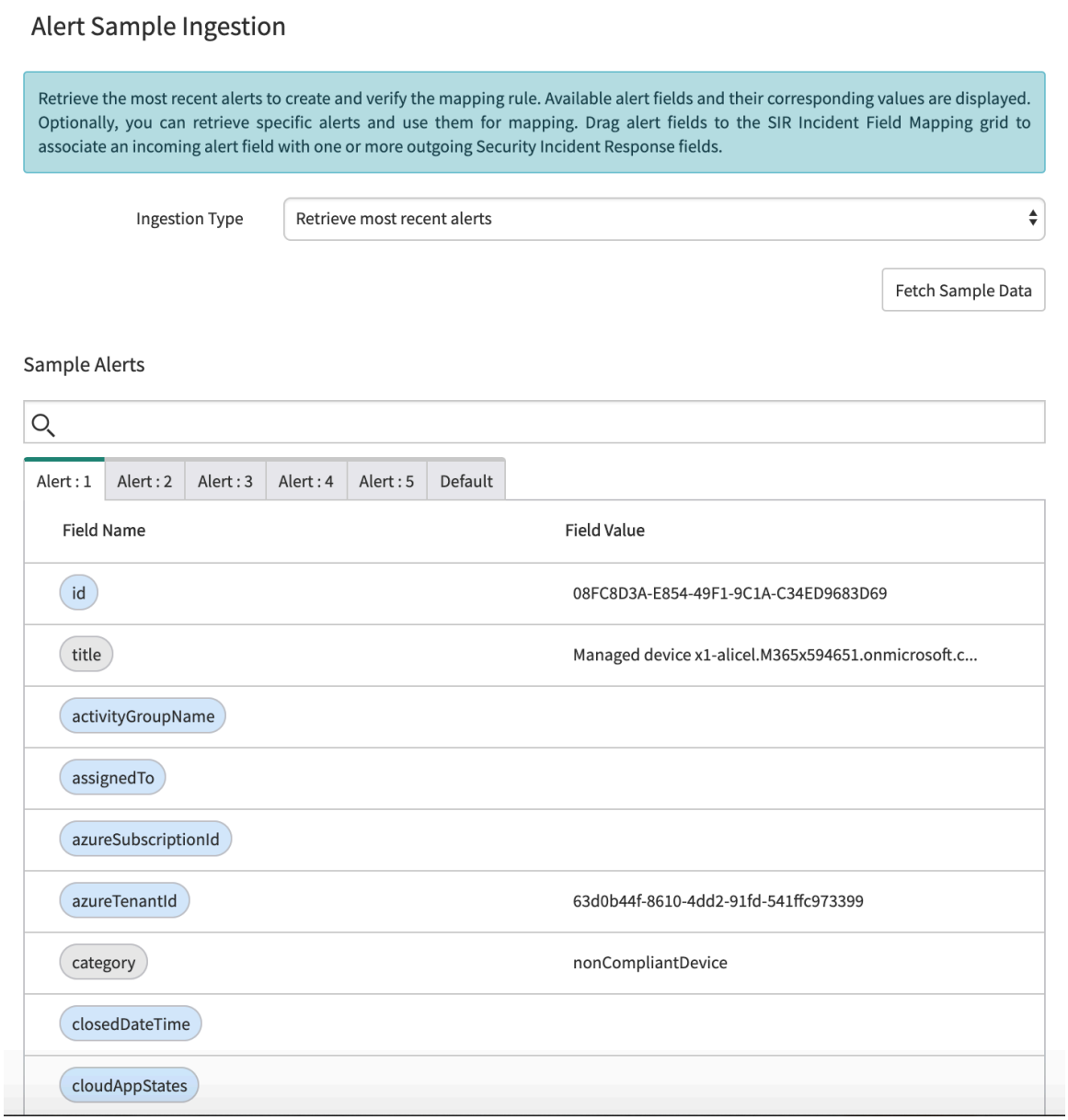
Role required: sn_si.admin

Procedure

1. You can either pull the 5 most recent sample alerts or provide the unique alert IDs for the specific alerts that you want to use for your mapping experience.
   From the **Ingestion Preference** choice list, select one of the following:
   - Retrieve most recent alerts: The 5 most recent alerts are retrieved.
   - Select alerts based on alerts ID: Specify the alert ID for the alerts to be retrieved. You can specify a maximum of 5 alert ids separated by commas.
2. Click **Fetch Sample Data** to pull the latest sample alert data from the Microsoft Azure tenant. The pull for sample alerts may take a few moments.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The sample alert field values are populated on the left side of the form when sample alerts are ingested by the profile. These are the alerts that you map to the SIR security incident fields. The alert fields and values results are displayed as individual tabs.



What to do next

After you have fetched the sample data, the next step is map the alert fields to the security incident.

Mapping alerts to security incident response fields

Map individual alert fields from triggered alerts to fields on a ServiceNow AI Platform security incident.

Alert field mapping

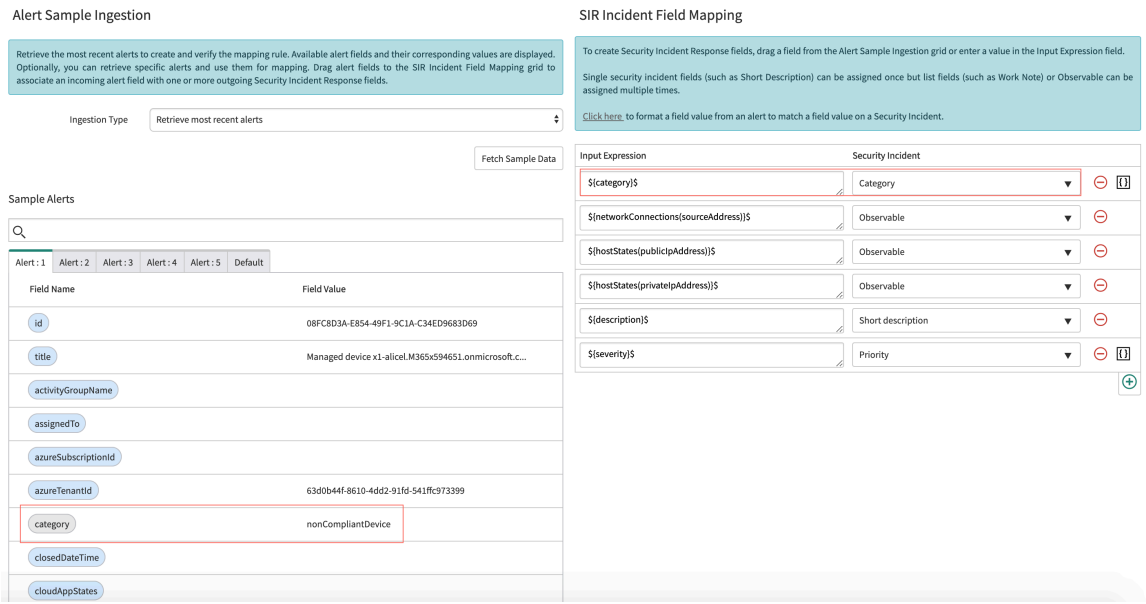
As a user with the sn_si.admin role, use the fields from the Sample Alerts section on the left and map them to the security incident fields in the SIR Incident Field Mapping column on the right panel. Edit the mapping configuration by dragging alert fields from the left side and dropping

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

them on the SIR incident mapping section on the right. The mapping on the right associates the incoming alert field with an outgoing security incident field.

1. After you have fetched the sample data, the next step is map the alert fields to the security incident. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
2. Drag the field name, for example, `category`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

   The field value is displayed in the Input Expression column. In the following image, `category` is mapped to the `Category` field on the security incident.



However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no alert fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the alert fields helps you keep track of the alert values that you have already mapped as they become greyed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important alert information remains unmapped.

Light blue fields on the left indicate that an alert field is not yet selected and mapped on the security incident. You may prefer to associate an incoming alert field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

Note:

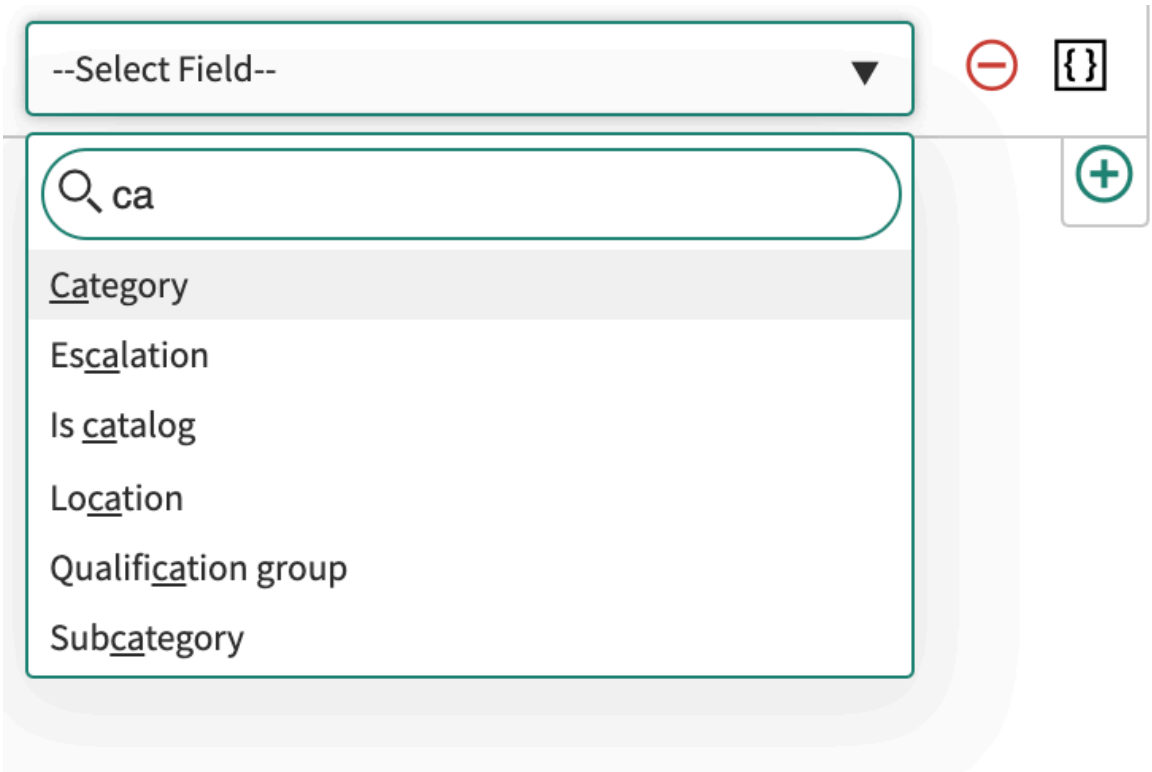
a. To manually enter a value in the Input Expression field, enter it in the format ${fieldname}$. The alert field will be mapped to the security incident field.

b. You cannot map ingested alerts to the MITRE-ATT&CK Framework fields in the security incident mapping section. If you still map the fields, the information will not be available as part of the MITRE-ATT&CK card in the MITRE-ATT&CK framework section in the security incident form. To associate the MITRE-ATT&CK Techniques, use the Auto Extraction Feature available as part of the MITRE-ATT&CK Framework in the Threat Intelligence Module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.
   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.
   b. In the Security Incident column, expand the choice list that is displayed, and select a field.

      In the expanded choice list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the alert fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.



   Note: As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

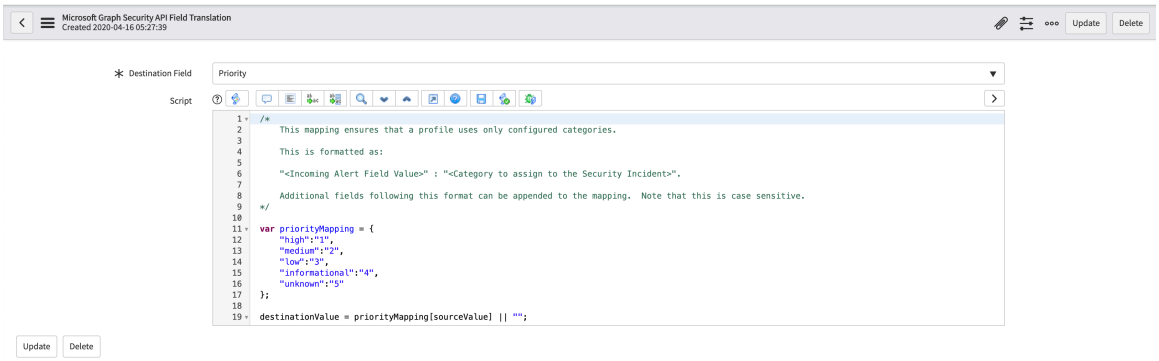
   c. Alternatively, type a value in the Search field for the new row.
   d. From the left side of the form, left-click to select the Alert ID that you want in the Input Expression field. With the drag-and-drop feature, map it next to your new field.
4. Continue mapping by adding or removing field values to the mapping.
5. After you have completed the preceding field mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming alert must satisfy to create a security incident. To set incident generation conditions, follow these steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Format field translation

In certain cases, alert field values in Microsoft Graph Security API may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the {} icon. The script editor is displayed.



Incident generation conditions

Once the mapping section is complete, you can set filter conditions so that you can specify which alerts should create security incidents versus which alerts should be filtered out, for example, low priority alerts. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming alert must satisfy to create a security incident. To set incident generation conditions, follow these steps.

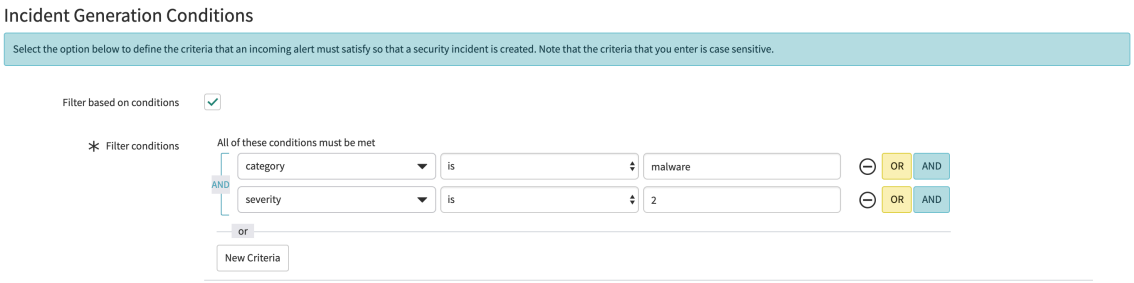
1. Scroll to the Incident Generation Conditions section on the form and select the Filter based on conditions option. The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

   The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the Alert Sample Ingestion section for the alert you ingested. These fields are dynamic and change depending on the alert that you ingest Criteria that you enter are case-sensitive, and they must match exactly the values of the alert. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Microsoft Azure tenant and review your alerts for the keywords.

2. Using the choice lists and fields of the conditions builder, set filters for the first row.
3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND**is selected, all conditions must be matched.
   - If **OR**is selected, either condition can be matched.
4. In the second row, set a second filter condition

   The following image is an example with two conditions that must be matched before security incidents are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



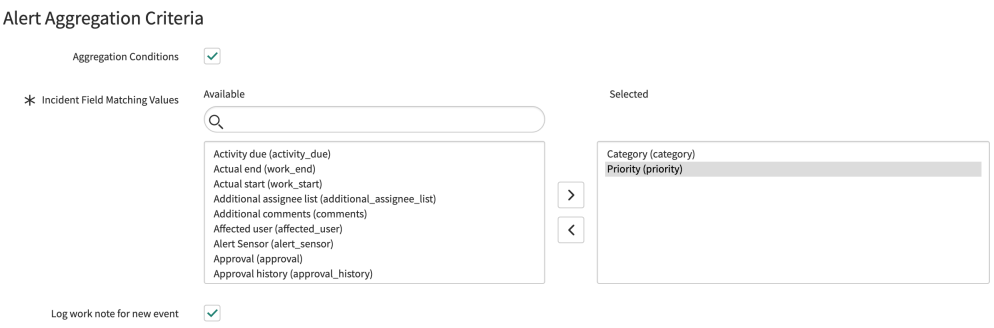
You have set the triggering conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of filtering helps you isolate security alerts, and it limits the number of security incidents that you create. If additional filtering criteria are set, only alerts that are required are ingested without having to change the query or the triggered alert configuration.

Alert aggregation criteria to handle similar alerts and prevent duplicate incidents

Define additional alert aggregation criteria that aggregates an incoming alert to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related alert data on a single security incident. To set the criteria, follow these steps below:

1. Scroll to the Alert Aggregation Criteria section on the form and select the Aggregation Conditions option. The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.
2. From the Available list, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform and move them to the Selected list. All the field values that you select must be matched to append this incoming alert to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple alert field values mapped to them. All values must match. If only a subset of the values are matched, the alert aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.



If a new alert matches all the values that are selected in the aggregation field conditions in the mapping step, the alert is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate alerts on a related list on a security incident. All of the aggregated alerts on a security incident are displayed on the Aggregated Microsoft Graph Alerts related list. This list details associated time stamps and aggregated field values. This

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

information helps you understand why alerts are added to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the **Show All Related Lists** link.

3. (Optional) To log a work note for a new alert that is recently added on the security incident, select the check box to enable this option. The work note logs that a new alert has been added along with a link to the alert details and any other details that may have been added to the work note field in your mapping section.

   You have successfully mapped values from an alert to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with filtering criteria. You also appended alerts or events to existing SIR security incidents.

4. Click **Continue** to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident

Preview the security incident for the Microsoft Graph Security API integration

After you complete the mapping step, preview the values that you mapped in a ServiceNow AI Platform SIR security incident. This preview step permits you to verify that you have mapped all the alert fields that you want displayed on the security incident.

Before you begin

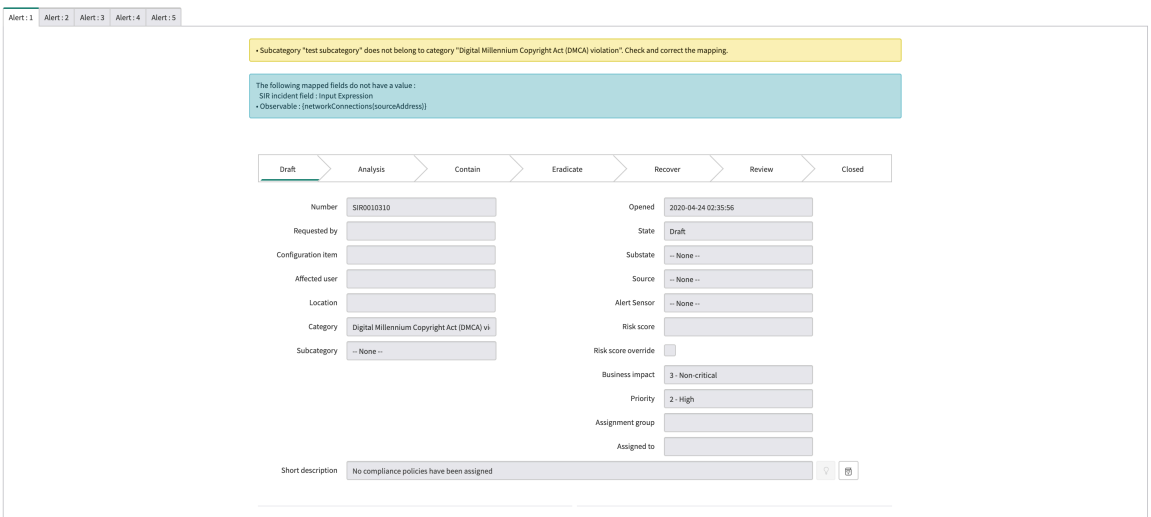
Role required: sn_si.admin

About this task

As a user with the sn_si.admin role, preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Procedure

1. If the security incident preview is not displayed, click **Preview** in the progress bar.
   All the ingested alerts and the field mappings defined in the Mapping page are displayed.
2. Click on an Alert ID to see a preview of the security incident.
   This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the alert values on the security incident.



The preceding image is an example of a preview with a mapping error of the samples that were ingested.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

What to do next

If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to define the schedule.

Define schedule for Microsoft Graph Security API integration

Verify the default settings for alert retrieval or modify the scheduling as needed. This step permits you to filter your alert retrieval based on a date range.

Before you begin

Role required: sn_si.admin

About this task

You also choose how often you will poll for future alerts that match the alert profile configuration. For automated alert ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This step is needed for scheduled alert profiles.

As a user with the sn_si.admin role, you configure these polling intervals on a per-profile basis. The performance of the Microsoft Graph Security API alert ingestion integration is impacted by the different polling intervals. When scheduling, you may prefer to balance system load against incident urgency. A five-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.

Procedure

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when alerts are pulled from the Microsoft Azure tenant.

Option	Description
Ongoing Alert Ingestion selected	Based on the default setting, the ServiceNow AI Platform instance pulls from the Microsoft Azure tenant for new alerts every five minutes. Security incidents are created if triggered alerts are found and incident generation fil tering criteria are matched. To balance alert ingestion against server load, and to pull the most current data, five minutes is the setting you may prefer. However, this value can be modified as needed.
○ **Ongoing Alert Ingestion selected** ○ **Set initial alert ingestion time**	Initial ingestion time If you want to schedule the initial ingestion at a specific time, follow these steps: ○ Select the Ongoing Alert Ingestion and Set initial alert ingestion time fields. ○ Specify the time in the Input initial alert in gestion time field. The initial ingestion will take place at the time specified here. Subsequent ingestions will be

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	based on the schedule defined in the Polling increment (minutes) field. As an example for scheduling, if you have a daily alert job that runs once a day at 4 AM local time, you can set up the corresponding alert profile in your ServiceNow AI Platform in stance to run at 4:05 AM local time to capture the alert right away and create a security inci dent. Enter 04 05 00 in the Initial alert ingestion field. In the Increment (Minutes) field, enter 1440 (24 hours) to schedule the next alert in gestion for 24 hours from the initial alert inges tion. Both the initial alert ingestion time and next alert ingestion time are displayed in the fields. To configure the settings in this example, fol low these steps: ○ Select the **Ongoing Alert Ingestion** option. ○ In the Polling Increment (minutes) field, en ter 1440 (24 hours). ○ Click the **Set Initial alert ingestion time** op tion to enable editing for the Initial alert in gestion time and Next alert ingestion (esti mated) time fields. ○ In the Initial alert ingestion time field, enter 04 05 00. In the Next alert ingestion (esti mated) time field, the time of the next alert ingestion is displayed.
One Time Retrieval field selected	One-Time Retrieval Use this configuration if you want a one-time pull to ingest historical alerts. When this setting is configured, a profile is used once to retrieve alerts from historical events that are based on a date range. To the right of the Since date field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the Since date value, alerts are retrieved up through the current date. Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve significant amounts of his torical alerts but rather a minimal amount of in-flight alerts that are being actively worked at the time of profile activation. After the alerts are pulled, this setting will not retrieve more alerts for this profile going for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	ward from the current date. This setting pop ulates the security incident with all the alerts that are found for the range you enter.

3. Click **Continue** to navigate to the Additional Options page.

Automate alert updates and closure based on SIR incident status

The Microsoft Graph Security API alert ingestion integration has a bi-directional interface that allows for both alerts to create security incidents, as well as an ability to update the alerts once the security incident is created and/or closed with relevant incident details such as SIR incident number, assignment group, SIR incident URL, and so on. T

Before you begin

Role required: sn_si.admin

Note: The initial and closure alert statuses are updated only if this functionality is supported by the service provider. For details, see the Microsoft Graph Security API documentation and the security provider documentation.

Procedure

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.
2. Follow the instructions below to complete the configuration for updating alerts when the security incident is created.

Option or Field	Description
Update alerts upon SIR Incident Creation	Select this option if you want to update the alert status and add additional comments when a security incident is created from the alert. This can occur for both the initial trigger ing alerts that create the security incident, as well as aggregated alerts.
Initial Alert Status Update	Select an initial alert status from the list. This status will be set for all alerts when a security incident is created for an ingested alert. This includes alerts that create new incidents and alerts that are ingested and aggregated to an existing open incident. **Note:** Based on the alert status select ed here, the alert status used by the se curity providers will be correspondingly updated.
Initial Comments posted back to Alert	Based on the stage you have selected, de fault comments are displayed. You can modi fy the default text and use the ${field name}$ format to add or modify any fields available in the security incident form.
Close out alerts upon SIR Incident Closure	Select this option if you want to use the au tomated alert closure option. This can occur for both the initial triggering alerts that create the security incident, as well as aggregated

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or Field	Description
	alerts. Alert status will be updated in the secu rity provider with the status and closure com ments after SIR incident is closed in the Servi ceNow AI Platform.
Closure Alert Status Update	Select an alert status from the list. Select the status value to be set for all alerts when a se curity incident is closed for an ingested alert.
Closure Comments Posted back to Alert	The default closure comments are displayed here. You can edit the default text and use the ${field name}$ format to add or modify any fields available in the security incident form.

3. Click **Finish** to complete the configuration and move the profile to the **Waiting** state.
   A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull alerts from the Microsoft Azure tenant based on your scheduling. A maximum of 1000 security incidents can be created within a 24 hour period.

Microsoft Graph Security API integration configuration settings

Use this option to modify the Microsoft Graph Security API ingestion integration default system properties.

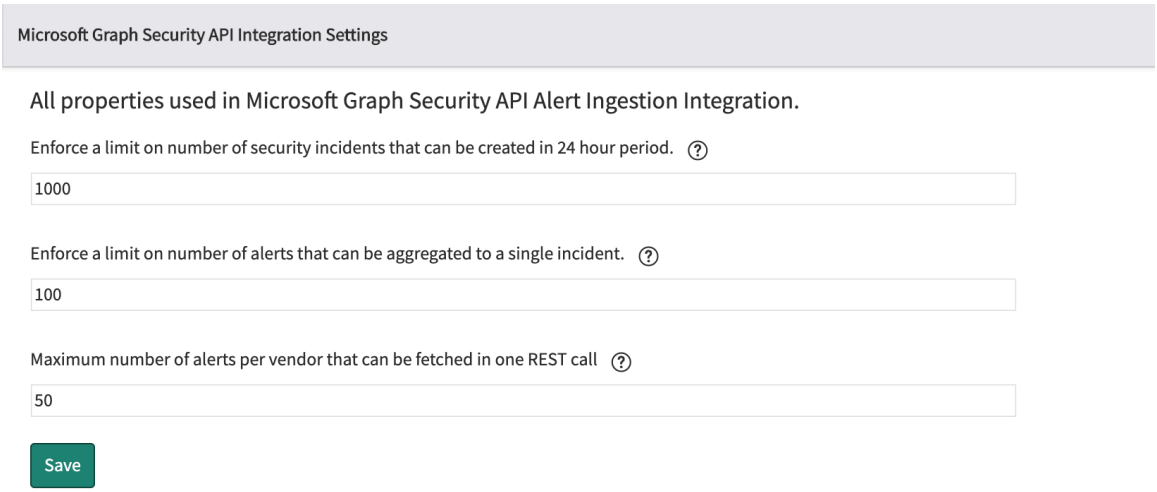
Before you begin
Role required: sn_si.admin

About this task
Modify the default configuration properties to limit the number of security incidents that can be created during a 24 hour period or the number of alerts that can be aggregated in one security incident.

To modify the system properties, log in as a user with the *sn_si.admin* role and navigate to **Microsoft Graph Security API Integration** > **Microsoft Graph Security API Integration Settings**.

The default configuration settings are displayed. You can modify these settings if required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



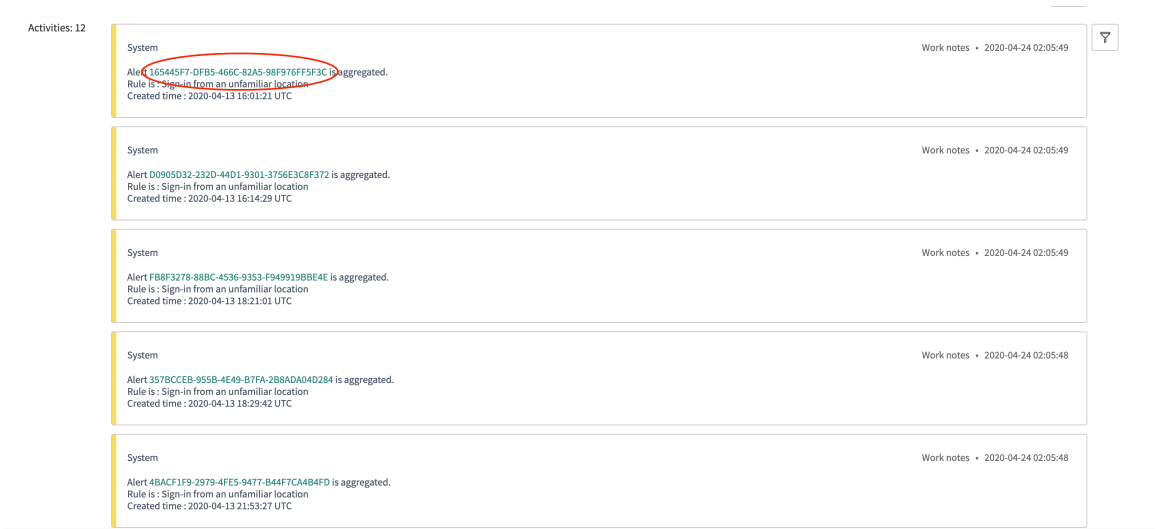
Any modified integration settings will be applied during the next polling interval as defined in the profile.

Security Incident Response form after alert ingestion

After a Microsoft Graph Security API alert has been ingested, a security incident is created and the corresponding updates are made to the security incident record.

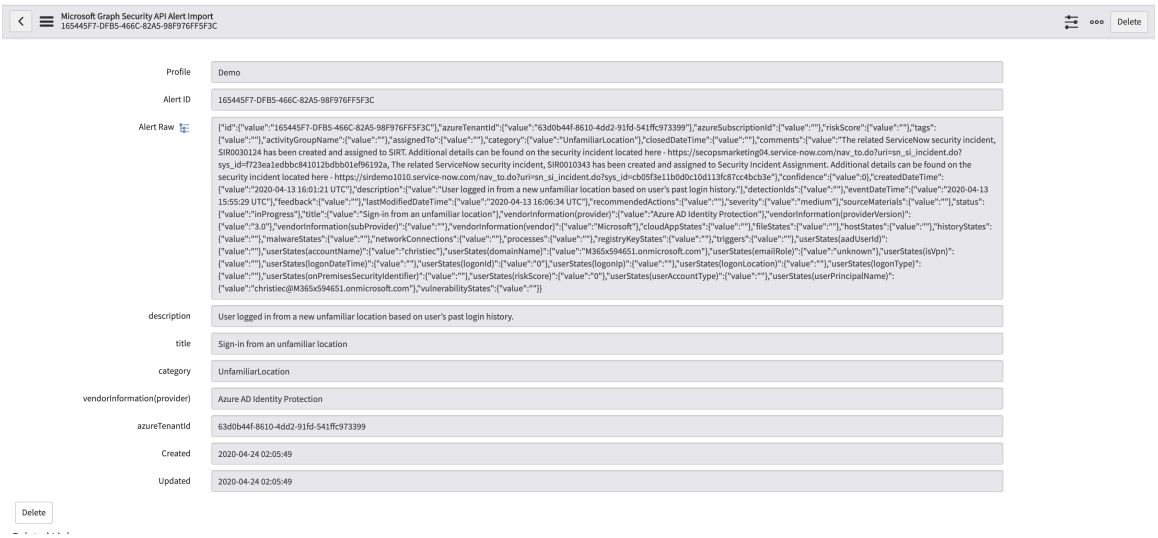
Worknotes

If you had selected the **Log work note for new alert** option in the alert Aggregation Criteria as described in the Mapping alerts to security incident response fields, a worknote is posted when the alert is aggregated.



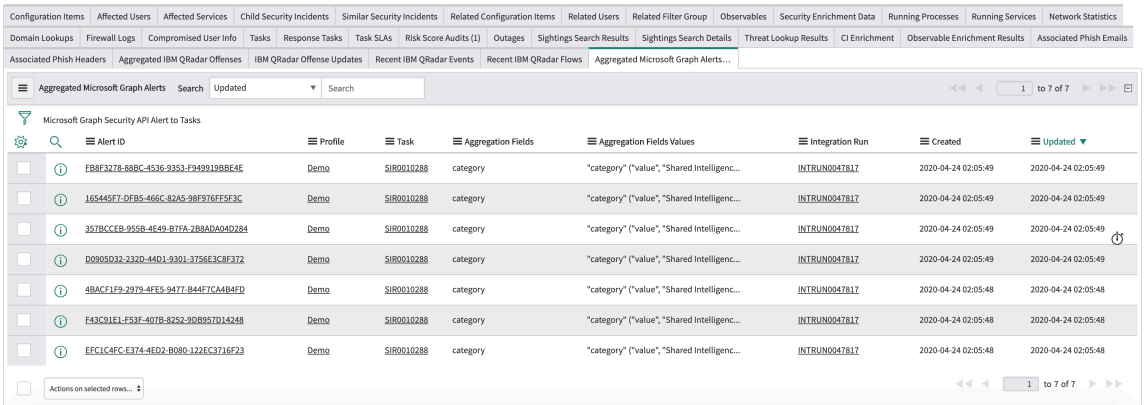
Click on the alert link to navigate to the internal alert import record that contains raw alert data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Aggregated alerts

Click **Related Lists** > **Aggregated Microsoft Graph Security alerts** to view the alerts aggregated to the security incident.



- **Create security incident**: Select an alert from the list, click the **Actions** menu and click **Create security incident**. This option creates a new security incident for the alert and this alert is de-aggregated from the parent security incident.
- **Delete alert record**: Select an alert from the list, click the **Actions** menu and click **Delete**. This option deletes the alert record.

Optional: Copy a Microsoft Graph Security API profile

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

Before you begin

Role required: sn_si.admin

About this task

As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Microsoft Graph Security API Integration** > **Microsoft Graph Security API Profile**.
2. In the Microsoft Graph Security API Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.
   The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

   You have successfully copied the settings from an existing profile to a new profile. Note that the **Active** column status is set to false as the profile needs to be activated.

What to do next

You are prompted to activate (enable) the new profile after you complete the configuration steps.

Domain separation and Microsoft Graph Security API alert ingestion

Domain separation is supported for this application. The Microsoft Graph Security API integration ingests alerts from Microsoft Graph security providers and automatically creates security incidents. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

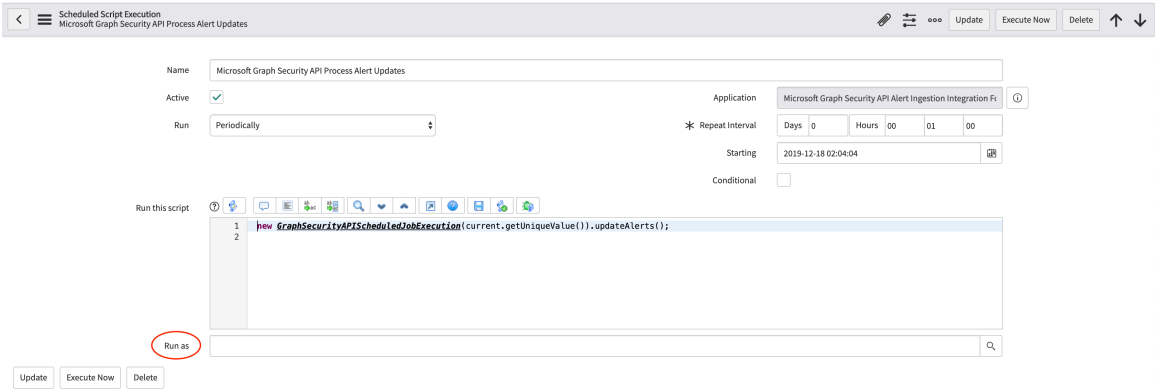
Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

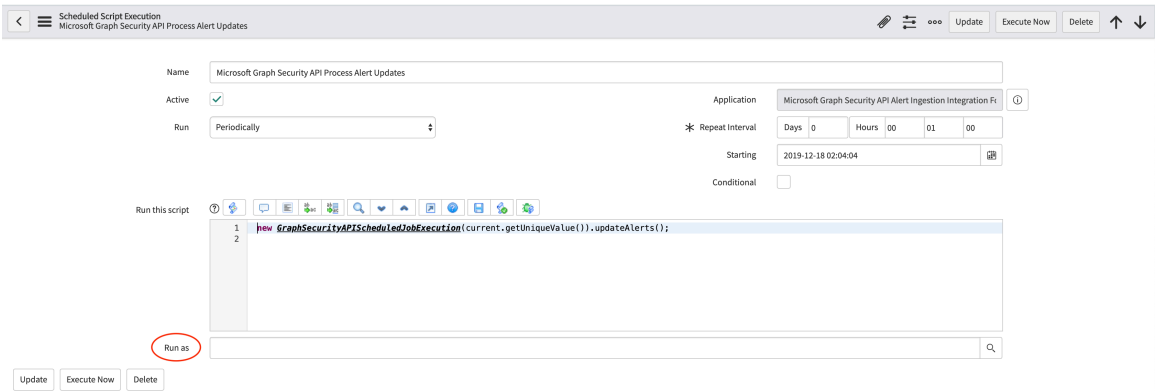
For more information on support levels, see Application support for domain separation.

How domain separation works in the Microsoft Graph Security API

To achieve domain separation, replicate the Microsoft Graph Security API Profile Process and SIR Process Alert Updates scheduled jobs and change the **Run as** users. By default, the system users execute these scheduled jobs. Change the **Run as** to a user with the sn_si.admin role in the respective domain and run the scheduled job.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.





Related topics

Domain separation for service providers

Flow Designer and Integration Hub usage in Microsoft Graph Security API integration

Using the Flow Designer and Integration Hub functionality, several subflows and actions have been built as part of the Microsoft Graph Security API integration.

The following subflows are available:

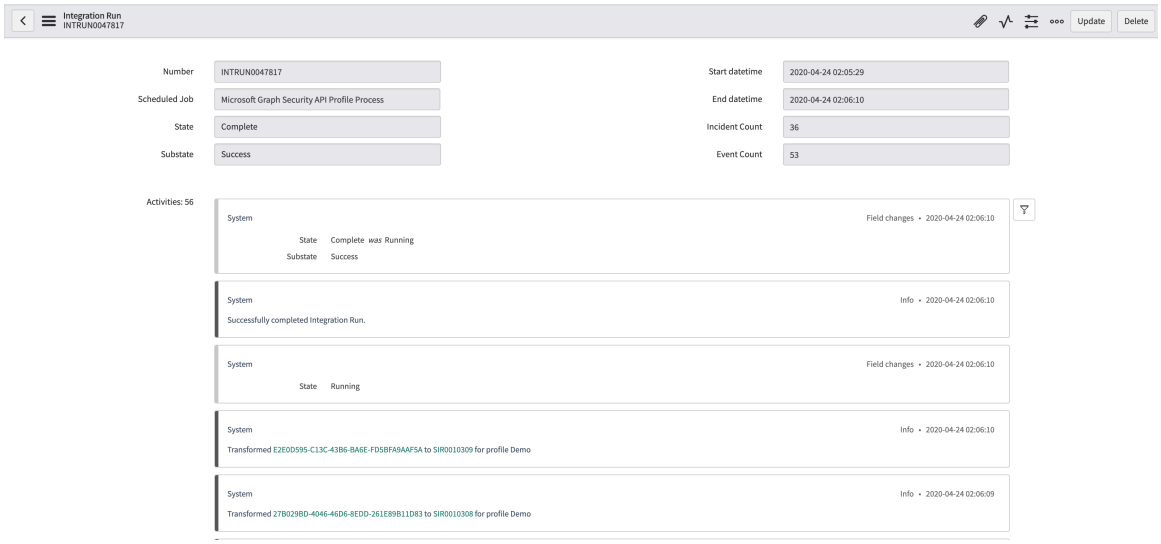
- Microsoft Graph Security API Configuration Validation: This is used in the configuration tile to validate the credentials in the initial setup.
- REST Call For Microsoft Graph Security API: This is used for any interactions with Microsoft Graph security API using REST calls.
- Retrieve Sample Alerts: This is used in the Mapping section of the profile setup to fetch sample data. This sub-flow is triggered asynchronously.

Troubleshooting Microsoft Graph Security API integration

This section covers important troubleshooting tips and frequently asked questions related to the Microsoft Graph Security API alert ingestion integration.

- **Integration run**: When a scheduled job starts executing, an integration run record with logs, errors, and warnings is displayed. The number of alerts pulled and the number of incidents created in a scheduled job run are also displayed. Users with the `sn_si.analyst` role can see if any errors/profiles pulling failed during the integration run. Users with the `sn_si.analyst` role can check the `sn_event_ingestion_integration_run` table for any errors that have occurred. To troubleshoot any integration issues, you must first check the integration run. Errors are logged as worknotes in the integration run records for every scheduled job run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **Incomplete profile**: While configuring the profile, in the Additional Options (Automate alert updates and closure based on SIR incident status) section, you must click the **Finish** button to ensure that the profile is moved to Waiting state indicating that it is waiting for ingestion.
- **Validate profile**: To validate if the integration is working correctly, check the profile states, last pulled date of profile, alert import table, alert to task table records.
- **SSL issues**: When connecting through the Microsoft Graph Security API, ensure that the instance has a valid CA certificate which has not expired. You can import RSA or your own certificates into the platform and ensure that the common name of the certificate matches host name. See KB0778285 for details.

Palo Alto Networks - AutoFocus integration

The Palo Alto Networks - AutoFocus integration base system includes a workflow and a series of workflow activities you can use to integrate Palo Alto Networks - AutoFocus with your instance.

Explore

Security Incident Response integrations

Set up

Activate and configure Palo Alto Networks - AutoFocus integration

---

Use

- Security Operations Palo Alto Networks - Check and Block Value workflow
- Get AutoFocus Session Info Enrichment Flow

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Activate and configure Palo Alto Networks - AutoFocus integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including Palo Alto Networks - AutoFocus. Before you can use the Palo Alto Networks - AutoFocus, you must download it from the ServiceNow Store.

Before you begin

Role required: sn_si_admin

Procedure

1. Download an application from the ServiceNow Store for the first time.
2. When the installation is complete, access Palo Alto Networks support site and obtain the API Key.
3. In your instance, navigate to **Security Operations** > **Integration Configuration**.
4. In the Palo Alto Networks AutoFocus card, click **Configure**.
5. Enter (or paste) the **API Key** you acquired from the Palo Alto Networks support site.
6. Click **Submit**.

Get AutoFocus Session Info Enrichment Flow

When the **Security Operations Palo Alto Networks- Get AutoFocus Session Info Enrichment** flow is executed, it queues a search query with AutoFocus for gathering information about a specified source IP. If AutoFocus has knowledge about previous sessions originating from that IP address, a JSON-formatted report is returned.

Before you begin

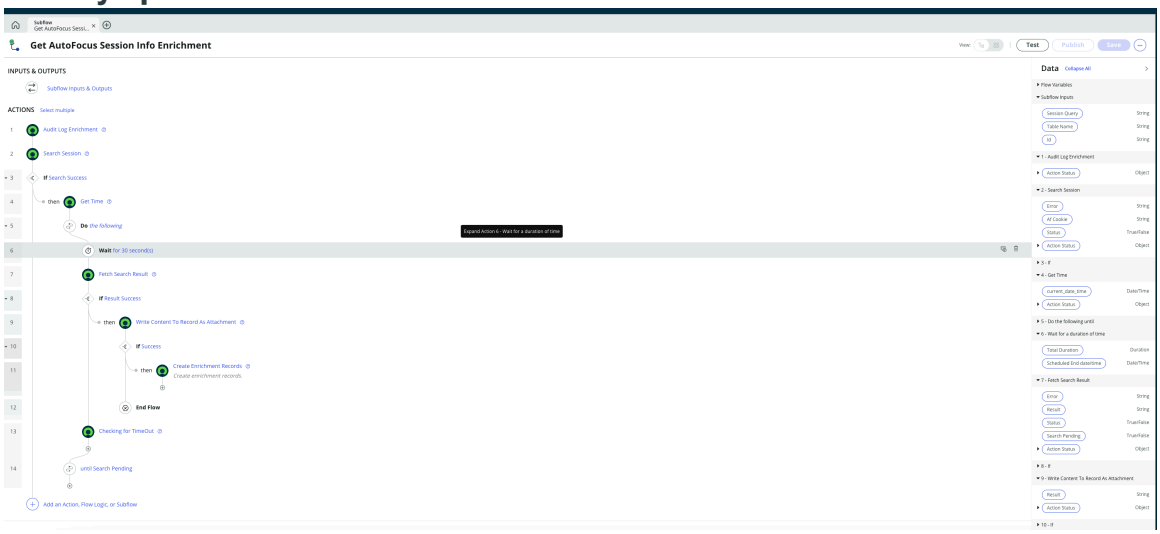
Role required: sn_si.analyst

About this task

The **Security Operations Palo Alto Networks- Get AutoFocus Session Info Enrichment** flow is executed when the **Source IP** field in a security incident is modified and the record is updated. The flow fetches the IP address and submits a query request to AutoFocus. If AutoFocus has previously identified sessions originating from the IP address, a JSON-formatted report is returned.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations Palo Alto Networks - Get Wildfire Data Enrichment Flow



Procedure

1. Navigate to **All** > **Security Incident** > **Show Open Incidents**.
2. Click the **Indicators of Compromise** tab and populate the **Source IP** field.
3. Click **Update**.
   AutoFocus scans the information from the IP address and a text file in JSON format is attached to the security incident.

   Actions specific to this integration are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

AutoFocus Search Session action

The **AutoFocus Search Session** flow action uploads information from an IP address assigned to a security incident to AutoFocus and queues it for a search query.

Input variables

Note:

When the action executes, it queues a search query with AutoFocus for gathering information for a specified source IP. If AutoFocus has previously identified sessions originating from that IP address, a JSON-formatted report is returned.

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
searchSessionQuery [string]	The search query for session information.

Fetch Search Results action

The **Fetch Search Results** flow action fetches search results identified by a cookie to the search query initiated by the **AutoFocus Search Session** action.

Input variables

Input variables determine the initial behavior of the action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Variable	Description
afcookie [string]	The AutoFocus cookie for the search request generated by the AutoFocus Search Session action.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
searchPending [Boolean]	True if the search request is still processing in AutoFocus.
result [string]	The search results data.
status [Boolean]	True if the search is completed and results have been successfully generated.
error [string]	The error, if any, that occurred in the action.

Palo Alto Networks - Firewall integration

To perform Palo Alto Networks - Firewall integration, ensure that you have a MID Server set up with SSH credentials. If a firewall is not already set up, add one.

Explore

Security Incident Response integrations

Set up

- Activate and configure the Palo Alto Networks Firewall Integration
- Set up SSH credentials to the MID Server

Use

Security Operations Integration Palo Alto Networks Firewall Launcher workflow

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Set up SSH credentials to the MID Server

Palo Alto Networks Firewall sends API calls to the MID Server. As such, ensure that SSH credentials have been created for the MID Server.

Before you begin

- The Orchestration plugin must be activated.

Role required: admin

Procedure

1. Navigate to **All** > **Orchestration** > **Credentials & Connections** > **Credentials**.
2. Click **New**.
3. In the Interceptor screen, click **SSH Credentials**.
4. Fill in the fields, as needed.

SSH Credentials

Field	Description
Name	Enter a name for the credential.
Active	Select this check box to activate this credential.
Applies to	Select **All MID servers** or **Specific MID servers**.
MID Servers	If you selected **Specific MID servers**, click the lock icon and select the MID Servers you want to apply these credentials to.
Order	Select the order to which the credentials are tried by the server. Smaller numbers are tried first.
User name	Enter the user name of the user associated with these credentials, if any.
Password	If you entered a **User name**, enter the user's password.
Tag	Enter a tag to be used for search criteria. The **Tag** field should contain the same value as the **Name**.

Activate and configure the Palo Alto Networks Firewall Integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including Palo Alto Networks - Firewall. Before you can use the Palo Alto Networks - Firewall, you must download it from the ServiceNow Store.

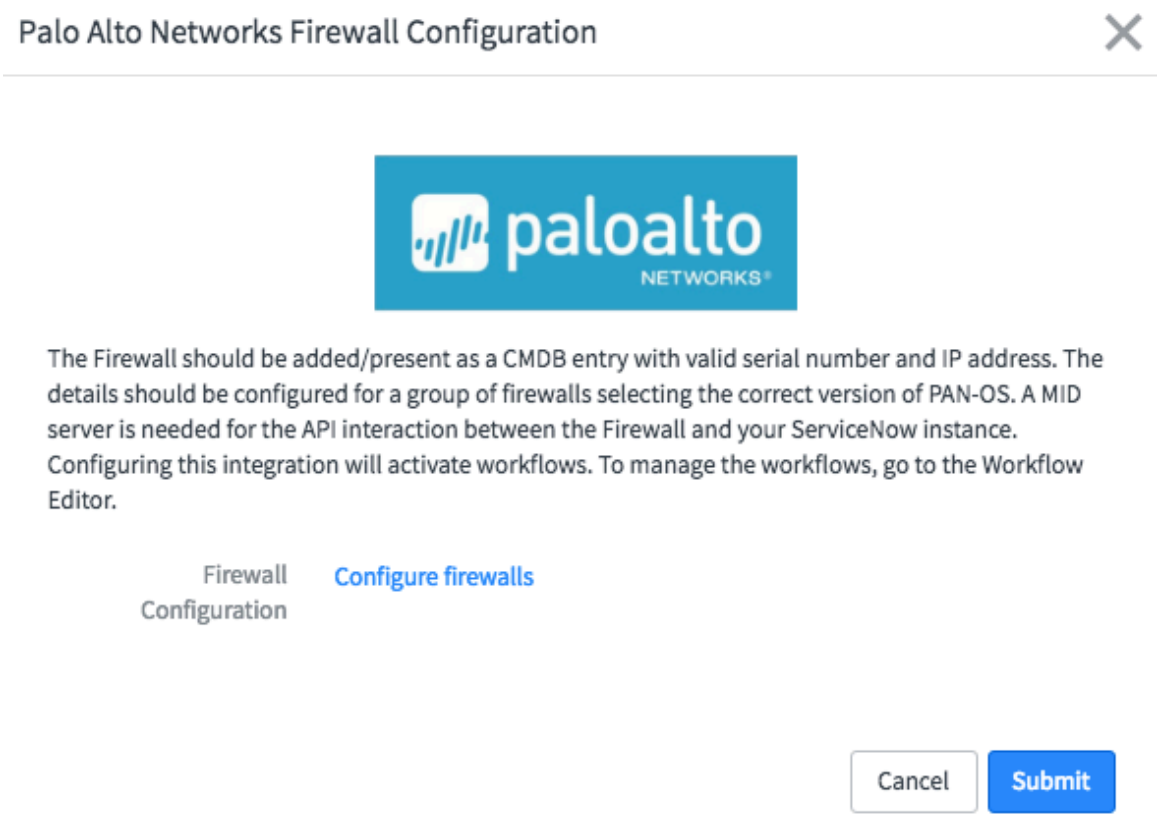
Before you begin

Role required: sn_si_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Before activating and configuring the integration, access the Palo Alto Networks Firewall dashboard.
   Take note of the names of the IP Dynamic List, URL Dynamic List, or Domain Dynamic List you are using for firewall blocking.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Security Operations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
4. In the Palo Alto Networks Firewall card, click **Configure**.



5. Click **Configure firewalls**.
6. In the Firewall Configurations screen, click **New**.
7. Fill in the fields on the form, as appropriate.

Field	Description
Firewalls	Click the lock icon and select the firewall to be configured.
Firewall Version	Select the Palo Alto Networks Firewall version.**PAN-OS-7.1** is the recommended version. Selecting earlier versions may return inconsistent results.
Username	Enter the username to use when connecting to the firewall via REST endpoints.
Password	Enter the password for the connecting user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
IP Dynamic List	Enter the name of the External Dynamic List or Dynamic Block List you use for IP addresses.
URL Dynamic List	Enter the name of the External Dynamic List or Dynamic Block List you use for URLs.
Domain Dynamic List	Enter the name of the External Dynamic List or Dynamic Block List you use for domains.

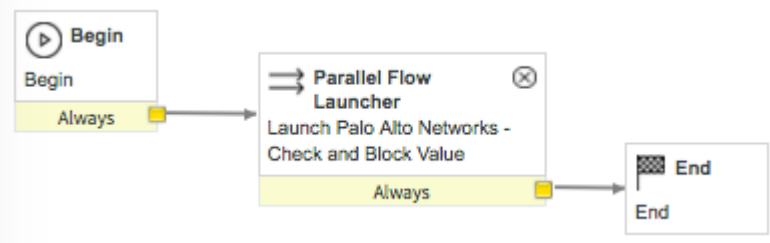
8. Click **Submit**.

Security Operations Integration Palo Alto Networks Firewall Launcher workflow

Security Operations Integration Palo Alto Networks Firewall Launcher workflow is the Palo Alto Networks Firewall implementation launched by the **Security Operations Integration - Block Request** capability workflow.

Before you begin
Role required: sn_si.analyst

About this task
Workflow process activities include:Security Operations Palo Alto Networks - Check and Block Value workflow.



Security Operations Palo Alto Networks - Check and Block Value workflow

As security incidents are created and triaged to identify potential threats, you can use the **Security Operations Palo Alto Networks - Check and Block Value** workflow to automatically check and update IP addresses, URLs, and domains using External Dynamic Lists defined in Palo Alto Networks - Firewall.

Before you begin
Role required: sn_si.analyst

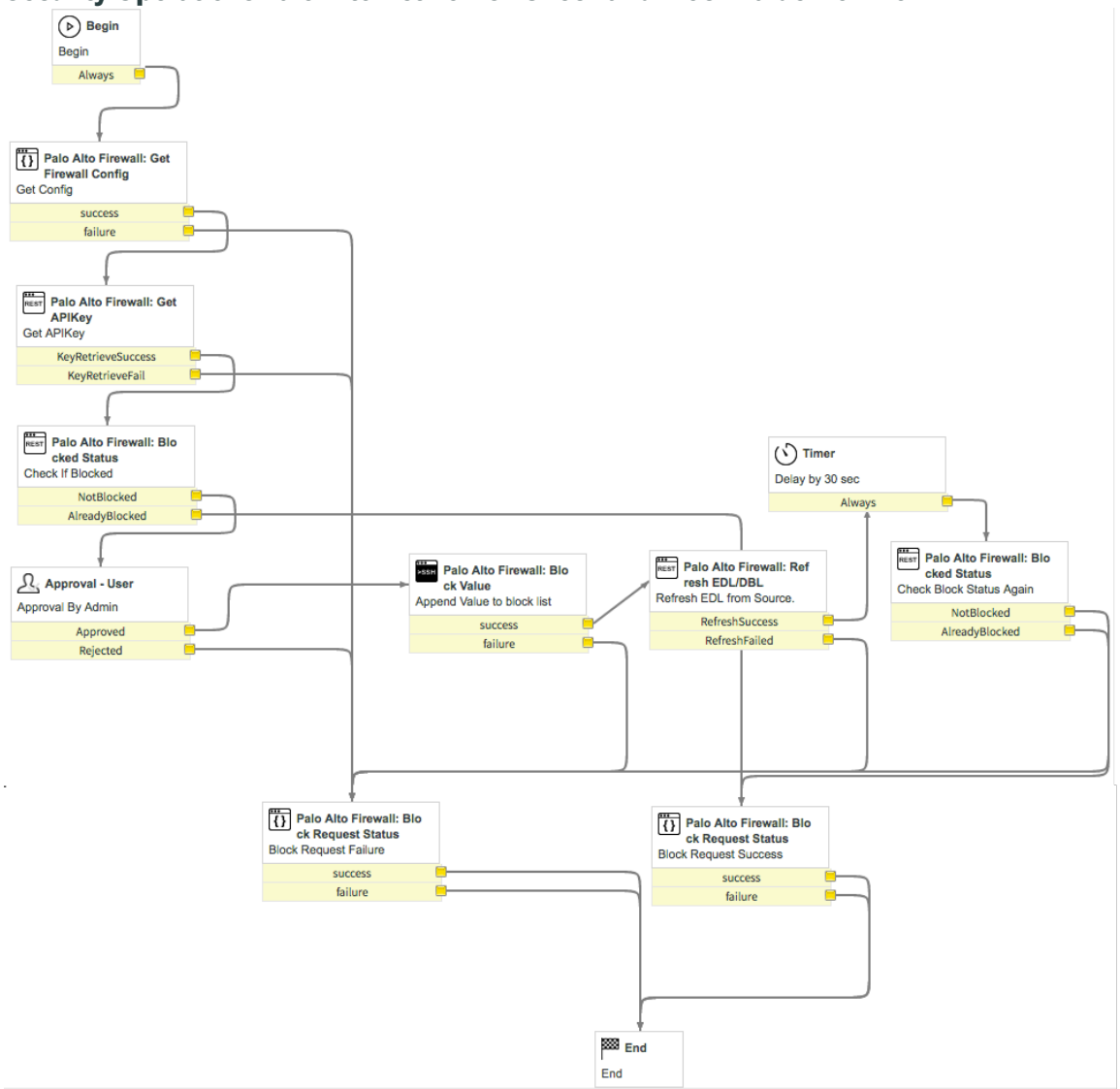
About this task
The **Security Operations Palo Alto Networks - Check and Block Value** workflow is executed when Firewall Block Requests are submitted. The block request specifies the firewall to be used, the type of observable to be checked and blocked (if needed), and the block value. That is, the IP address, URL, or domain in question.

During workflow execution, commands defined under **Palo Alto Networks Integration** > **Firewall** > **Commands** are run. The Show type commands (for example, Show-IP-ExternalDynamicList) determine whether the value exists on the firewall. The Refresh type commands (for example, Refresh-IP-ExternalDynamicList) add value that do not exist on the firewall to the block list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the Blocked Status activity executes, approval by a system administrator is required before the workflow can proceed.

Security Operations Palo Alto Networks - Check and Block Value workflow



Procedure

1. Navigate to **Palo Alto Networks Integration** > **Firewall** > **Block Requests**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Firewall	Select the firewall to be used.
Block Type	Select the type of value to be checked: ○ IP ○ URL ○ DOMAIN

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Block Value	Enter the value of the selected type to be checked on the firewall.

4. Click **Submit**.

Palo Alto Firewall- Block Request Status activity

This activity is called by other activities to set the Firewall block request status to success or failure.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
firewallBlockRequestSysid [string]	The system id of the firewall block request. This input variable is mandatory.
status [string]	Indicates whether the refresh job ran: success or failure.

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
result [string]	Indicates whether the success or failure of the refresh job.

Palo Alto Firewall- Block Value activity

After the workflow has identified a value that is not on the firewall, the record is routed for approval. Upon approval, this activity connects to the MID Server via your SSH credentials and invokes a script that adds the value to the firewall External Block List.

Input variables

Input variables determine the initial behavior of the activity.

Note: You must manually enter the input variables for this activity and then publish the workflow. If the workflow is not published, the input variables will not be saved for non-admin users.

Input variables

Variable	Description
toBeBlockedValue [string]	The value to be added to the EDL if not already present. This input variable is mandatory.
typeToBeBlocked [string]	The type of value to be blocked: IP, URL, or Domain. This input variable is mandatory.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables (continued)

Variable	Description
targetHost [string]	The MID Server on which the script is executed.
SSHCredentialTag [string]	The SSH credential tag defined on the MID server.
scriptCommand [string]	The AppendValueToList.sh script used to add the value to the EDL. It requires the full path to the MID Server.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
result [string]	The result passed to the EDL.

Palo Alto Firewall- Blocked Status activity

This activity checks if the value (IP, URL, or domain) is included in its respective External Dynamic List/Dynamic Block List (EDL/DBL) on firewall. The EDL/DBL details are obtained from the firewall using an operational command, and a routine is performed to check if the value is blocked on the firewall.

Input variables

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

Input variables

Variable	Description
valueToBeChecked [string]	The value in the block request.
showEDLDetailsCommand [string]	The External Dynamic List command being used to determine whether the value exists on the firewall.
FirewallIpAddress [string]	The IP address of the firewall used.
FirewallApiKey [string]	The firewall API key.

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as data dynamically generated using the Palo Alto Firewall Operational Command API message.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
commandResult [string]	The results from the firewall for the show EDL Details command.
blockedStatus [Boolean]	True indicates blocked. False indicates not blocked.
commandResponse [string]	The response status obtained from the firewall for the show EDL Details Command.

Palo Alto Firewall: Get API Key Action

This action retrieves the API key from the firewall.

Input variables

Input variables determine the initial behavior of the action. All input variable entries listed are mandatory.

Input variables

Variable	Description
Username [string]	The user name of the firewall administrator.
Password [string]	The firewall administrator password.
FirewallIpAddress [string]	The IP address of the firewall.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
APIKey [string]	The firewall API key.

Palo Alto Firewall: Get Firewall Config Action

The **Palo Alto Firewall: Get Firewall Config** flow action gets all the related firewall configuration information from the database, and makes it available for use by the subsequent action.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
firewallSysid [string]	The system id of the firewall. This input variable is mandatory.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables (continued)

Variable	Description
typeOfValueToBeBlocked [string]	The type of value to be blocked on the firewall: IP, URL, or Domain.
firewallIPAddress [string]	The IP address of the firewall.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
ipEDLName [string]	The External Dynamic List name for IP addresses.
urlEDLName [string]	The External Dynamic List name for URLs.
domainEDLName [string]	The External Dynamic List name for domains.
firewallVersionSysId [string]	The system id for the firewall version.
refreshEDLCommand [string]	The command to be used to refresh the EDL from the source.
ShowEDLDetailsCommand [string]	The command to be used to get the EDL details.
status [Boolean]	True indicates success. False indicates failure.
error [string]	The error, if any, that occurred in the action.
endpoint [Encrypted]	The encrypted endpoint from the database.

Palo Alto Firewall- Refresh EDL/DBL activity

This activity executes an operational command on the firewall to refresh the External Dynamic List from the source configured on the firewall. The output of this activity indicates whether the Refresh job has been queued up.

Input variables

Input variables determine the initial behavior of the activity. All input variable entries listed are mandatory.

Input variables

Variable	Description
FirewallIpAddress [string]	The IP address of the firewall being refreshed.
FirewallApiKey [string]	The refreshed firewall API key.
FirewallCommand [string]	The operational command to be executed to queue up the refresh job.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

The output variables contain data that can be used in subsequent activities. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
activity.Output.result [string]	A text string to indicate whether refresh job was queued to run: success or failure.

Get Log Data Flow

If Security Incident Response, Threat Intelligence, and Palo Alto Networks - Firewall are activated, the **Security Operations Palo Alto Networks - Get Log Data** flow automatically executes when the Source IP for observables in a security incident is changed.

Before you begin

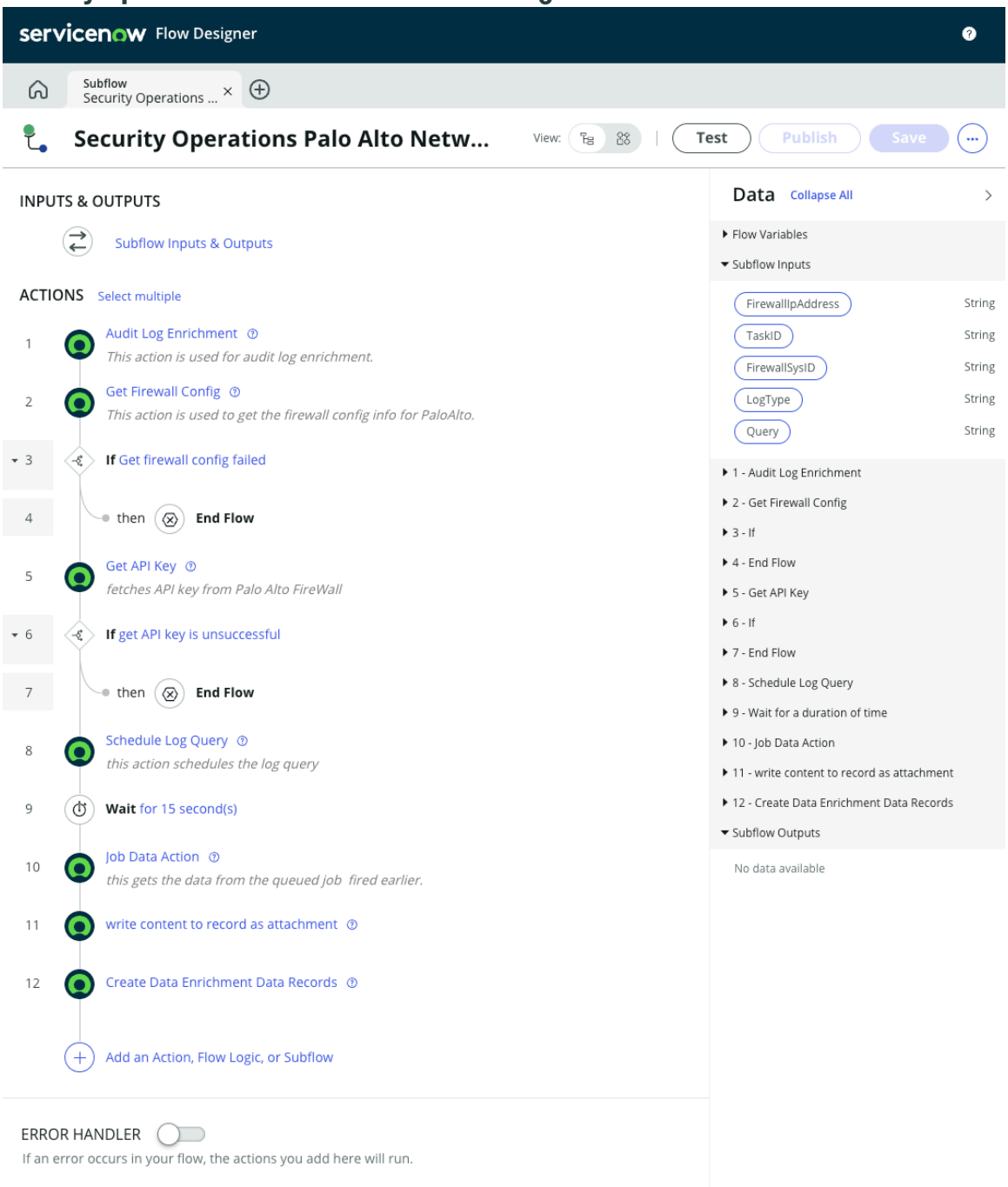
Role required: sn_si.analyst

About this task

During flow execution, firewall configuration information is retrieved from the database and the API Key is retrieved from the firewall. The Get Log action queues up a search query on the firewall. When the query runs, it returns a Job ID that is used to retrieve threat logs data from the firewall. It attaches the log data as an XML file to the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations Palo Alto Networks - Get Log Data flow



Procedure

1. Navigate to a security incident that contains observables.
2. Click the **Security Incident Observables** tab.
3. In **Source IP**, add or modify the IP address.
4. Click **Update**.
   The **Security Operations Palo Alto Networks - Get Log Data** flow executes and enriched threat log data is attached to the security incident. The information is also parsed and displayed in the **Firewall Logs** section under the **Enrichment Data** tab.

Palo Alto Firewall: Get API Key Action

This action retrieves the API key from the firewall.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Input variables determine the initial behavior of the action. All input variable entries listed are mandatory.

Input variables

Variable	Description
Username [string]	The user name of the firewall administrator.
Password [string]	The firewall administrator password.
FirewallIpAddress [string]	The IP address of the firewall.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
APIKey [string]	The firewall API key.

Palo Alto Firewall: Get Firewall Config Action

The **Palo Alto Firewall: Get Firewall Config** flow action gets all the related firewall configuration information from the database, and makes it available for use by the subsequent action.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
firewallSysid [string]	The system id of the firewall. This input variable is mandatory.
typeOfValueToBeBlocked [string]	The type of value to be blocked on the firewall: IP, URL, or Domain.
firewallIPAddress [string]	The IP address of the firewall.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
ipEDLName [string]	The External Dynamic List name for IP addresses.
urlEDLName [string]	The External Dynamic List name for URLs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables (continued)

Variable	Description
domainEDLName [string]	The External Dynamic List name for domains.
firewallVersionSysId [string]	The system id for the firewall version.
refreshEDLCommand [string]	The command to be used to refresh the EDL from the source.
ShowEDLDetailsCommand [string]	The command to be used to get the EDL details.
status [Boolean]	True indicates success. False indicates failure.
error [string]	The error, if any, that occurred in the action.
endpoint [Encrypted]	The encrypted endpoint from the database.

Palo Alto Firewall- Get Log Action

The **Palo Alto Firewall: Get Log** flow action schedules a query on the firewall to retrieve logs and returns a JobID used to retrieve the log data.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
FirewallIpAddress [string]	The IP address of the firewall. This input variable is mandatory.
FirewallApiKey [string]	The API access key of the firewall. This input variable is mandatory.
FirewallLogType [string]	The type of log data to be retrieved (set to threat). This input variable is mandatory.
FirewallLogFilterQuery [string]	The query to be executed to search for logs on the firewall. This input variable is mandatory.
LogDirection [string]	Specifies whether logs are shown oldest first (backward) or newest first (forward) order.
LogNumber [string]	Specifies the number of logs to retrieve.
LogSkipCount [string]	Specifies the number of logs to skip when doing a log retrieval.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
QueuedJobID [string]	The Job ID returned from the firewall.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables (continued)

Variable	Description
JobScheduled [string]	Specifies (success or failure) whether the job was sent to the firewall.
error [string]	Any errors returned.

Palo Alto Firewall- Job Data Action

After the **Palo Alto Firewall: Get Log** action queues the search query to the firewall and the job runs, the **Palo Alto Firewall: Job Data Action** action retrieves the threat log data from the firewall.

Input variables

Input variables determine the initial behavior of the action. All input fields are mandatory.

Input variables

Variable	Description
FirewallIpAddress [string]	The IP address of the firewall.
FirewallApiKey [string]	The API access key of the firewall.
JobID [string]	The ID of the queued job.

Output variables

The output variables contain data that can be used in subsequent actions. The output consists of data from the firewall configuration, as well as dynamically generated data.

Output variables

Variable	Description
commandStatus [string]	Specifies (success or failure) whether data was retrieved from the firewall.
JobData [string]	The data collected from the firewall.
error [string]	Any errors returned.

Palo Alto Networks - WildFire integration

Palo Alto Networks - WildFire is a cloud-based application that interacts with your system firewall.

Explore

Security Incident Response integrations

Set up

Activate Security Operations Palo Alto Networks - WildFire

Use

Get WildFire Data Enrichment Flow

Develop

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Activate Security Operations Palo Alto Networks - WildFire

Before you can use the Security Operations Palo Alto Networks - WildFire integration, you must download the integration from the ServiceNow Store.

Before you begin

Role required: admin

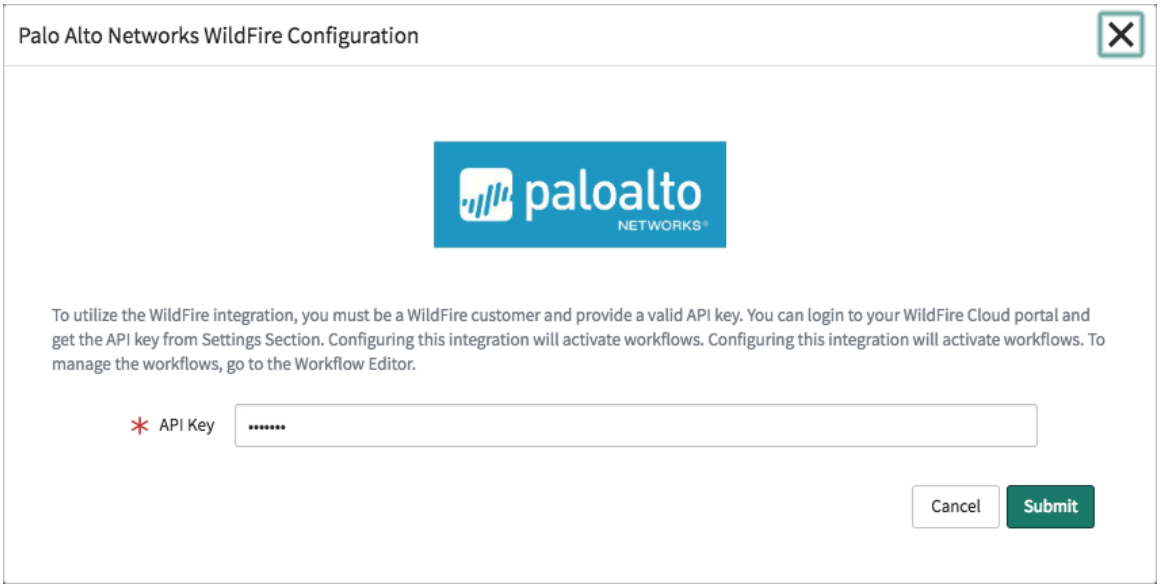
Procedure

1. Download the integration from the ServiceNow Store.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
   The available security integrations appear as a series of cards.



3. In the Carbon Black card, click **Configure**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter the API key, and click **Submit**.
   The integration configuration card displays.
5. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Get WildFire Data Enrichment Flow

When the **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** flow is executed, a hash file is uploaded to WildFire. The data is enriched, and reports are downloaded to the instance to aid in processing potential malware attacks.

Before you begin

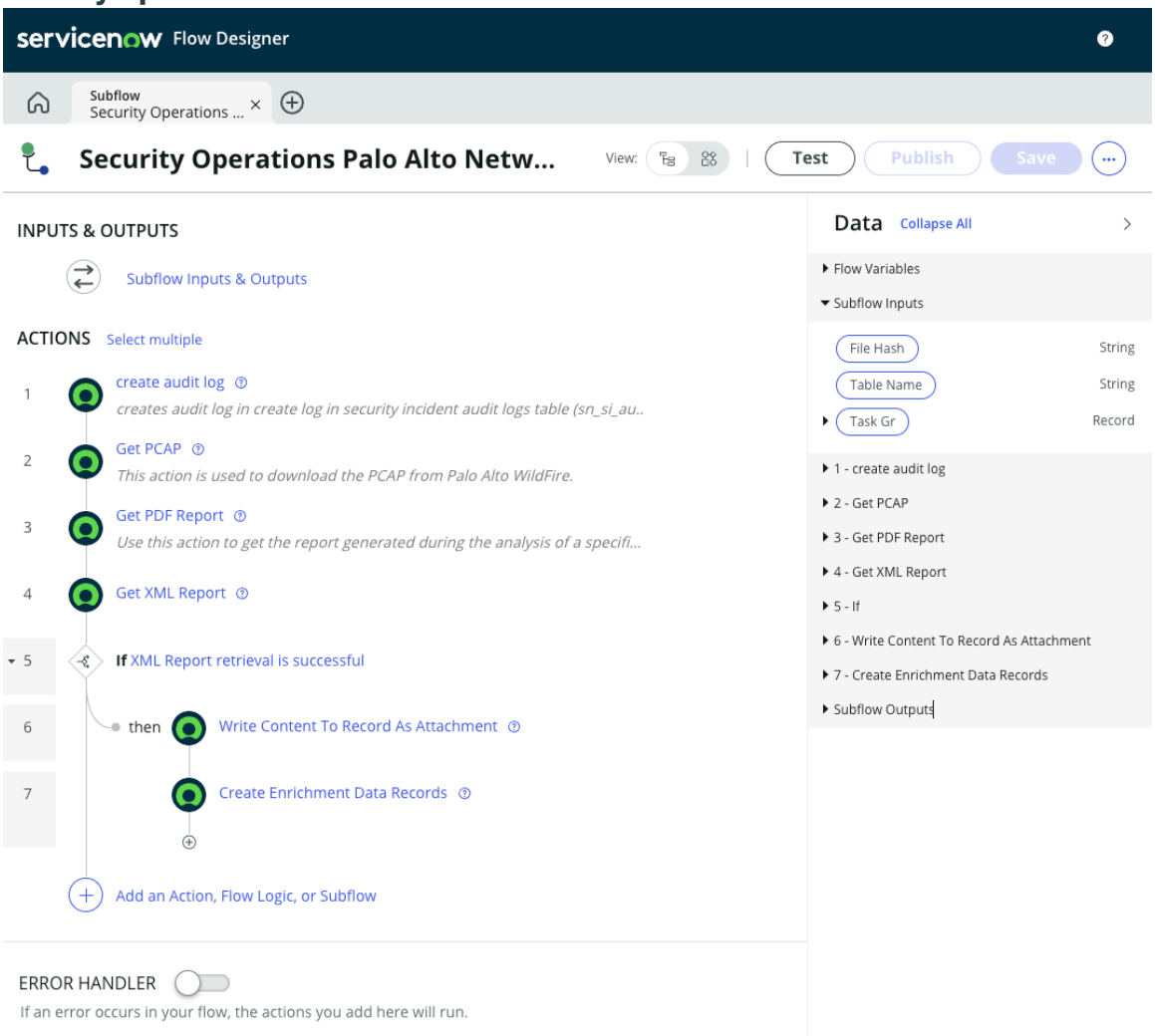
Role required: sn_si.analyst

About this task

The **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** flow is executed when a security incident is created from an alert received from the Palo Alto Network Firewall application. A malware hash from the email notification received from Firewall is entered on the **IoC** tab of the security incident, and the record is updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations Palo Alto Networks - Get WildFire Data Enrichment flow



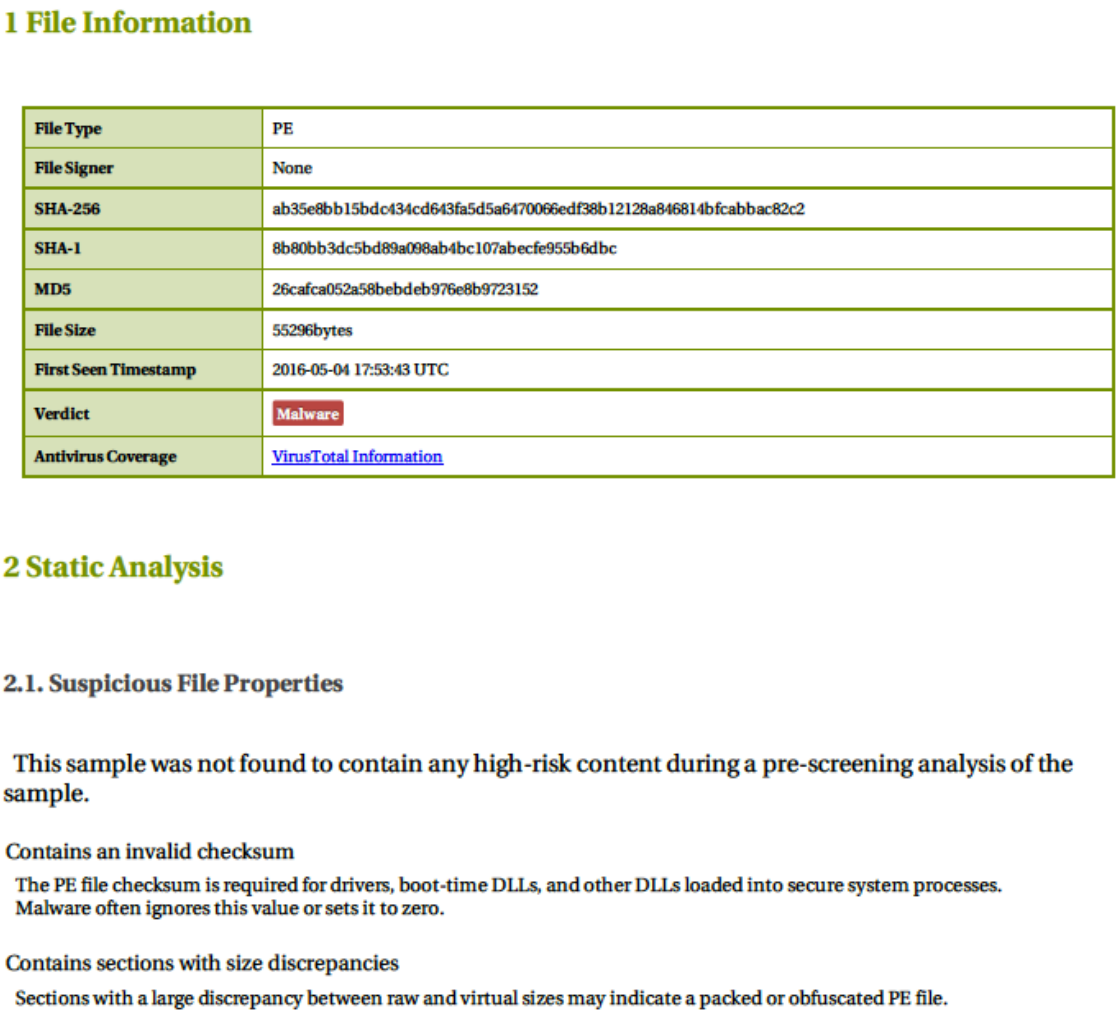
Procedure

1. Navigate to **All** > **Security Incident** > **Show Open Incidents**.
2. Based on the email notification received from Firewall, locate and open the security incident that was created.
3. Click the **Indicators of Compromise** tab and populate the **Malware hash** with the hash you received in the alert.
4. Click **Update**.
   The flow causes the hash file to be uploaded to WildFire where the data is enriched. Reports in the PDF and XML formats are attached to the record (security incident or IoC) in your instance to aid in processing potential malware attacks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If the enriched data includes packet capture information, PCAP information is also downloaded. PCAP data captures what actions the file was performing. For example, it can report on what servers the file was contacting. To view PCAP files, you need a packet analyzer, such as Wireshark.

Sample PDF generated by Wildfire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire- get PCAP action

The **WildFire: Get PCAP** flow action gets the packet capture (PCAP) information generated during the analysis of a specified file hash on WildFire. The result of this action is attached to a specific record as identified by the **TableName** and **RecordId**.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
FileSHA256Hash [string]	The hash of the file received from the Palo Alto Network Firewall application.
TableName [string]	The affected table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables (continued)

Variable	Description
RecordId [string]	The security incident or IoC being updated.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
commandStatus [Boolean]	True if a result is obtained and attached successfully.
errorMessage	The error, if any, that occurred in the action.

WildFire- get PDF report action

The **WildFire: Get PDF Report** flow action gets the report generated during the analysis of a specified file hash on WildFire in PDF format. The result of this action is attached to a specific record as identified by the **TableName** and **RecordId**.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
TableName [string]	The affected table.
FileSHA256Hash [string]	The hash of the file received from the Palo Alto Network Firewall application.
RecordId [string]	The security incident or IoC being updated.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
commandStatus [Boolean]	True if a result is obtained and attached successfully.
errorMessage	The error, if any, that occurred in the action.

WildFire- get XML report action

The **WildFire: Get XML Report** flow action gets the report generated during the analysis of a specified file hash on WildFire in XML format. The result of this action is attached to a specific record as identified by the **TableName** and **RecordId**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Input variables determine the initial behavior of the action.

Input variables

Variable	Description
TableName [string]	The affected table.
FileSHA256Hash [string]	The hash of the file received from the Palo Alto Network Firewall application.
RecordId [string]	The security incident or IoC being updated.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
commandStatus [Boolean]	True if a result is obtained and attached successfully.
errorMessage	The error, if any, that occurred in the action.

Palo Alto Networks Next-Generation Firewall integration

Once installed and configured, the security incident analyst uses this integration to block malicious IP addresses, URLs, and domains using External Dynamic List (EDL) capabilities with the ServiceNow Security Incident Response (SIR) products. The security incident analyst creates entries for an EDL from observables determined to be malicious on ServiceNow SIR security incidents.

An EDL is a text file that is hosted on an external web server. For this integration, this web server is your ServiceNow AI Platform instance, which permits the Palo Alto Networks Next-Generation Firewall to import objects that are included in the list, IP addresses, URLs, and domains, and to enforce policy.

To enforce policy on the EDL entries, the list is referenced in a policy rule or profile. As the EDL entries are modified, the firewall dynamically imports the list at the configured interval and enforces policy without a configuration change or a commit on the firewall. For this integration, ServiceNow AI Platform has created a table containing EDL entries that are retrieved by authorized Palo Alto Networks Next-Generation Firewall at the configured retrieval intervals.

The integration includes the following features:

- Flexibility to create multiple EDLs that apply to different firewall deny or allow policies.
- Detailed reporting on the types of sites being blocked (phishing, malware, and allow listed sites).
- Tagging of ServiceNow AI Platform security incidents with EDL entries by the observable type (URL, domain, IP address).
- Configuring EDL expiration periods to maintain EDL list size by automatically expiring or removing older entries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Searching, deleting, or migrating EDL entries between EDL lists.
- Linking EDL entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

The integration requires that the (com.snc.security_incident) and (com.snc.secops.orchestration) plugins from the Security Incident Response product are activated.

This integration only supports Palo Alto Networks (PAN-OS 8.x). Earlier versions are not supported.

Note: The following topics are numbered. For a smooth installation, configuration, and verification of expected results, follow the topics in the order they are presented.

Create a certificate profile for the Palo Alto Networks Next-Generation Firewall

The integration requires a certificate profile to validate and authenticate the secure connection between the ServiceNow AI Platform® server and the Palo Alto Networks Next-Generation Firewall server.

Role required: Palo Alto Networks Next-Generation Firewall Administrator.

A Palo Alto Networks Next-Generation Firewall authenticates to a ServiceNow AI Platform® instance, retrieves EDL entries from the database table, and incorporates the entries into corresponding firewall policy rules. This retrieval requires the API user account role in the ServiceNow AI Platform® instance, which is used by the PAN firewall admin to access the ServiceNow AI Platform® API.

Follow the steps below on how to download DigiCertificates and configure the certificate profile.

1. Download DigiCert or Entrust CA Gateway Certificate based on the use case. For more information, see the KB1702083 article in the Now Support Knowledge Base.
2. Configure the certificate profile. For more information, see Palo Alto Networks documentation.

Related topics

"Configure a Certificate Profile" in the PAN-OS 10.0 Administrator's Guide

Set up and install Palo Alto Networks Next-Generation Firewall

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

Before you begin

Role required: (admin)

Setup task	Description
Verify that you have the required ServiceNow AI Platform and Security Incident Response roles assigned.	The following roles are required: • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees the configuration, and creates, activates, and removes EDLs. This role also assigns the sn_si.analyst role. • The (admin) assigns the ServiceNow AI Platform® API account role

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	(sn_sec_panfw.api_account_access), which is used exclusively for entering credentials required for authentication on Palo Alto Networks so the firewalls can retrieve EDLs from the ServiceNow AI Platform®. • (sn_si.analyst), or Security Operations Center (SOC) Analyst, creates EDL entries and works with security incidents.
Verify that you are using Palo Alto Networks Next-Generation Firewall version-OS 9.x, and 10.x.	This integration only supports Palo Alto Networks Next-Generation Firewall OS 9.0 and later.
Set up any EDL profiles, security policy rules, and certificate profiles in Palo Alto Networks as recommended in Palo Alto Networks documentation.	Refer to Palo Alto Networks general documentation and requirements at the: Paloalto Networks Documentation website.
Verify that you have downloaded and configured the DigiCert Root Authority Certificate.	The integration requires this certificate to validate and authenticate the secure connection between the ServiceNow AI Platform server and the Palo Alto Networks Next-Generation Firewall server. For more information on setting up the certificate, see "Configure a Certificate Profile" in the PAN-OS 10.0 Administrator's Guide. For the download, see Create a certificate profile for the Palo Alto Networks Next-Generation Firewall and DigiCert Trusted Root Authority Certificates.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	3. Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.
If your organization has ServiceNow AI Platform® change management and approval processes for email deletion, verify that email send/receive capability is enabled.	To verify that email send/receive capability is enabled in your ServiceNow AI Platform® instance, navigate to **Email properties** > **Administration** > **Email Properties**. In Outbound Email Configuration, verify **Email sending** and **Email receiving** are selected.

Procedure

If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.

Create the API account role for Palo Alto Networks Next-Generation Firewall

An API account role is required in your ServiceNow AI Platform® instance for this integration. The Username and Password associated with this account are created in the ServiceNow AI Platform® and entered in Palo Alto Networks so the Palo Alto Networks Next-Generation Firewall authenticates with the ServiceNow AI Platform® when retrieving EDL entries.

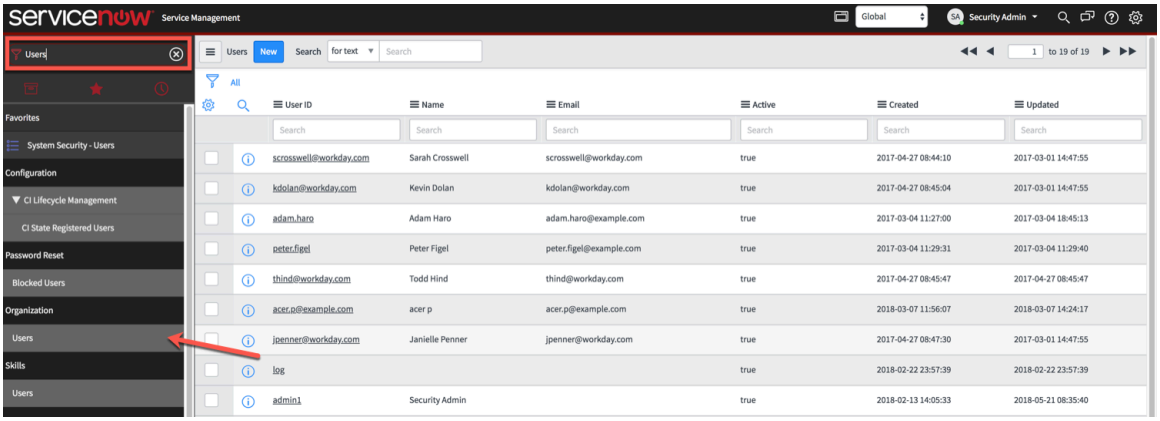
Before you begin
Role required: admin

About this task
The ServiceNow AI Platform® admin creates an API account role (sn_sec_panfw.api_account_access). This account is used exclusively for entering credentials required for authentication on Palo Alto Networks so the firewalls can retrieve EDLs from the ServiceNow AI Platform®. This account is a separate, unique API user account in the ServiceNow AI Platform® instance, and assigned to the Palo Alto Networks Next-Generation Firewall administrator.

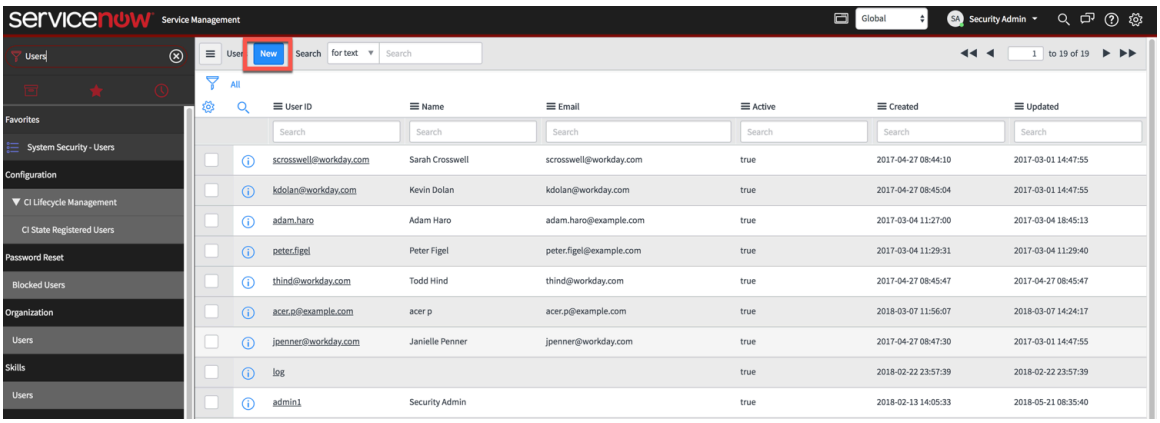
Procedure

1. Navigate to **All** > **Organization** > **Users**.
2. Click the **Users** module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. On the Users list that is displayed, click **New**.



A new user form is displayed.

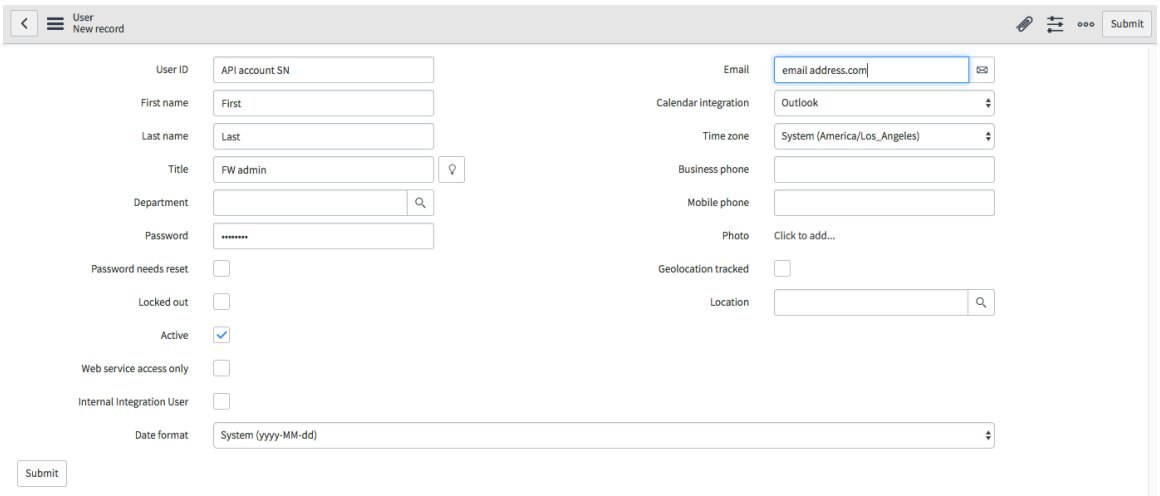
4. Fill in the form.

Note: The values for User ID title, and email address shown in the following table and figure are example values.

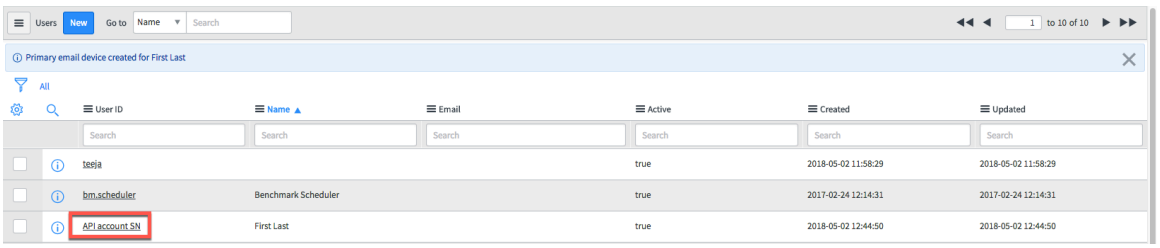
Field	Description
User ID	Unique User ID for the role in your ServiceNow AI Platform® instance. This user ID is entered in the **Username** field in the **Client Authentication** section of the External Dynamic Lists dialog on the Palo Alto Networks site. An example is `API account` SN.
First name	Person you are assigning.
Last name	Person you are assigning.
Title	Job title, for example, `FW admin`.
Password	Unique password created for this role. This password is entered in the **Password** field in the **Client Authentication** section of the External Dynamic Lists dialog on the Palo Alto Networks site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

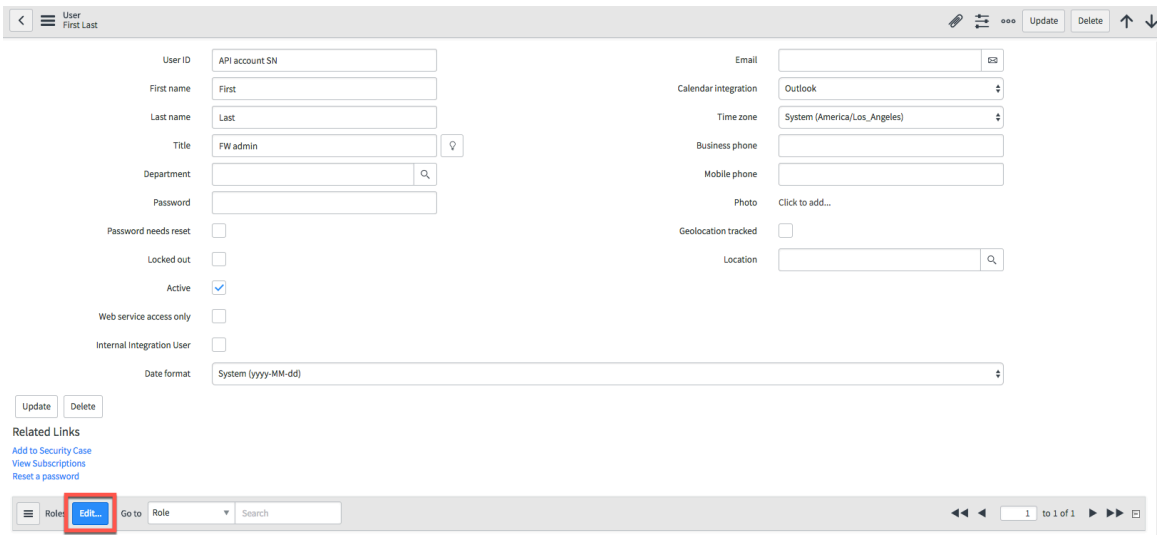
Field	Description
Email	Unique email address.



5. Click **Submit**.
   Once submitted, you can assign the role.
6. On the Users list in the **User ID** column, click the name of the user ID you entered, `API account SN`, for example.

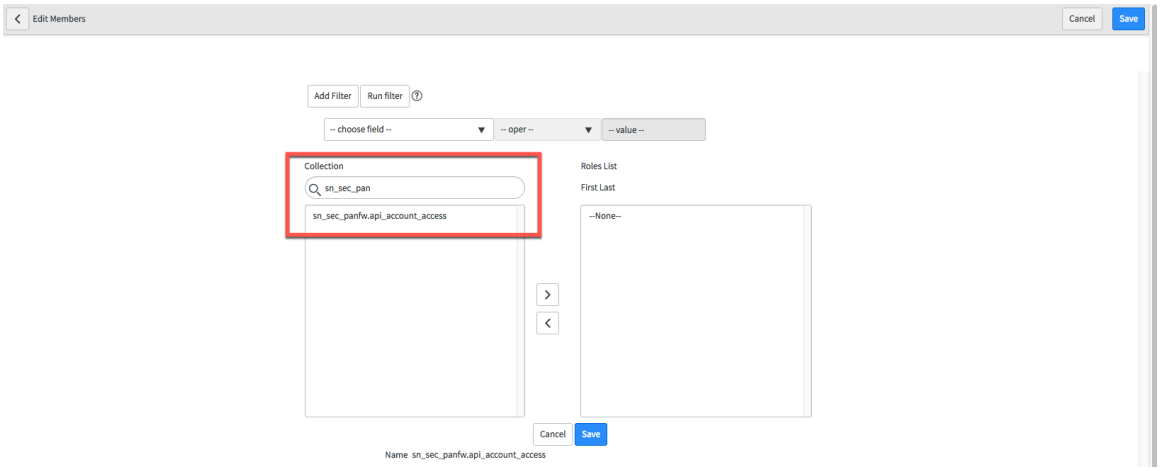


7. On the open record in the Roles section, click **Edit**.

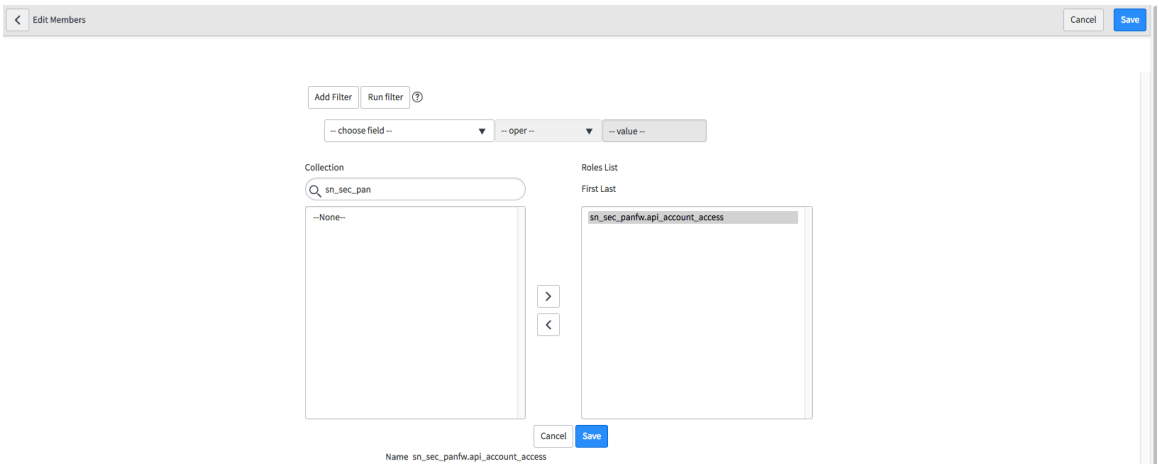


8. On the **Edit Members**form that is displayed, enter `sn_sec_panfw.api_account_access` in the **Collection** field.
   Below the **Collection** field, the role is displayed in the column.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

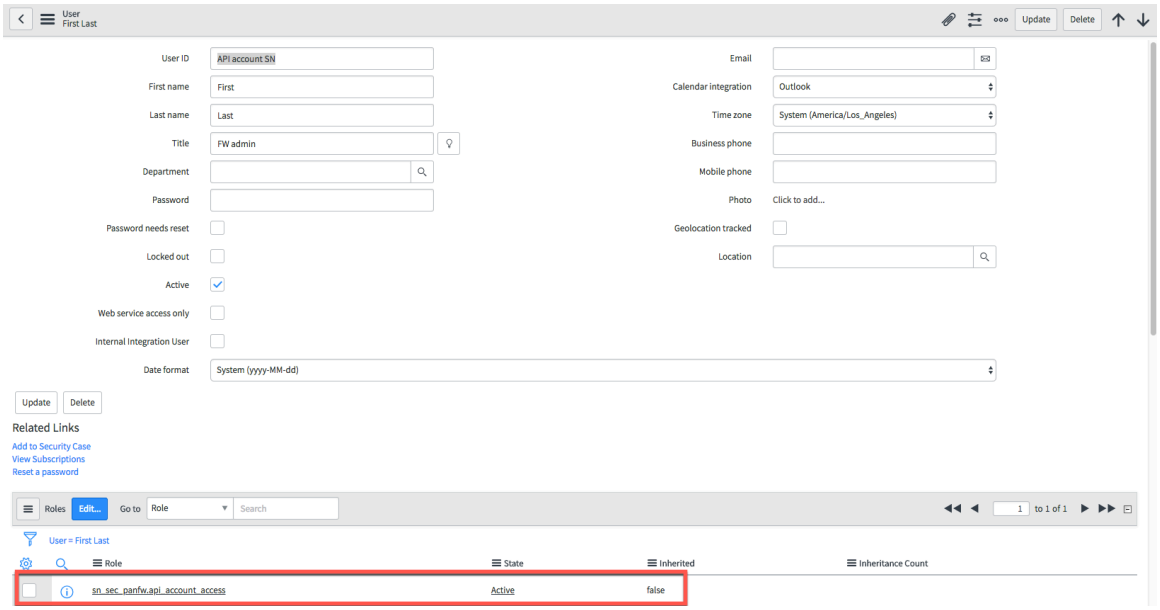


9. In the **Collection** column, select then move `sn_sec_panfw.api_account_access` to the **Roles List**.



10. Click **Save**.
11. Navigate to **Users**, and in the **User** column on the list, click the ID name that you created for the role (`API account SN`).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The user record is displayed. This record verifies that the user account has been assigned. The **State** is active, and the role is not inherited.

Supported External Dynamic Lists for Palo Alto Networks Next-Generation Firewall

The ServiceNow Palo Alto Networks Next-Generation Firewall integration supports External Dynamic Lists (EDLs) that accept IP, URL, and domain observables.

Supported EDLs and observables

An External Dynamic List is a text file that is hosted on an external web server, which for this integration is the ServiceNow AI Platform instance. The Palo Alto Networks Next-Generation Firewall can then import objects — IP addresses, URLs, domains — included in the list and enforce policy. To enforce policy on the EDL entries, the list is referenced in a policy rule or profile.

This integration supports three types of EDLs:

- IP (This includes a single IP Address, as well as CIDR blocks (ranges) of addresses).
- URL
- Domain

The following table lists descriptions of the observables supported by this integration and example formats for each type.

Supported observables and example formats

Observable	Example formats	Description
IP Address	• 95.153.103.54 (IPv4) • (IPv6): 2001:00B8:130F:FE03:0000:09C0:088F:190B	Represents a single, distinct interface address. The integration supports IPv4, IPv6, and CIDR formats. Support for IP address observables includes CIDR (Classless Inter-Domain

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supported observables and example formats (continued)

Observable	Example formats	Description
		Routing) ranges, for example, 95.153.100.0/22. Note: An error message is displayed when you try to attach a single IP address to an EDL that you have already blocked as a part of a CIDR range. For example, the single address 95.153.103.54 is part of the CIDR range represented by 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Wildcards are supported. The ServiceNow AI Platform reformats URL entries to comply with Palo Alto Networks EDL format requirements.
Domain	• www.example.com • example.com • mail.example.com	Wildcards are not supported.

For more information about formatting guidelines and EDLs, see "Formatting Guidelines for an External Dynamic List" in the PAN-OS 10.0 Administrator's Guide on the Palo Alto Networks website.

Create an EDL for Palo Alto Networks Next-Generation Firewall

Create an External Dynamic List (EDL) in your ServiceNow AI Platform instance. Once approved and activated, you can create entries for EDLs from observables determined to be malicious on ServiceNow AI Platform Security Incident Response (SIR) incidents and request approval to block them.

Before you begin

Role required: sn_si.admin

About this task

Create the EDL on your ServiceNow AI Platform instance so that the firewall can import objects — IP addresses, URLs, domains — included in the list and enforce policy. To enforce policy on the EDL entries, the list is referenced in a policy rule or profile.

The figures in the following section are shown with **Tabbed forms** cleared in System Settings. For more information about selecting and clearing tabbed forms, see the "Display tabbed forms" section in Configuring the form layout.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. After the application installation is complete, navigate to **Integrations** > **Integration Configurations**.
2. Locate the Palo Alto Networks Next-Generation Firewall tile and click **Configure**.



3. Click **Create new EDL List**.



4. On the form, fill in the fields.

Palo Alto Networks Firewall External Dynamic List form

Field	Description
Name	Palo Alto Networks Firewall Dynamic List name. Include the observable type (URL, IP, domain) in this field so the security analyst can easily recognize the intention of the EDL by its name. The name should also clearly indicate what firewall policy these EDL objects are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

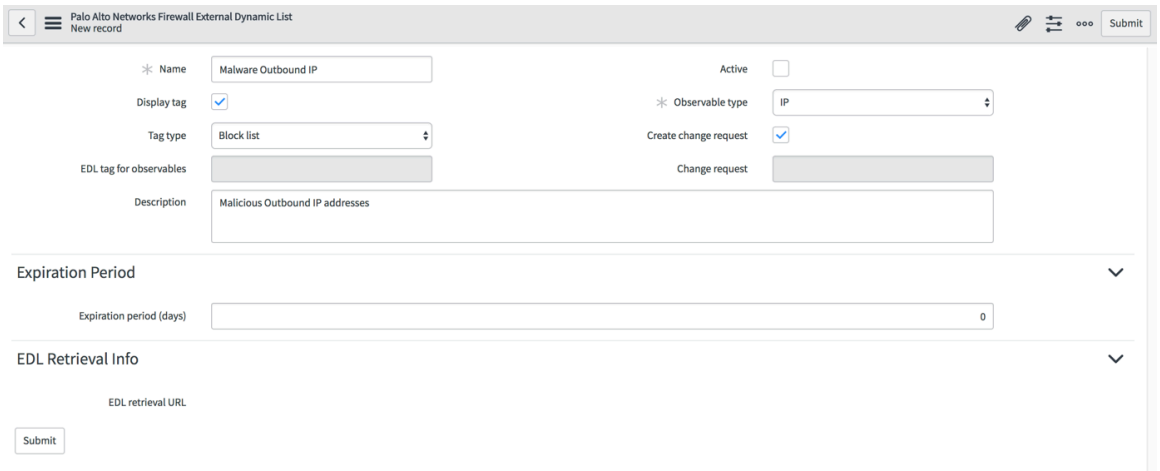
Field	Description
	mapped to. Some examples of EDL names are, Outbound Malware IP, or Outbound Phishing URL.
Active	This check box is cleared by default to indicate that the EDL is inactive. When inactive, the EDL is unable to receive additional entries. When the check box is selected, the EDL is activated and available for EDL entries.
Display tag	Check box is selected by default to automatically tag the observable and the associated security incident record if the observable is blocked on an EDL. When selected, the Tag type and EDL tag for observables fields are available on the form. **Note:** A tag name is created by default from the value you enter in the **Name** field with an EDL- prefix, for example, EDL-Malware OutBound IP. You can change the tag name and color. See: (Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall. The tag name is displayed in the EDL tag for observables field once the EDL is saved. When the check box is cleared, no tag is created, and the Tag type and EDL tag for observables fields are not available on the form.
Observable type	Select an observable type this EDL accepts from the choice list: IP (including CIDR), URL, or domain.
Tag type	Tags that are available from the choice list. A Block list is a list of observables that you want the Palo Alto Networks Next-Generation Firewall to block. An Allow list is a list of observables you want the Palo Alto Networks Next-Generation Firewall to allow. By default, the Block list tag color is black, and the Allow list tag color is gray. You can change the color. See: (Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

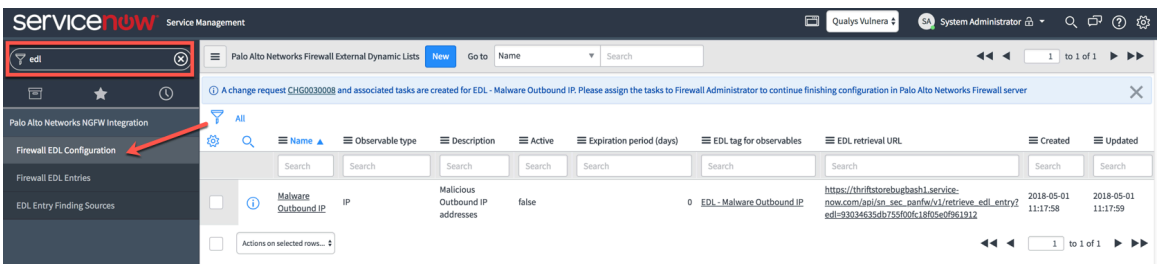
Field	Description
Create change request	This check box is selected by default to automatically create a change request and change tasks in your ServiceNow AI Platform instance, which are attached to the EDL record. The change request is used to configure the EDL list retrieval URL in the Palo Alto Networks Next-Generation Firewall server. This option is recommended if your firewall administrator is also using the ServiceNow AI Platform for firewall policy or rule changes. If you create a request, once it is closed, the EDL list is automatically activated. Clear the check box to manually activate the EDL after receiving notice via email from the firewall administrator that the configuration on Palo Alto Networks is completed. When the check box for Create change request is cleared, the Change request field is unavailable.
EDL tag for observables	This field is displayed only if the Display tag check box is selected. Field is automatically populated after the EDL is saved with a default value from the Name field. For more information on changing the default tag name and color, see (Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall
Change request	When the Create change request check box is selected, the change request number is displayed on the ServiceNow AI Platform instance once the EDL is saved. When the check box for Create change request is cleared, this field is not displayed.
Description	Description of the Palo Alto Networks Firewall Dynamic List. The name generally contains the types of sites and observables you would expect to be on this EDL, and you can use this field for more details.
Expiration period (days)	Expiration period of the EDL. 0 (the default) indicates that the EDL entry never expires. If you change this value, this entry is active for the number of days you enter. You can

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

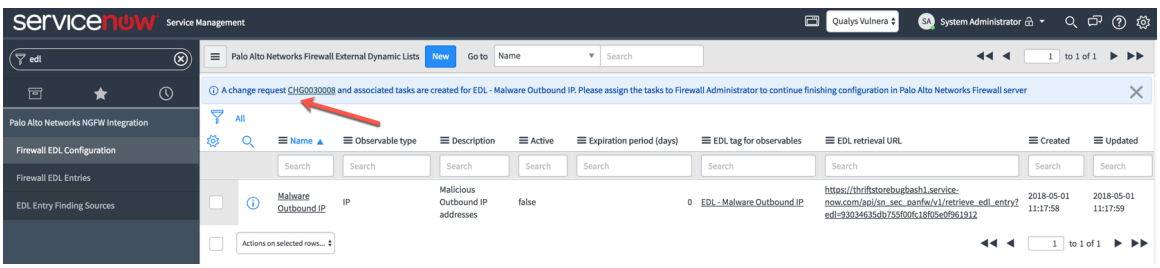
Field	Description
	enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the EDL will expire at 2:01 PM on May 31. All entries in this EDL then inherit this value by default unless you override the value on individual entry basis.



5. Click **Submit**.
6. If the Palo Alto Networks Firewall External Dynamic Lists list is not displayed, navigate to **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration** and click **Firewall EDL Configuration**.



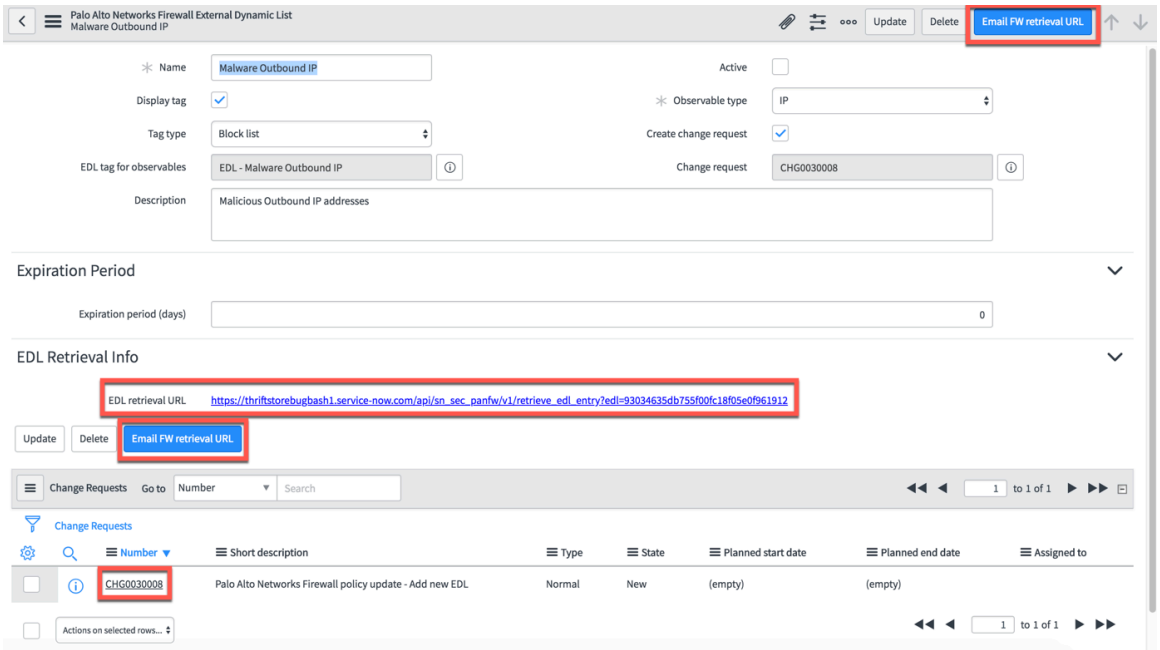
The new EDL is displayed. The EDL status is still inactive (`false`), which means the EDL is not available to accept entries. If **Create change request** was configured, a message is displayed indicating a change request and tasks have been created in your ServiceNow AI Platform instance.



7. In the **Name** column, click an item to open the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The EDL record is displayed. This example shows a Malware Outbound IP EDL. The following fields, options, and links are displayed on the new record after submission and described in the following table.



Retrieval URL and change request links on EDL record

Option	Description
Email FW retrieval URL	Emails a notice that the EDL link is available for configuration to the Palo Alto Networks firewall administrator.
EDL retrieval URL	This URL is placed in the **Source** field in the External Dynamic Lists authentication dialog box on the **Create List** tab on the Palo Alto Networks website. The URL link the Palo Alto Networks firewall administrator uses for configuration in the Palo Alto Networks firewall is automatically generated and displayed. **Note:** If you have your System Settings set to **Tabbed forms**, this link is displayed on the **EDL Retrieval Info** tab at the bottom of the record.
ServiceNow AI Platform change request	A link to the change request record is displayed in the Change Requests section when configured, and the request number is displayed in the Change request field.
Update	Modify data and update the editable fields.
Delete	Delete the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Create and add more EDLs as required.
   The EDLs are displayed on the Palo Alto Networks External Dynamic Lists list.

What to do next
Activate an EDL manually, or with a ServiceNow AI Platform change request.

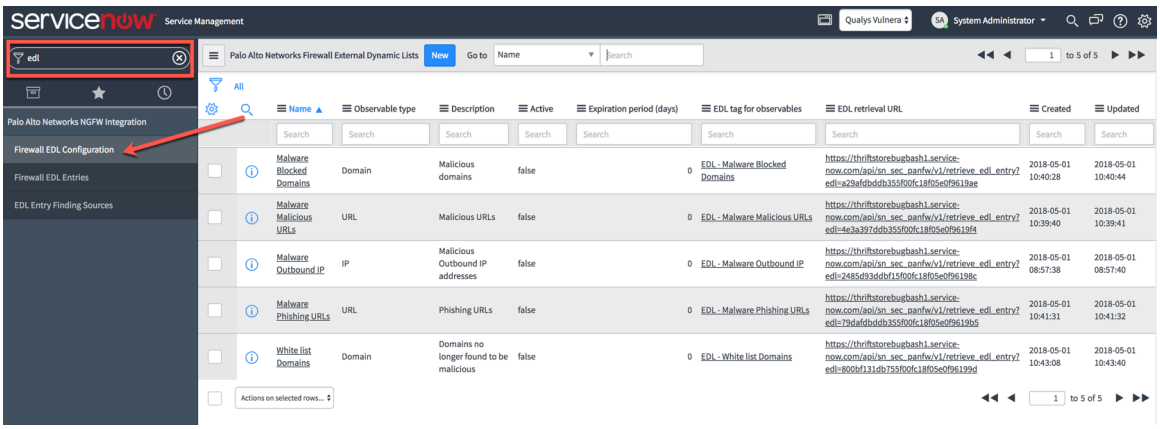
Activate an EDL for Palo Alto Networks Next-Generation Firewall

After the External Dynamic List (EDL) has been created in your ServiceNow AI Platform® and the URL is available, the Palo Alto Networks firewall administrator configures the EDL in the Palo Alto Networks Next-Generation Firewall. The retrieval URL is used by the Palo Alto Networks firewall administrator to configure the EDL in the Palo Alto Networks Next-Generation Firewall server. Before it can accept EDL entries, the EDL must be configured in Palo Alto Networks and activated in the ServiceNow AI Platform®.

Before you begin
Role required: sn_si.admin

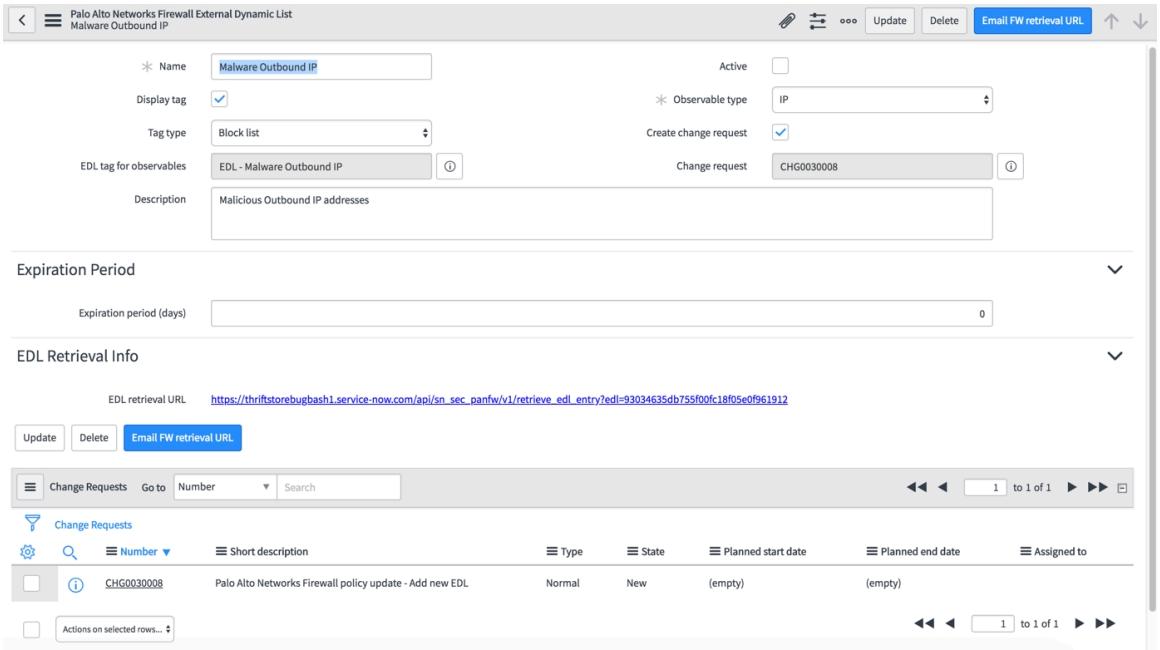
About this task
After the EDL is configured, as the security incident administrator, you can activate the EDL manually, or, the EDL is automatically activated upon completion of a ServiceNow AI Platform® Change Request. The EDL must be approved and moved from the inactive state to the active state before it can accept EDL entries.

Procedure
1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration** and select the **Firewall EDL Configuration** module.



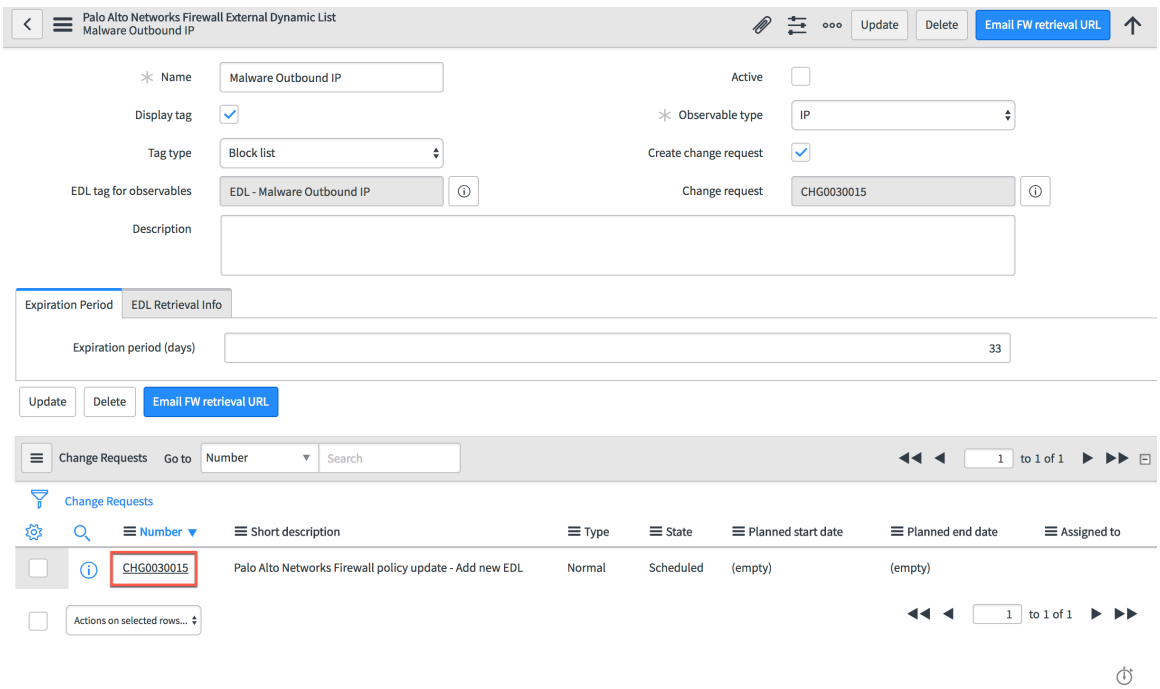
2. In the Palo Alto Networks Firewall Dynamic Lists list that is displayed, select your new EDL in the Name column.
3. On the record that is displayed, note the **Email FW retrieval URL** buttons, the active EDL Retrieval URL link, and, if configured, the ServiceNow AI Platform® change request in the Change Requests section.
   Make sure that the **Active** check box is cleared.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: With **Tabbed forms** cleared in your system settings, the EDL Retrieval URL appears in **EDL Retrieval Info** section as shown in the previous figure.

The following figure shows the **EDL Retrieval Info** displayed as a tab with **Tabbed forms** selected in your system settings. Click the **EDL Retrieval Info** tab to display the retrieval URL. The link to the change request (**CH0030015**) is also displayed.



4. To complete the configuration and move the EDL from inactive to active, you must choose one of the following options to notify the firewall administrator that the retrieval URL is available.

Option	Description
Click Email FW retrieval URL.	Email EDL Retrieval URL directly to the firewall administrator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	This option permits the firewall administrator to finish the configuration on the Palo Alto Networks platform. Choose this option if the firewall administrator is not using the Service Now AI Platform®. **Note:** The security incident adminis trator manually activates the EDL in the ServiceNow AI Platform® after receiving notice that the Palo Alto Networks Next-Generation Firewall configuration is com pleted. See: Activate an EDL manually for Palo Alto Networks Next-Generation Firewall.
Complete the ServiceNow AI Platform® change request and assign the configura tion tasks to the firewall administrator.	This option is available only if the firewall ad ministrator for Palo Alto Networks is also us ing the ServiceNow AI Platform®, and the Ser viceNow AI Platform® change management and approval processes are configured. **Note:** Users with the sn_si.admin role can approve the ServiceNow AI Plat form® change request. Once the con figuration tasks are completed and the change request has been closed, the EDL is activated automatically. See: Acti vate an EDL for Palo Alto Networks Next-Generation Firewall with a change re quest.

After you notify the firewall administrator that the retrieval URL is available and you confirm the EDL has been configured in Palo Alto Networks, as the security incident administrator, your next step is to activate the EDL. You either activate the EDL manually, or, if configured, use the ServiceNow AI Platform change request form to activate the EDL.

Related topics

Configure an EDL in Palo Alto Networks Next-Generation Firewall

Activate an EDL manually for Palo Alto Networks Next-Generation Firewall

If the Palo Alto Networks firewall administrator is not using the ServiceNow AI Platform, and you are directly notified that the Palo Alto Networks Next-Generation Firewall is configured, you can activate the External Dynamic List (EDL) manually.

Before you begin

In Palo Alto Networks, assign an EDL object, policy, and the source URL to the EDL you created. For more information about configuring the EDL to the Palo Alto Networks Next-Generation Firewall in Palo Alto Networks, see Configure an EDL in Palo Alto Networks Next-Generation Firewall.

Role required: sn_si.admin

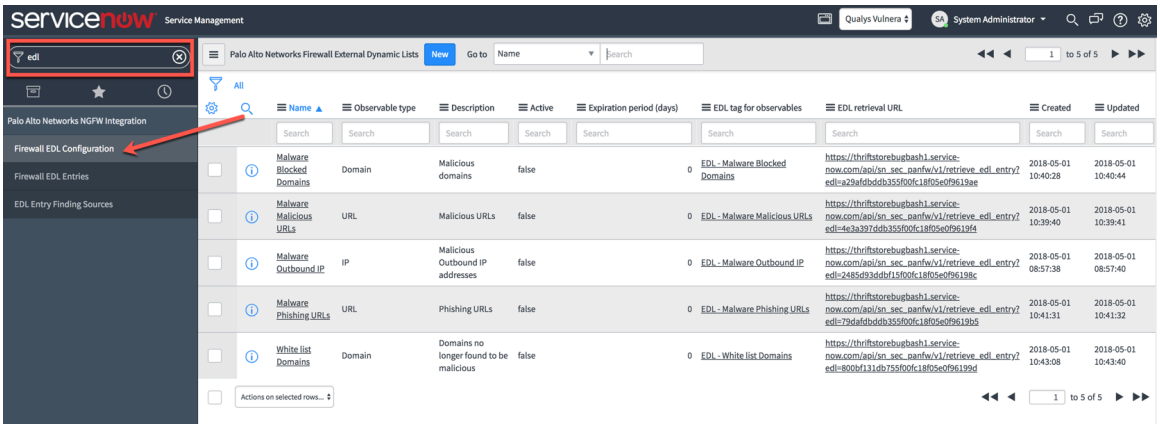
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

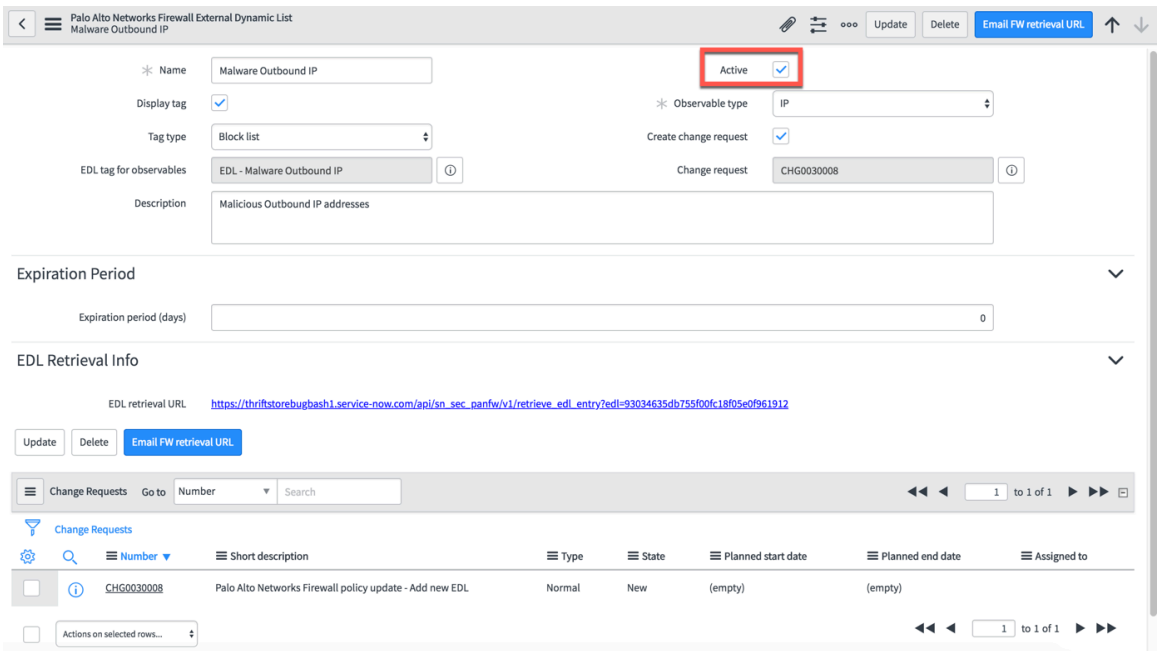
As the ServiceNow AI Platform security incident administrator, you are notified by the Palo Alto Networks firewall administrator when the EDL configuration is complete in the Palo Alto Networks Next-Generation Firewall.

Procedure

1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration**.



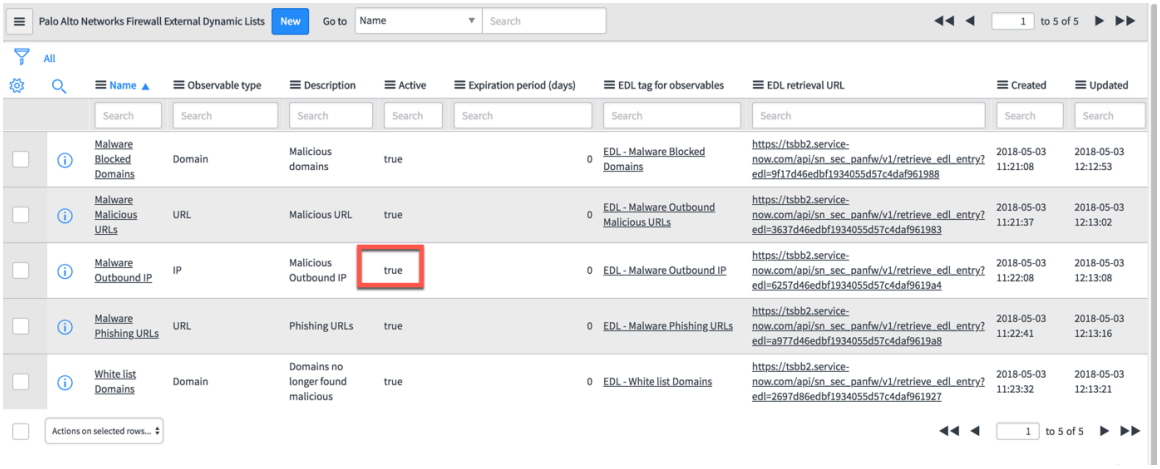
2. Select the **Firewall EDL Configuration** module.
3. In the Palo Alto Networks Firewall External Dynamic Lists list, click an item in the **Name** column to open it.
4. On the record that opens, select the **Active** check box.



5. Click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the **Active** column of the Palo Alto Networks Firewall External Dynamic Lists list, `true` is displayed for the state of the EDL.



Result
The EDL is activated and ready to receive EDL entries

What to do next
Submit EDL entries from a security incident or from the blocklist.

Configure an EDL in Palo Alto Networks Next-Generation Firewall

The Palo Alto Networks firewall administrator configures an EDL to the Palo Alto Networks Next-Generation Firewall once notified the Retrieval URL is available from the ServiceNow AI Platform. Before the EDL can accept EDL entries, it must be configured in Palo Alto Networks, and activated in the ServiceNow AI Platform®.

Before you begin
Role required: Palo Alto Networks firewall administrator

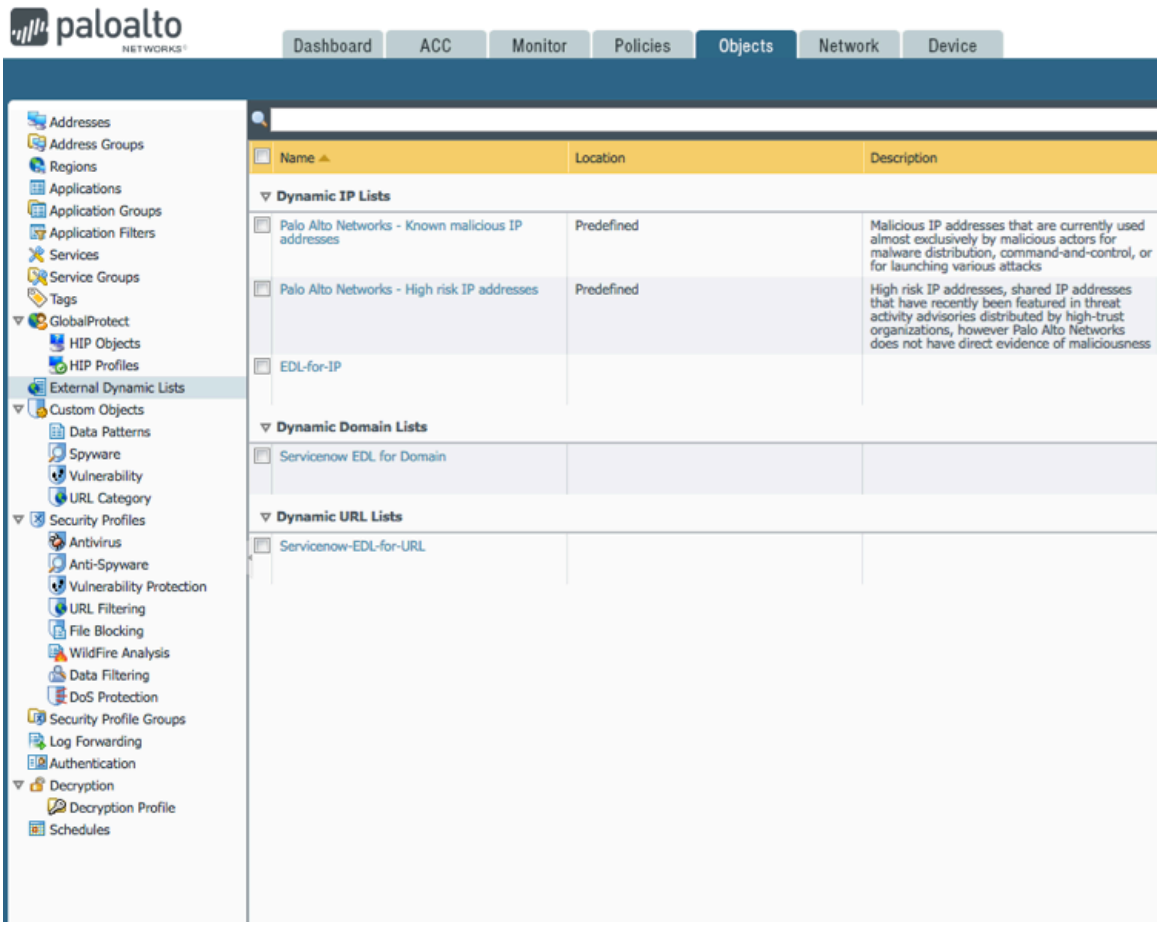
About this task
The Palo Alto Networks Next-Generation Firewall administrator creates an EDL object, and assigns the source (Retrieval) URL and policy to the EDL. These tasks are performed in Palo Alto Networks before the EDL is activated in the ServiceNow AI Platform.

The images in the following section are used by permission and are PRIVILEGED and PROPRIETARY.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

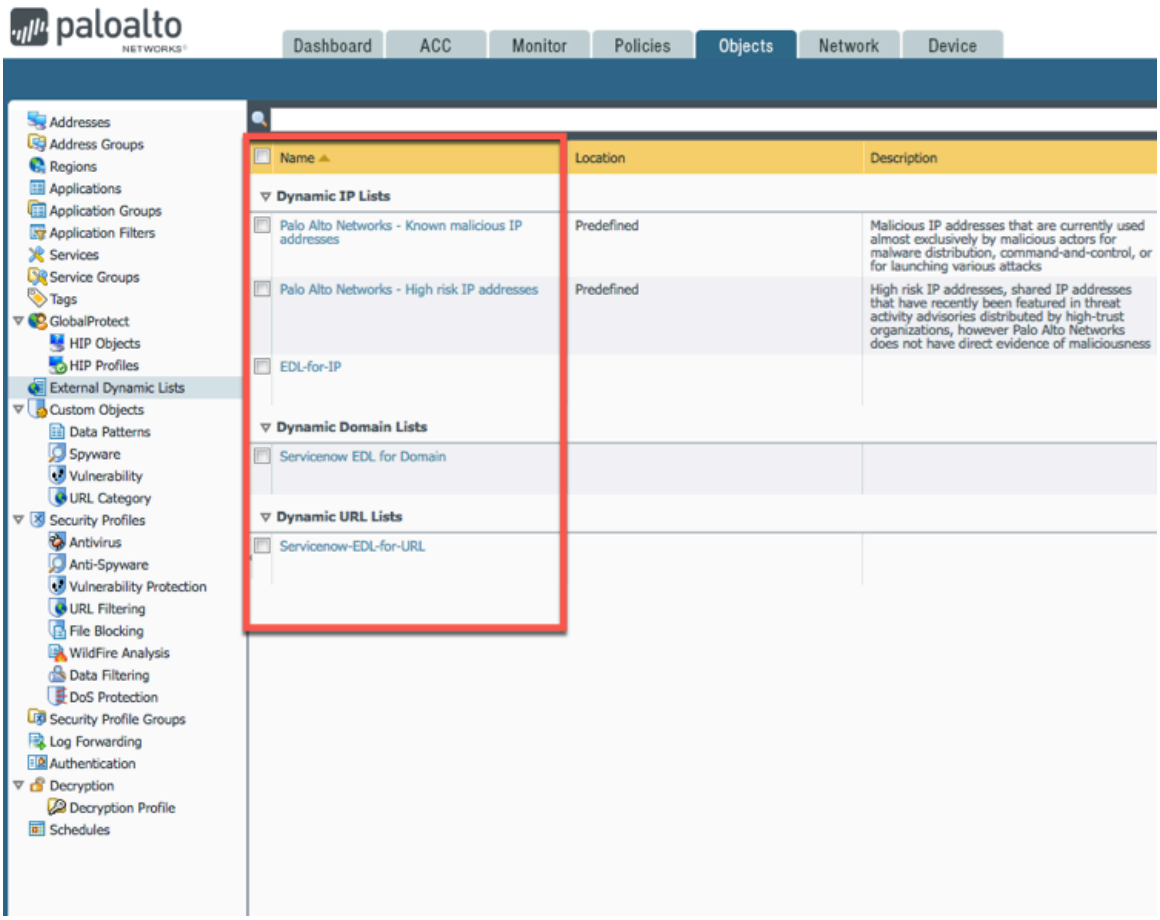
Procedure

1. If you have not configured the EDL to the firewall, navigate to **External Dynamic Lists** > **Objects** in Palo Alto Networks.



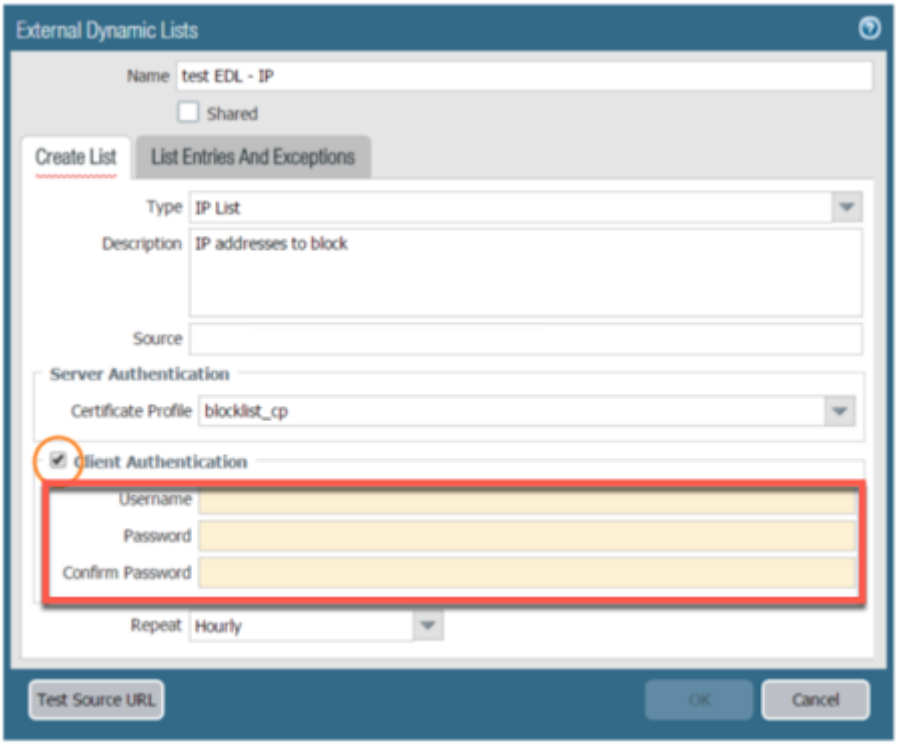
2. In the **Name** column, select the ServiceNow EDL you want to configure from the list, for example, **ServiceNow EDL for URL**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

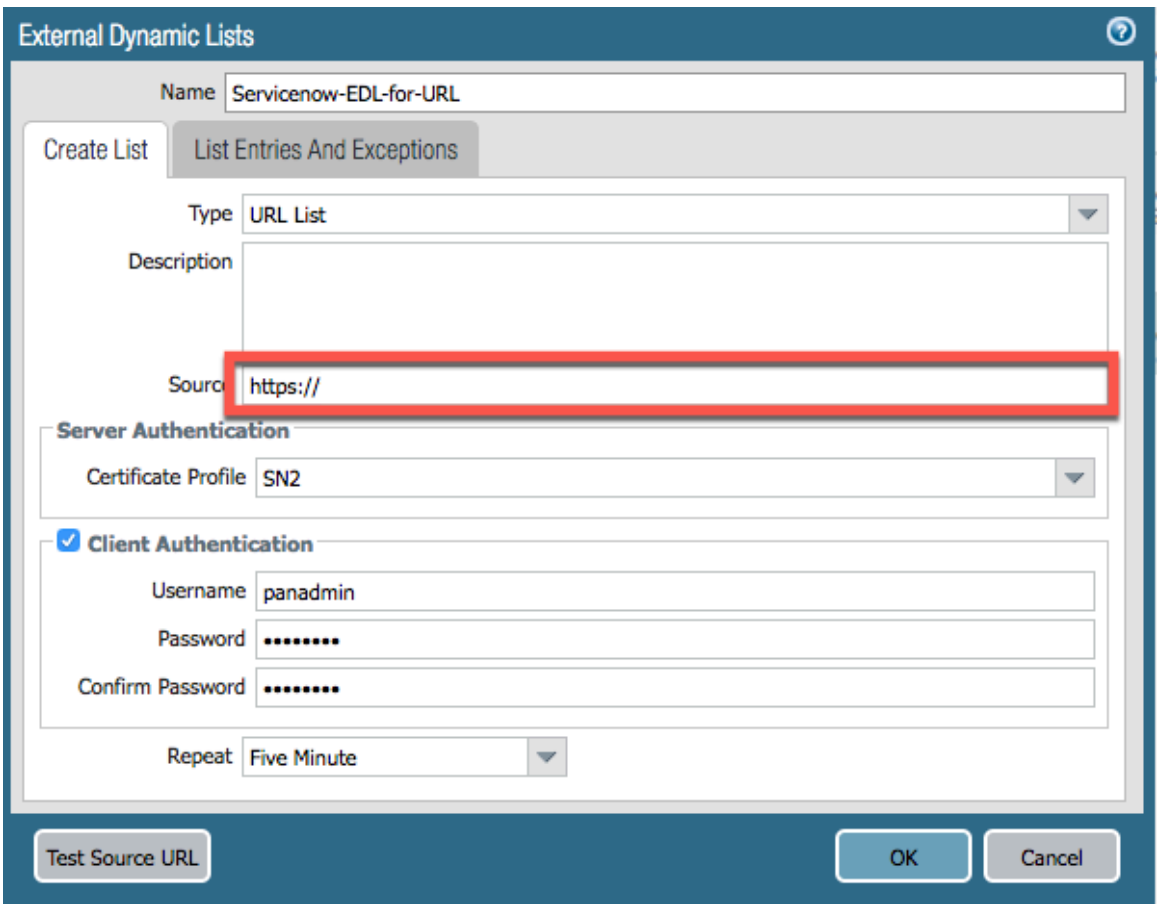


3. In the External Dynamic Lists dialog box, enter the Username and Password to authenticate with the ServiceNow AI Platform®.
   These credentials are the Username and Password you created for the API account role (sn_sec_panfw.api_account_access) in your ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In the Source field, enter the URL that was generated on the EDL list in your ServiceNow instance.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select a Certificate Profile from the choice list, SN2, for example.
6. Click OK.

Activate an EDL for Palo Alto Networks Next-Generation Firewall with a change request

If configured, the ServiceNow change request form is used to activate the External Dynamic List (EDL). This option is recommended if your firewall administrator is also using the ServiceNow AI Platform for firewall policy or rule changes. The EDL is activated automatically and ready to receive EDL entries upon closure of the ServiceNow AI Platform change request.

Before you begin

Note: The figures in the following section are shown with **Tabbed forms** selected in System Settings. For more information about selecting and clearing tabbed forms, see the section titled Display tabbed forms in Configuring the form layout on the ServiceNow Product Documentation website.

Role required: sn_si.admin for approving the change request and change tasks

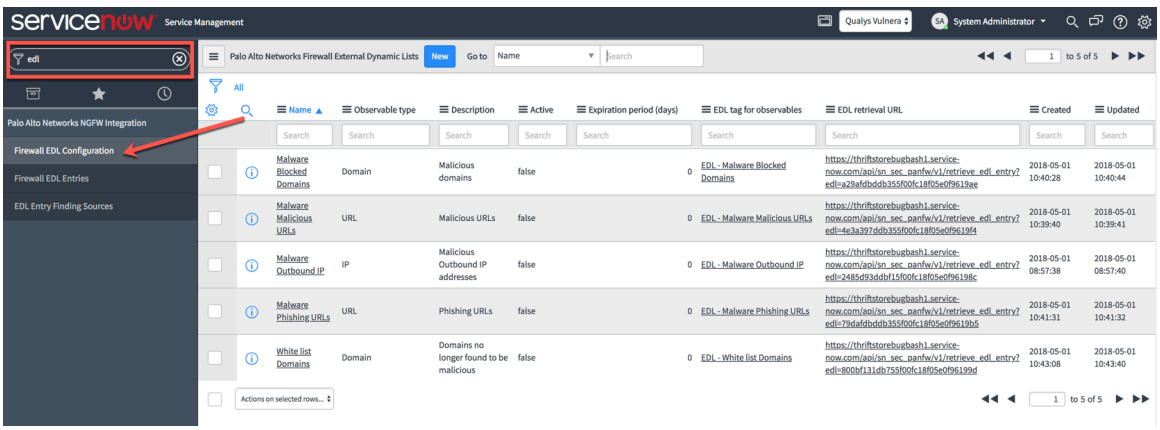
Palo Alto Networks firewall administrator for completing configuration tasks in Palo Alto Networks

About this task

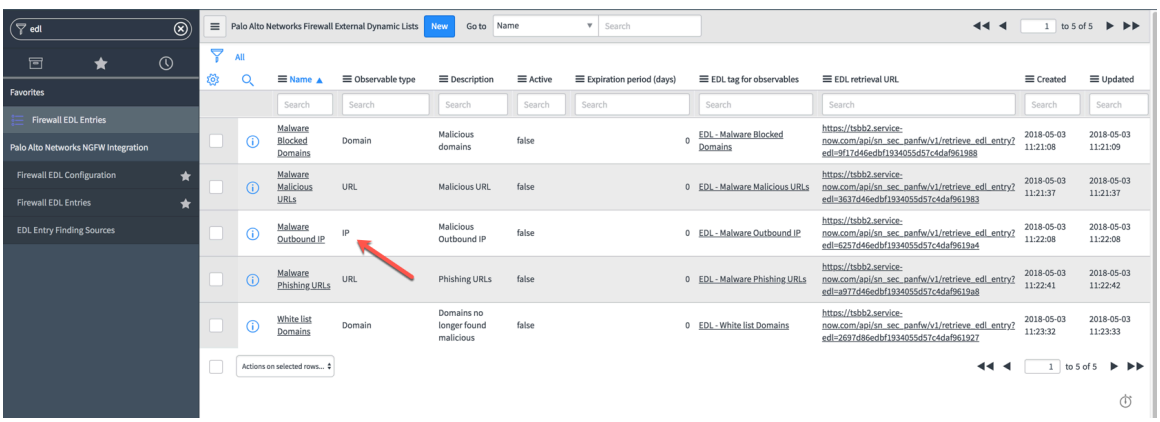
If configured, monitor your ServiceNow AI Platform change request and assign any tasks that are required to configure the Palo Alto Networks Next-Generation Firewall. After these tasks are completed, close the ServiceNow AI Platform change request to activate the EDL automatically.

Procedure

1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration**.

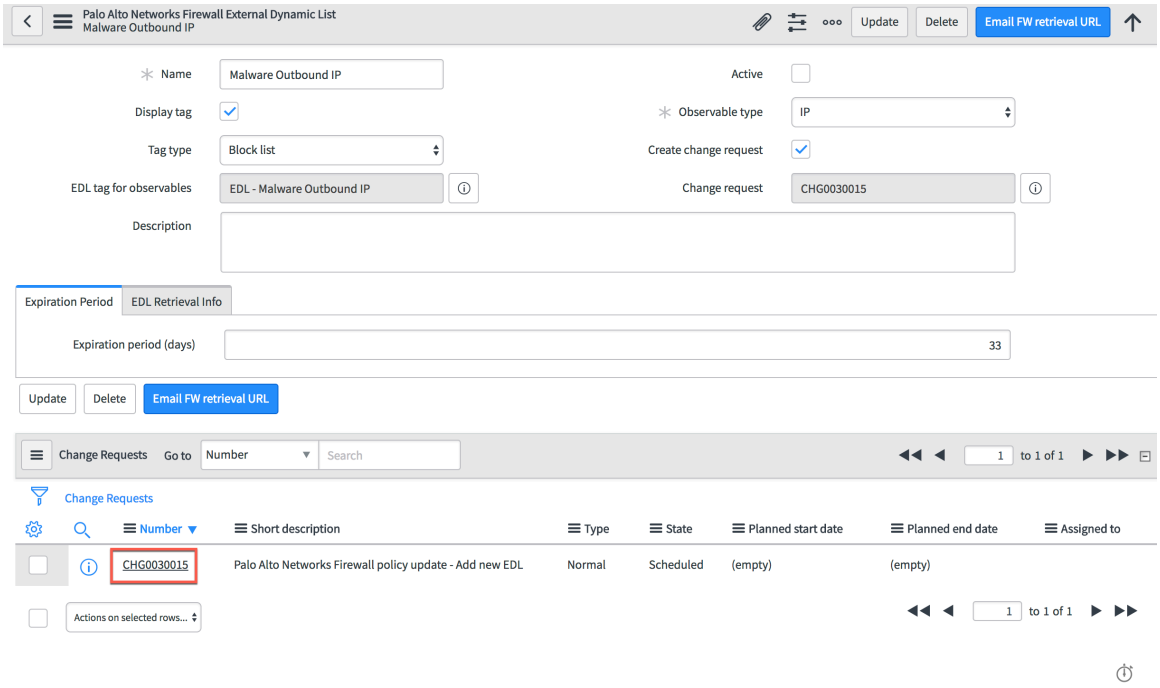


2. Select the EDL module and click an EDL in the **Name** column.

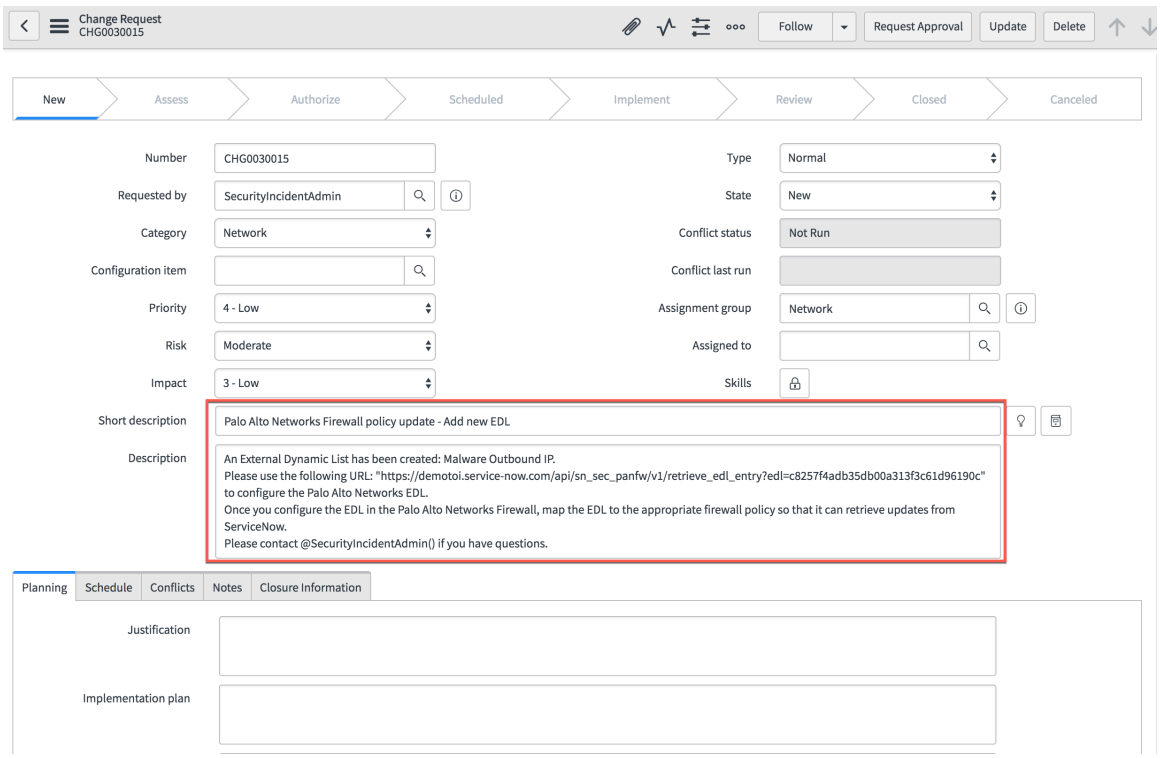


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In the open EDL record, click the change request number in the Change Requests related list.

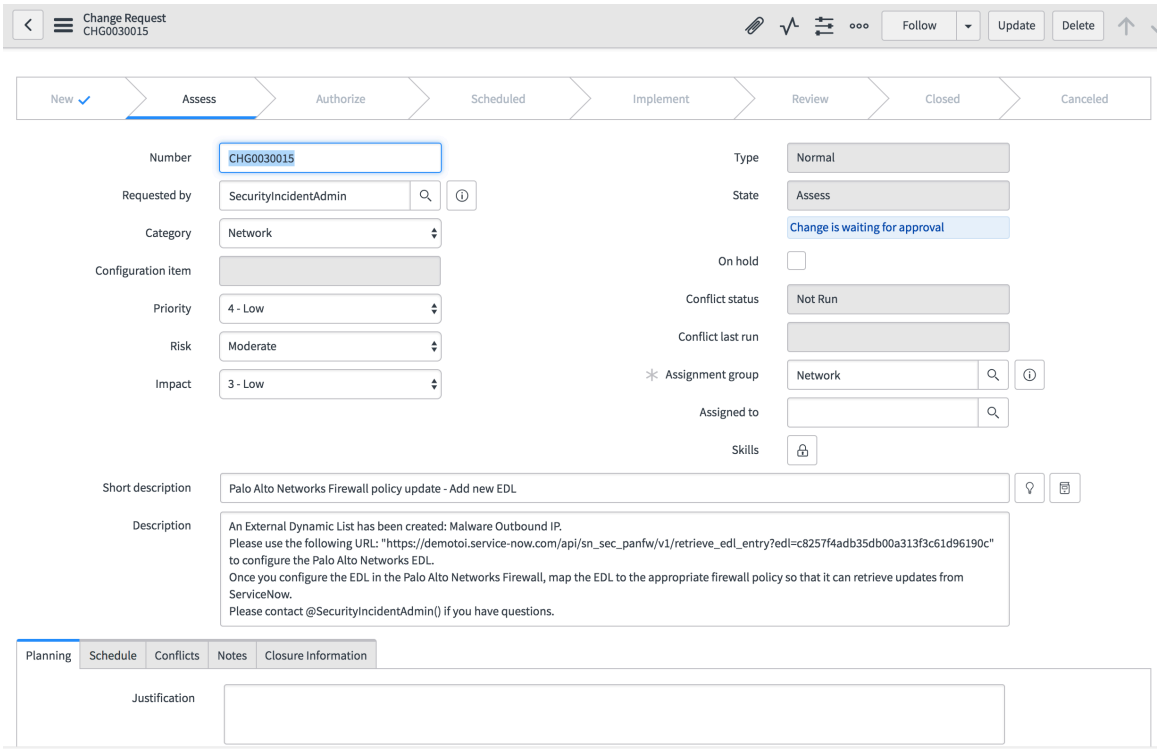


The change request record is displayed. The **Description** field lists the retrieval URL used to configure the Palo Alto Networks EDL. Details about mapping the EDL to the appropriate Palo Alto Networks Next-Generation Firewall policy are also included. In the **Short description** field, a comment indicates that there is a request to add a new EDL.



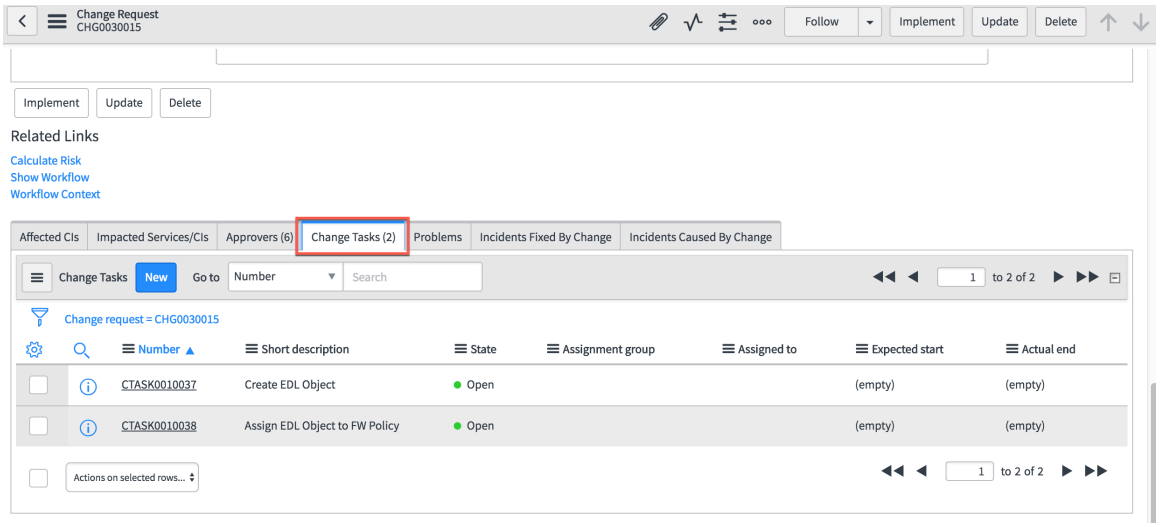
4. In the upper-right corner of the record, click **Request Approval**.
The State changes to Assess, and a message is displayed that the change request is waiting for approval.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



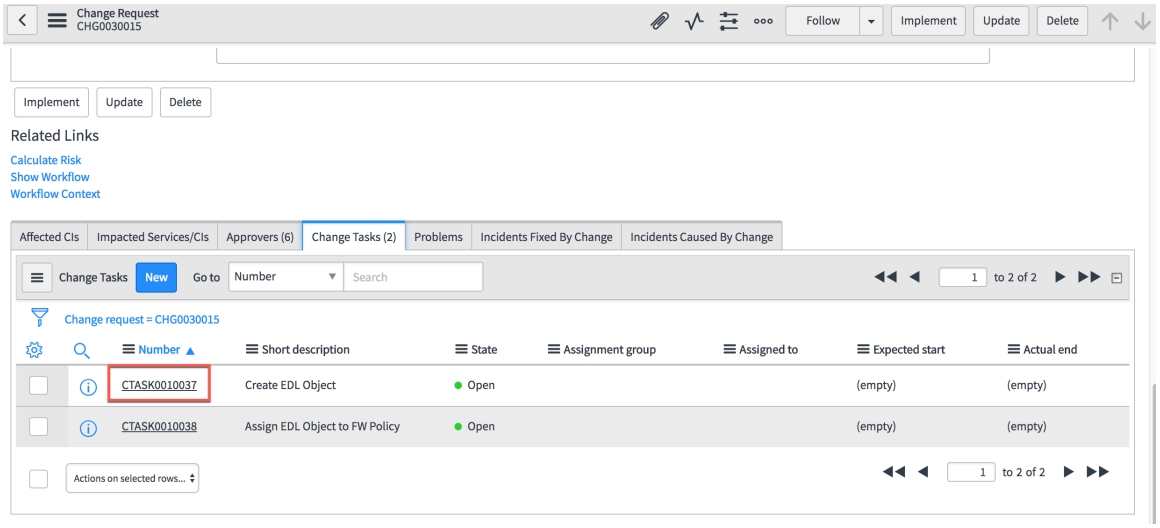
5. To complete the change request and activate the EDL, follow the steps to assign the tasks and close the change request.

a. If not displayed, open the change request and select the **Change Tasks** tab.



b. Click the task associated with creating the EDL object to open it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. On the record that is displayed, assign the task to the Palo Alto Networks firewall administrator, and click **Update**.
The firewall administrator is notified and creates the EDL object in the Palo Alto Networks Next-Generation Firewall.

To create the EDL object, the ServiceNow AI Platform retrieval URL is copied in Palo Alto Networks at **External Dynamic Lists** > **Create Lists** > **Source**.

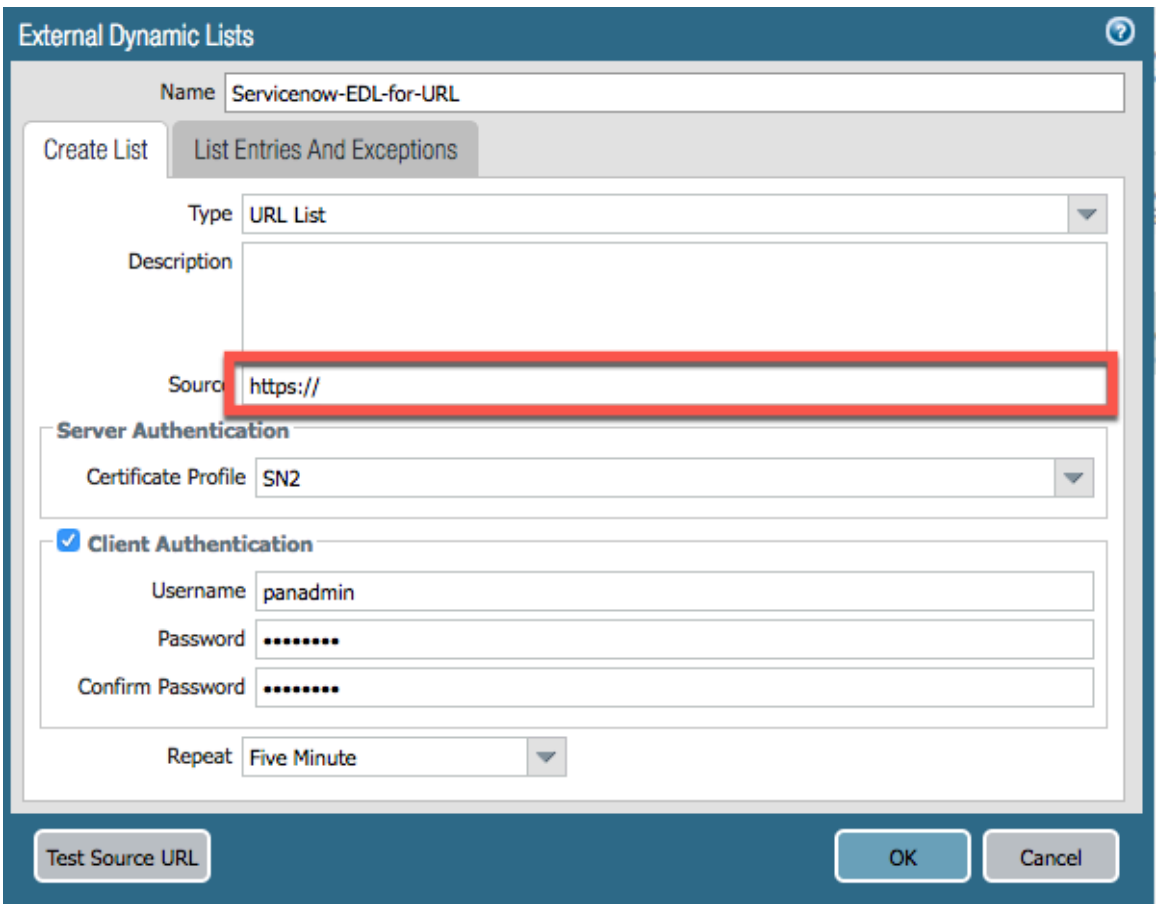


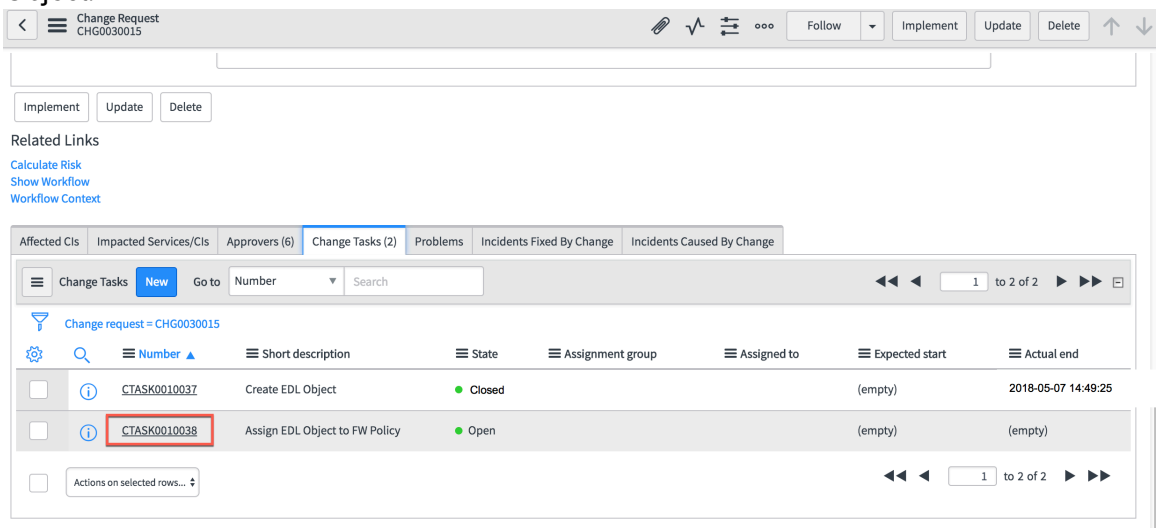
Image is used by permission and is PRIVILEGED and PROPRIETARY.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. After you have verified that the EDL object has been created in Palo Alto Networks, in the ServiceNow AI Platform, navigate to the change request associated with creating the EDL object and click **Close task**.

On the task record for this example, CTASK0010037 was closed for this task.

e. Navigate to the Change Tasks tab and click the task for assigning a firewall policy to the EDL Object.



The status for CTASK0010037 is `Closed`.

f. Open the record and assign the next task.

After the task has been assigned, in Palo Alto Networks, the firewall administrator navigates to the **Policies** tab to assign the policy.

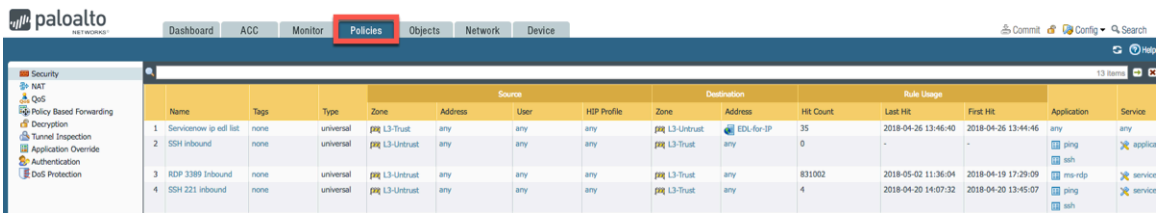


Image is used by permission and is PRIVILEGED and PROPRIETARY.

g. In the **Name** column, locate and click the security policy rule you want to add the EDL to, for example, **ServiceNow ip edl list**.

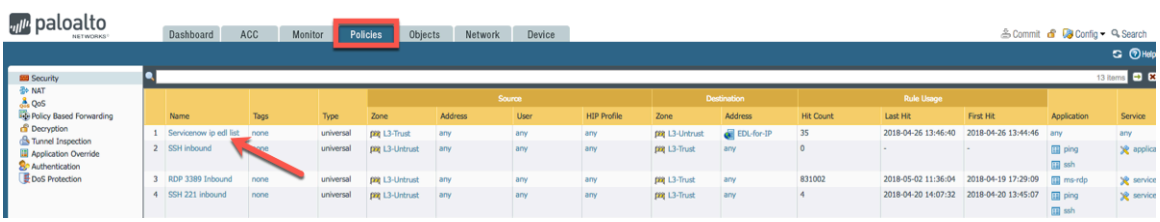


Image is used by permission and is PRIVILEGED and PROPRIETARY.

h. In the Security Policy Rule dialog box, select the **Destination** tab to add an EDL in the **Destination Address** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

i. To view all the available EDLs, click the **Add** icon.

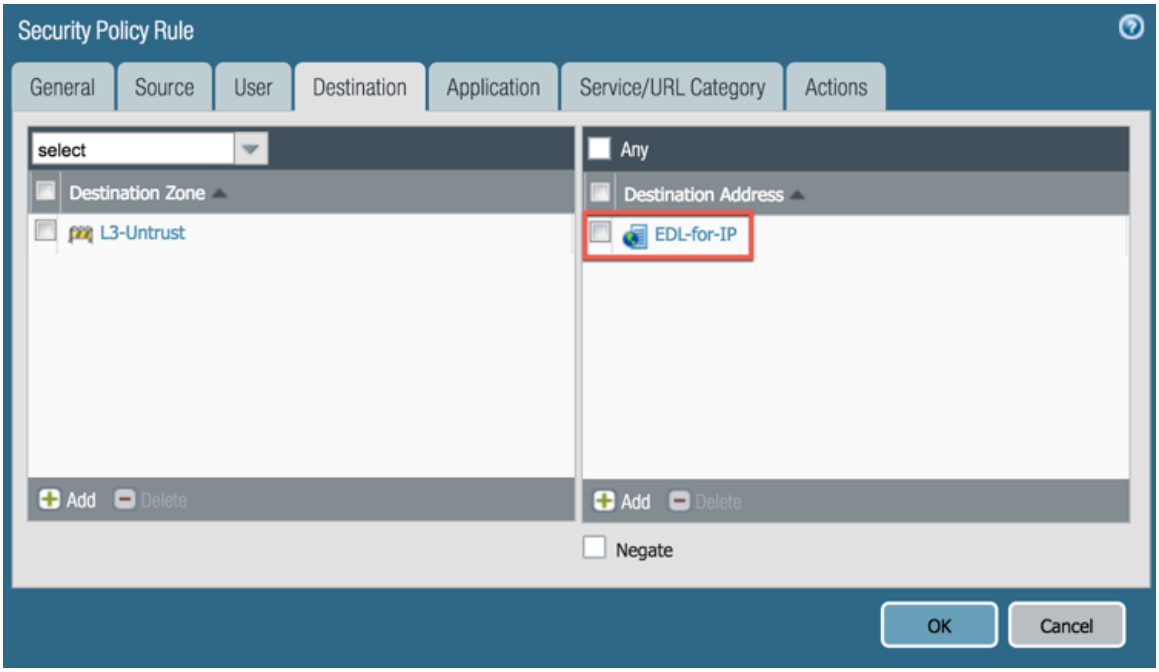


Image is used by permission and is PRIVILEGED and PROPRIETARY.

j. Click **OK**.

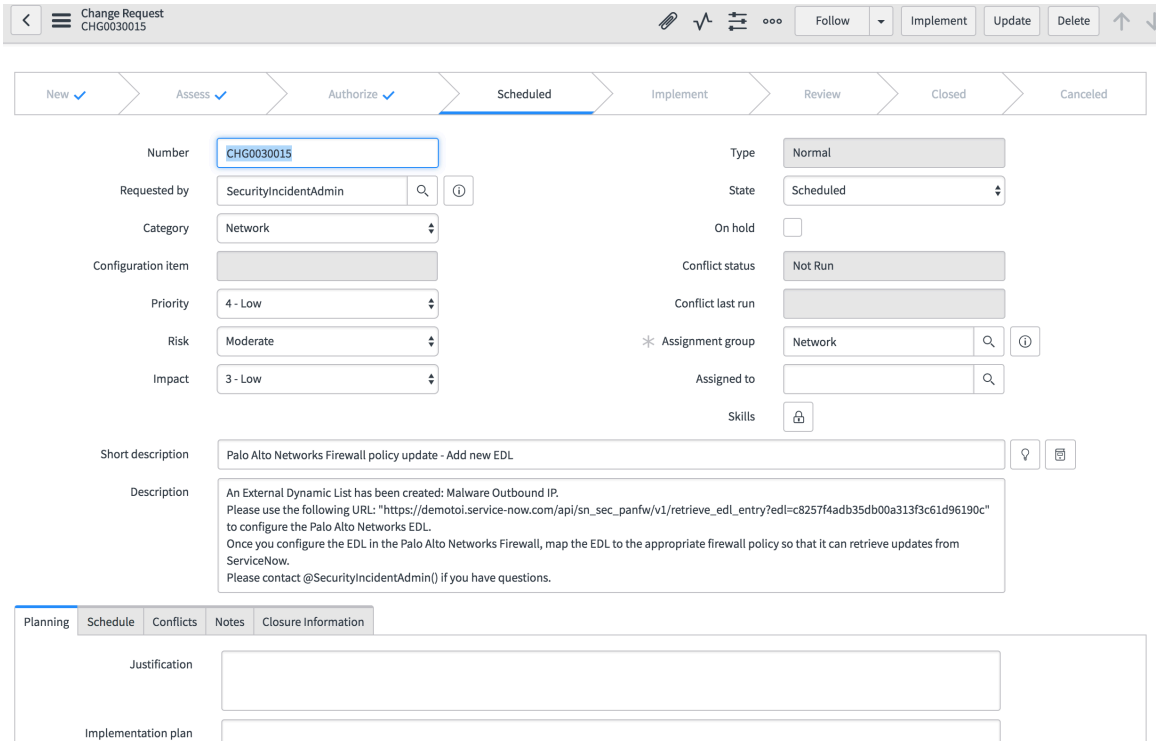
k. After you have verified that the EDL object has been assigned to a security policy, in the ServiceNow AI Platform, navigate to the change request, open the task associated with assigning the EDL object, and click **Close task**.
After both tasks are closed, the change request is ready for approval.

l. On the change request record, click the **Approvers** related list, and select an item in the **State** column to open the request used for creating the EDL.



m. On the open approval request form, click **Approve**.
The change request state moves to Scheduled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



n. Click **Implement**.

o. Click the **Closure Information** related tab and enter notes to close the request.

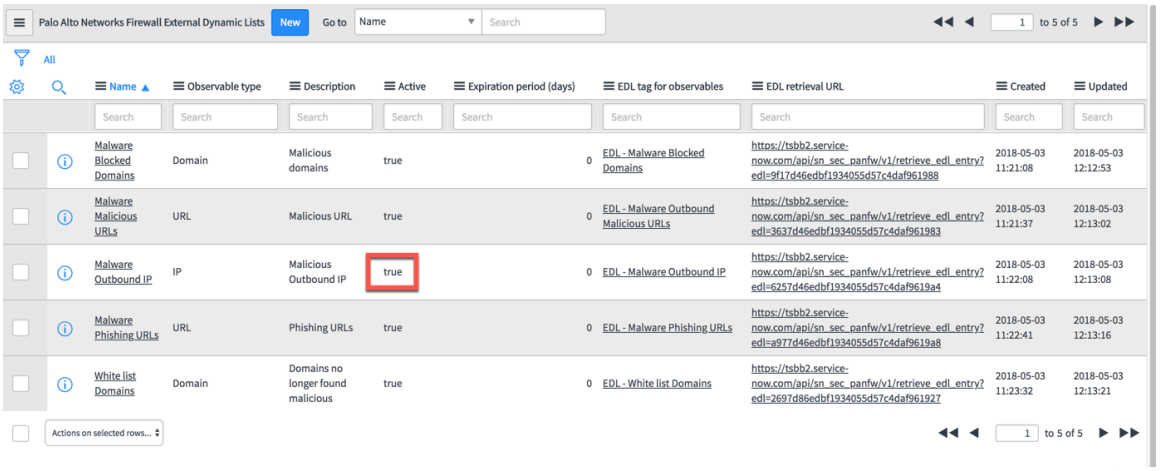
An entry in this field is required to close the change request.



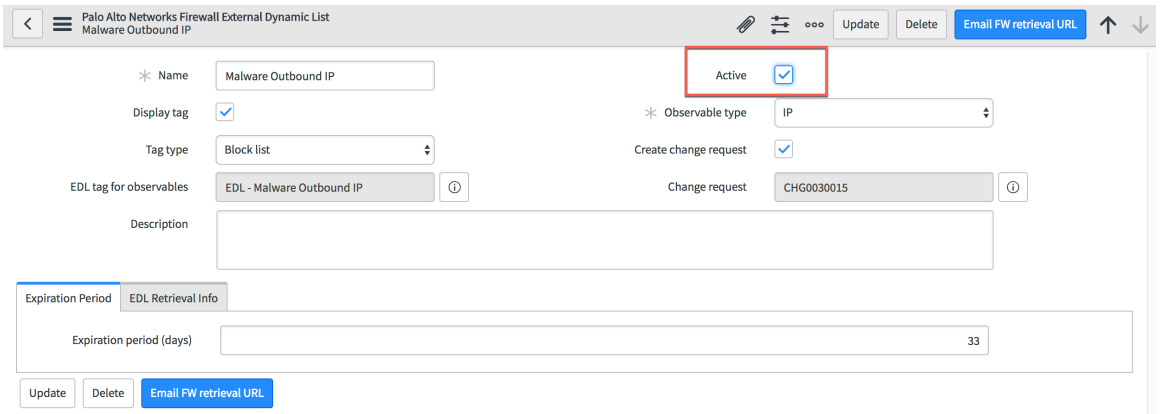
After the change request is closed, the EDL is activated automatically. If you have not verified that the EDL is activated, navigate to **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration**.

In the Active column in the list, note that the status for the EDL is (`true`).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



In the Name column, click the EDL name, and in the open record, note that the **Active** check box is also selected.



The EDL is now ready to accept EDL entries.

What to do next

Submit EDL entries from a security incident or from the blocklist.

Submit EDL entries from a security incident record for Palo Alto Networks Next-Generation Firewall

Observables attached to a security incident record are submitted for approval as External Dynamic List (EDL) entries to EDLs. An approval process for EDL entries is part of the preconfigured workflow. The firewall imports EDL entries — IP addresses, URLs, domains — that are included in EDL lists and enforces policy.

Before you begin

Role required: sn_si.analyst for submitting EDL entries. To approve EDL entries: Approval is assigned to sn_si.admin by default, but this authority can be assigned as required by your organization.

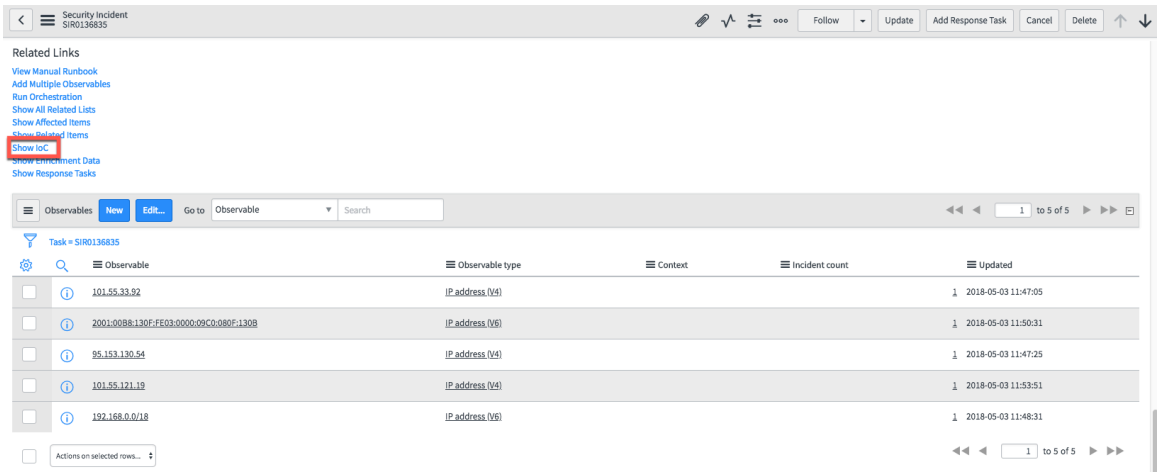
About this task

Users with the sn_si.analyst role submit EDL entries by requesting a block on observables attached to a security incident record. Once submitted, an EDL entry with a status of Pending is generated and sent for approval. The following example shows a block request for a URL observable.

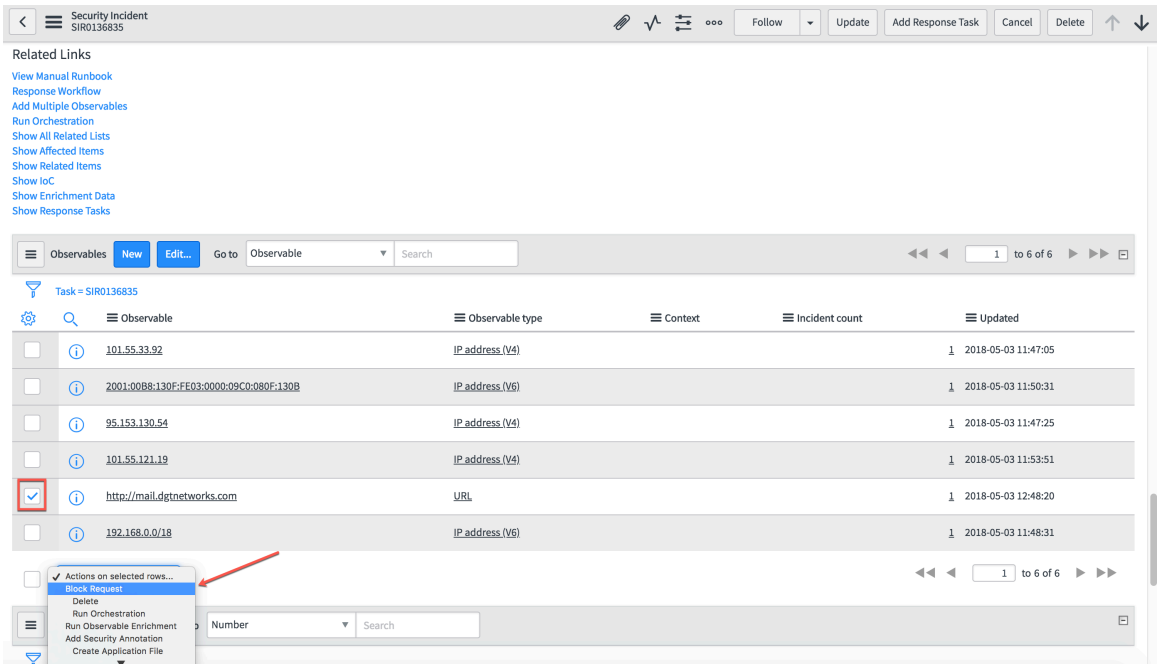
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**, and click a security incident record to open it.
2. Click the **Show IoC** related link.



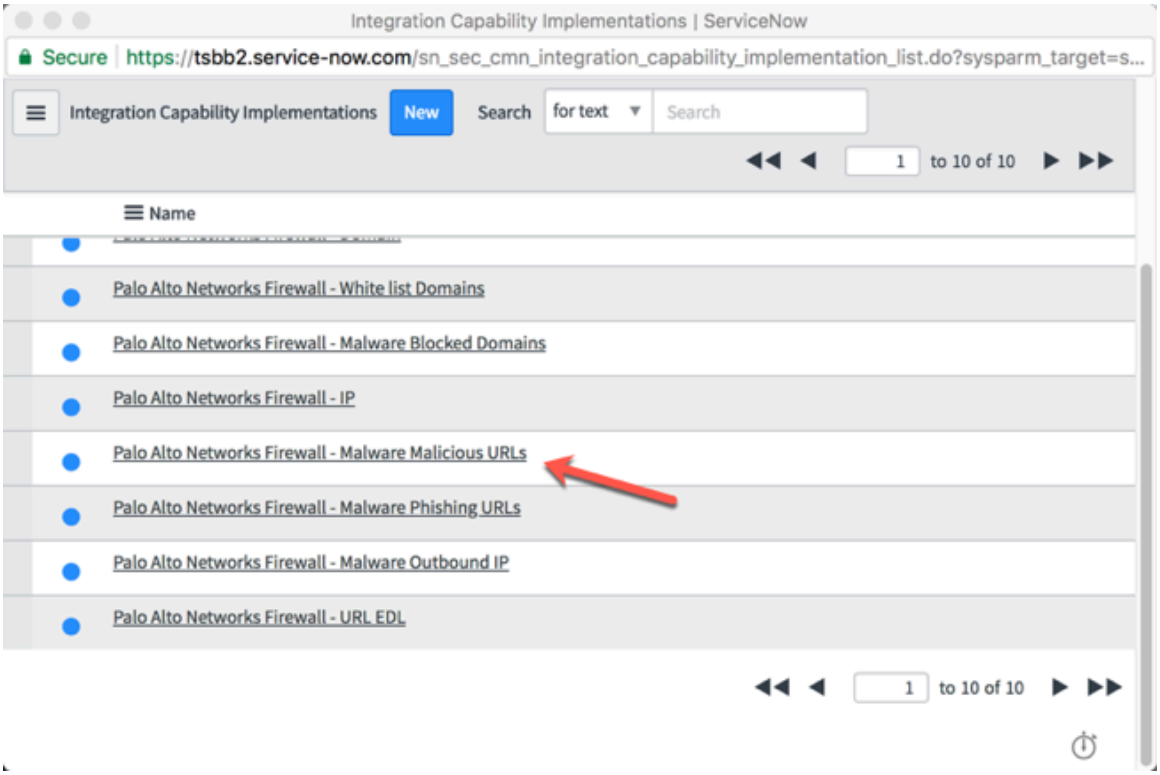
3. In the Observables related list, select the observables you want to block and from the **Actions on selected rows** list, select **Block Request**.



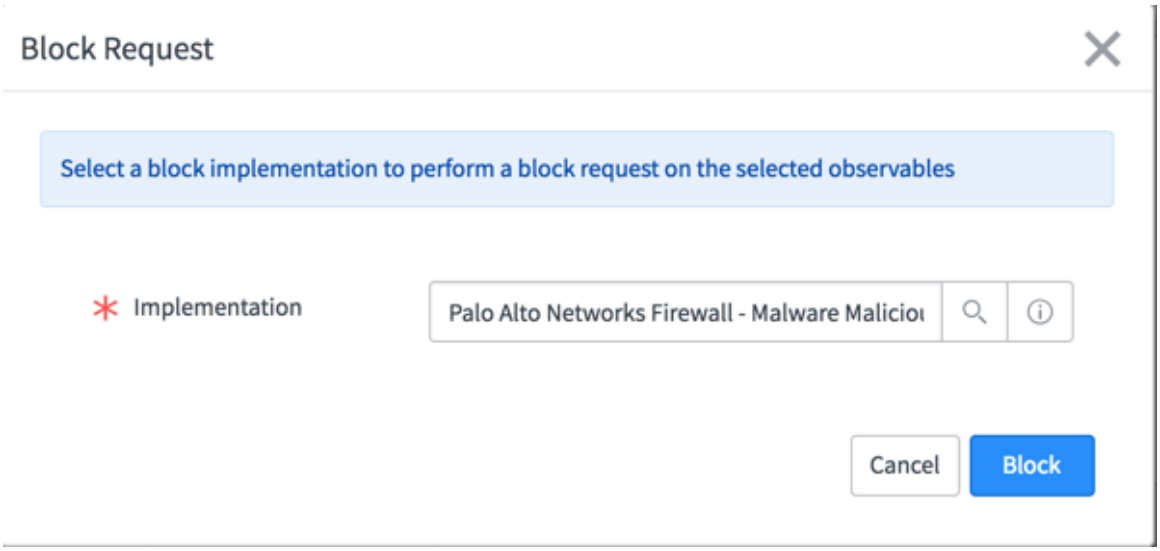
4. In the dialog box that is displayed, click the search icon ( ).
5. From the list that is displayed, select the EDL you want to attach this entry to.

> **Note:** For this example, the entry observable type (URL) should match the EDL observable type (URL).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

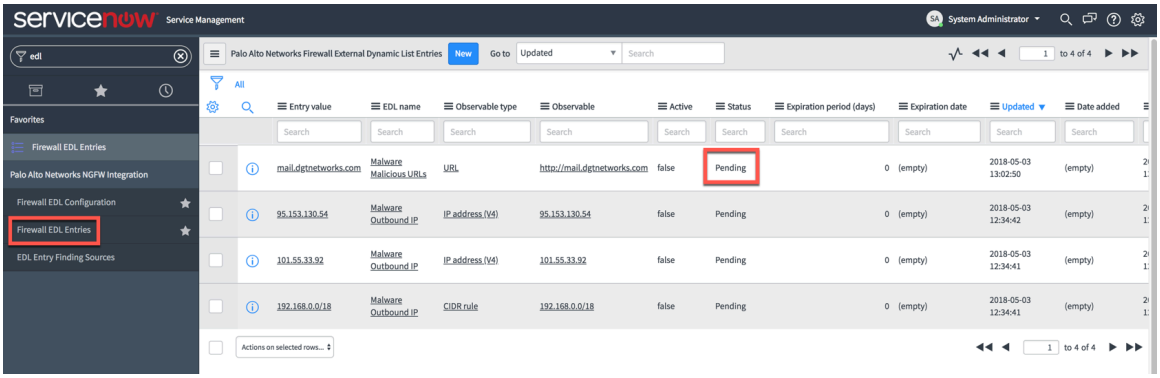


6. In the Block Request dialog box with the EDL name displayed in the **Implementation** field, click **Block**.



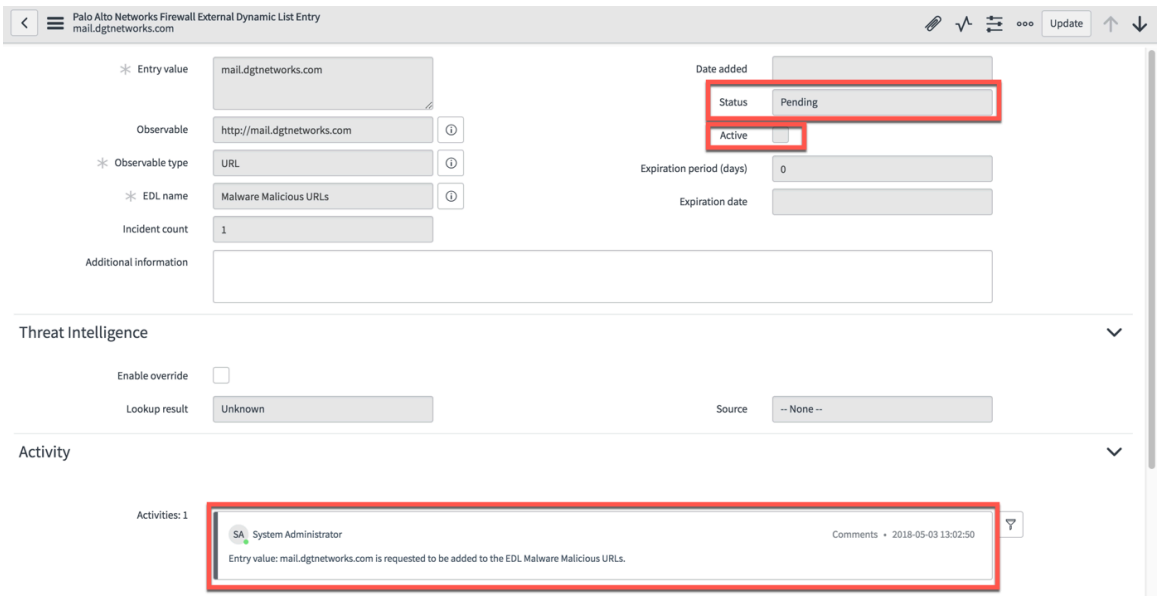
7. Navigate to **Palo Alto Networks NGFW Integration** > **Firewall EDL Entries** and click **Firewall EDL Entries**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. In the Palo Alto Networks Firewall External Dynamic List Entries list, click your observable in the **Entry value** column to open the record.

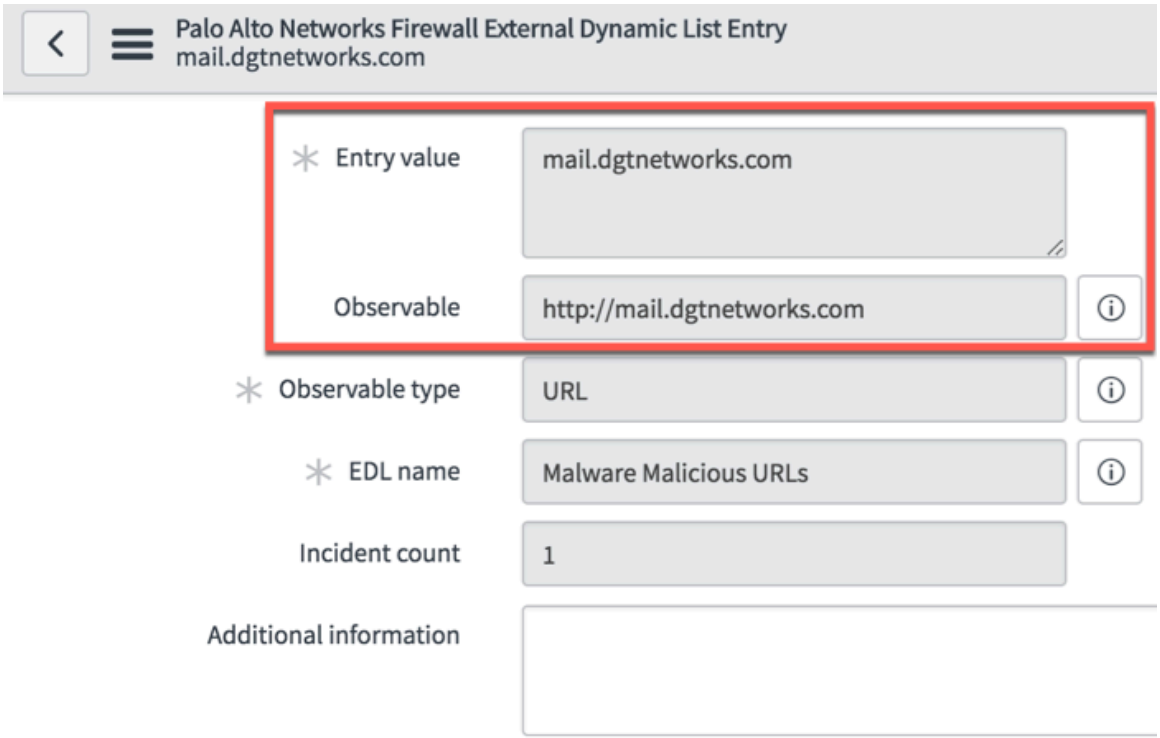
   For this example, the record for **mail.dgtnetworks.com** is displayed.



   The status is Pending, the Active check box is cleared, and the work notes show that there is a request to add the observable. This EDL Entry request is ready for approval.

   The Entry value and Observable fields show different formats for the URL observable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The icon next to the `Observable` field is a link to the ServiceNow AI Platform® Observable table.

The value in the `Observable` field (`http://mail.dgtnetworks.com`) links to the Observable table, and it matches the format that was brought over from the Security Incident Response incident-triggering event.

The ServiceNow AI Platform® may automatically modify EDL entries so that they are compatible with the Palo Alto Networks EDL URL format.

In this example, the observable was created with the http:// protocol (`http://mail.dgtnetworks.com`), and this format is displayed in the Observable field. The http:// protocol is stripped off automatically from the observable by the ServiceNow AI Platform® so it is compatible with Palo Alto Networks and can be retrieved. As a result, `mail.dgtnetworks.com` is displayed in the `Entry value` field.

What to do next
Approve EDL entries.

Related topics
EDL entry exceptions for Palo Alto Networks Next-Generation Firewall

Submit EDL entries from the blocklist for Palo Alto Networks Next-Generation Firewall

For observables determined to be malicious, and not associated with a specific ServiceNow AI Platform security incident, you submit External Dynamic List (EDL) entries from the blocklist.

Before you begin
Role required: sn_si.analyst

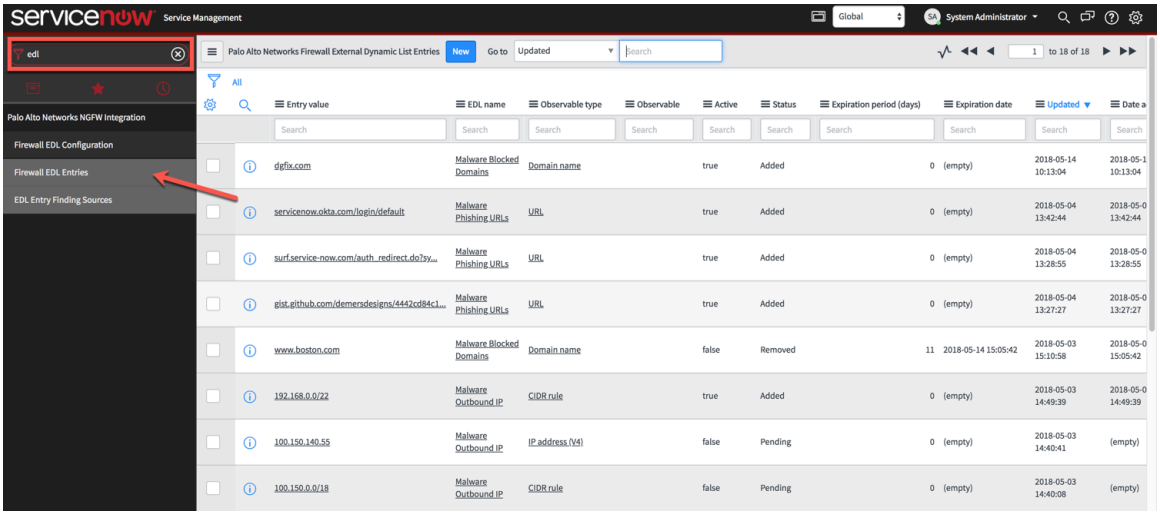
About this task
When you want to block an observable that you have determined is malicious, or allow an observable you have determined is not malicious, and the observable is not associated with a

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

specific ServiceNow AI Platform security incident record, you submit EDL entries directly from the blocklist. Examples of these types of EDL entries might be URLs or domains for specific sites.

Procedure

1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Entries**.



2. Click the **Firewall EDL Entries** module.
3. In the Palo Alto Networks Firewall External Dynamic List Entries list, click **New**.
4. In the new record that is displayed, in the **Entry value** field, enter a value for your observable. The two possible outcomes of this entry:

   The remaining fields on the form are completed automatically.

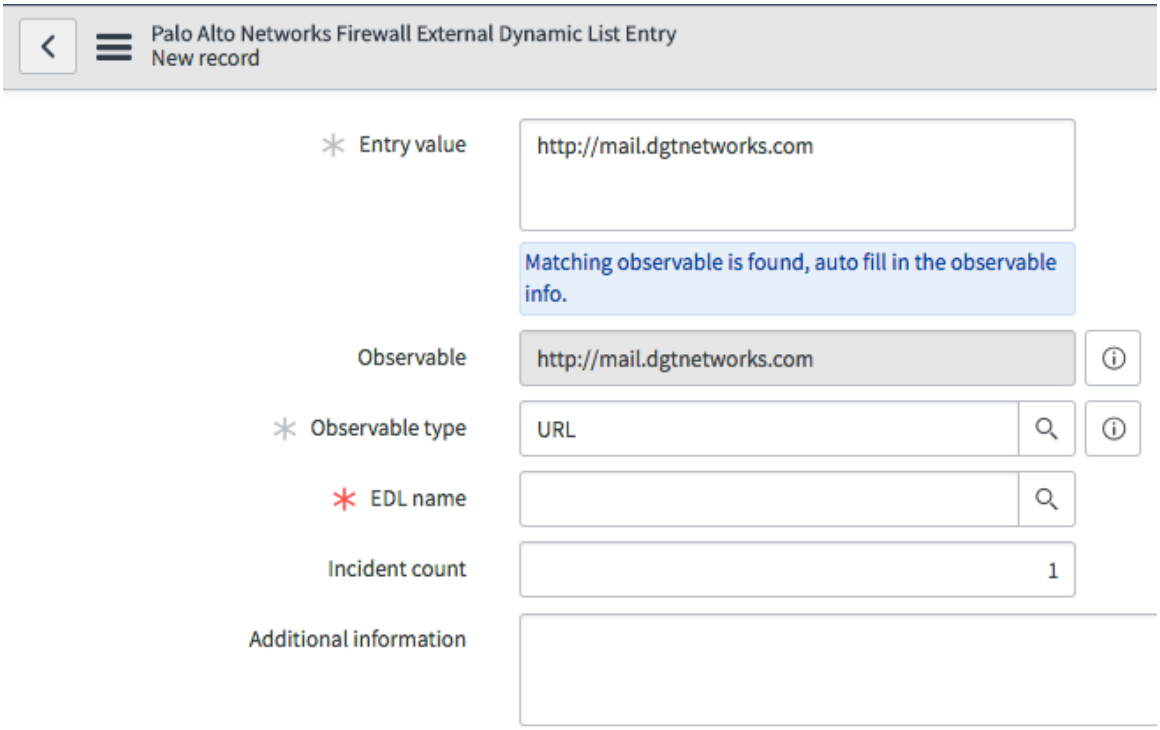
   A matching observable is found, and a message is displayed that a matching observable exists. Select the EDL you want to attach this entry to and click **Submit**. Select the EDL you want to attach this entry to prior to setting the Expiration period.

   A message is displayed that instructs you to complete the form.

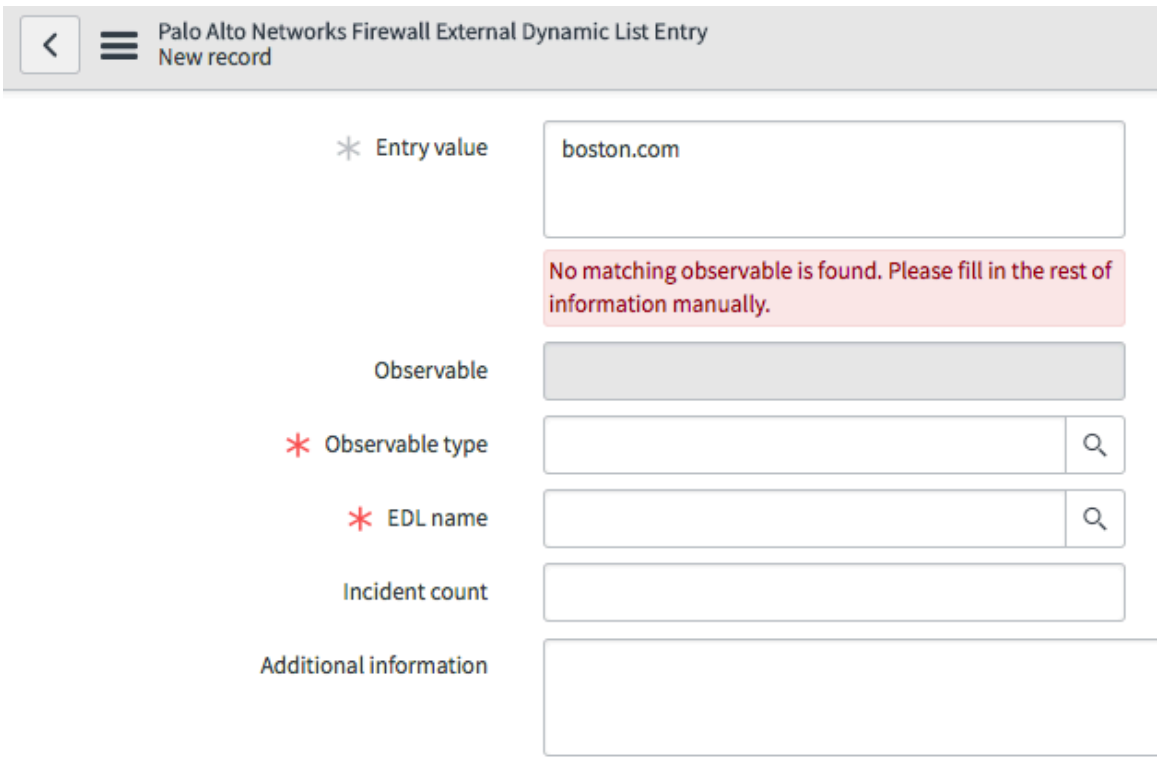
   A matching observable has not been found, and you must complete the form. After you complete it, select the EDL you want to attach the observable to and click **Submit**. An observable record is created.

   The following figure shows an example of an existing domain observable and how the fields are completed automatically.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



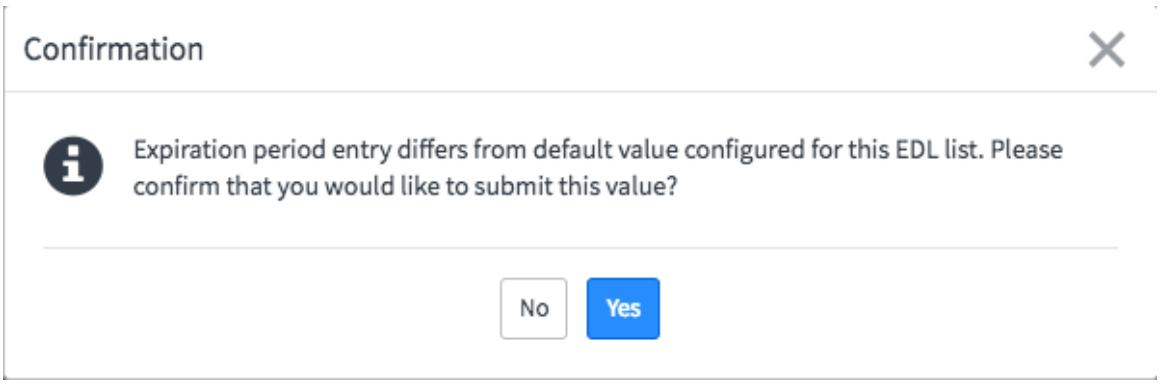
5. Click the search icon to select the EDL you want to attach the entry to.
6. Click **Submit**.
   If you have email approval configured in your workflow, an approval email request is sent.
7. If a message is displayed that requests you to fill in the rest of the information manually, fill in the fields.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Observable type	Observable type that is supported from the di alog.
EDL name	EDL you want to attach the entry to. **Note:** Select the EDL want to attach the entry to prior to setting the Expira tion period.
Enable override (default is selected)	Lookup result or source. When configured, permits you to enter a **Lookup result** and the source used to find the results. These fields are typically populated when a security in cident record is created. In this case, there is no lookup result or source, and you fill in these fields in manually.
Lookup result	Select **Unknown** or **Malicious**.
Source	Source that performs a threat lookup on the EDL entry, for example, ThreatCrowd, etc.
Expiration period	The expiration period inherited from the EDL by default. You can override this value, but on ly during the creation of the entry. 0 indicates that the EDL entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on May 1, the EDL entry will expire at 2:01 PM on May 31.

8. Click **Submit**.
   If you have changed the default expiration period of the EDL entry, a warning confirmation dialog box is displayed indicating that the period differs from the selected EDL.

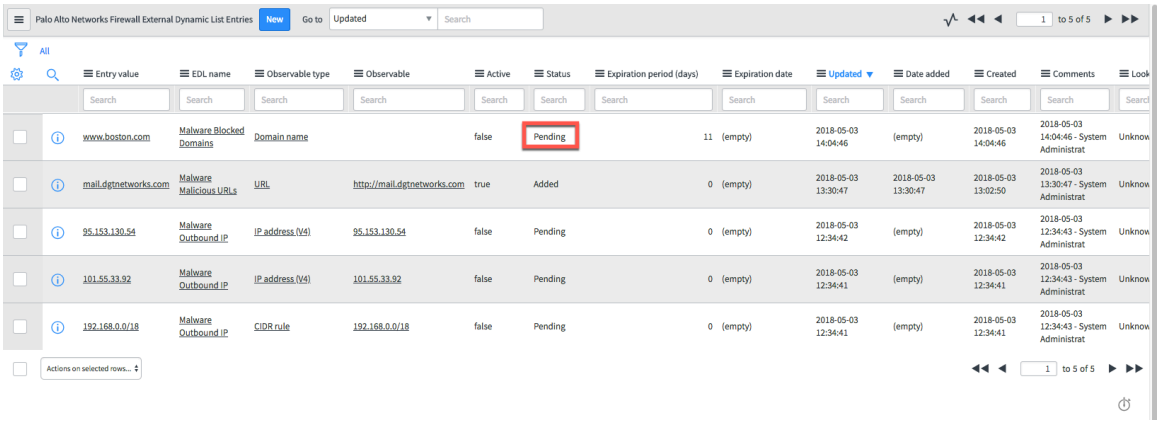


9. Choose one option to configure the expiration period.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Yes	Confirms your expiration override, saves the record, and returns you to the **Palo Alto Networks Firewall External Dynamic List Entries** list. If you have email approval configured in your workflow, an approval email request is sent.
No	Cancels the override. At this point, you can change the value for the **Expiration period**. After changing the value, click **Submit** to return to the **Palo Alto Networks Firewall External Dynamic List Entries** list.

10. If not displayed, navigate to the **Palo Alto Networks Firewall External Dynamic List Entries** list and note that the status for the entry is Pending.



The entry is now ready for approval.

What to do next

Approve EDL entries.

Related topics

EDL entry exceptions for Palo Alto Networks Next-Generation Firewall

Approve EDL entries for Palo Alto Networks Next-Generation Firewall

An approval process for External Dynamic List (EDL) entries is part of the preconfigured workflow. You approve EDL entries before the entries are activated on EDLs. One you approve the EDL entry, the firewall retrieves the entry, and your observable is blocked from that point forward.

Before you begin

Role required: Approval for EDL entries is assigned to sn_si.admin by default, but this authority can be assigned as required by your organization. In the following example, the ServiceNow AI Platform admin has approval authority.

About this task

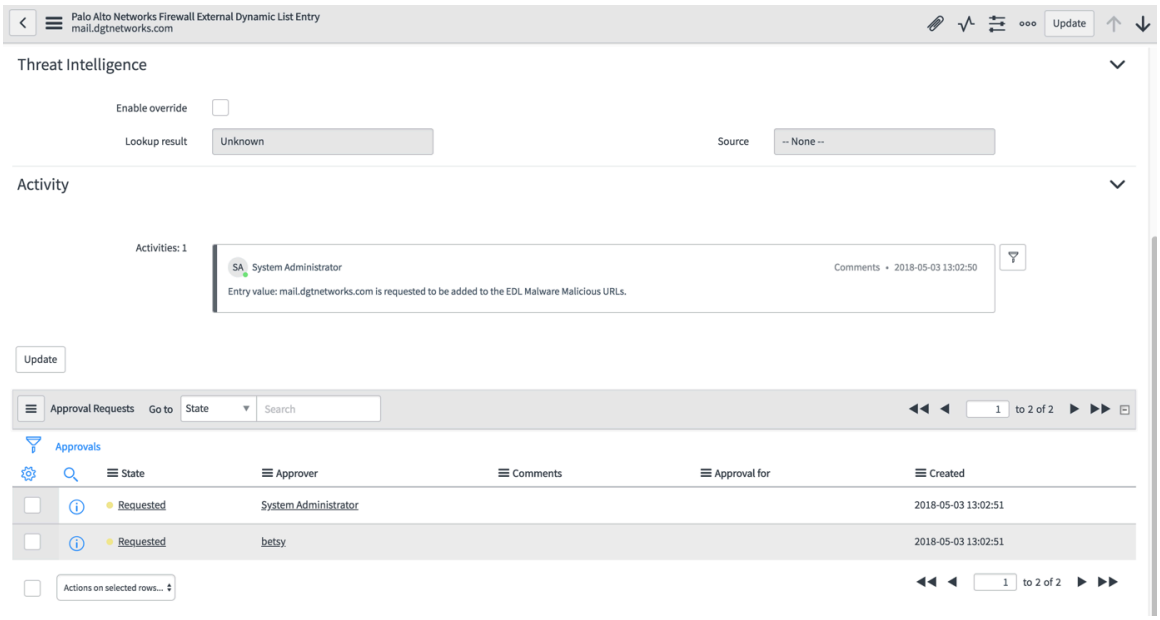
When the approval process is enabled, an EDL entry is not activated or deactivated on the EDL until it is approved.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

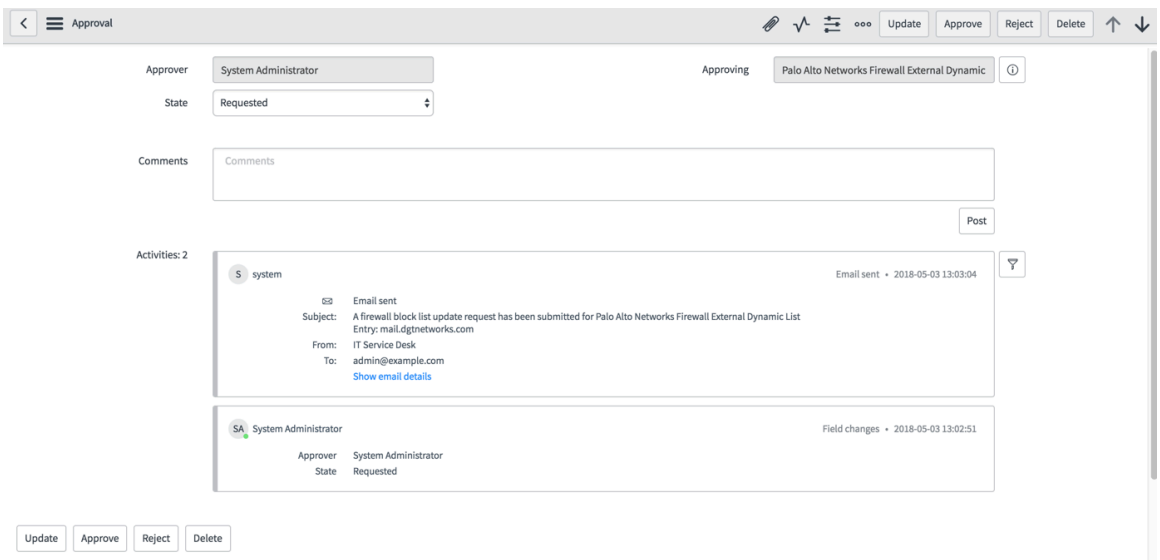
Procedure

1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Entries** and open the EDL record.
2. On the EDL record, scroll to the Approval Requests section.

   Note: If you have Tabbed forms selected in System Settings, the section appears as a tab on the record.



3. In Approval requests, click an item in the **State** column to open it.
   The approval record is displayed.



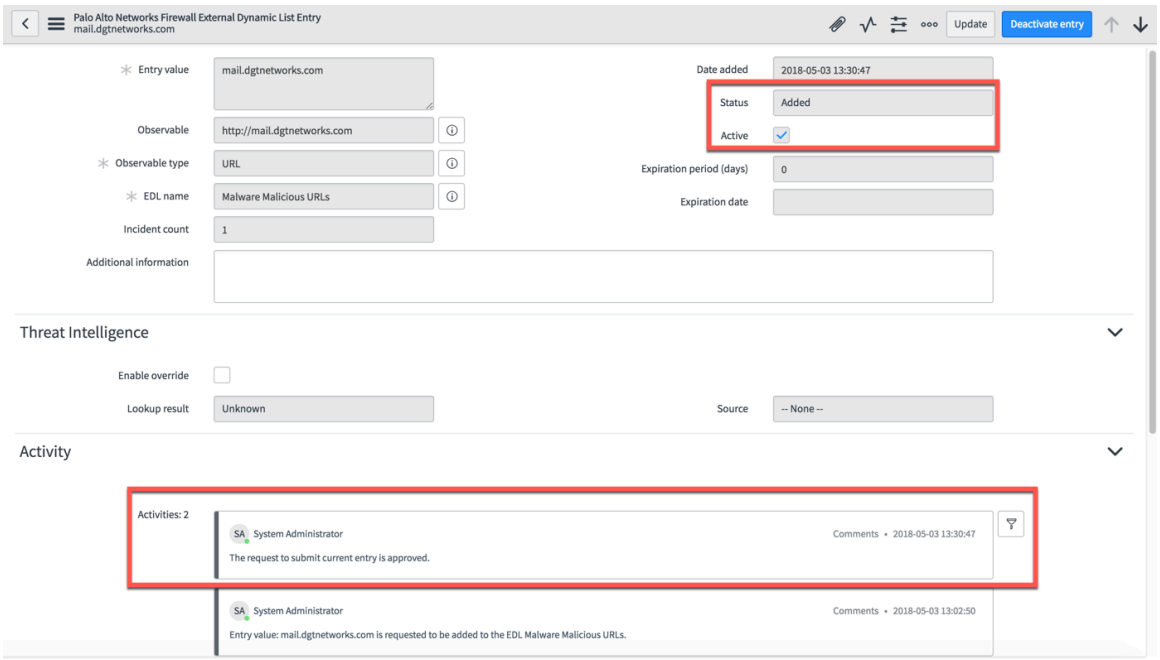
4. Choose one option for approving the EDL entry.

Option	Description
Approve	On the entry record, the **Status** field changes to Added, and the **Active** check box is selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

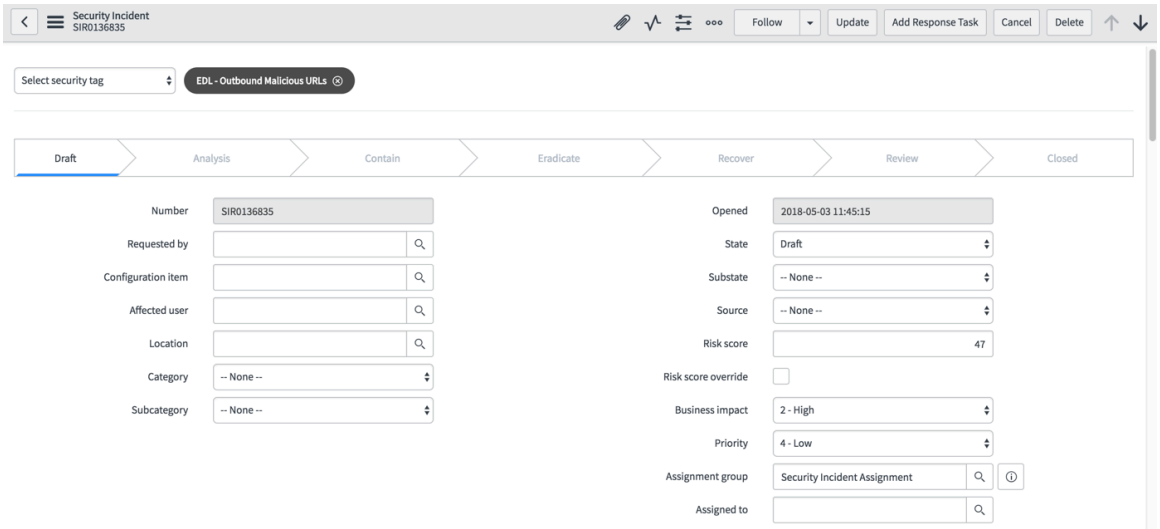
Option	Description
	The **Deactivate**button is displayed and ac tive. Work notes show that the request for the EDL entry has been approved.
Reject	On the entry record, the Status field changes to **Rejected**, and the **Active** check box is cleared indicating the entry is not blocked on the firewall. Work notes show that the request for the EDL entry has been rejected.

After you have approved the EDL entry and it is activated, the Palo Alto Networks Next-Generation Firewall retrieves the EDL entry after the next retrieval interval. After the entry is retrieved, the observable is blocked from that point forward. In the following figure, note that the Active check box is selected, the status is Added, and the work notes indicate that the request has been approved.

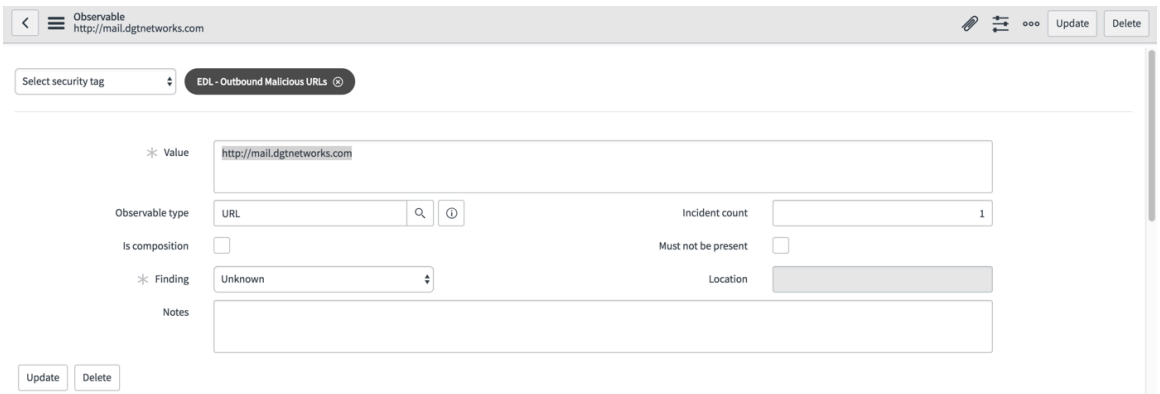


After the EDL entry is approved and activated, the security incident record is marked with a security tag. The tag is displayed at the top of the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The security tag is also displayed on the observable record.



EDL entry exceptions for Palo Alto Networks Next-Generation Firewall

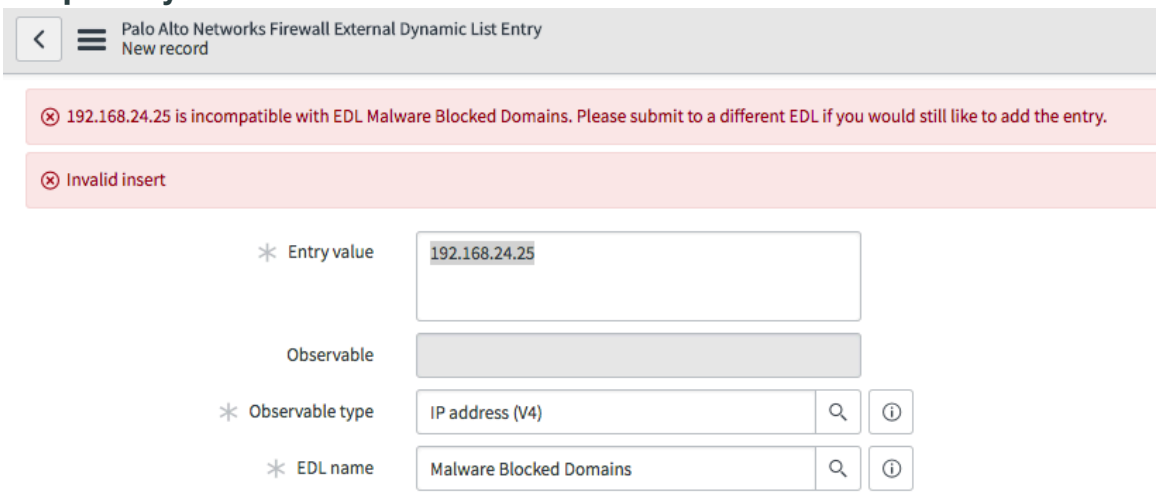
There are restrictions for adding External Dynamic List (EDL) entries to EDLs. If duplicate, compatibility, or CIDR (Classless Inter-Domain Routing) conflicts exist when you try to add EDL entries to EDLs, error messages are displayed that help you resolve these errors.

Compatibility exception

Each EDL only accepts entries that are compatible with its observable type. If you create a Domain EDL and you try to attach an IP address observable to it, an incompatible error message is displayed. For example, a domain EDL can only accept domain observables, as illustrated in the following figure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

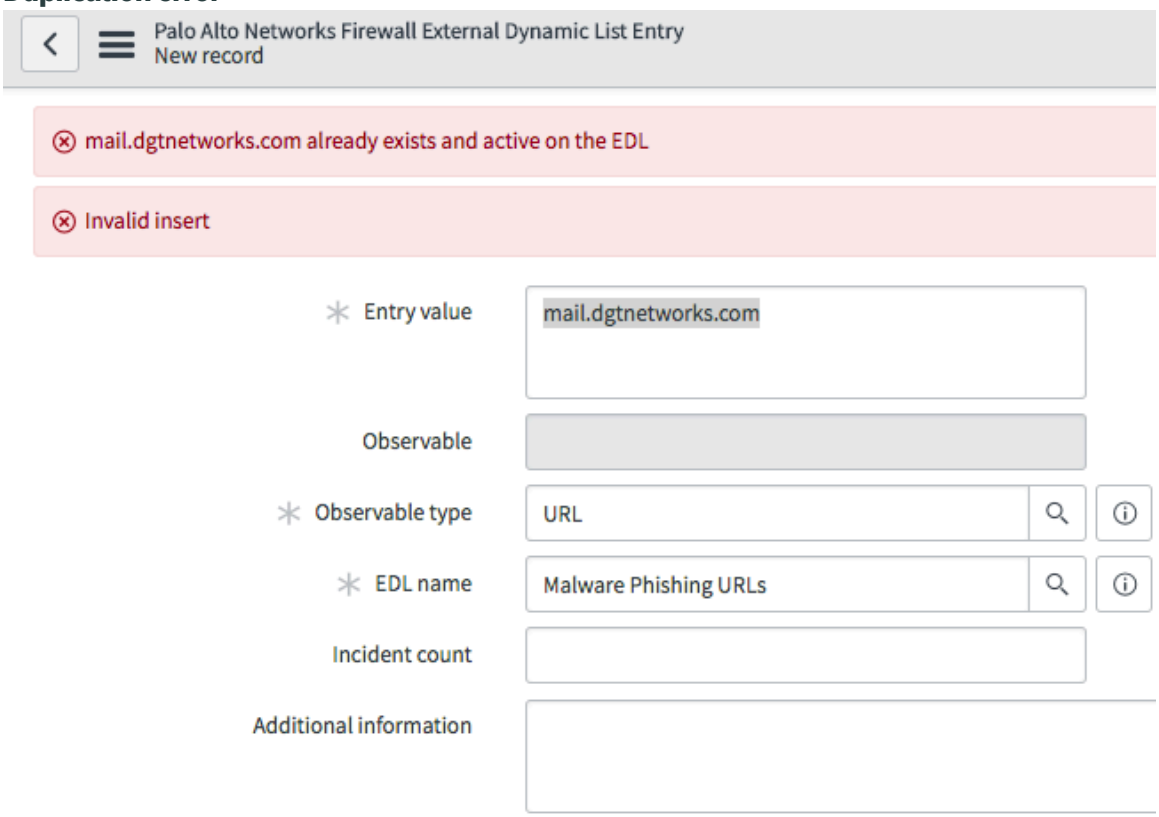
Compatibility error



Duplication exception

An observable cannot be activated on multiple EDLs of the same observable type. If a URL observable is already activated on a URL EDL, and you try to activate the same observable on a Phishing URL EDL, a duplication error message is displayed.

Duplication error

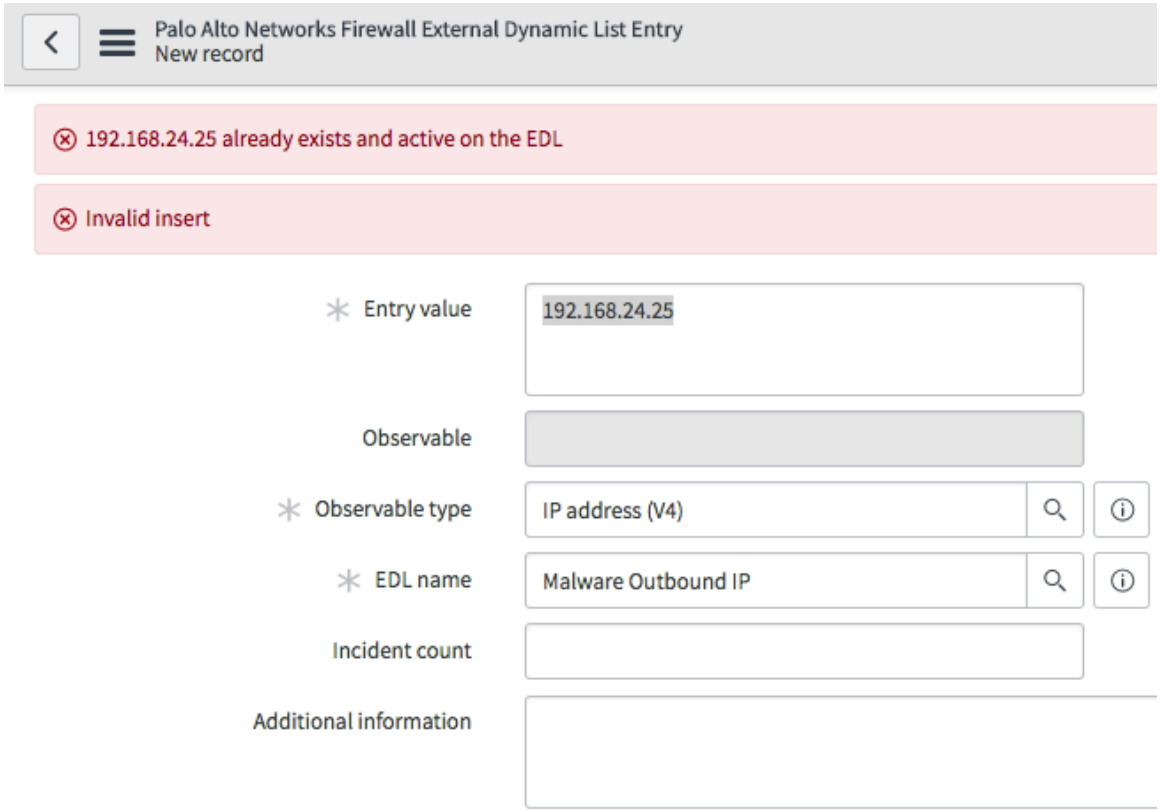


CIDR (Classless Inter-Domain Routing) exception

If you attempt to attach a single IP address to an EDL, and this IP address is part of a CIDR observable already on an EDL, a CIDR conflict error is displayed. This error indicates that the single IP address is already included on the EDL as part of the CIDR observable. For example, 192 . 168 . 24 . 25 is part of the CIDR block 192 . 168 . 0 . 0 / 22.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CIDR conflict



(Optional) Edit the security tag name for Palo Alto Networks Next-Generation Firewall

If the **Display tag** check box is selected when you create the External Dynamic List (EDL) record, you can edit the tag names and colors of the security tags. Security tags help you track observables that are already blocked.

Before you begin

Role required: sn_si.admin

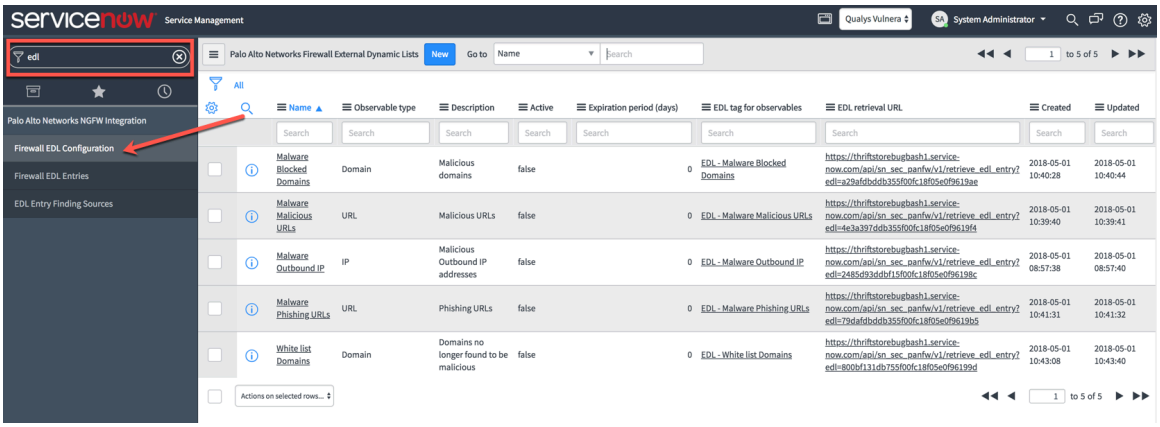
About this task

Security tags help you quickly identify which security incidents have observables on a block list. Tags also help you identify whether an observable is already blocked, or, if it has been removed from an EDL. By default, the color of the security tag is black for block list entries and gray for allow list entries. You can change the names and colors of the tags to help you recognize certain tags more easily.

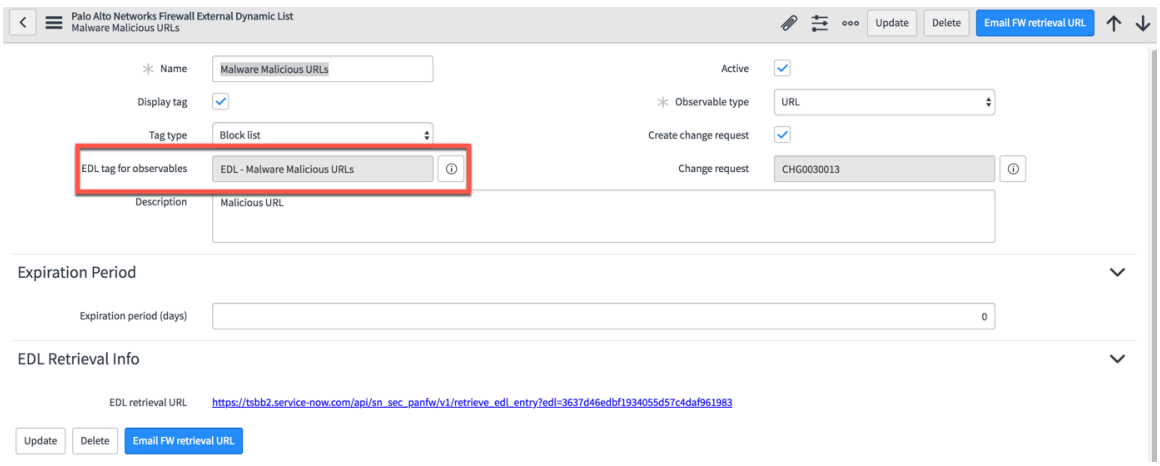
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

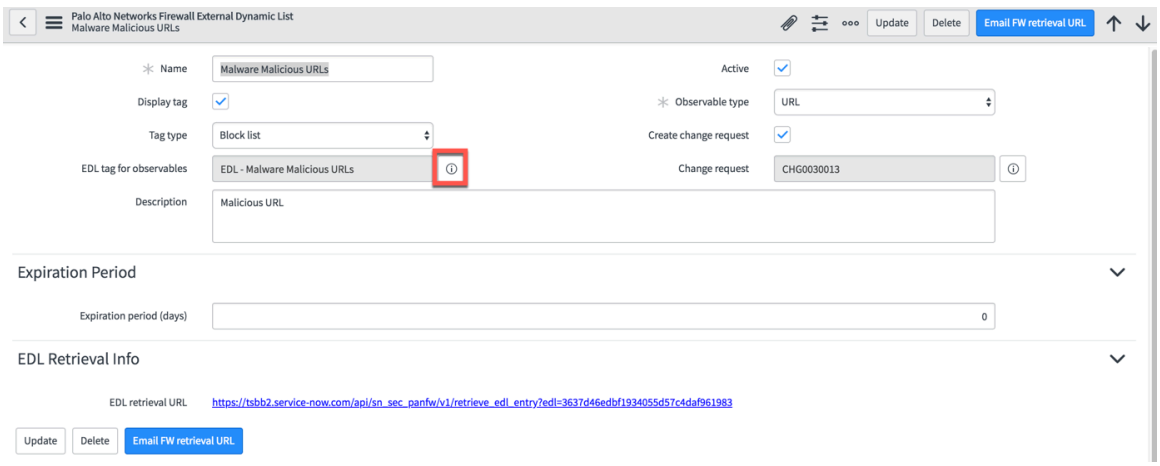
1. Navigate to **All** > **Palo Alto Networks NGFW Integration** > **Firewall EDL Configuration**.



2. Click an item in the **Name** column to open it
   The EDL record is displayed. By default, the security tag name is the same value you entered in the **Name** field of the EDL when you created it. By default, the name also includes an EDL prefix, for example, EDL – Malware Malicious URLs.

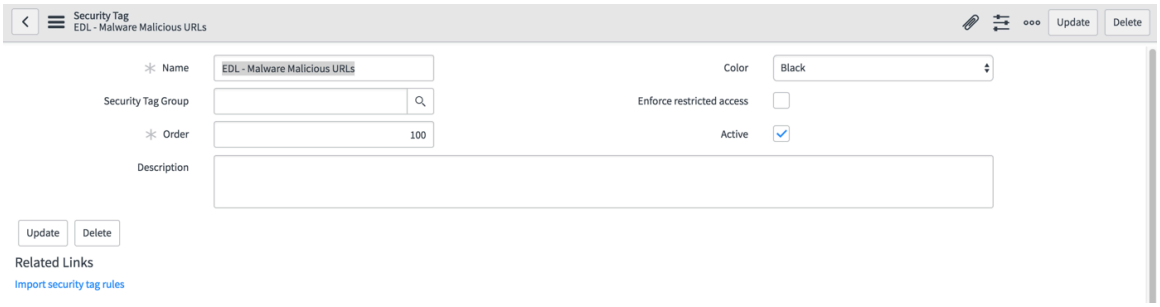


3. Click the information icon (ⓘ) next to **EDL tag for observables** then **Open record**.

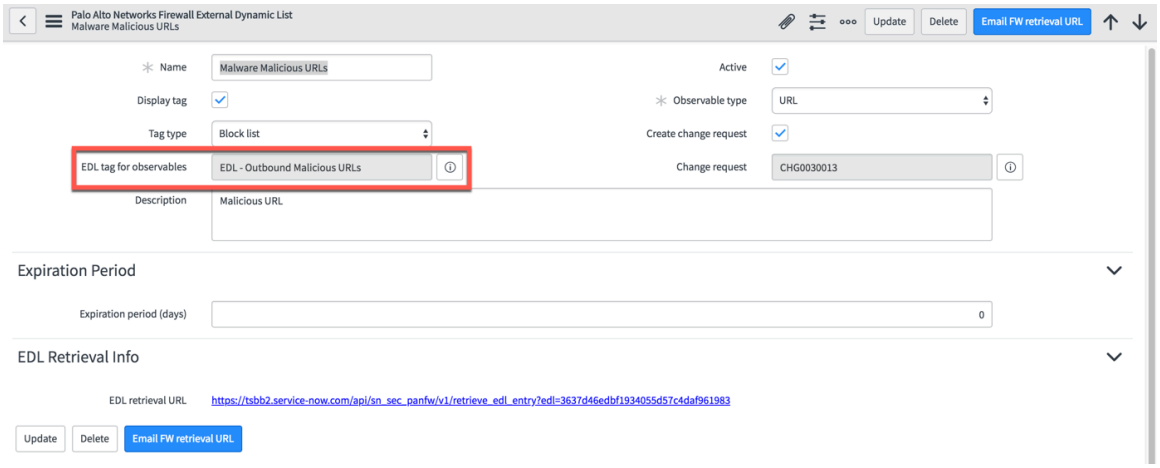


The Security Tag Form is displayed.

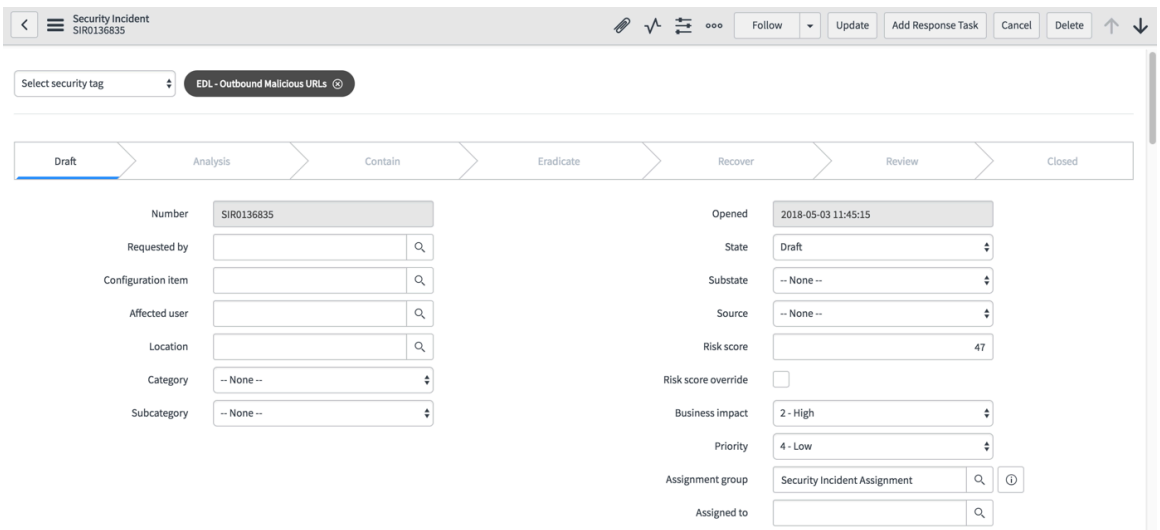
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In the **Name** field, modify the security tag name and click **Update**.
   The updated EDL record is displayed with the modified tag name. In the following example, `Outbound` has been added to the tag name. Keep the `EDL` prefix in your new tag name to help you identify the tag is associated with the Palo Alto Networks Next-Generation Firewall integration.



   The security tags are displayed for each observable type (IP, URL, Domain) on the Security Incident record and the Observable record each time that observable is added to an EDL.



   If an observable has already been added to an EDL, and a security tag is displayed on a security incident for this observable, the EDL security tag also is displayed automatically on any subsequent security incident records that are created. This duplication tells you that the observable is already on a block list. You do not need to add this observable and re-block it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When an observable is no longer blocked, a security tag is not displayed on the security incident record or the observable record. In this instance, no security tag indicates that the expiration date of the observable may have passed, or the observable has been deactivated from an EDL.

Uninstall Palo Alto Networks Next-Generation Firewall

If you want to uninstall Palo Alto Networks Next-Generation Firewall from your ServiceNow AI Platform instance and remove all remnants from the integration, refer to the ServiceNow documentation site for instructions on uninstalling applications.

Before you begin

Role required: System Administrator (admin)
See Uninstall applications on the ServiceNow Product Documentation website.

PhishTank integration

PhishTank is a community-based phishing verification system into which users submit suspected threats, and other users in the system vote to determine whether the phishing threats are legitimate. When integrated with the ServiceNow AI Platform Security Operations product, the threat intelligence results provide analysts with additional insight into phishing-related security incidents or investigations.

The PhishTank integration performs lookups on potential phishing site URLs.

The workflow checks for new observables as they arrive in security incidents. If the observables are of a type recognized by the API integration, the observables are evaluated. Observables determined to be malicious are tagged.

Install and configure PhishTank

Before you run the integration on your instance, complete the installation and configuration steps so the PhishTank application properly integrates with ServiceNow AI Platform Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Setup tasks	Description
Verify that you have assigned the required ServiceNow AI Platform roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module.
Obtain an API key.	Visit the PhishTank website for information on API keys and to create an account: PhishTank website.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

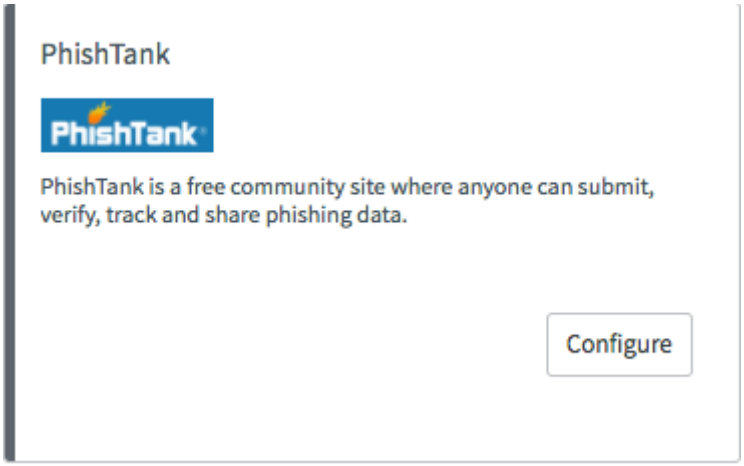
Setup tasks	Description
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Role required: admin

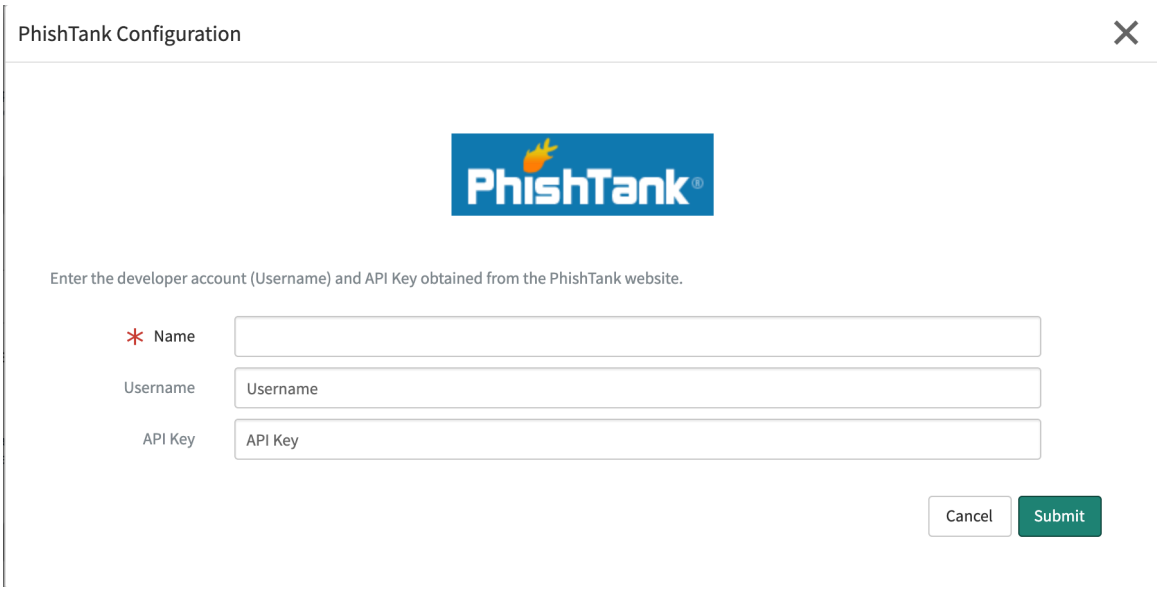
Procedure

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the PhishTank tile.
3. Click **Configure**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. In the **PhishTank Configuration** dialog box, enter the Name of the configuration, the Username (developer account created in PhishTank), and the API key you obtained from the PhishTank website and click **Submit**.



5. Verify successful configuration.
   Configuration is successfully completed unless an error message is displayed.

   Trouble?

   If an error message is displayed during the configuration, the PhishTank API key may be invalid.

Verify expected results for PhishTank

Observables are generated automatically by a security incident and scanned by the application. Lookup results are displayed on the Threat Lookup Results tab at the bottom of the security incident record.

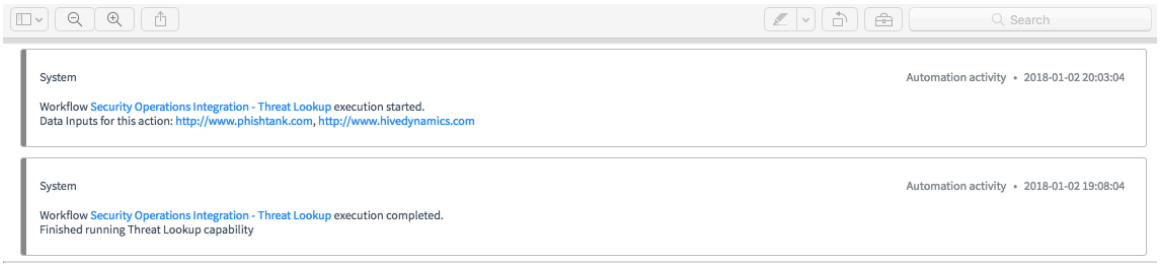
Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Open the security incident form you are working with and verify that the lookup has run successfully.

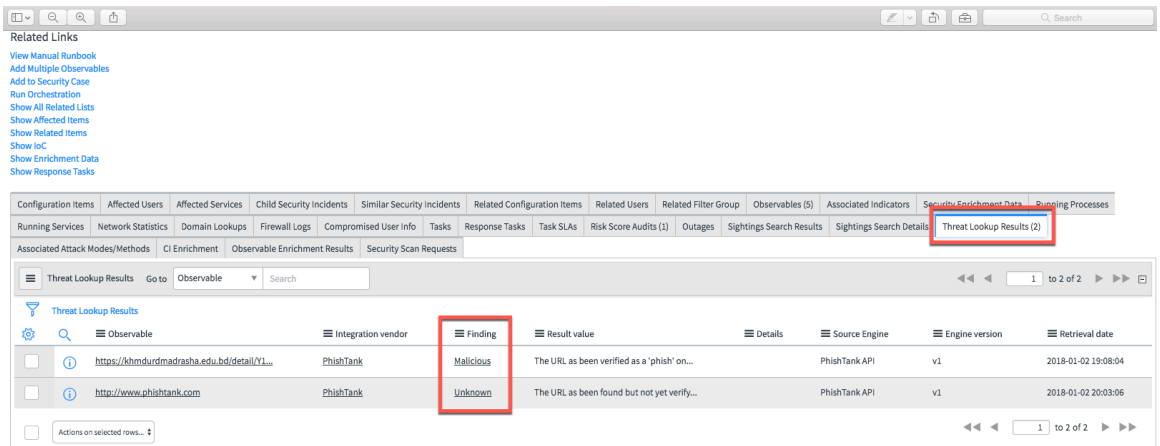


   After the application is configured, the flow launches automatically upon incident creation. The execution and completion status of the lookup is then displayed in the work notes in the security incident record.

2. Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

3. Navigate to the bottom of the security incident and click the **Show All Related Lists** related link.

   Note: The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. If tabbed forms are not displayed, in the upper-right corner of the banner frame, click the Settings gear icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.

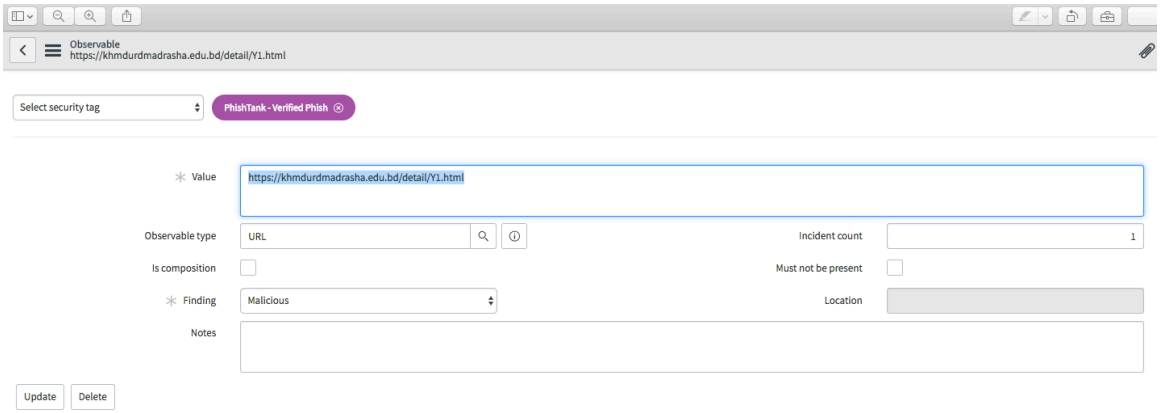


   The **Threat Lookup Results** tab at the bottom of the security incident record displays the lookup results.

   The **Finding** column displays `Unknown` for records not determined to be malicious. For results matching malicious, `Malicious` is displayed in the **Finding** column.

4. In the **Observable** column, click an observable to open a record and display more information.

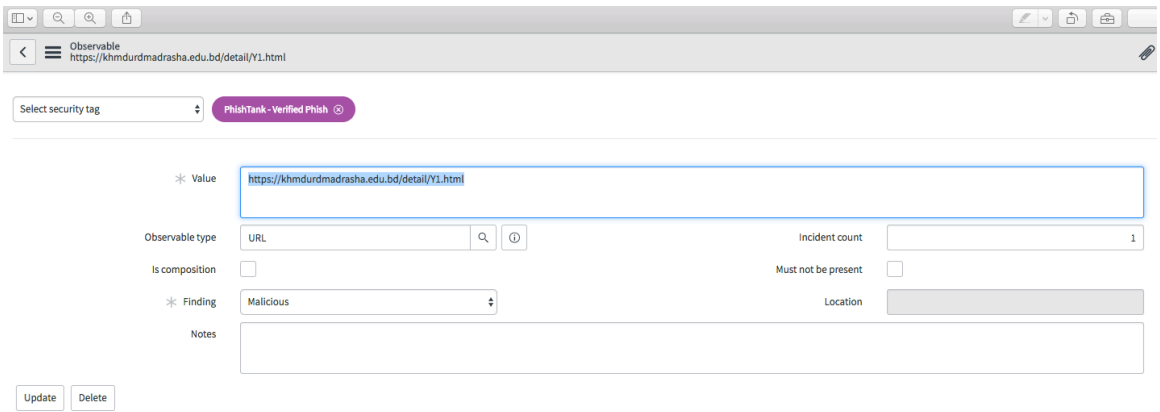
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



On the observable record, for lookups matching malicious, `Malicious` is displayed the **Finding** field. The observable is tagged with the Threat Intelligence source that found it to be malicious, in this case, the PhishTank application.

5. To view raw data, navigate back to the security incident and click the blue information icon next to an observable.

6. In the window that is displayed, click **Open Record**.



The link created by the API and the **Finding** field displayed with the results.

Trouble?

If you do not see results under the **Threat Lookup Results** tab, verify that the observable is a type that is supported for lookup by the integration.

(Optional) Manually attach an observable for PhishTank

You can manually attach observables to a security incident. You manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

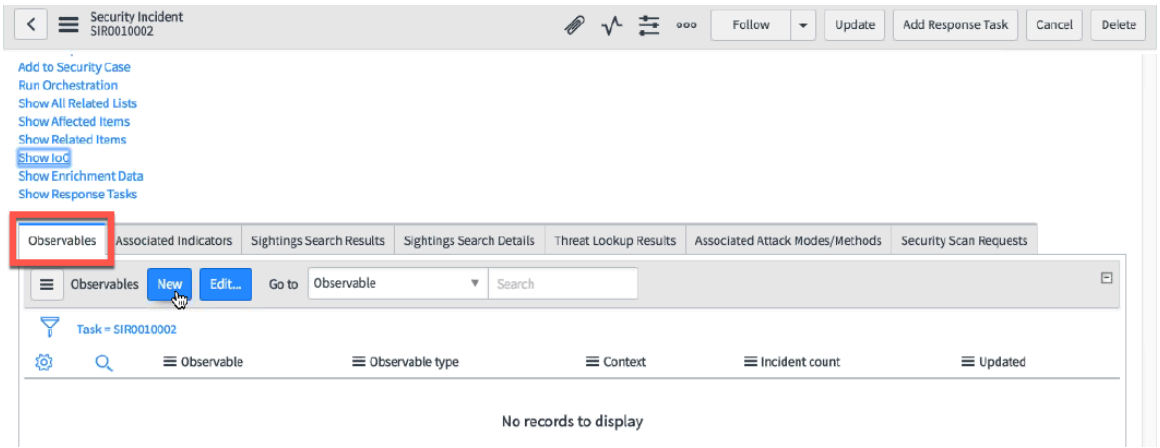
Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

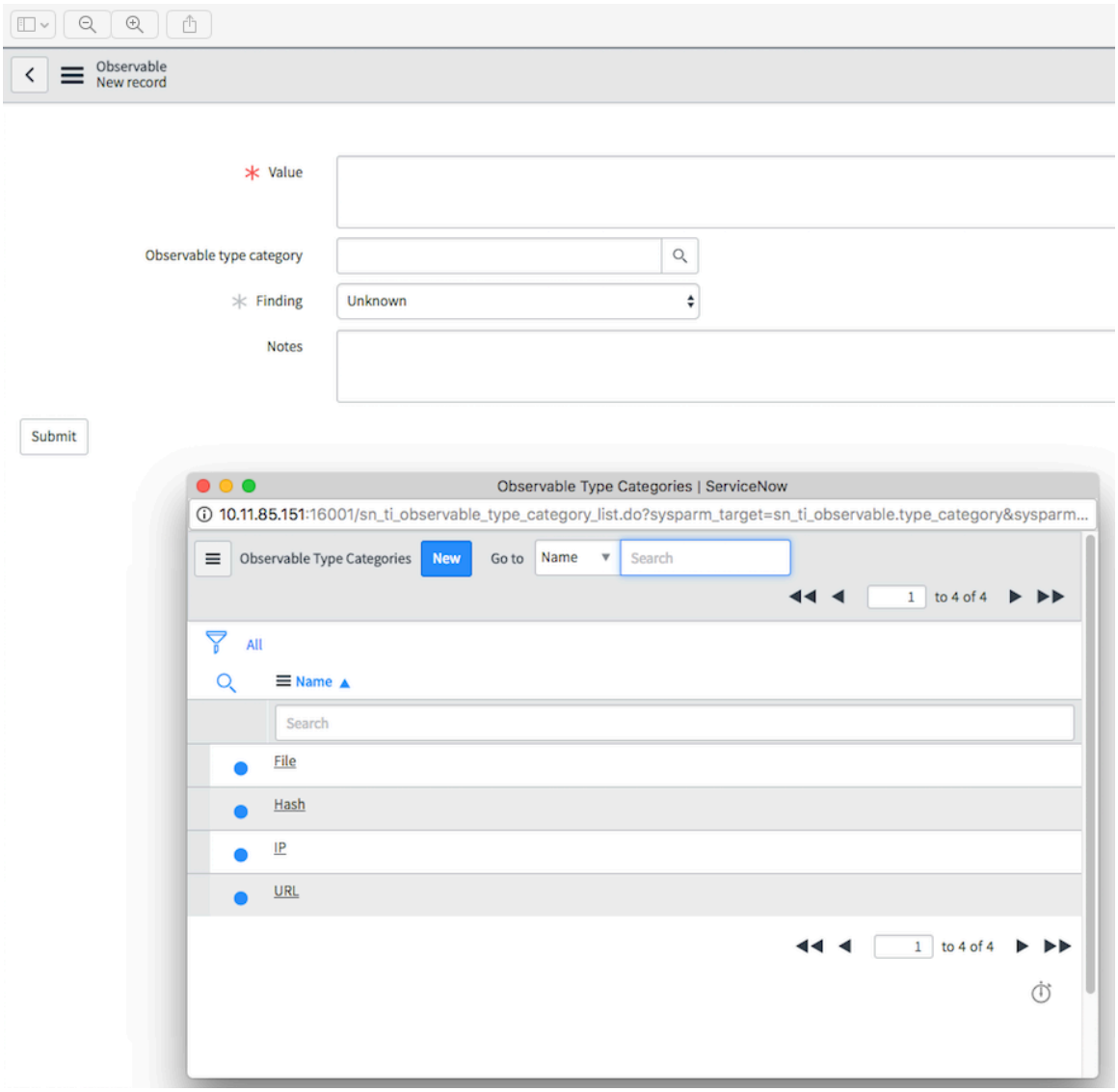
Procedure

1. Navigate to your open security incident.
2. On the open security incident record, click the **Show IoC**link in **Related Links** to display the **Observables** tab.



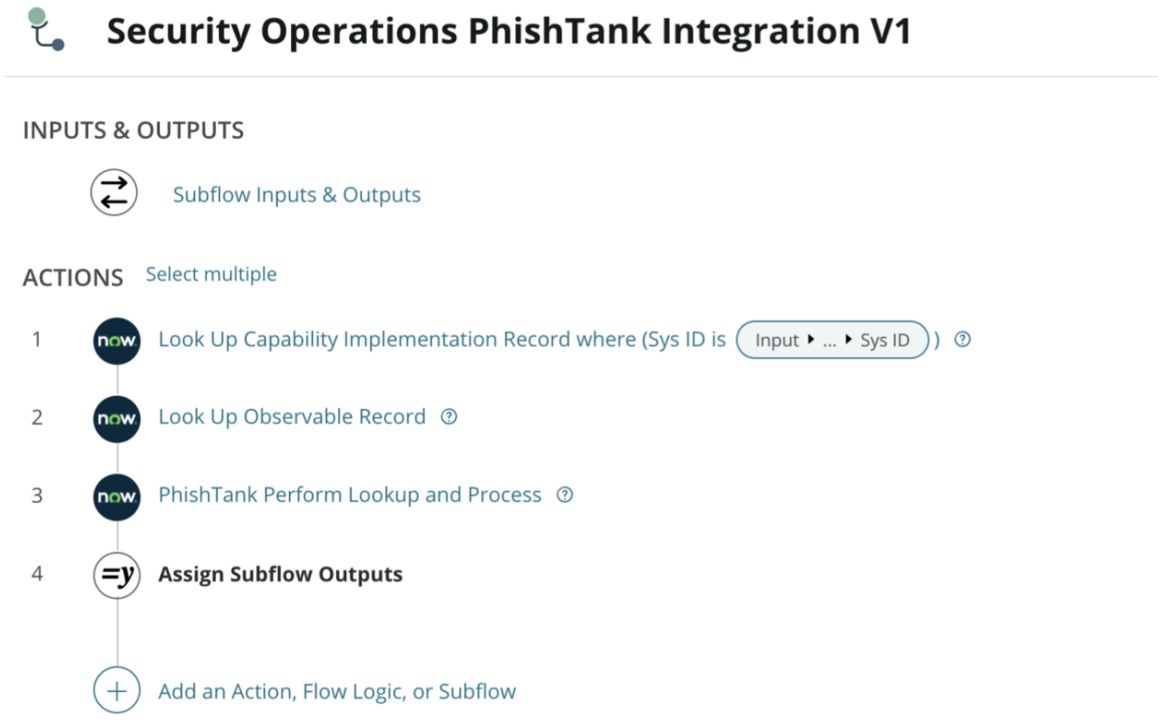
3. Click **New**.
   The Observable form is displayed.
4. In the **Value** field, enter a URL.
5. Click the search icon and from the **Observable Type Categories** dialog box, click **URL** in the list to populate the field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

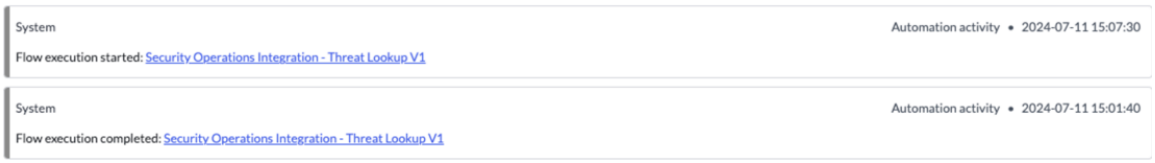


6. Click **Submit**.
   The flow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the Security Incident record.

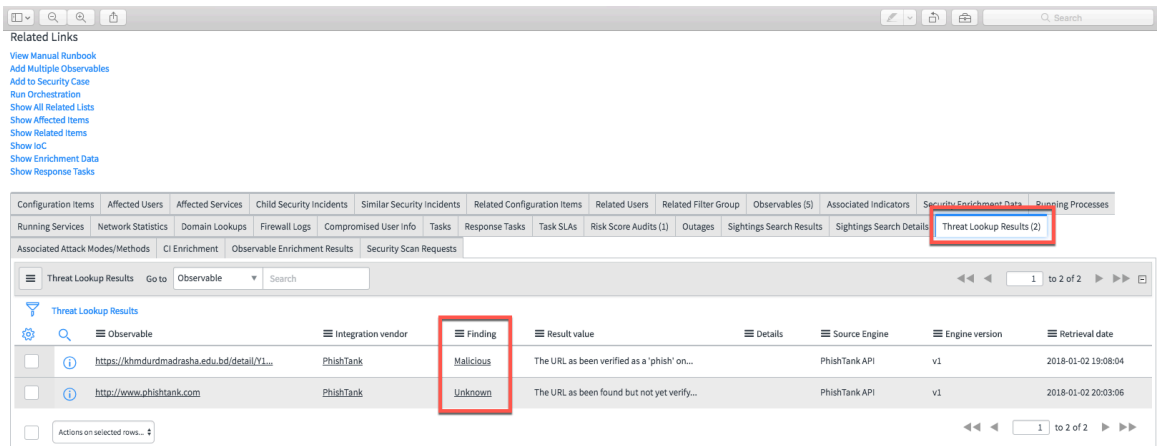
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Navigate to your security incident and review the work notes.



8. Click the **Show All Related Lists** related link at the bottom of the security incident.
9. Click the **Threat Lookup Results** tab to view the results.



10. In the **Observable** column, click the blue information icon next to a given observable for more information and raw data.

11. In the dialog box that is displayed, click **Open Record**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Trouble?
Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.

Proofpoint Integration for Security Operations

The Proofpoint SIR integration supports the ingestion of events from Proofpoint. SIR creates an incident for each ingested event which analysts can review or work on.

Get started

Explore	Configure
	
Learn about Proofpoint integration	Configure Proofpoint for SIR Workspace

Exploring the Proofpoint Integration for Security Operations

You can configure event profiles in SIR to ingest events from Proofpoint. SIR creates an incident for each ingested event which analysts can review or work on.

Proofpoint Integration for Security Operations users

Users

User	Description
Security admin	Create event profiles for filtering the ingested events. SIR creates incidents for these the ingested events.

Proofpoint Integration for Security Operations benefits

Proofpoint Integration for Security Operations benefits

Benefit	Feature	Users
Pull event data into your instance and create security incidents. Review security incidents from a single location for events deemed suspicious or malicious.	If the delivered email messages and permitted clicks are later deemed malicious, chances are these messages were opened and interacted with by your employees. To track these messages for review,	Managers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Proofpoint Integration for Security Operations benefits (continued)

Benefit	Feature	Users
	automatically create security incidents based on the event profiles you create and configure for message traffic for the integration. Additionally, you can also enable creating security incidents for the blocked messages and clicks for audit purposes.	

What to explore next

To learn more about configuring and using Proofpoint, see:

- Configuring the Proofpoint Integration for Security Operations
- Review Proofpoint integration settings
- View Proofpoint Analytics Dashboard

Configuring the Proofpoint Integration for Security Operations

Configure your implementation of the Proofpoint Integration for Security Operations.

Configuration overview

1. Install and configure the Proofpoint Integration for Security Operations.

   Download, install and activate the integration application.

2. Create an event profile for the Proofpoint Integration for Security Operations.

   Create an event profile to identify the events you want to import from the Proofpoint product and the conditions you want to use to create security incidents from the imported data.

3. Configuring the Proofpoint Integration for Security Operations

   Review the integration settings for creating the event profiles.

Install and configure the Proofpoint Integration for Security Operations

Install and configure the#Proofpoint Integration for Security Operations application from the #ServiceNow® Store on your#ServiceNow AI Platform instance.

Before you begin
Role required: sn_si_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Download the#Proofpoint Integration for Security Operations application from the #ServiceNow® Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Locate the#`Proofpoint Integration for Security Operations` tile and select **Configure**.
4. On the form, fill in the fields.

Proofpoint Integration Configuration form

Field	Description
Name	Name of the Proofpoint Integration for Security Operations configuration.
Service Principal	User name of Proofpoint tenant.
Secret	The ID of Proofpoint tenant.

5. Select **Submit**.
   After you successfully validate and submit the configuration, the integration is saved on the Security Integrations page as a tile.

Create an event profile for the Proofpoint Integration for Security Operations

Create an event profile to identify the events you want to import from the Proofpoint product.

Before you begin

Role required: sn_si_admin

Procedure

1. Navigate to **All** > **SIR Integration with Proofpoint** > **Proofpoint Events Profile**.
2. Select **New**.
3. Fill in the fields.

   The progress bar is displayed starting with Name.

Field	Description
Name	Name for the event profile. You might select names that describe the following Event Types that are supported and included with the application: ○ Clicks Blocked ○ Clicks Permitted ○ Messages Blocked ○ Messages Delivered
Source	Select the source you configured for the integration on the Integration Configurations page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Order	Order this profile is run. Default is 100.
Active	Select this check box to activate the profile.
Description	Text to help you identify this event profile.

4. Select **Continue**.
   The Proofpoint Event Selection step is displayed and the supported Event Types included with the application are displayed in the `Available` column:
   - Clicks Blocked
   - Clicks Permitted
   - Messages Blocked
   - Messages Delivered
5. Choose one or more to move to the `Selected` column.
6. Select **Continue**.

   The profile(s) you selected are displayed. For example, if you select a messages event, the Message Mapping configuration step is displayed in the progress bar. If you select a message profile and a clicks profile, both configuration steps are displayed in the progress bar.

   The values for the Source Fields are provided on this page from the targeted attack protection (TAP) data in your environment as a reference.

   The default mapping of the source fields data to the target fields is displayed on the right side of the page. Basic data is included as a guide, but you can modify this mapping.
7. Select the **f(x)** icon to view the default translations included with the application.

   These translations accommodate multiple values for a field by inserting commas between the values.
8. Select **Continue**.
9. In the Filtering and Aggregations page, configure the following:

Filtering and Aggregation properties

Option	Description
Filter based on conditions for Message Events	Select to enable filtering based on message events.
Message Events Filter Conditions	Create the message event filter conditions.
Filter based on conditions for Click Events	Select to enable filtering based on click events.
Click Events Filter Conditions	Create the click event filter conditions.
Aggregation Conditions	Select to allow an incoming incident to be appended to an open security incident instead of creating a new one.
Incident fields with matching values	Add Security Incident Response fields. All field values that are selected must

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	be matched for an incident to meet an aggregation criteria.
Log work note for New Incident	Select to enable work notes logging to the parent Security Incident Response.
Enable ThreatID Relation	Select to enable aggregation of all the incidents for which the ThreatID is same.

10. Select **Continue**.
    The Scheduling step is displayed.
11. Select one for the import type and how often you want to import event data.

Option	Description
Ongoing Events Ingestion	Select this to import events on a regular inter val. Provide a start date, the end date, and the polling interval in minutes. ○ **Polling increment (minutes)**: Interval in minutes between imports ○ **Set Initial Events Ingestion Time** ○ **Input initial Ingestion Time**
One Time Retrieval	Select this to import events only once on the basis of the date configured. All the events from the selected date are imported. Provide a start date for the event import (**Since date**).

12. Select **Finish**.
    Lists the newly created event profile with the existing profiles.

Review Proofpoint integration settings

Review the Proofpoint integration settings so that you can modify the system properties for your environment.

Before you begin

Role required: sn_si_admin

Procedure

1. Navigate to **All** > **SIR Integration with Proofpoint** > **Proofpoint Integration Settings**.
2. Modify the following settings.

Proofpoint Integration Settings

Property Name	Description
TimeOut for the restAPI calls. sn_sec_proofpoint.http_timeout	The timeout (in seconds) for fetching data from the api calls. Type: Integer

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property Name	Description
	Default value: 3000
Logging level - debug, info, warn, error sn_sec_proofpoint.logging_verbosity	The log verbosity level of the application, meaning the name of the type of information. You can update the value to the following options: ○ error ○ warn ○ info ○ debug Default value: info
Enforce a limit on number of Proofpoint Events that can be aggregated to a single incident. sn_sec_proofpoint.max_aggregations_per_si	The maximum number of Proofpoint events that can be aggregated to one incident. Type: Integer Default value: 100
Enforce a limit on number of security incidents that can be created in 24 hour period. sn_sec_proofpoint.max_si_per_day	The maximum number of incidents that can be created in 24 hours. Type: Integer Default value: 1000
No of days, we need to use in api call for top clickers, vap. sn_sec_proofpoint.default_days	The number of days of data to fetch for top clickers and VAP. You can also update the value to the following options: ○ 14 ○ 30 ○ 90 Type: Integer Default value: 90
Boolean flag, if enabled it makes api call and populates Topclickers details. sn_sec_proofpoint.call_topclickers_api	Activate the option to enable and fetch top clicker data. Type: Boolean Default value: True
Boolean flag, if enabled it makes api call and populates VAP details. sn_sec_proofpoint.call_vap_api	Activate the option to enable and fetch VAP data. Type: Boolean Default value: False
It is to restrict the maximum number of users to display for topClickers, VAP Users.	The maximum number of users to display for top clickers and VAP users.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property Name	Description
sn_sec_proofpoint.maxresults	Type: Integer Default value: 100
Enables/Disables using overlapping period during scheduled polling of Proofpoint Events. sn_sec_proofpoint.allow_overlap	Enable or disable overlapping period when scheduled polling is configured. Type: Boolean Default value: False
Overlap time in minutes to be used during scheduled polling of ProofpointEvents when overlap is enabled. sn_sec_proofpoint.overlap_time	The overlap time in minutes when scheduled polling is configured. Type: Integer Default value: 5

3. Select **Save**.

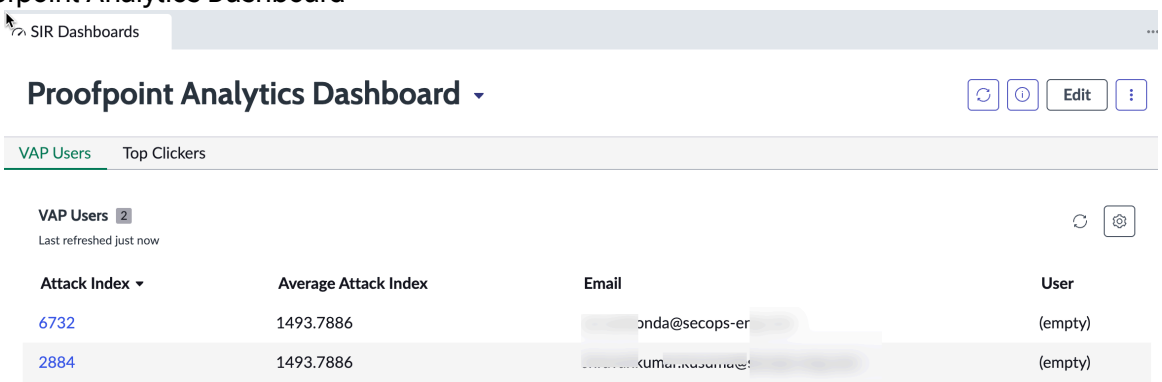
Result
Configures the integration settings with new values.

View Proofpoint Analytics Dashboard

This Proofpoint analytics dashboard provides details of VAP Users and Top Clickers.

Before you begin
Role required: sn_si_admin

Procedure
1. Navigate to **All** > **Workspaces** > **Security Incident Response Workspace**.
2. Select **SIR Dashboards**.
3. Select **Proofpoint Analytics Dashboard** from the drop-down list.
   The Proofpoint Analytics Dashboard



   appears.
4. Select **VAP Users** tab to view the list of VAP users.
   Select a VAP user to view its details.
5. Select **Top Clickers** tab to view the list of Top Clickers.
   Select a top clicker to view its details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reverse Whois integration

Reverse Whois is a service that performs searches on domain names registered by individuals or organizations.

Perform domain lookups using search terms in observables that you attach to a security incident. The Reverse Whois API searches domain records based on search terms you enter, and it returns all records that correspond with those terms.

Analysts sometimes use this integration along with the Whois integration for security incident research. The Whois integration provides additional enrichment information based on the domain lookups from the Reverse Whois integration.

Install and configure Reverse Whois

Before you run the integration on your instance, complete the installation and configuration steps so the Reverse Whois application properly integrates with the Security Operations product.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Setup task	Description
Verify that you have assigned the required ServiceNow roles.	The following roles are required for installation, configuration, and verification of expected results: • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees the configuration. The security incident administrator also assigns the Security Incident Analyst (sn_si.analyst) role. • The Security Incident Analyst (sn_si.analyst) performs domain lookups with Reverse Whois and analyzes and works with security incidents.
Obtain an API key.	Visit the WhoisXML API website for information on API keys and to create an account: WhoisXML API website. The configuration requires that you enter the API keys.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security

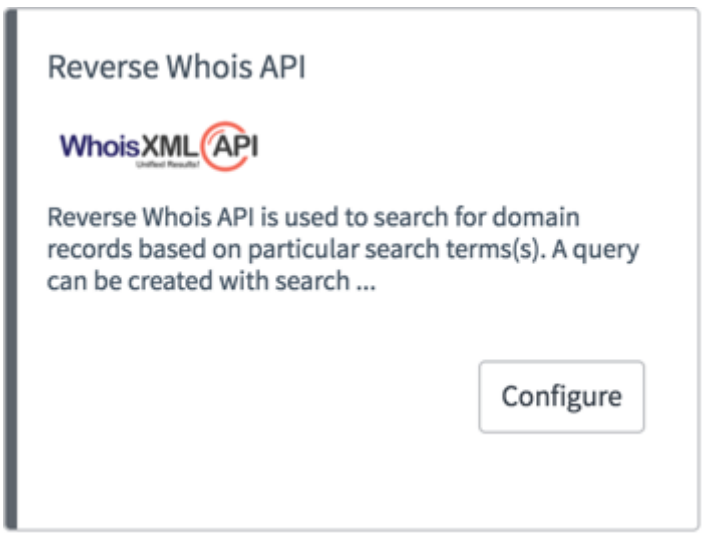
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Role required: admin

Procedure

1. If you have already installed and configured the Reverse Whois application, follow these steps:
   a. Delete the existing configuration.
   b. Install and create a new configuration using the API key that you have obtained.
2. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
3. After the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the Reverse Whois API tile.
4. Click **Configure**.

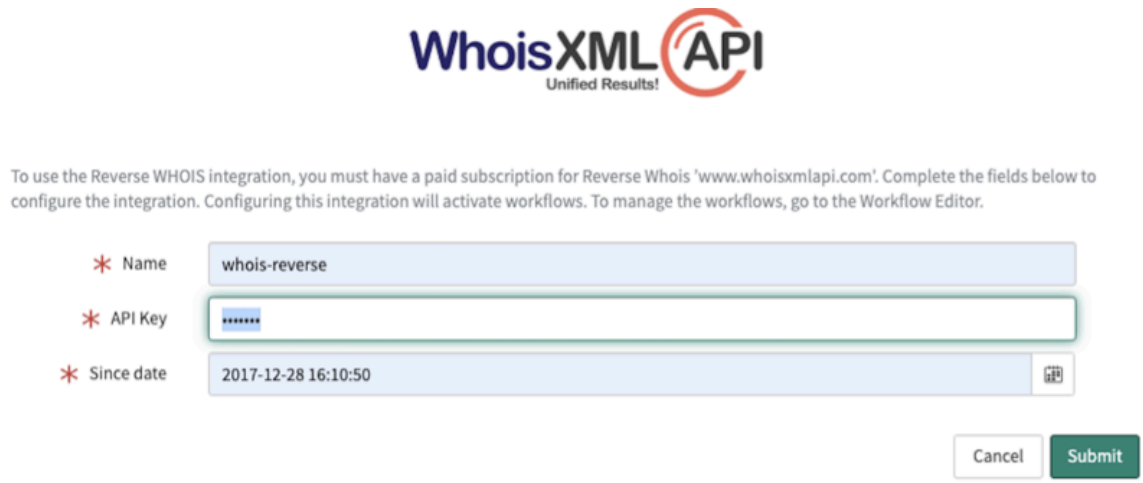


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. In the **Reverse Whois API Configuration** dialog box, enter the API key you obtained from the Whois XML API website.
6. Choose one option in the following table to filter domain lookups for your search terms.

Description	Setting
Your search includes all domains, active and expired, that were registered after the Since date for the search terms you enter. **This is the recommended setting.**	**Since date**: Date entered in yyyy-mm-dd for mat. For example, `1991-06-01` for June 1, 1991.
Your search includes all active domains for the search terms you enter.	**Since date**: Field cleared.

These configuration settings remain saved until you change them and apply to all Reverse Whois API searches.



7. Click **Submit**.
   Configuration is successfully completed unless an error message is displayed.

Trouble?
If an error message is displayed, the API key may be invalid.

Error message

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Optional) Install and configure Whois

Install the Whois plugin to provide additional enrichment information on your domain lookups from the Reverse Whois API. This lookup provides additional enrichment data on the domain, such as the registration date, name of registrar, and country of origin.

Before you begin

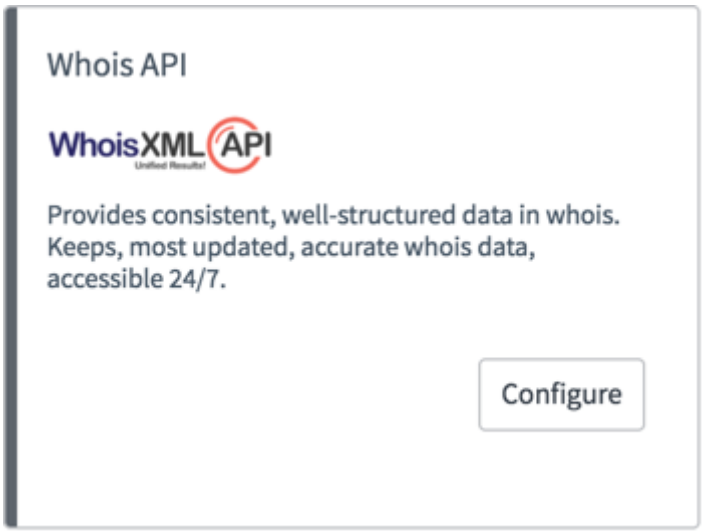
1. If you have not requested entitlement for the application, see Get entitlement for a Security Operations product or application for the Whois application from the ServiceNow Store.
2. Obtain credentials for the Whois API key from the product website: WHOIS API website.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

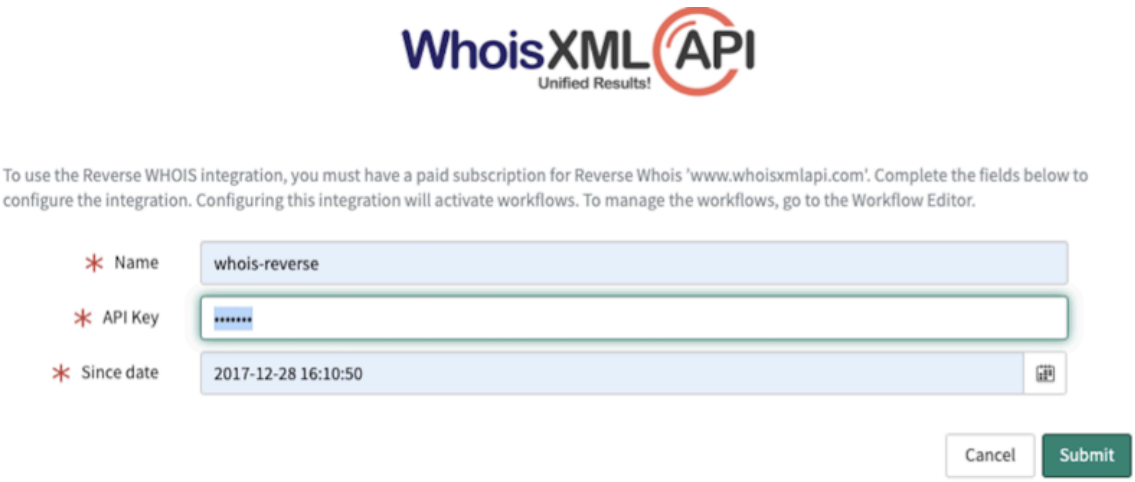
Role required: admin

Procedure

1. If you have not installed the application, see Install a Security Operations integration and follow the steps to install it.
2. After the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the Whois API tile.
3. Click **Configure**.



4. In the **Whois API Configuration** dialog box, enter the API key you obtained from the product website.



5. Click **Submit**.
   Configuration is successfully completed unless an error message is displayed. You can now run enrichment lookups on the domains returned from the Reverse Whois integration.

Trouble?

If an error message is displayed, the API key may be invalid.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Troubleshooting

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Initiate the lookup for Reverse Whois

Initiate domain lookups using search terms in observables that you manually attach to a security incident record.

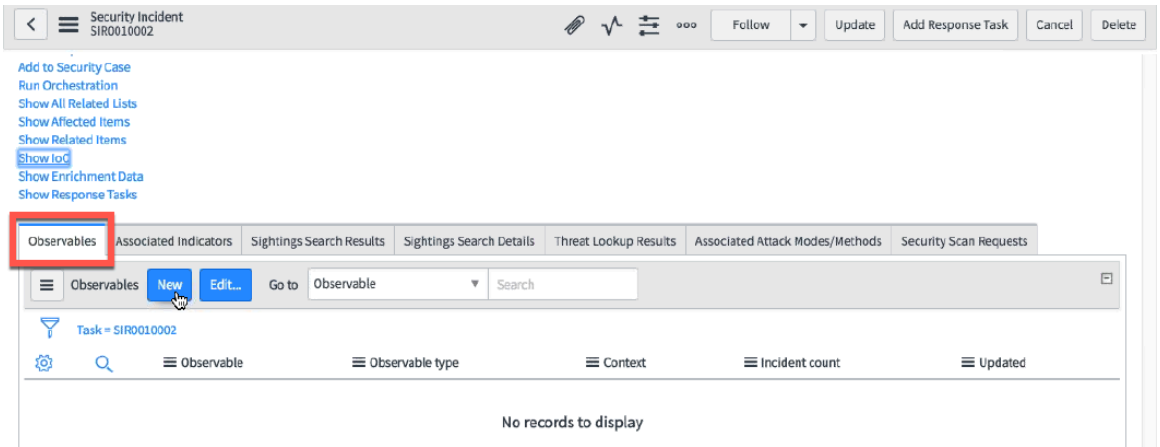
Before you begin

Role required: sn_si.analyst

Procedure

1. If not open, navigate to **Security Incident** > **Incidents** > **Show All Incidents** and open the security incident you are working with.
2. At the bottom of the record, click the **Show IoC** related link to display the Observables tab.

> **Note:** The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. If you do not see tabs on the security incident, in the upper-right corner of the banner frame, click the **Settings** gear icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.

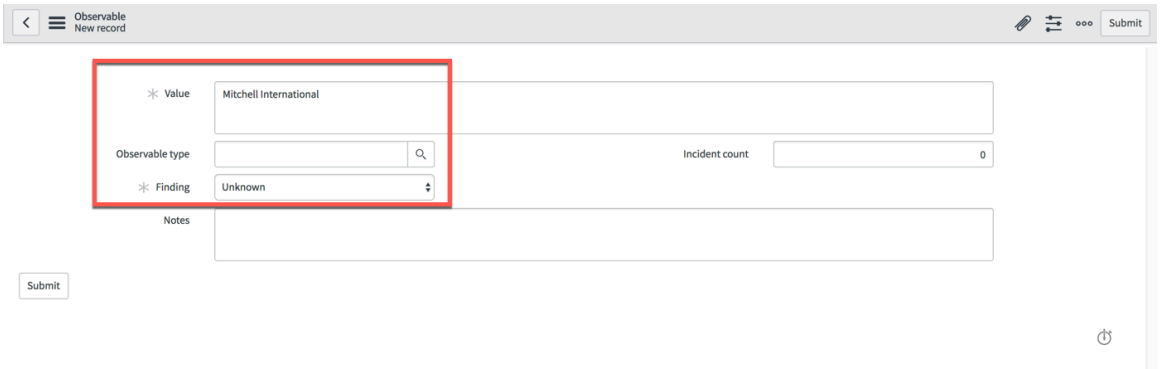


3. On the Observables tab, click **New**.
4. Fill in the fields.

Required fields on the new record

Field	Description
Value	Unique search term for a domain.
Observable type	This field is automatically cleared.
Finding	This field is automatically set to **Unknown**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.
   You are returned to the security incident record and the flow initiates the lookup.

What to do next
Verify the lookup results on the security incident. See Verify expected results for Reverse Whois.

Verify expected results for Reverse Whois

Enrichment results are displayed on the **ReverseWhois Domains** tab at the bottom of the security incident record. Locate the lookup results to verify that the lookup ran successfully.

Before you begin
Role required: sn_si.analyst

Procedure
1. If not already open, navigate to **Security Incidents** > **Incidents** > **Show All Incidents** and locate the security incident you are working with.

   System — Automation activity • 2024-06-11 20:44:18
   Flow execution started: Security Operations Integration - Enrich Observable V1

   After the application is configured and you have attached an observable, the flow launches automatically. The work notes on the security incident record display the execution and completion status of the lookup.

   System — Automation activity • 2024-06-11 20:44:30
   Flow execution completed: Security Operations Integration - Enrich Observable V1

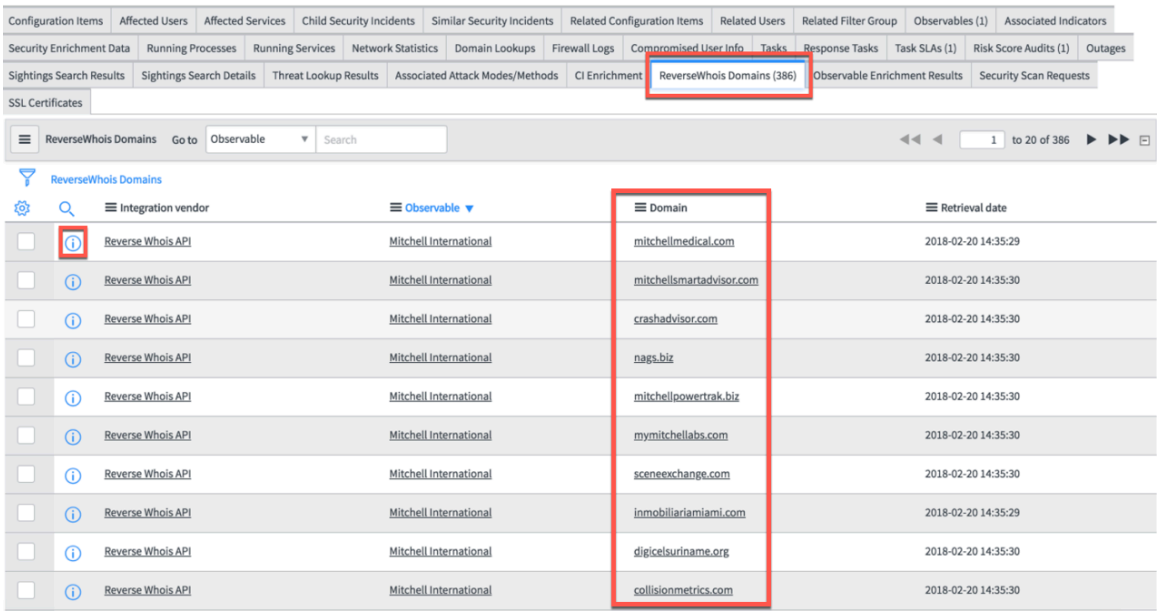
2. If you cannot verify that the lookup ran successfully, review the work notes for more information on how to proceed.

   S System — Automation activity • 2024-06-28 11:02:21
   Integration flow execution completed: Security Operations Integration - Enrich Observable V1. The following error's occurred:
   EX0002320 Completed Reverse WHOIS Flow with errors.

3. Navigate to the bottom of the security incident and click the **Show All Related Lists** related link.

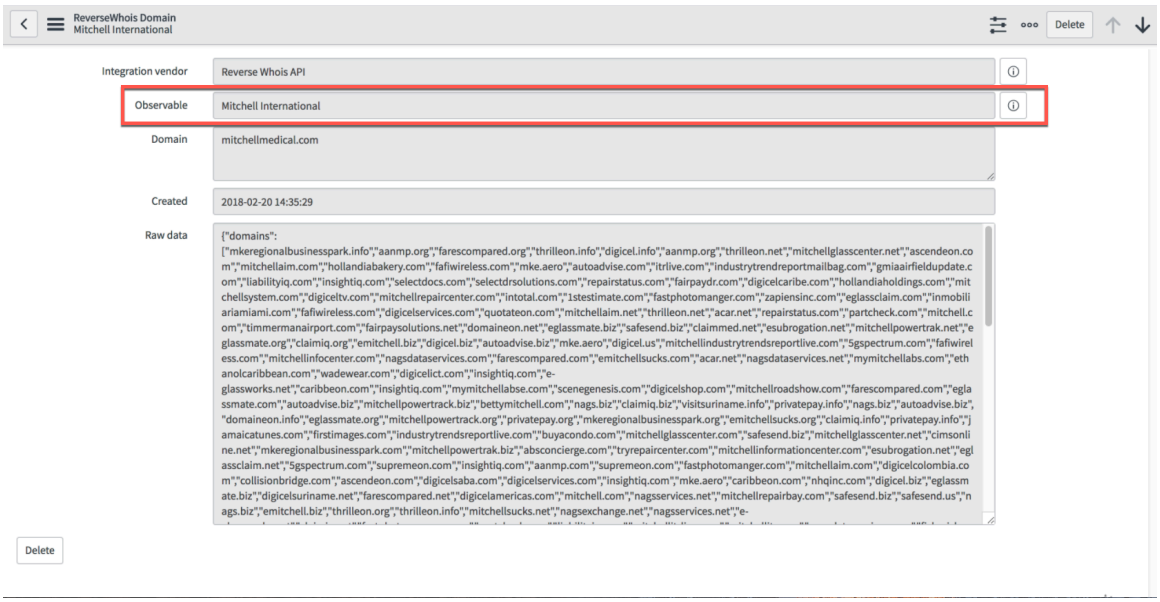
   Note: For the filtered lookup results shown in the following figure, the configuration settings in the Reverse Whois API configuration tile were saved with **1991-06-01** entered in the **Since date** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Enrichment results are displayed on the **ReverseWhois Domains** tab. The active domains for this observable are displayed in the **Domain** column.

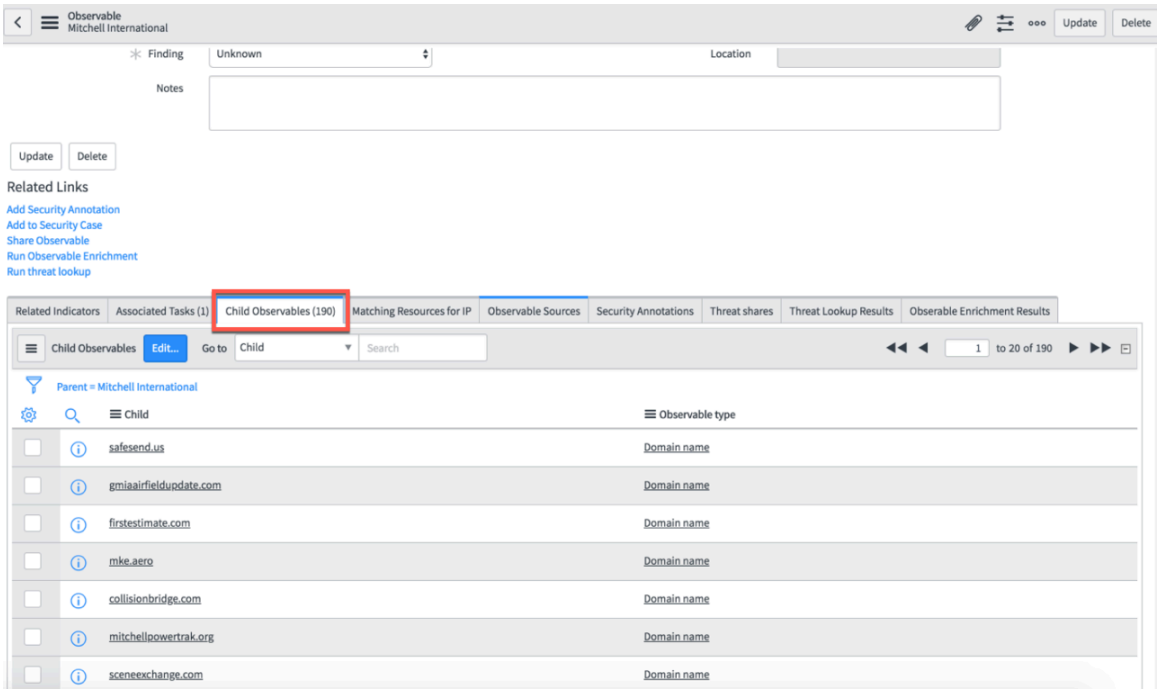
4. Click the blue information icon next to an item then click **Open record** in the dialog box that is displayed.



The record is displayed with enrichment details, including the raw data.

5. Navigate back to the security incident, and with the **ReverseWhois Domains** tab selected, click an observable in the **Observable** column to open a record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The child observables are displayed on the **Child Observables** tab on the Observable record. The child observables are generated only if the Reverse Whois application has returned domains.

Trouble?

If the lookup does not successfully complete, verify that the search terms you entered are supported by the integration. Review the work notes for more information.

What to do next

For more enrichment data on the domain lookup results, you can run the Whois integration to perform enrichment lookups on the child observables returned by the Reverse Whois integration. This enrichment data on the child observables includes information on registration date, name of registrar, and country of origin.

(Optional) Run enrichment lookup and verify expected results for Whois

Run the Whois integration to perform enrichment lookups on the domains returned from the Reverse Whois integration.

Before you begin

Verify that you have installed and configured the Reverse Whois and Whois plugins. Perform these steps only after you have run the domain lookup with the Reverse Whois plugin successfully.

Role required: sn_si.analyst

About this task

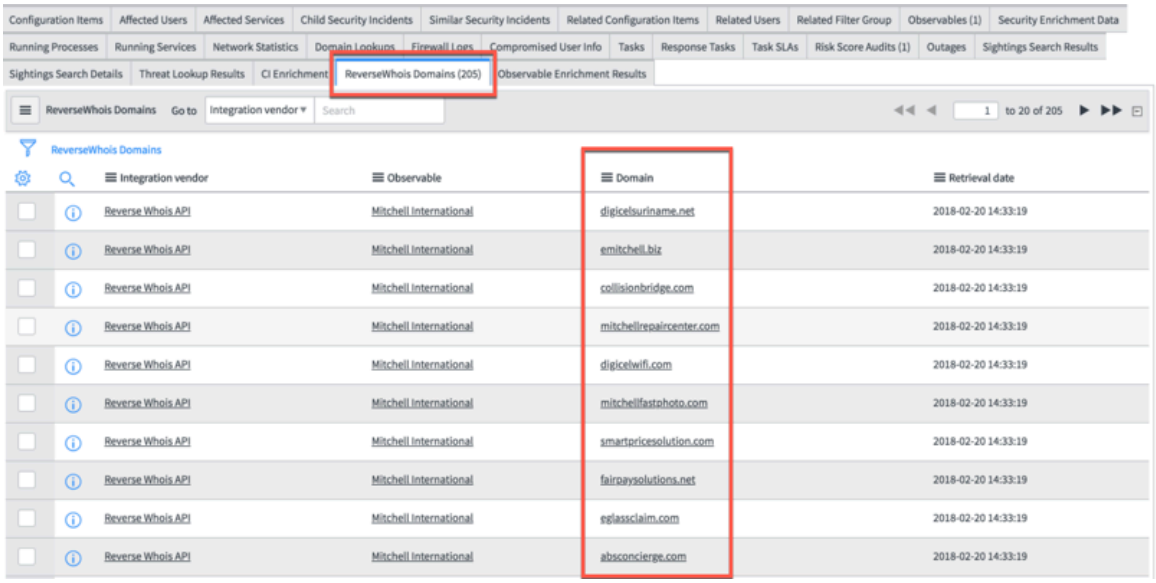
Results are displayed on the **Observable Enrichment Results** tab on the Observable record.

Procedure

1. Navigate to **All** > **Security Incidents** > **Incidents** > **Show All Incidents** and locate the security incident you are working with that has run the domain lookup successfully.
2. Open the record and click the **Show All Related Lists** related link.

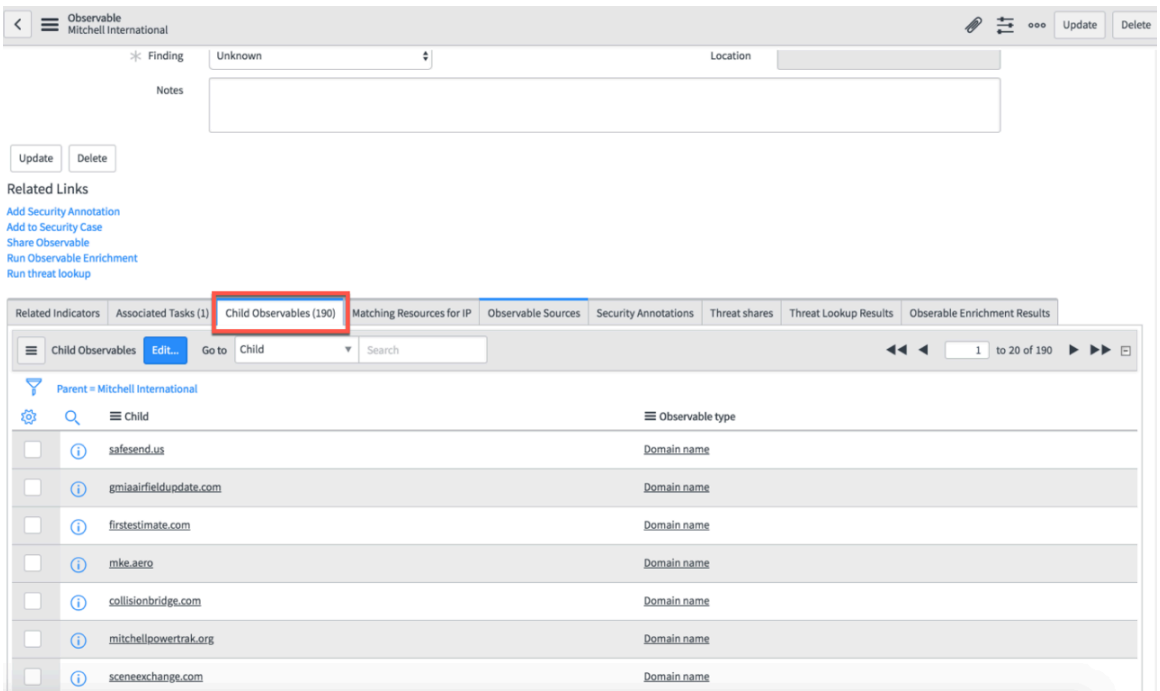
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the **Reverse Whois Domains** tab at the bottom of the record.



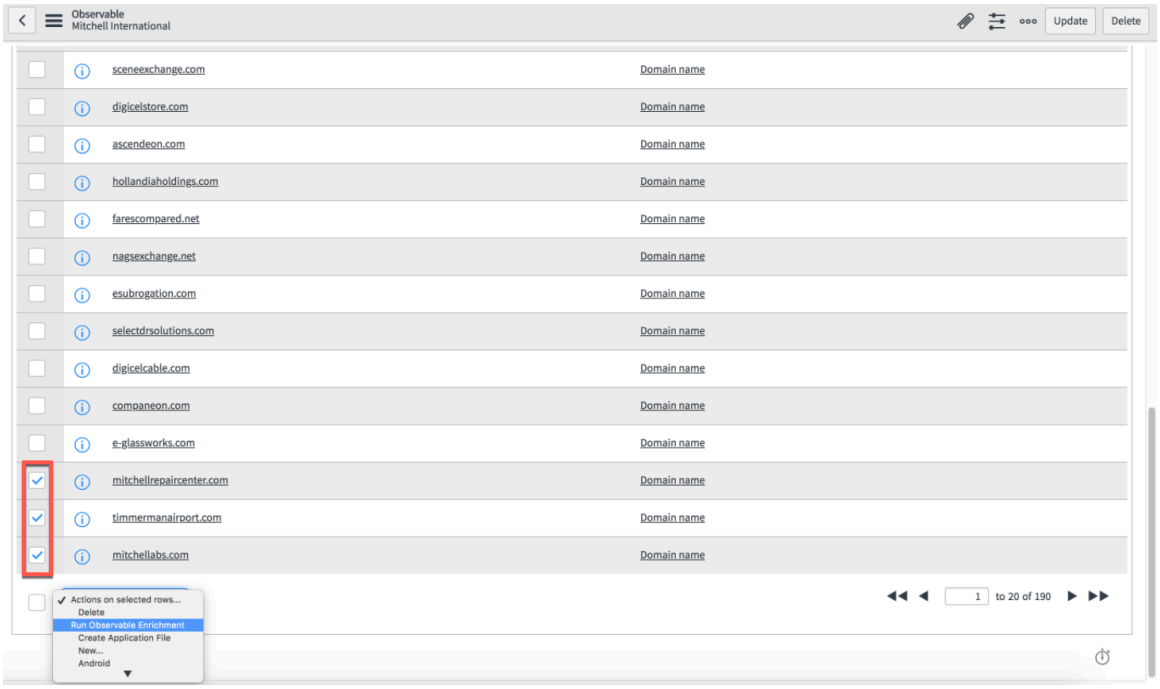
In the **Domains** column, the list of returned domains is displayed.

4. In the **Observable** column, click an observable.
On the **Child Observables** tab, the child observables are displayed. The child observables are generated only if the initial scan of the observable by the Reverse Whois application returned domains.



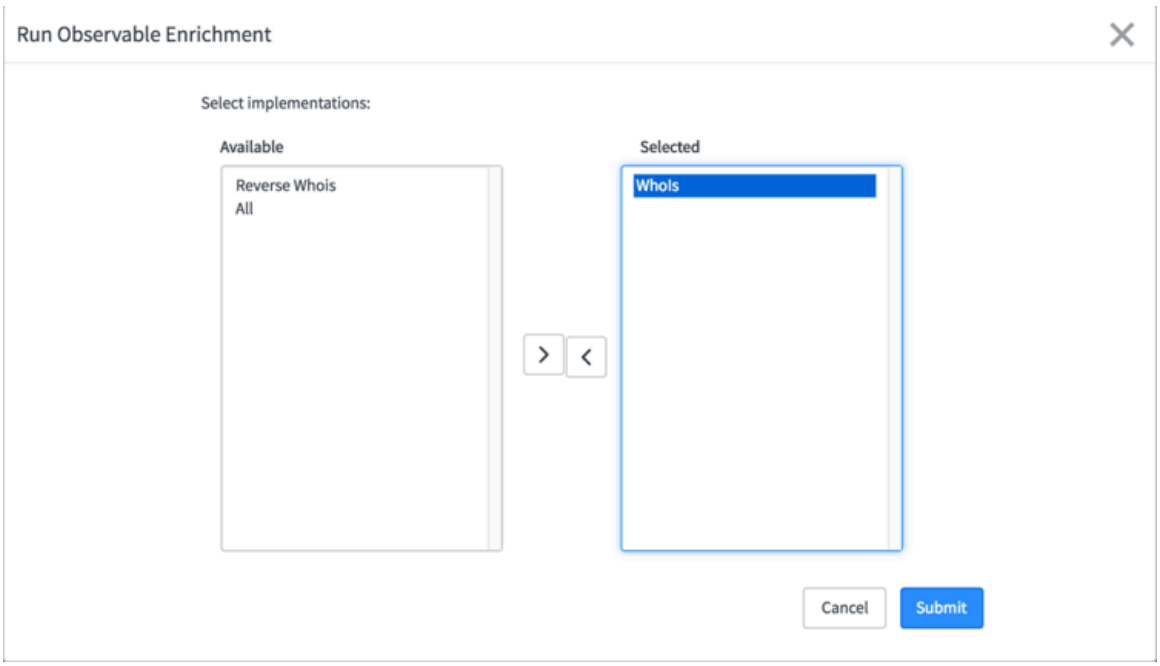
5. Select the child observables you want to run the observable enrichment on, and, in the **Action on selected rows** choice list, select **Run Observable Enrichment**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Run Observable Enrichment** dialog box is displayed.

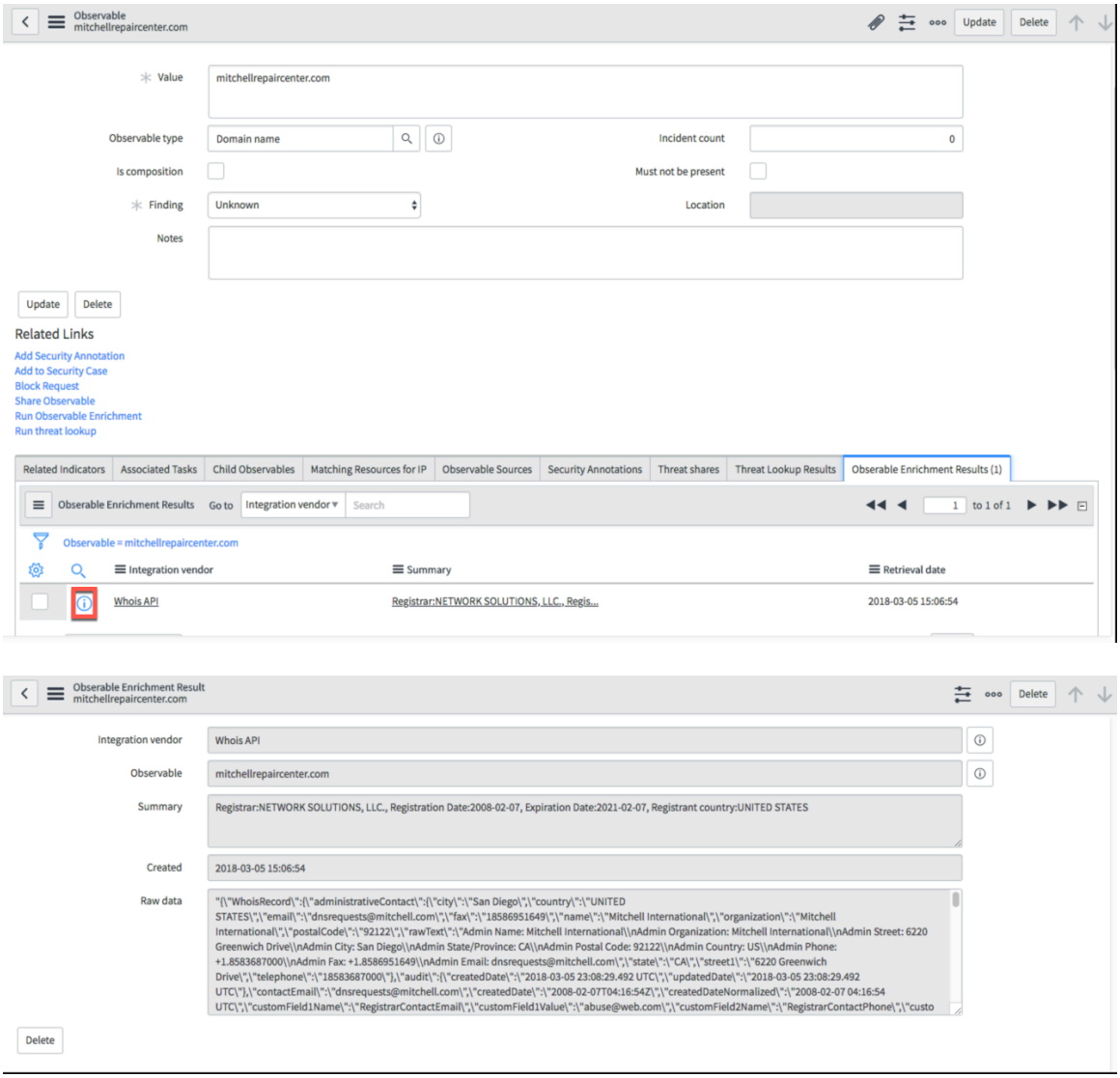
6. Move the Whois integration from **Available** to **Selected** and click **Submit**.



Results are displayed on the **Observable Enrichment Results** tab of the observable record.

7. Click the blue information icon then click **Open Record** in the dialog box that is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



More information and raw data related to the original domain lookup is displayed, such as the registration date, name of registrar, and country of origin.

Trouble?
If you cannot locate child observables or enrichment results, verify that the Reverse Whois integration ran successfully and returned domains. Also, refer to the work notes on the record for more information.

Related topics

- Install and configure Reverse Whois
- Verify expected results for Reverse Whois

RISKIQ and WHOISIQ integration

With the integration of RISKIQ and WHOISIQ APIs with the ServiceNow AI Platform® Security Operations product, security analysts are provided with additional enrichment data and insight into the validity of websites.

The RISKIQ SSL Certificates API performs lookups on SSL Certificates, which include details on the issuing certificate authority, organizations who request certificates, the entity certificates are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

issued to, and the domain. SSL certificate lookups are performed automatically when security incidents are created.

The RISKIQ WHOISIQ API performs lookups on other observable types, such as domain, email, nameserver, organization, address, and phone number. URL and domain observables are enriched automatically when security incidents are created.

The integration requires the Security Incident Response and Threat Intelligence products.

Supported observables for RISKIQ and RISKIQ WHOISIQ

The RISKIQ API supports automatic SSL certificate lookups on IP address, file hash, Certificate Serial Number, domain, and URL observables. URL and domain observables are enriched automatically with the WHOISIQ API. For observable enrichment on other types of observables with the WHOISIQ API, create observables and run lookups manually from the Observables table.

Supported observables

The following table lists the type of APIs used in this integration, and the observables each API supports. The table also indicates whether a lookup occurs automatically when security incidents are created, or if the lookup is run manually from the Observables table.

Supported observables and lookup

API	Supported observables	Lookup (automated or manual)
RISKIQ SSL certificate API	• IP address • File hash (certificate thumb print). See the following figure for an example of a file hash. • Certificate Serial Number, or Serial Number. This string is a unique ID for the entity. See the following figure for an example of a certificate serial number. • Domain (`www.site.com`, or `site.com`) • URL **Note:** automatic scans are run for the URL format using the `https://` protocol, for example, `https://example.com/index.html`	Automated lookup when incidents are created. Results are displayed on the **SSL Certificates** tab of the security incident record.
RISKIQ WHOISIQ API	• Domain • URL	Automated lookup when incidents are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supported observables and lookup (continued)

API	Supported observables	Lookup (automated or manual)
		Results are displayed on the **Observable Enrichment Results** tab on the security incident record.
RISKIQ WHOISIQ API	• Email address • Organization name • Phone number • Mailing address	Manual lookup is run from the Observables table. Results are displayed on the **Observable Enrichment Results** tab on the Observable record.

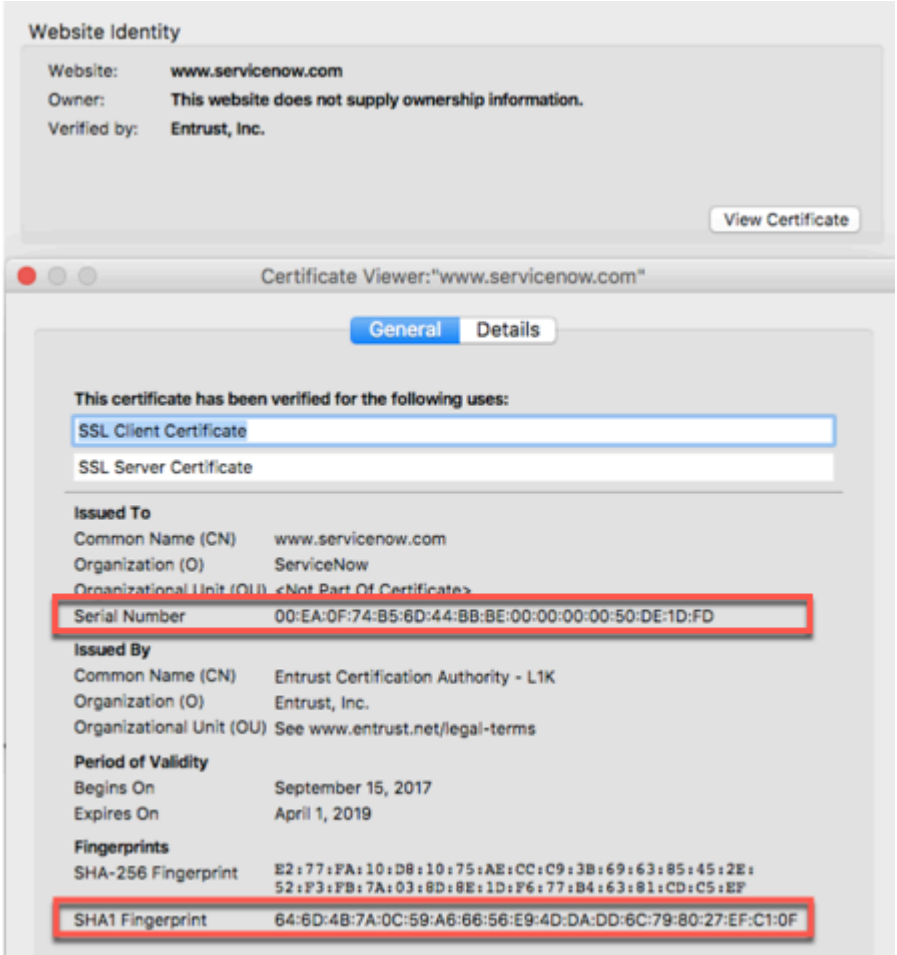
Example of a file hash and certificate serial number

This figure shows an example of the file hash and certificate serial number observables used for the SSL certificate lookups for this integration. The file hash refers to a SHA-1fingerprint. This value is displayed in your ServiceNow AI Platform instance without the colon separators. For example, 646D4B7A0C59A66656E94DDADD6C798027EFC10F.

The certificate serial number observable refers to the unique ID or serial number for the entity. This value is also displayed without the colon separators. For example, 00EA0F74B56D44BBBE0000000050DE1DFD.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File hash and certificate serial number



Install and configure RISKIQ and WHOISIQ

Before you run the integration on your instance, complete the installation and configuration steps so the RISKIQ and WHOISIQ applications properly integrate with ServiceNow AI Platform Security Operations.

Before you begin

Role required: admin, RISKIQ and WHOISIQ admin.

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Setup task	Description
Verify that you have assigned the required roles.	The following roles are required for installation, configuration, and verification of expected results: • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees configuration and verifies expected results. This role also has access to the Security Operations module

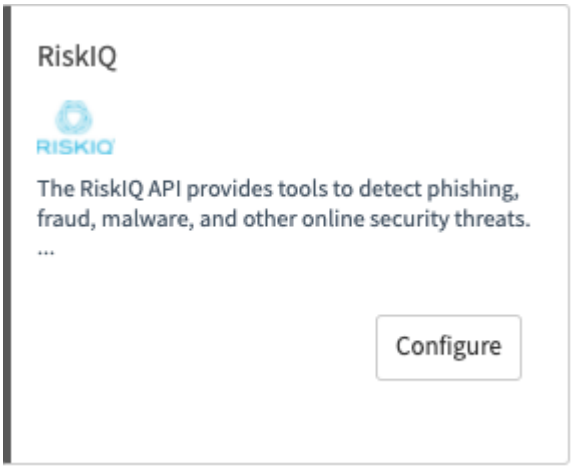
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
	and assigns the Security Incident Analyst (sn_si.analyst) role. • The Security Incident Analyst (sn_si.analyst) works with Security Incident records.
Obtain an Username and API key.	Visit the website for information on the API key and how to create an account: RISKIQ website. The configuration requires that you enter the API key.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Madrid and later release requirements For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

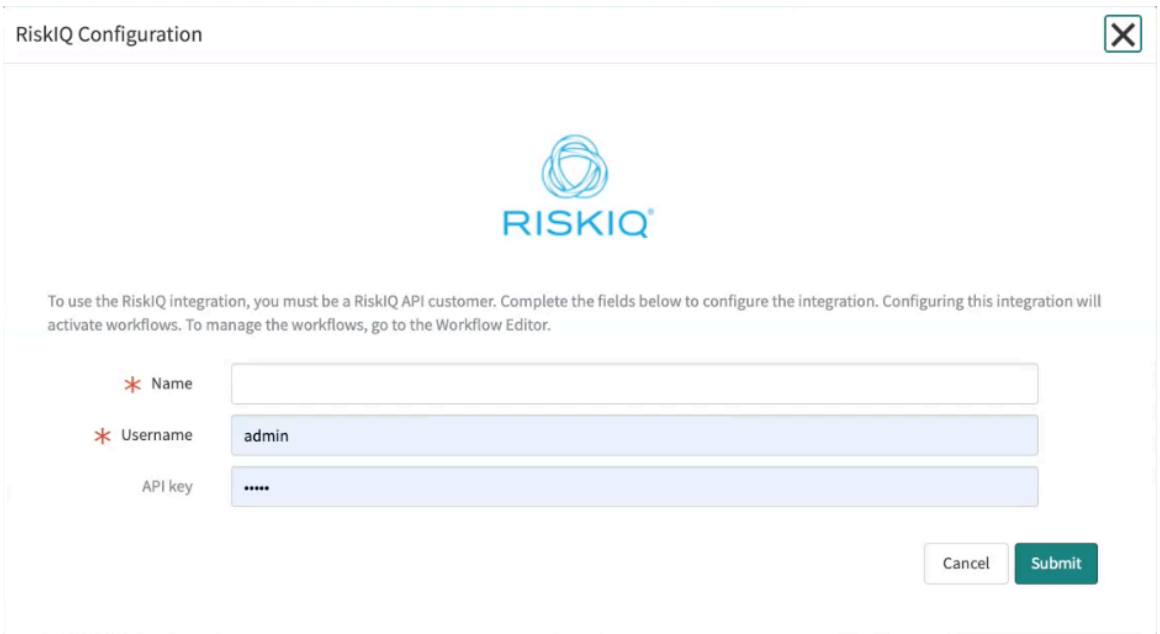
Procedure

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
2. Once the installation completes, navigate to **Security Operations** > **Integrations** > **Integrations Configurations** and locate the API tile.
3. Click **Configure**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



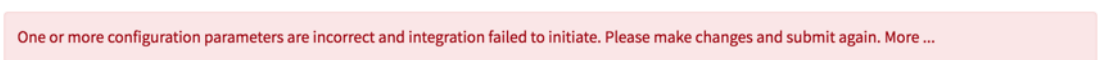
4. In the RiskIQ Configuration dialog box that is displayed, enter the **Username** and **API key**.



5. Click **Submit**.
6. Verify successful configuration.
   When configuration is successfully completed, the Security Integrations page with the integration tiles is displayed.

Trouble?
If an error message is displayed, the Username or API key may be invalid. Verify that your username and API key are correct:

Troubleshooting



Verify expected results for RISKIQ SSL certificate lookups

When a security incident generates observables for URLs, domains, IP addresses, certificate file hashes (SHA-1 fingerprint), and certificate serial numbers, security incident analysts use the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

SSL certificate lookup results to verify sites have certificates that have been issued by a trusted public Certificate Authority (CA).

Before you begin
Role required: sn_si.analyst

About this task
For supported observables, the ServiceNow AI Platform scans for the most recent occurrence of URLs, domains, IP addresses, certificate file hashes (SHA-1 fingerprint), and certificate serial numbers. These are possible outcomes from the scan:

An exact match is found

A valid issuer of an SSL certificate is listed on the Security Incident record.

No certificate results are found

No results are listed on the Security Incident record.

An exact match is found for a self-signed, or internally generated certificate

Results for an internally generated SSL certificate are displayed on the Security Incident record.

An exact match is not found for a primary SSL certificate

A lookup value returns multiple entries and a primary certificate cannot be identified. A summary message is displayed on the Security Incident record.

Procedure
1. To view the observables and verify lookup results, open the security incident record you are working with and locate the work notes.

   Example
   To illustrate examples for the possible lookup results for this integration, suppose that a security incident was generated with the following observables:

   - community.servicenow.com
   - invalidsubdomain.servicenow.com
   - mail.dgnetworks.com
   - servicenow.com

   Observables and location of lookup results

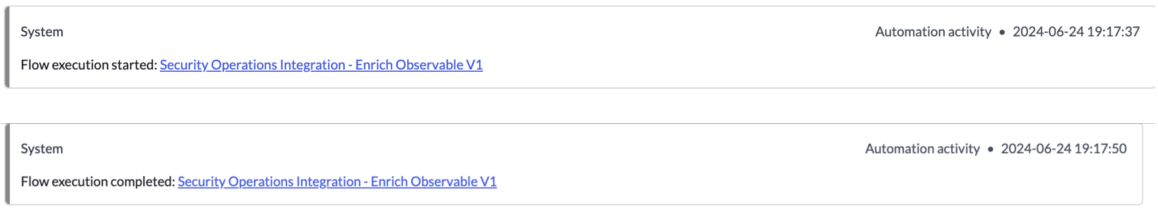
Observable (example)	Scan results	Description and location
community.servicenow.com	Found certificate with a SHA1 hash.	An exact match is found, and a valid issuer of an SSL certificate is listed. Results for the exact match are displayed on the **SSL Certificates** tab on the security incident record.
invalidsubdomain.servicenow.com	No certificates found.	A summary that indicates no certificate results were found is displayed on the **Observable Enrichment Results** tab on the security incident record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Observable (example)	Scan results	Description and location
mail.dgnetworks.com	Found certificate with SHA1 hash.	An exact match is listed for a self-signed, or internally generated certificate. Results are displayed on the **SSL Certificates** tab on the security incident record.
servicenow.com	Search returned 138 certificates, and a single primary certificate could not be identified.	An exact match is not found for a primary SSL certificate, because a lookup value returns multiple certificates. A summary that indicates no primary certificate was found is displayed on the **Observable Enrichment Results** tab on the security incident record.

After the application is configured, the flow launches automatically. The lookup status and the observables are displayed in the work notes.

2. Verify that the lookup ran successfully.



Trouble?
If you cannot view expected results, verify that the observable is supported by the SSL certificate lookup for the integration.

Related topics

Supported observables for RISKIQ and RISKIQ WHOISIQ

RISKIQ SSL certificate lookups that return an exact match

RISKIQ SSL certificate lookup results for an exact match are displayed on the **SSL Certificates** tab on the security incident record. An exact match provides a valid certificate authority name, which helps a security incident analyst determine the validity of a website.

Example: Exact match for a valid SSL certificate

The following example shows a valid issuer of an SSL certificate from an exact match in the lookup results. Follow the steps to view the results and raw data.

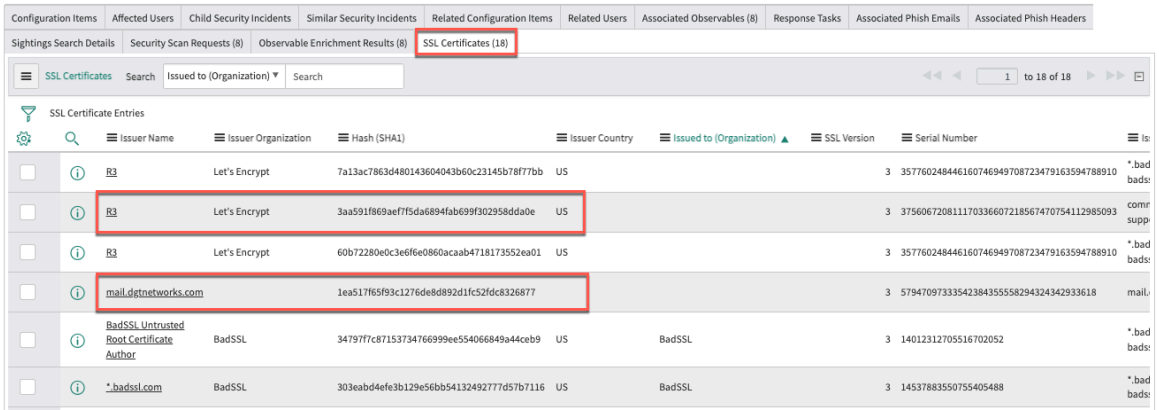
Note: The figures in the following examples are shown with the **Tabbed forms** setting active in the System Settings. If your screen does not match the view shown below, follow the steps to set tabbed forms.

1. In the upper-right corner of the banner frame, click the Settings icon.
2. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. In the security incident record, click the **SSL Certificates** tab.

SSL Certificates tab



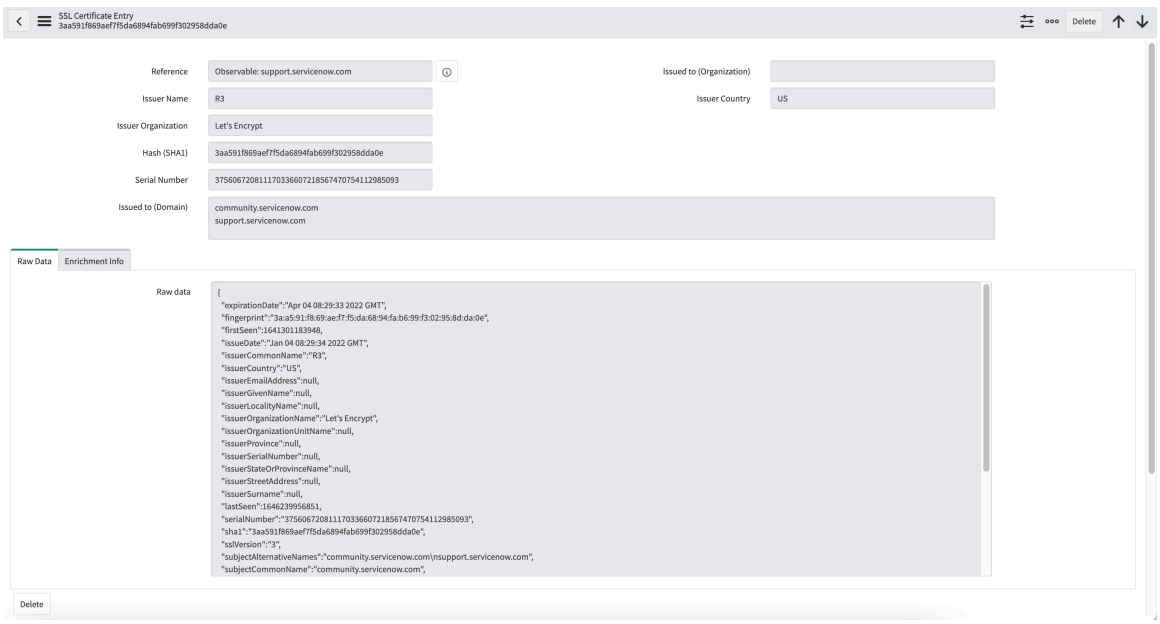
Information about the certificate issuer's name, the issuer's organization, and who the certificate is issued to (Organization) is displayed along with other data.

18 items are displayed in the **Issuer Name** column. The second item (R3) provides a valid certificate authority name (`Let's Encrypt`) in the **Issuer Organization** column.

No information in the **Issuer Organization** and **Issued to** columns is displayed for the second item (`mail.dgtnetworks.com`).

2. Click the second item in the **Issuer name**column, which is (**R3**) to open the entry record. Alternatively, click the information icon next to the item followed by **Open record**.
3. Select the **Raw Data** tab.

Raw Data tab



The SSL Certificate Entry record includes the observable in the **Raw Data** tab under the **Entity name** column, as well as other data.

Note in the **Category** column, the `Subject`, and `Issuer` correspond to recognizable entities in the **Entity name** column. The issuer of this certificate is most likely valid and from a trusted public certificate authority. Also note, the `Subject`, and `Issuer` are different entities. These separate entities indicate that the certificate is not an internally signed certificate from an unknown certificate authority.

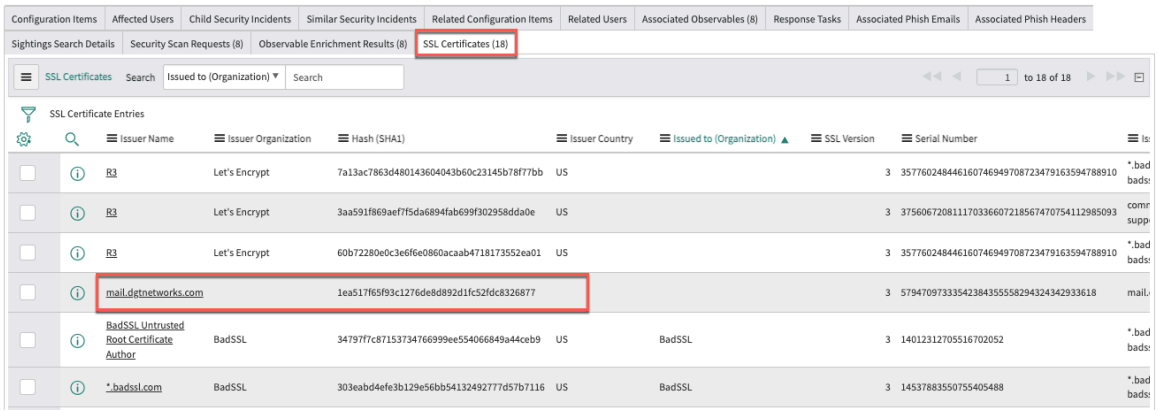
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example: Exact match for a self-signed SSL Certificate

The following example shows results for a self-signed SSL certificate from the lookup. Follow the steps to view the results and raw data.

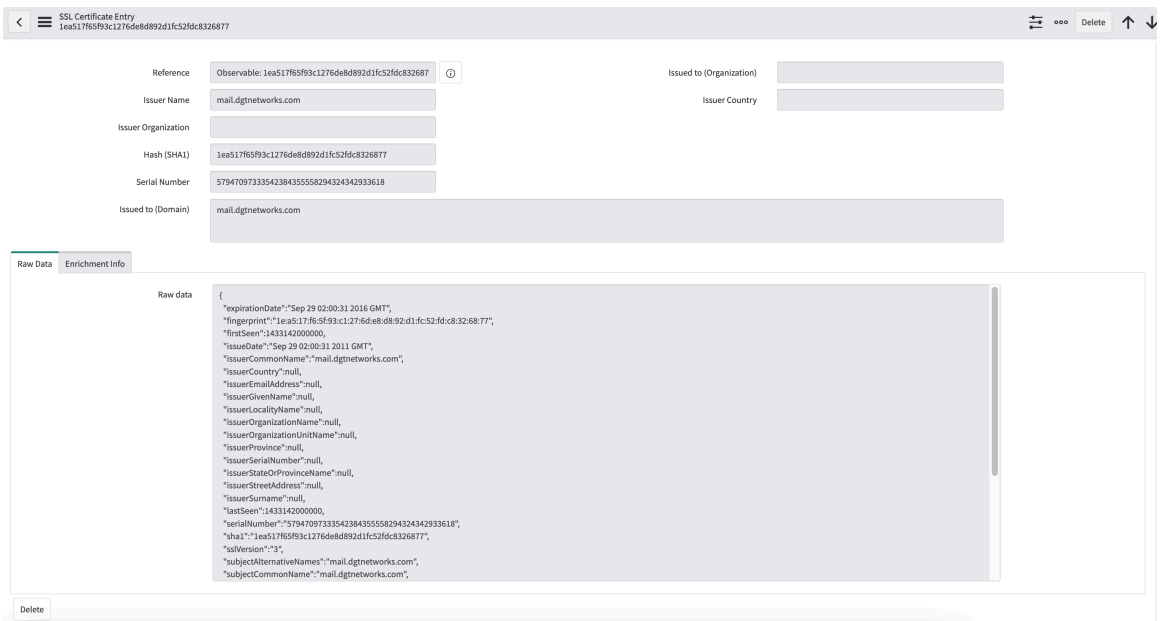
1. Navigate back to the security incident record. In the **Issuer Name** column, click the other item (**mail.dgtnetworks.com**).

SSL Certificates tab



2. On the open record, select the **Raw Data** tab.

Raw Data tab



The **Category** column indicates the `Issuer` (`mail.dgtnetworks.com` and `dgtsbs.DGTNetworks.local`) are not trusted public certificate authorities. Also note the `Issuer` and `Subject` are the same entity (`dgtsbs.DGTNetworks.local`), and each contains the name of the observable (`dgtsbs`). This certificate is possibly a self-signed certificate. Self-signed certificates may warrant further investigation, as these certificates are not issued by a known certificate authority.

RISKIQ SSL certificate lookups that return multiple certificates or no certificates

A security incident analyst can use multiple SSL certificate results to determine whether a site is part of a common, recognizable entity. No SSL certificate results may indicate sites with obscure or suspicious names have no trusted certificates. Lookup results for observables that do not

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

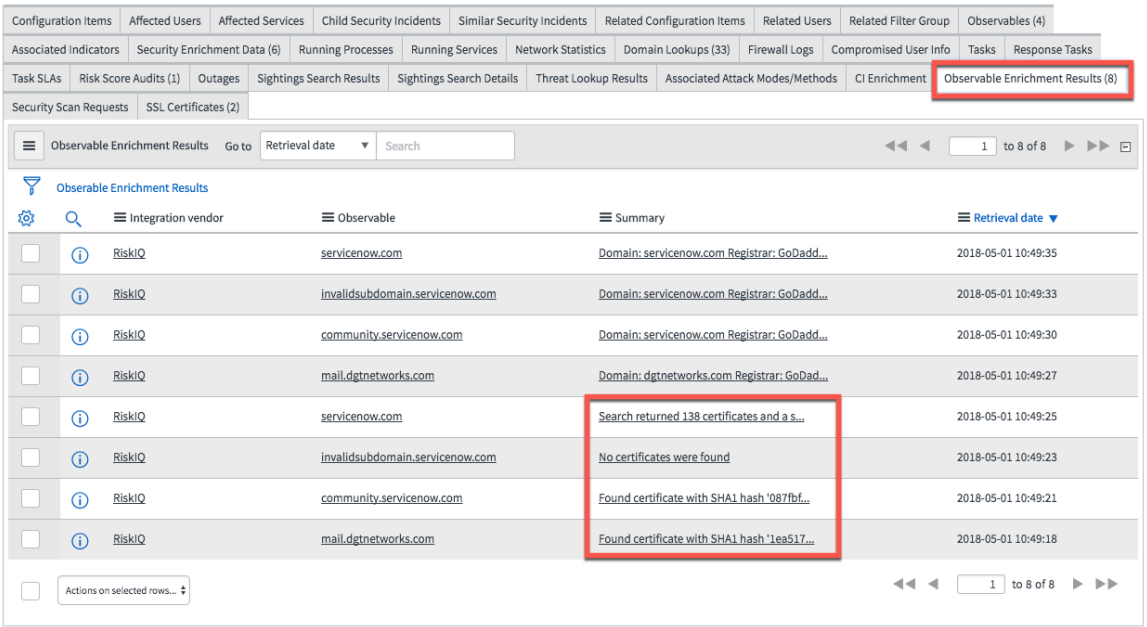
return SSL certificates, or that return multiple SSL certificates, are displayed on the Observable Enrichment Results tab on the security incident record.

Example: No SSL certificate results or multiple SSL certificate results

Follow the steps to view the results for observables that do not return SSL certificates, or that return multiple certificates.

1. In the security incident record, click the **Observable Enrichment Results** tab.

Observable Enrichment Results tab

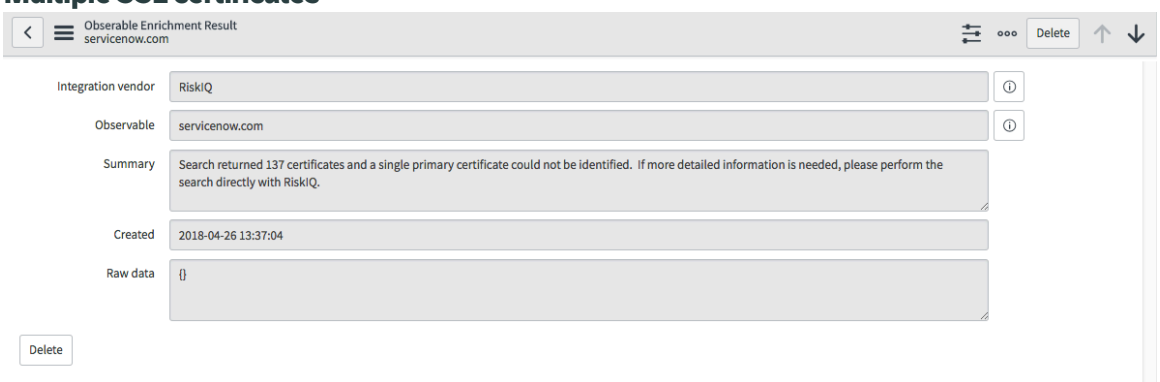


The observable enrichment results for the RISKIQ and WHOISIQ lookup are displayed.

In the **Observable** column, `servicenow.com` corresponds to the `Search returned 138 certificates` message in the **Summary** column. Similarly, `invalidsubdomain.servicenow.com` corresponds to `No certificates were found` in the **Summary**column. These summaries indicate that multiple SSL certificates were found, and that no exact matches for SSL certificates were found, respectively.

2. In the **Observable** column, click **servicenow.com**.

Multiple SSL certificates



The summary message that is displayed on the record indicates that multiple results for SSL Certificates were returned for `servicenow.com`, and a primary SSL Certificate could not

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

be matched. This message is often returned on lookups that include common domain names, such as `servicenow.com`.

If you require more information on a common domain, you can perform the search directly with the RISKIQ API.

3. Navigate back to the **Observable Enrichment Results** tab, and in the **Observable** column, click **invalidsubdomain.servicenow.com**.



Note:

- If no SSL certificates are found for the current observable, then the Summary field displays the message, No `certificates were found`.
- If no active SSL certificates are found for the current observable, then the Summary field displays the message, No `active certificates were found`.

Verify expected results for WHOISIQ URL lookups

When a security incident generates observables for URLs or domains, the WHOISIQ API performs the observable enrichment automatically upon security incident creation. The lookup results are displayed on the **Observable Enrichment Results** and **SSL Certificates** tabs on the security incident record.

Before you begin

Note: The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings.

Role required: sn_si.analyst

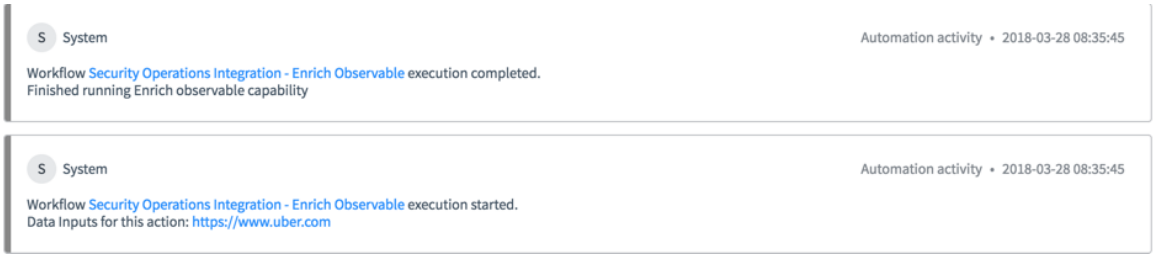
About this task

Observable enrichment results are displayed on the **Observable Enrichment Results** tab at the bottom of the security incident record. For supported observables, an SSL certificate search is also run and the results are displayed on the **SSL Certificates tab**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

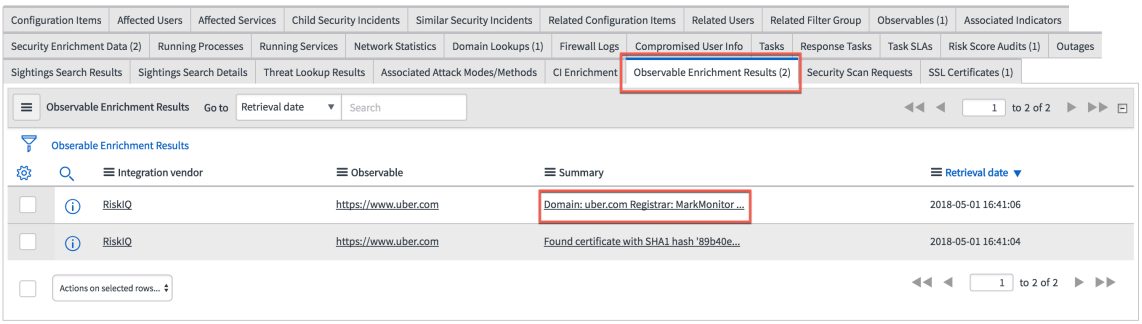
Procedure

1. Open the security incident record you are working with and verify that the lookup has run successfully in the work notes.



   Once the application is configured, the flow launches automatically upon incident creation. The execution and completion status of the lookup is displayed in the work notes in the Security Incident record.

2. If you cannot verify that the lookup ran successfully, review the work notes for more information on how to proceed.
3. On the open security incident, click the **Show All Related Lists** related link.
4. Click the **Observable Enrichment Results** tab to select it.
5. In the **Summary** column, click the first item, **Domain: uber.com Registrar: Markmonitor...**.

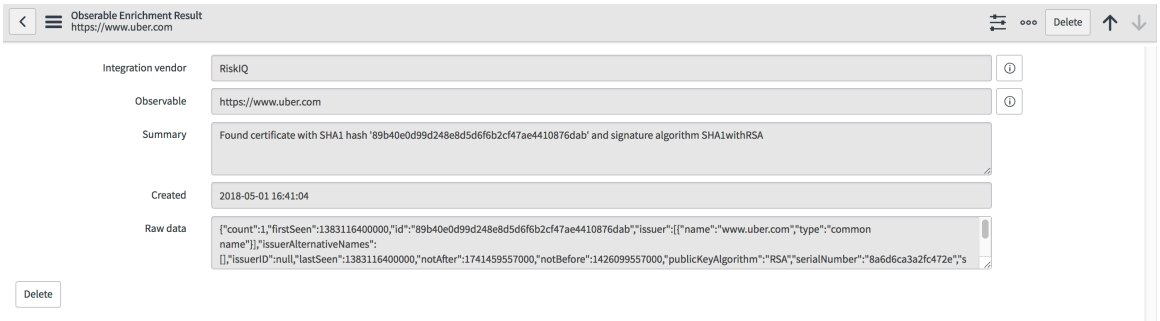




   The record that is displayed contains information about the domain.

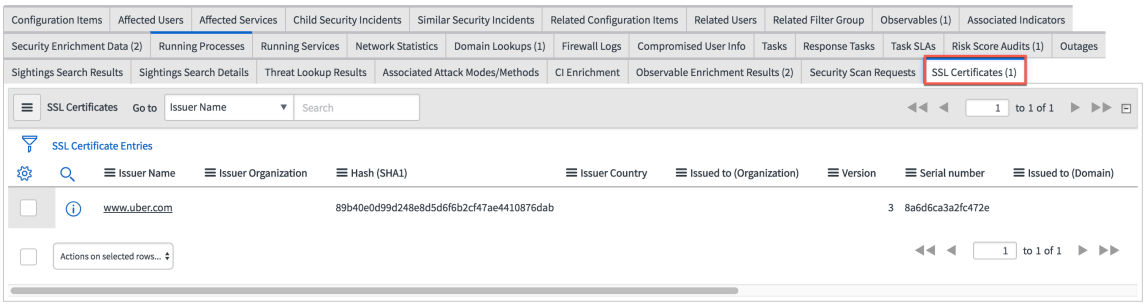
6. Navigate back to the **Observable Enrichment Results** tab, and, in the **Summary** column, click the second item, **Found certificate with SHA1 hash...**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



This record indicates that an SSL Certificate was found with a file hash.

7. Navigate back to the security incident record and click the **SSL Certificates** tab.



The SSL Certificate results for the file hash are also displayed here.

Trouble?

If you cannot view expected results, review the work notes. Also, verify the observable is supported for the lookup by the integration.

Related topics

Supported observables for RISKIQ and RISKIQ WHOISIQ

Create an observable for manual WHOISIQ lookups

Security incident analysts use information from observable enrichment with the WHOISIQ API to learn more about the email addresses, names, and phone numbers of organizations.

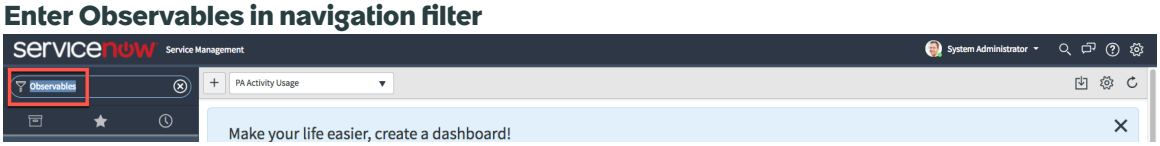
Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to **All** > **IoC Repository** > **Observables**.

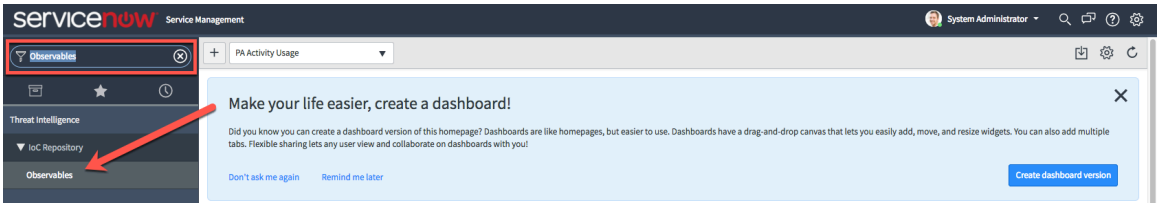
Enter Observables in navigation filter



Under the navigation panel, the Observables module is displayed.

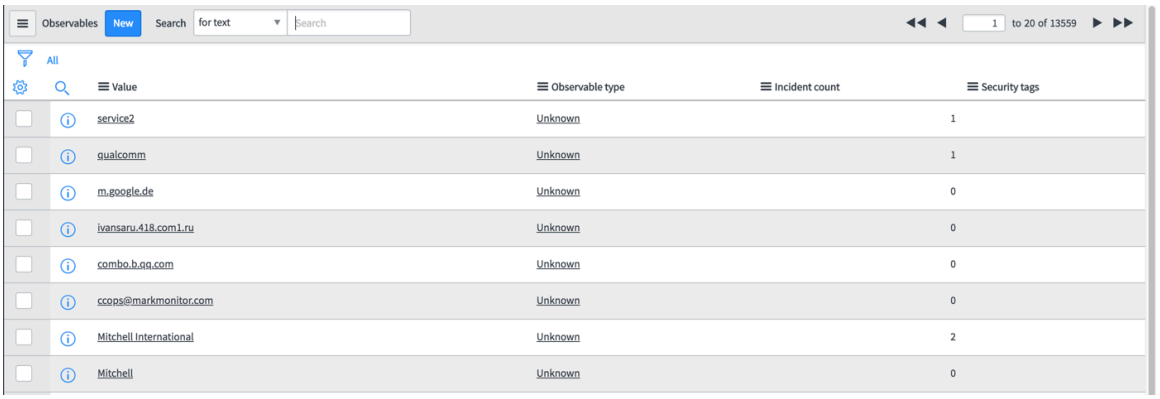
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Observables module



2. Click the **Observables** module to display the Observables list.

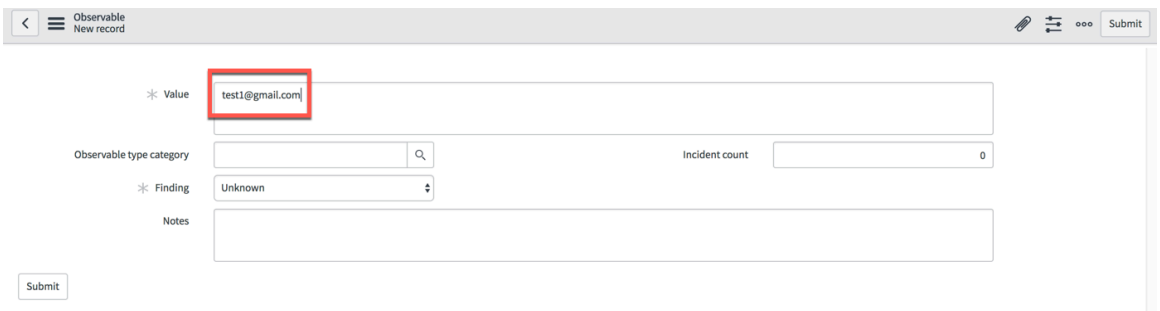
Observables list



3. Click **New** to create a new observable.
4. On Observable form, fill in the fields.

Field	Description
Value	Email address, organization name, phone number, or mailing address. For example, `test1gmail.com`
Observable type	The field is automatically cleared.
Finding	The field is automatically set to **Unknown**.

Create a new observable



5. Click **Submit**.
   You are returned to the Observables list. In the **Value** column, your new observable is displayed.

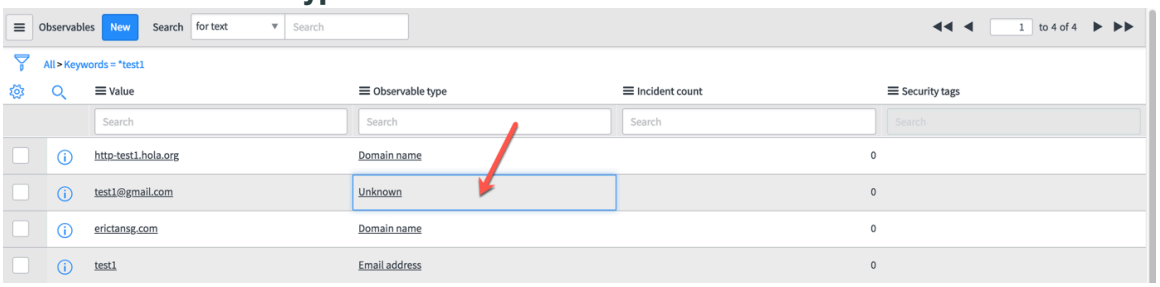
> **Note:** If you cannot locate your observable on the part of the list that is displayed, use the search functionality to find it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Edit the **Observable type** field to change the type from **Unknown** to **Email address** to match your observable.

   a. In the **Observable type** column, single-click to the right of the **Unknown** text to select it.

Select the Observable type field

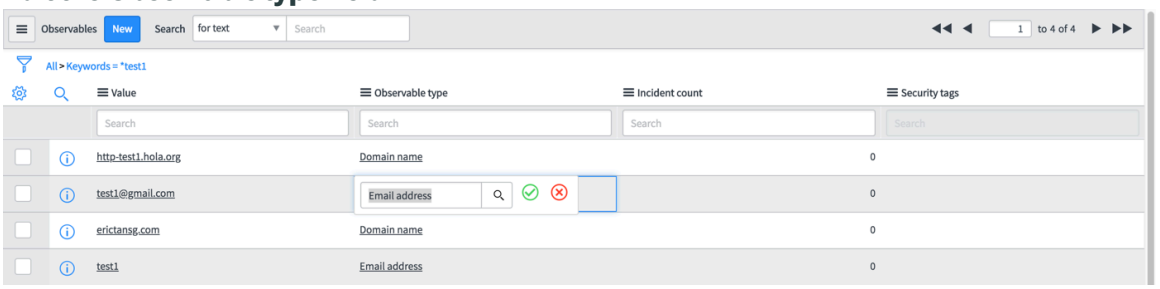


   The selected field is outlined in blue.

   b. With the field outlined in blue, double-click anywhere inside the highlighted field to open the editor.

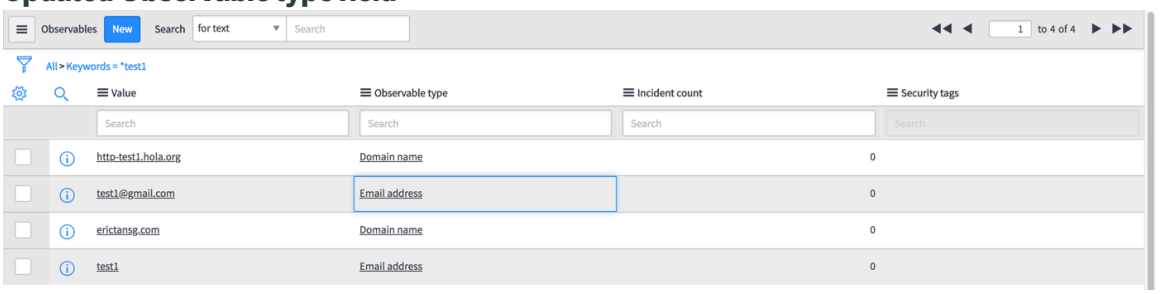
   c. In the field that is displayed, enter the observable type (`Email address`) and click the green check mark to save the value.

Edit the Observable type field



   In the **Observable type** column on the list, `Email Address` is displayed for your new observable.

Updated Observable type field



What to do next

If you have created and edited an observable for lookup, run the observable enrichment lookup from the Observable record with the WHOISIQ API.

Verify expected results for manual WHOISIQ lookups

Run a manual lookup on an observable when it does not automatically generate a security incident. For observable enrichment lookups using the WHOISIQ API for email addresses,

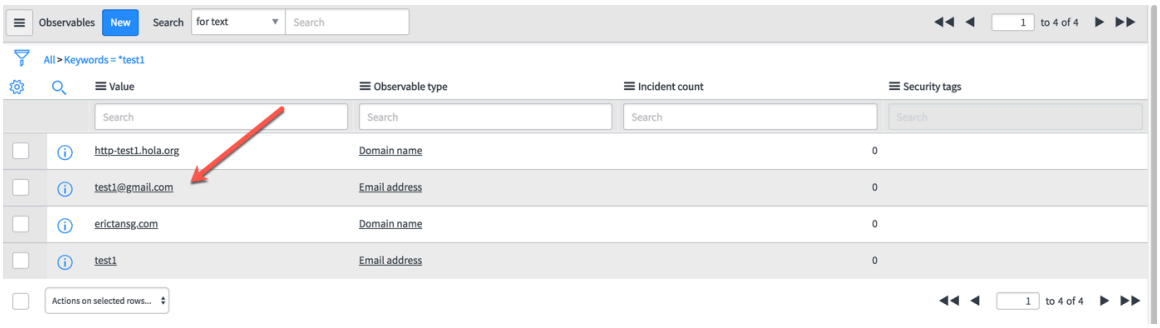
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

organization names, phone numbers, or mailing addresses, initiate the lookup manually from the Observables table.

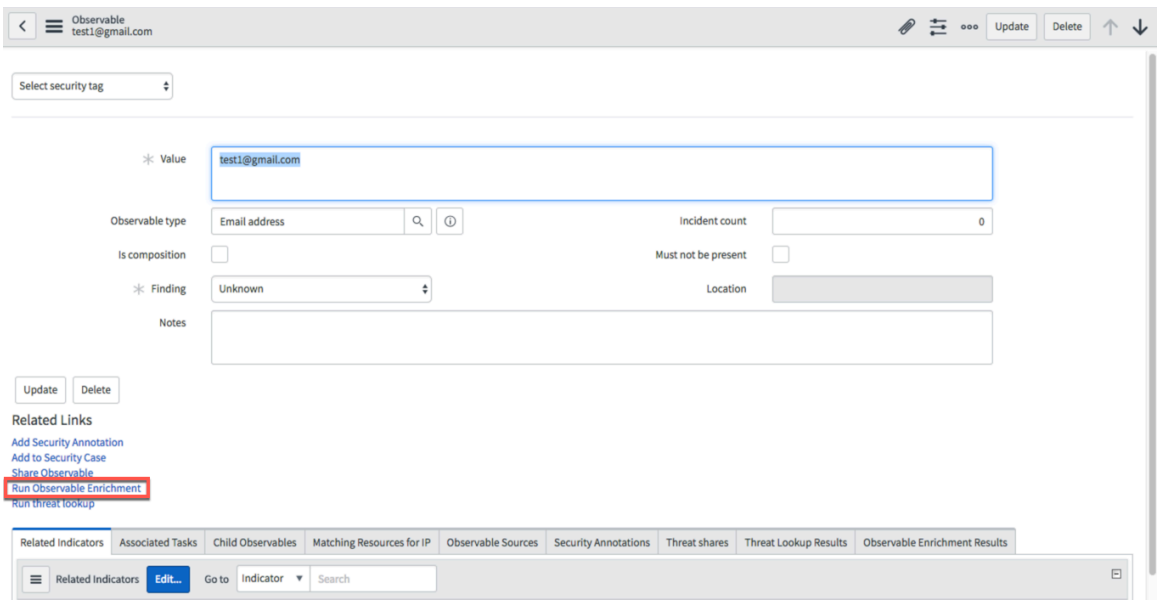
Before you begin
Role required: sn_si.analyst

About this task
Create an observable for a manual lookup using the WHOISIQ API. For more information on how to create and edit an observable, see Create an observable for manual WHOISIQ lookups.

Procedure
1. Navigate to **All** > **IoC Repository** > **Observables** and locate the observable in the list you are working with.
2. Click your observable in the **Value** column to open the record.

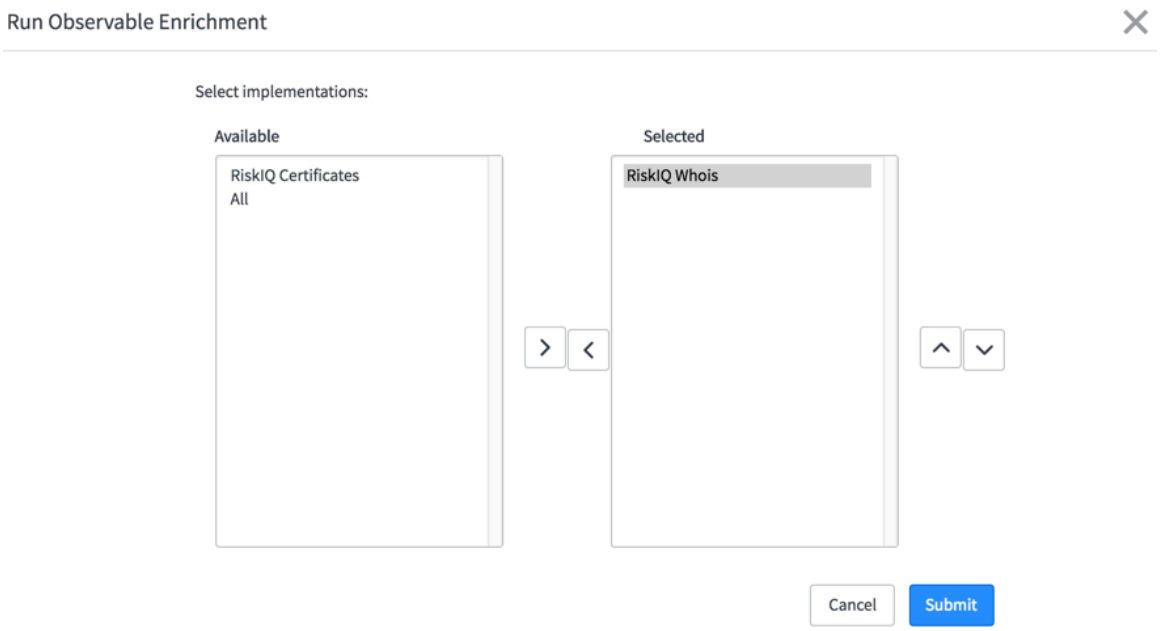


3. Click the **Run Observable Enrichment** related link to run the lookup.

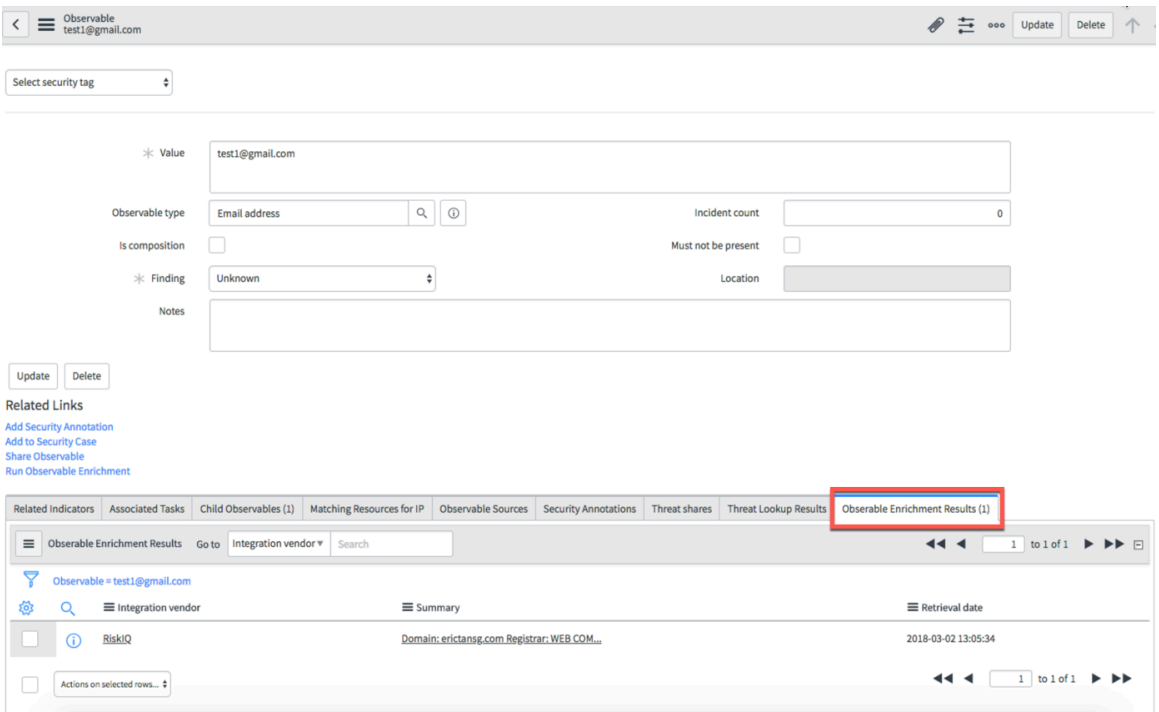


4. In the **Run Observable Enrichment** window, move **RiskIQ Whois** to the Selected list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.
   Lookup results are displayed on the **Observable Enrichment Results** tab on the observable record.



Trouble?
If no results are returned for the observable, a message is displayed in the **Summary** column. If you do not see results, verify the observable is supported by the API.

Related topics

Supported observables for RISKIQ and RISKIQ WHOISIQ

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Shodan integration

Shodan is a search engine that analyzes service banner information from connected devices all around the globe. Service banners include information about a computer system, such as host name, device type, operating system, geographic location, and connected ISP. When integrated with the ServiceNow AI Platform Security Operations product, this service banner information provides analysts with additional enrichment data and insight for security incidents or investigations.

The integration requires the Security Incident Response and Threat Intelligence plugins.

The Shodan integration performs enrichment on the following observables:

- IP addresses
- URLs

The application checks for new observables every five minutes. If the observables are of a type recognized by the Shodan integration, the observables are enriched.

Install and configure Shodan

Before you run the integration on your instance, complete the installation and configuration steps so the Shodan application properly integrates with ServiceNow AI Platform Security Operations.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Setup tasks	Description
Verify that you have assigned the required ServiceNow AI Platform roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • The System Administrator (admin) installs the app and assigns the Security Incident Administrator (sn_si.admin) role. • The Security Incident Administrator (sn_si.admin) oversees the configuration and verifies the expected results. This role also has access to the Security Operations module.
Obtain the Shodan API key.	Create an account and obtain the API key from the Shodan website: Shodan website.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	For the Madrid release and later family releases, the Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration.

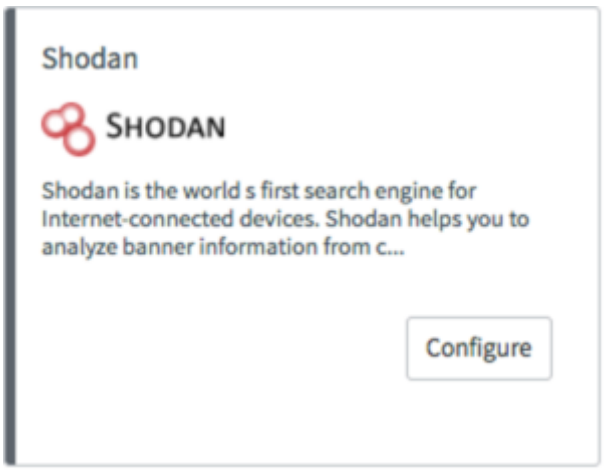
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup tasks	Description
	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Role required: admin

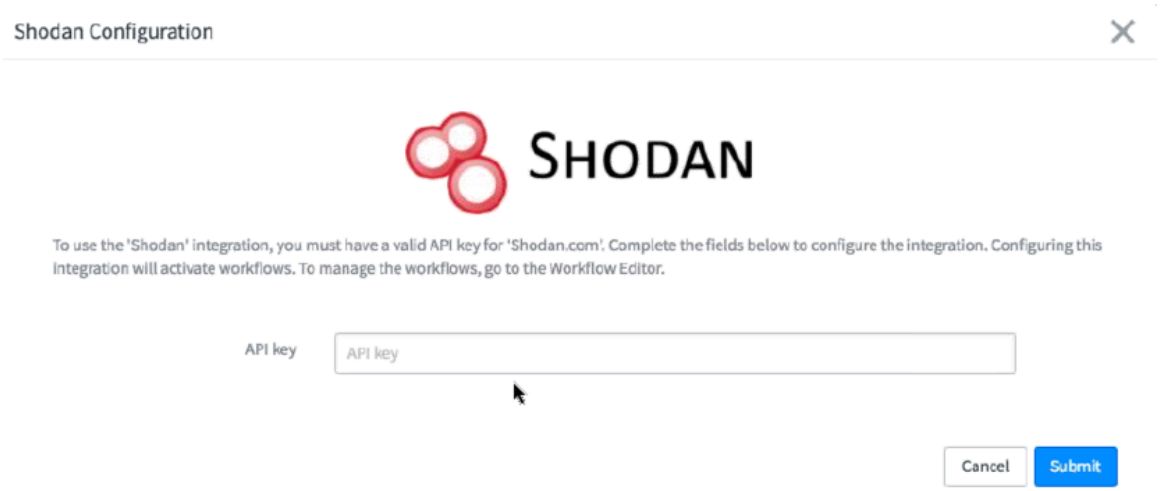
Procedure

1. If you have not installed the application for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After the installation completes, navigate to **Integrations** > **Integrations Configurations** and locate the Shodan tile.



3. Click **Configure**.
4. In the **Shodan Configuration** dialog box, enter the API key you obtained from the Shodan website and click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Verify successful configuration.
   Configuration is successfully completed unless an error message is displayed.

   Trouble?

   If an error message is displayed during the configuration, the Shodan API key may be invalid.

Verify expected results for Shodan

Observables are generated automatically by a security incident and scanned by the application. Enrichment results are displayed on the **Observable Enrichment Results** and **Network Banners** tabs.

Before you begin

Role required: sn_si.analyst.

Procedure

1. Open the security incident you are working with and verify that the lookup has run successfully.

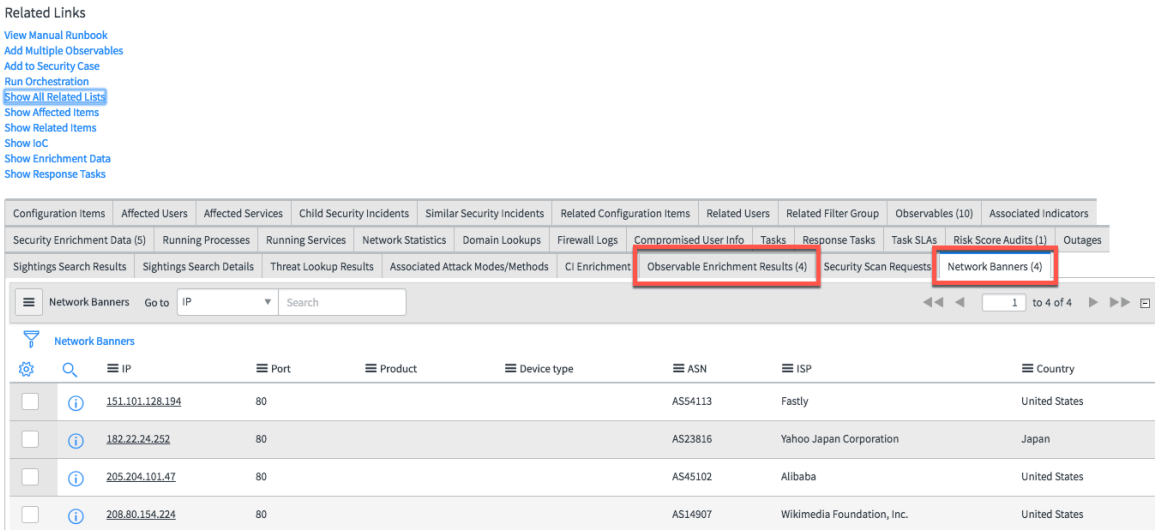


   Once the application is configured, the workflow launches automatically upon incident creation. The execution and completion status of the lookup is displayed in the work notes in the security incident.

2. Review the work notes for more information and how to proceed if you cannot verify that the lookup ran successfully.
3. Navigate to the bottom of the security incident and click the **Show All Related Lists** link in **Related Links**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The figures in the following steps are shown with the **Tabbed forms** setting active in the System Settings. If tabbed forms are not displayed, in the upper-right corner of the banner frame, click the Settings gear icon. In the **System Settings** dialog box that is displayed, click **Forms** and verify that **Tabbed forms** and **With the Form** are selected.



Results are displayed in the **Observable Enrichment Results** and **Network Banners** tabs at the bottom of the security incident.

4. With the **Network Banners** tab selected, click the blue information icon next to an observable.

5. In the dialog box that is displayed, click **Open Record** to view raw data and more details.

Trouble?
If you do not see results under the **Observable Enrichment Results** and **Network Banners** tabs, verify that the observable is a type that is supported for lookup by the integration.

(Optional) Manually attach an observable for Shodan

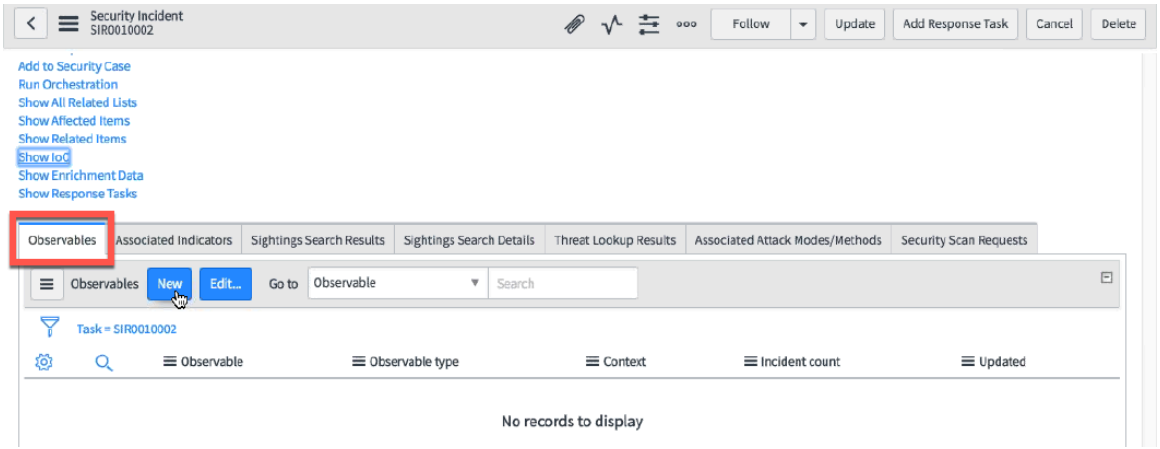
You can manually attach observables to a security incident. You manually attach observables when you want to perform threat lookups on observables that are not attached to a security incident on the initial event trigger. Also, you might perform this task when you want more information about a related observable.

Before you begin
Role required: sn_si.analyst

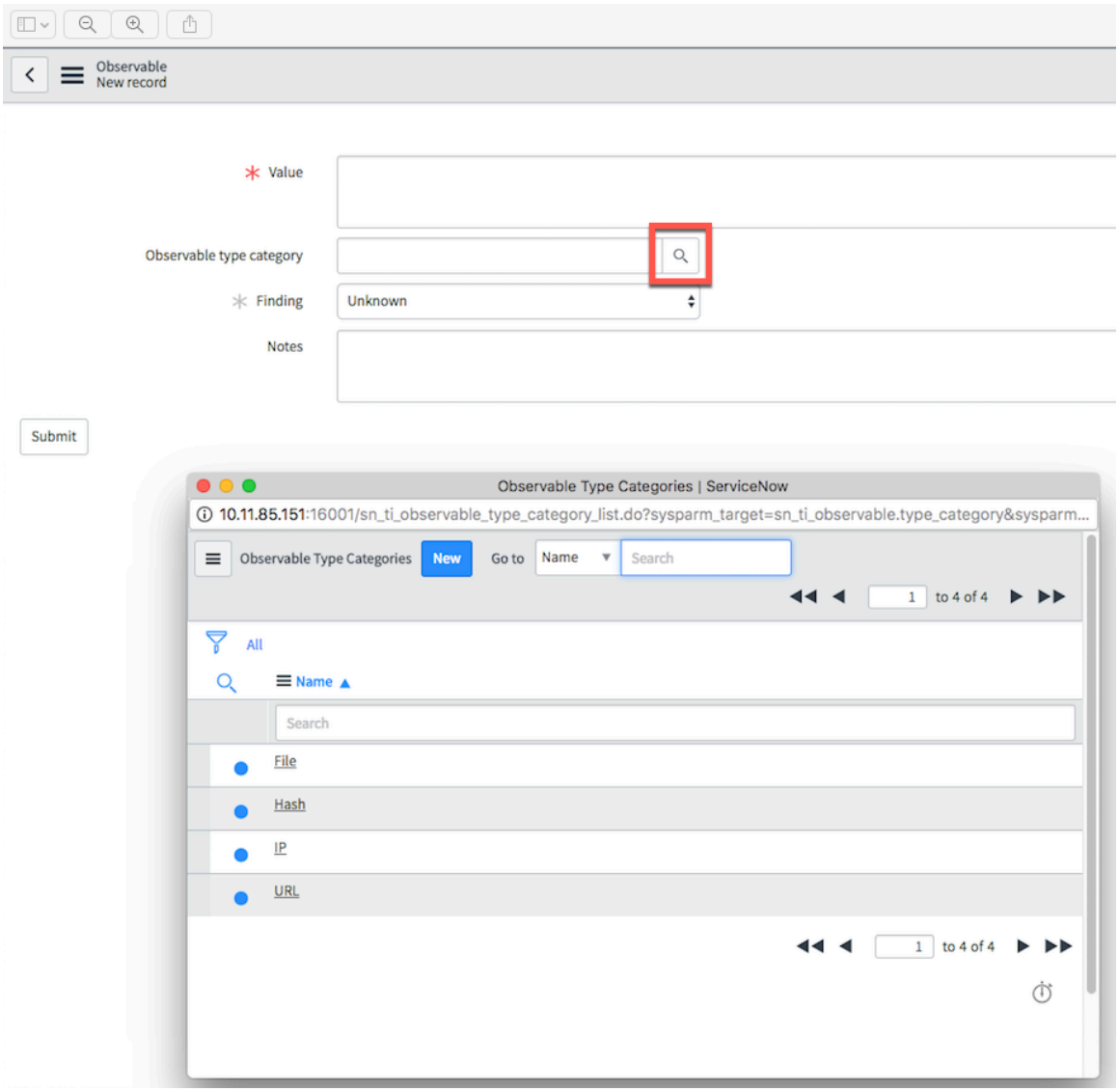
Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents** and open a security incident to which you want to attach the observable.
2. At the bottom of the record, click the **Show IoC**link in **Related Links**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. On the **Observables** tab, click **New**.
   The Observable form is displayed.
4. In the **Value** field, enter an observable (IP address or URL).
5. Click the search icon and from the **Observable Type Categories** dialog box, click the desired observable type in the list to populate the field.

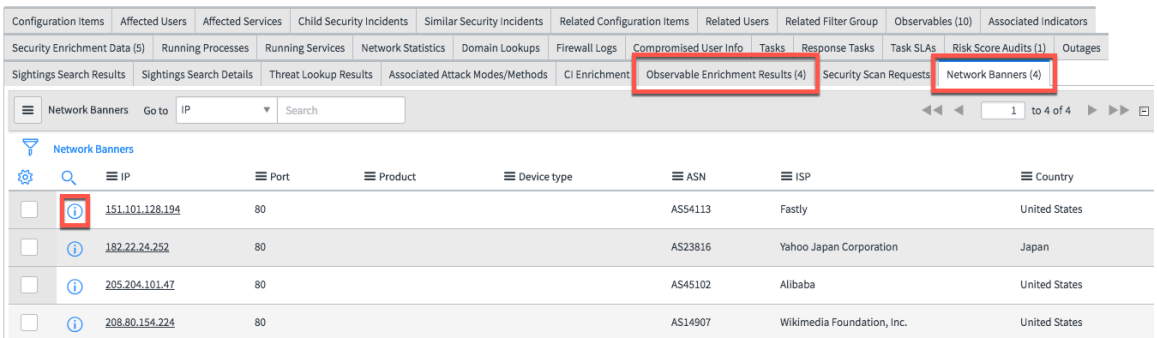


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Submit**.
   The workflow launches and checks for the new observable. The execution and completion status is displayed in the work notes section on the security incident record.
7. Navigate to your security incident and review the work notes.



8. At the bottom of the record, click the **Show All Related Lists** related link.
9. Click the **Observable Enrichment Results** or **Network Banners** tabs for results, and click the blue information icon next to an observable for more information on a specific item.



10. In the dialog that is displayed, click **Open Record** to view raw data and more details.
11. **Optional:** Click the blue settings icon near the search icon to personalize column output and order.
12. In the **Personalize List Columns**, select available settings, move them to the **Selected** column, and click **OK**.

Trouble?
Review the **Work notes** for more information and how to proceed if you cannot verify that the lookup ran successfully.

Secureworks CTP Ticket Ingestion Integration

The Secureworks Counter Threat Platform ticket ingestion integration enables you to automatically fetch Secureworks CTP tickets, convert them into security incidents and perform automated response actions.

The key features of this integration include:

- Automatic ingestion of selected tickets (including attachments) based on a pre-defined schedule.
- Mapping of ticket and event fields to Security Incident Response fields.
- Preview of security incidents mapped to the ticket fields.
- Filtering and aggregation of tickets.
- On demand retrieval of events associated with a ticket.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Periodic tracking of key updates to tickets.
- Automating ticket updates and closures based on SIR incident status
- Master ticket update.
- Synchronization of Secureworks worklogs with Security Incident Response worknotes.

Set up your ServiceNow AI Platform instance for the Secureworks CTP ticket ingestion integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform instance prior to installing the application from the ServiceNow Store.

Before you begin

Role required: sn_si.admin

About this task

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Setup task	Description

Verify that you have assigned the required ServiceNow AI Platform and Security Incident Response roles.	The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform instance.
	• A user with the ServiceNow AI Platform administrator role (admin) installs the application from the ServiceNow Store and assigns the SIR administrator (sn_si.admin) role.
	• A user with the sn_si.admin role oversees the following tasks in the ServiceNow AI Platform:
	  ○ Names, creates, and edits profiles.
	  ○ Selects and maps Secureworks CTP ticket fields to the security incident fields.
	  ○ Previews security incident details for accuracy prior to finalizing the configuration.
	  ○ Schedules on-going ticket ingestion.
	  ○ Enables ticket updates when a SIR SIR incident is created and closed.
	  ○ Assigns the security incident analyst (sn_si.analyst) role.
	  ○ Users with the sn_si.analyst work with security incidents.
	For more information about roles and assigning roles to users, see Managing roles

Verify that you are using the following versions:	If you have access to the Secureworks CTP portal, you have access to the API that is required for this

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setup task	Description
• Secureworks Ticket API 4.0 • Secureworks Event API 1.0 • Secureworks Enrichment API 1.0	integration. There is no other special setup required for the API.
Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you install the application for the integration.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. **1.** Security Incident Response **2.** Event and Alert Ingestion for Security Operations (Required for SIEM integrations): This application requires: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => ServiceNow IntegrationHub Action Step - REST **Note:** The Integration Hub components are installed along with the Event and Alert Ingestion plugin. If these are not installed, contact Customer Support for assistance. For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

Install and configure the ServiceNow application for the Secureworks CTP ticket ingestion integration

Before you run the integration on your ServiceNow AI Platform instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your ServiceNow AI Platform instance.

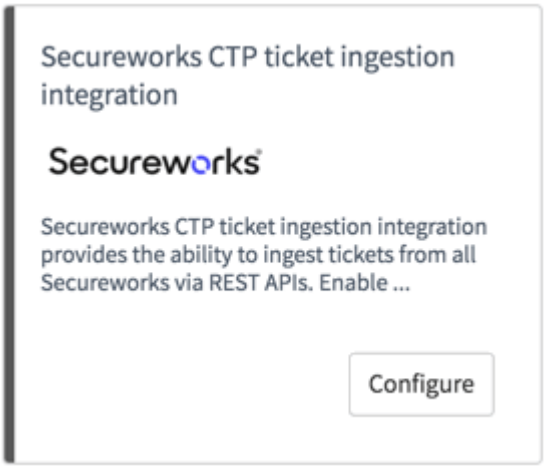
Before you begin

Role required: sn_si.admin

Procedure

1. If you have not installed the Secureworks CTP ticket application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **Integrations** > **Integrations Configurations** and locate the Secureworks CTP Ticket Ingestion Integration tile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. To configure the application, click **New**.
4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.
5. In the dialog that is displayed, fill in the fields.

Field	Description
Name	Name of the Secureworks CTP instance used for the integration. You can enter only alphanumeric values and hyphens (-) in this field.
Description	Enter a description for the user account.
Username	Enter the username for the Secureworks CTP API account. Note that the username is case sensitive. To find the username, follow these steps: ○ Login to the Secureworks CTP portal. ○ Navigate to **Account** > **Account Management** > **API Credentials**. The username is displayed on the API Credential page.
API Password	Enter the Secureworks CTP API Password. To find the API Password, follow these steps: ○ Login to the Secureworks CTP portal. ○ Navigate to **Account** > **Account Management** > **API Credentials**. The API Password is displayed on the API Credential page. For more information on how to obtain the username and API password, follow the steps in the Generating a Persistent API Key section of the Secureworks Ticketing API Guide.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Submit**.
   After it is successfully validated and submitted, each configuration is saved on the Security Integrations page as a tile.

Result

If your saved configuration tiles are not displayed on the Security Integrations page. On the top right corner of the page, from the **Show Configurations** choice list, click **Yes**.

Create a profile for Secureworks CTP ticket ingestion integration

Create a profile in your ServiceNow AI Platform instance and determine which tickets need to be ingested and which tickets will be used to create security incidents. Before security incidents are created from ingested tickets, the field values from tickets are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident will be displayed.

The integration allows you to ingest tickets based on the profiles that you configure in the Security Operations environment of your instance. All tickets are initially ingested for a configured ticket type in a profile. Ingested tickets can then be further filtered to specify which tickets create security incidents.

For example, you may prefer filters that create security incidents only for tickets that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested tickets, individual field values on the tickets are mapped to corresponding fields on a layout of security incident for a preview.

Identify the source of the profile

Specify the name and source of the profile.

Before you begin

Role required: sn_si.admin

Procedure

1. To create a profile for a ticket in your ServiceNow AI Platform instance, navigate to **Secureworks Ticket Ingestion Integration** > **Secureworks Profiles**.
2. Click **New**.
3. Fill in the fields.

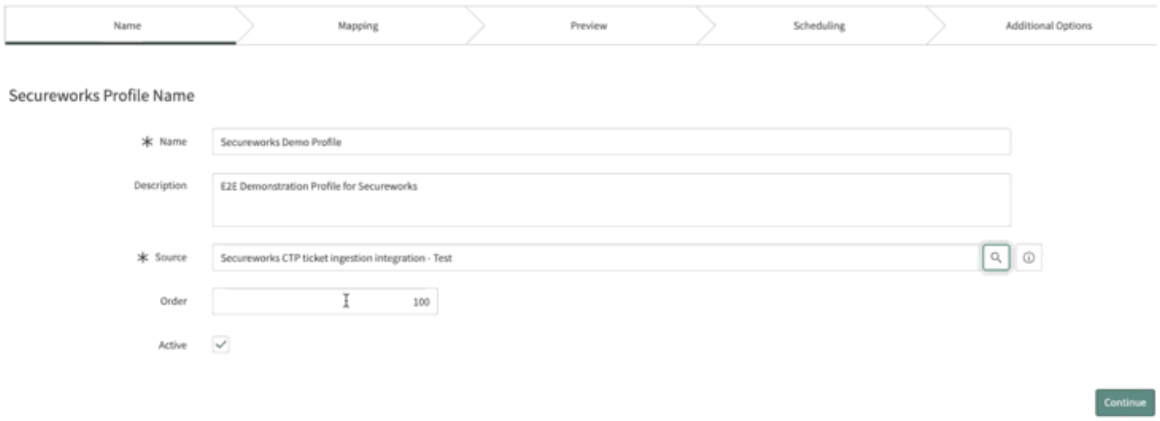
   An example of a completed form follows the table.

Field	Description
Name	Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Source	Select the source from where you want to ingest the data.
Order	Default is 100. If you have created multiple profiles, this value provides a run time execution priority

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	when two or more profiles share the same triggering conditions. The lower the order value, higher the priority.
Active	This option is cleared by default. If this option is disabled, the profile is not active. **Note:** You should complete all sections in the profile before making it active.

The following figure is an example of a completed form.



What to do next
Map the ticket fields.

Mapping of ticket fields for the SecureWorks CTP integration

Map the ticket and event fields to the fields in the security incident form.

For the mapping step, you must first ingest sample tickets and then ensure that all the relevant ticket fields are mapped to the appropriate place on the Security Incident Response form and then visualize the security incident in the preview section.

Mapping of the sample ticket fields involves the following:

- Fetching and populating of the sample data: See Ingesting the sample Secureworks tickets
- Mapping the ticket fields to the security incident: See Mapping Secureworks ticket fields to security incident response fields

Ingesting the sample Secureworks tickets

Select the sample tickets that are to be ingested.

Before you begin
Role required: sn_si.admin

Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. You can either pull the five most recent sample tickets or provide the unique ticket IDs for the specific tickets that you want to use for your mapping experience.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

From the **Ingestion Preference** choice list, select one of the following:

- Retrieve most recent tickets: The 5 most recent tickets are retrieved.
- Select tickets based on ticket ID: Specify the ticket ID for the ticket to be retrieved. You can specify a maximum of 5 ticket ids separated by commas.

3. Click **Fetch Sample Data** to pull the latest sample ticket data from the Secureworks CTP server. The pull for sample tickets may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen. The retrieved tickets are displayed as individual tabs. Click on a tab to view the ticket data. For each ticket, you can see the ticket fields and their values, and details of the contributing event that triggered the ticket.

Note: You will see details of contributing events only if they have occurred in the last 7 days. Events older than 7 days are not displayed.

What to do next

After you have fetched the sample data, the next step is map the ticket fields to the security incident.

Mapping Secureworks ticket fields to security incident response fields

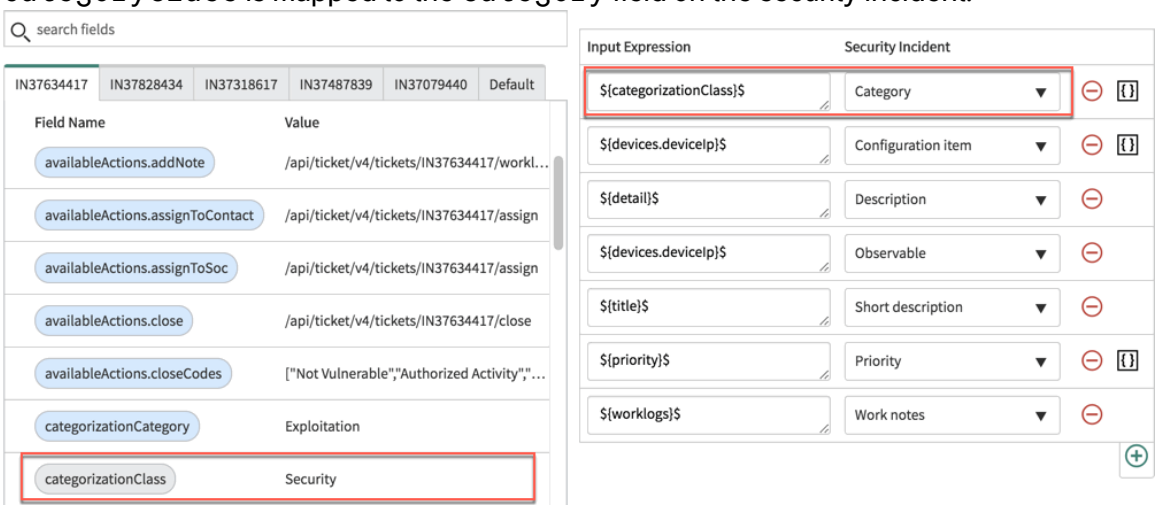
Map individual ticket or event fields to fields on a ServiceNow AI Platform SIR security incident.

Ticket field mapping

As a user with the sn_si.admin role, use the fields from the Sample Tickets section on the left and map them to the security incident fields in the **SIR Incident Field Mapping** column. Edit the mapping configuration by dragging ticket or event fields from the left side and dropping them on the SIR Incident Field Mapping section on the right. The mapping on the right associates the incoming ticket field with an outgoing security incident field.

1. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
2. You can manually enter the field name in the Input Expression column or drag and drop the field name. For example, `description`, and drop it on a field in the **Input Expression** column next to a field name in the **Security Incident** column.

   The field value is displayed in the Input Expression column. In the following image, `categoryClass` is mapped to the `Category` field on the security incident.



Note: If you enter the event field name manually in the **Input Expression** section, you must add a prefix as *`${Event:eventfield}$`* before the name of the field being mapped.

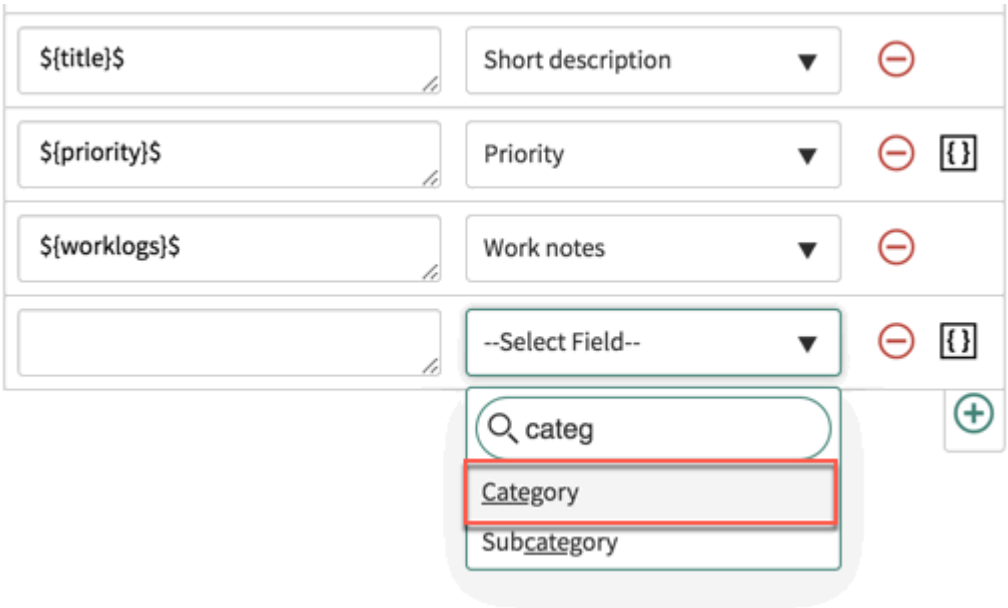
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To help you ensure that no ticket or event fields are overlooked or duplicated in the mapping process, fields are color-coded. Color-coding of the ticket fields helps you keep track of the ticket values that you have already mapped as they become greyed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important ticket information remains unmapped.

Light blue fields on the left indicate that a ticket field is not yet selected and mapped on the security incident. You may prefer to associate an incoming ticket or event field with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.

3. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps:
   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus (+) icon. A new field is displayed.
   b. In the Security Incident column, expand the choice list that is displayed, and select a field.

      In the expanded choice list for the new field, some fields are shaded. In the following figure, Category has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the ticket fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.



> **Note:** As multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a choice list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the choice list, the field is not populated on the security incident.

   c. Alternatively, type a value in the Search field for the new row.
   d. From the left side of the form, select the ticket field and drag-and-drop it to an appropriate security incident field on the right.

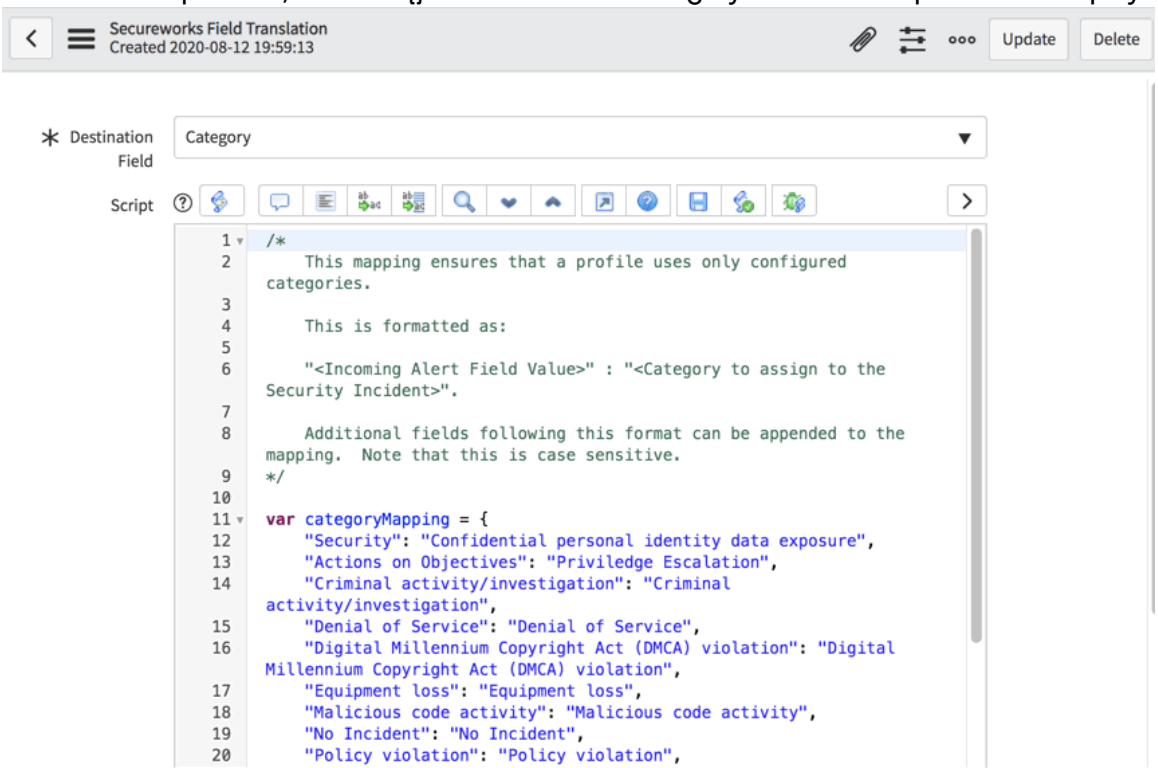
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Remove fields by using the - icon next to the field name in the SIR Incident Field Mapping section.
5. Continue mapping by adding or removing field values to the mapping.

Format Field Translation

In certain cases, ticket fields may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

To use the script editor, click the {} icon next to the Category field. The script editor is displayed



.

Enter any changes to the script and click **Update** to save the changes and return to the Mapping page.

Incident generation conditions

Once the mapping section is complete, you can set filter conditions so that you can specify which tickets should create security incidents versus which tickets should be filtered out, for example, low priority tickets. You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming ticket must satisfy to create a security incident. To set incident generation conditions, follow these steps.

1. Scroll to the **Incident Generation Conditions** section on the form and select the **Filter based on conditions** check box to enable the option.

   The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The options in the choice lists for the first field in the Filter conditions builder match the fields that are displayed on the **Sample Ticket Ingestion** section for the ingested tickets. These fields are dynamic and change depending on the tickets that you ingest. Criteria that you enter are case-sensitive, and they must match exactly the values of the Secureworks CTP ticket. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Secureworks CTP console and review your tickets for the keywords.

Note: The *worklogs*, *devices*, *attachments*, *watchers*, *availableactions*, and *closeCodes* ticket fields can have multiple values (as the values are stored in arrays). As the filter condition can retrieve only strings, you must use the *contains* filter condition for these fields to ensure that the data is filtered correctly.

2. Using the choice lists and fields of the conditions builder, set filters for the first row.
3. To add more conditions, to the right of the fields, click **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
4. (Optional) In the second row, set a second filter condition.

   This type of incident generation condition filtering helps you narrow down the tickets, and limit the number of unnecessary security incidents that you create without modifying the underlying rule or filters. If additional filtering criteria are set, only tickets that match all criteria are mapped to security incidents.

Ticket aggregation criteria to handle similar tickets and prevent duplicate incidents

Define additional ticket aggregation criteria that aggregates an incoming ticket to an existing SIR security incident instead of creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related ticket data on a single security incident. To set the criteria, follow these steps below:

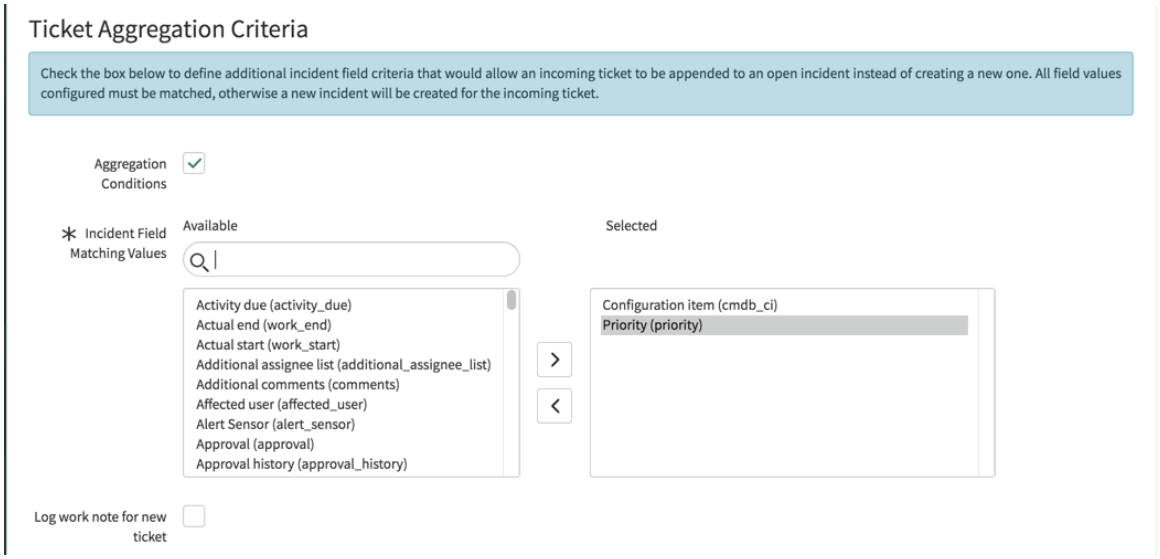
1. Scroll to the **Ticket Aggregation Criteria** section on the form and select the **Aggregation Conditions** check box to enable this option.

   The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

2. From the Available list, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform and move them to the Selected list.

   All the field values that you select must be matched to append this incoming ticket to an existing security incident. This includes fields, such as Observables and Configuration Items, that may have multiple ticket field values mapped to them. All values must match. If only a subset of the values are matched, the ticket aggregation conditions will not be met and a new security incident will be created. See screen shot below for multi-value field mapping.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



If a new ticket matches all the values that are selected in the aggregation field conditions in the mapping step, the new ticket is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregated tickets on a related list on a security incident. This list details associated time stamps and aggregated field values. This information helps you understand why these tickets are being aggregated to existing security incidents. If this tab is not displayed in a security incident, scroll to the left side of the record under **Related Links** and click the **Show All Related Lists** link.

Note: The Secureworks Aggregated Tickets related list is not available with the base system. You must configure the Related List layout and explicitly include it with the other related lists.

3. (Optional) To log a work note for a new ticket that is recently added on the security incident, select the check box to enable this option. The work note logs that a new ticket has been added along with a link to the ticket details and any other details that may have been added to the work note field in your mapping section.

   You have successfully mapped values from a Secureworks CTP ticket to fields on a security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also appended tickets to existing security incidents when ticket field values match the configured aggregation criteria.

4. Click **Continue** to continue with the profile configuration. The next step is to preview the fields you mapped on a SIR security incident

Preview the mapped values in the security incident

After you complete the mapping step, preview the values that you mapped in a SIR security incident. This preview step permits you to verify that you have mapped all the ticket fields that you want displayed on the security incident.

Before you begin

Role required: sn_si.admin

About this task

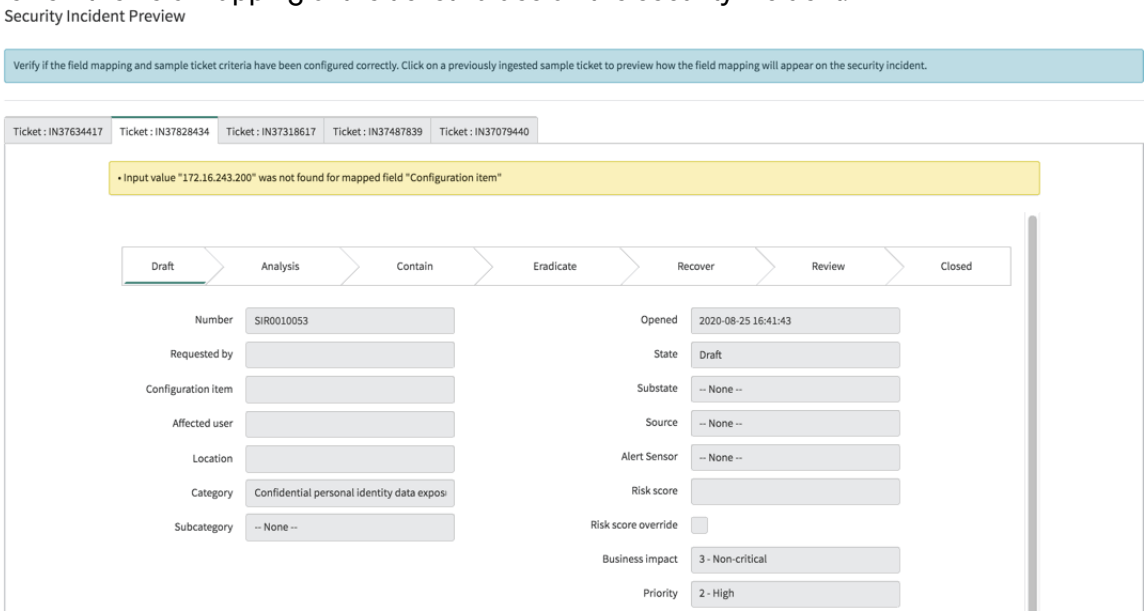
Preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the Security Incident Response product.

Procedure

1. If the security incident preview is not displayed, click **Preview** in the progress bar.
   The tickets are displayed as tabs.
2. Click on a tab to preview the security incident.
   This view is a read-only view, and a record of this security incident is not saved.
3. Review the field mapping of the ticket values on the security incident.



   The preceding image is an example of a preview with a mapping error of the samples that were ingested.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

What to do next

If no error messages are displayed, and you are satisfied with the field mapping on the security incident. Define the schedule.

Define schedule for the Secureworks CTP Ticket ingestion

Verify the default settings for ticket retrieval or modify the scheduling as needed. This step permits you to filter your ticket retrieval based on a date range and a polling interval.

Before you begin

Role required: sn_si.admin

About this task

You also choose how often you will poll for future tickets that match the ticket profile configuration. Configure these polling intervals on a per-profile basis. When scheduling, you may prefer to balance system load against incident urgency. A one-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

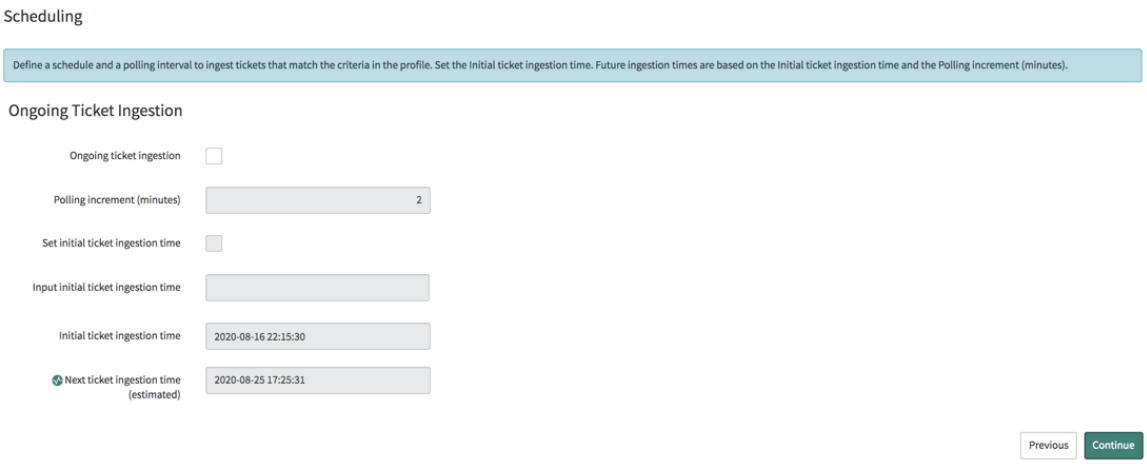
Procedure

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when tickets are pulled from the Secureworks CTP portal.

Option	Description
Ongoing ticket ingestion selected	Based on the default setting, the ServiceNow AI Platform instance pulls from the Secure works CTP portal for new tickets every five minutes. Security incidents are created if tick ets are found and incident generation filtering criteria are matched. To balance ticket inges tion against server load, and to pull the most current data, five minutes is the setting you may prefer. However, this value can be modi fied as needed.
○ **Ongoing ticket ingestion selected** ○ **Set initial ticket ingestion time**	Initial ingestion time If you want to schedule the initial ingestion at a specific time, follow these steps: ○ Select the Ongoing ticket ingestion and Set initial ticket ingestion time fields. ○ Specify the time in the Input initial ticket in gestion time field. The initial ingestion will take place at the time specified here. Subsequent ingestions will be based on the schedule defined in the Polling increment (minutes) field. As an example for scheduling, if you have a daily ticket job that runs once a day at 4 AM local time, you can set up the corresponding ticket profile in your ServiceNow AI Platform instance to run at 4:05 AM local time to cap ture the ticket right away and create a securi ty incident. Enter 04 05 00 in the Initial ticket ingestion field. In the Polling increment (minutes) field, enter 1440 (24 hours) to schedule the next ticket ingestion for 24 hours from the initial ticket ingestion. Both the initial ticket inges tion time and next ticket ingestion time are dis played in the fields. To configure the settings in this example, fol low these steps: ○ Select the **Ongoing ticket ingestion** option. ○ In the Polling Increment (minutes) field, en ter 1440 (24 hours). ○ Select the **Set initial ticket ingestion time** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ In the Input initial ticket ingestion time field, enter 04 05 00. The time of the next ticket ingestion is displayed in the Next ticket in gestion time (estimated) field.



3. Click **Continue** to navigate to the Additional Options page.

Automate ticket updates and closure based on SIR incident status

The Secureworks CTP ticket ingestion integration has a bi-directional interface that allows for both tickets to create security incidents, as well as an ability to update the tickets once the security incident is created and/or closed with relevant incident details such as security incident number, assignment group, security incident URL, and so on.

Before you begin

Role required: sn_si.admin

Procedure

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.
2. Complete the configuration for updating tickets when the security incident is created.

Option or Field	Description
Update SIR worknotes with Secureworks worklogs	Select this option to enable the Secureworks worklogs and SIR work notes synchroniza tion feature. This allows you to track updates made to the ticket in Secureworks CTP after the security incident is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or Field	Description
	Note: ○ If the Secureworks worklogs field has been mapped to the SIR Worknotes field, the Secureworks worklogs are re trieved till the security incident is cre ated. ○ If the synchronization feature is en abled, only worklogs created or updat ed after a security incident has been created are retrieved.
Update Secureworks tickets upon SIR Inci dent Creation	Select this option to update the Secureworks CTP ticket and add additional comments when a security incident is created from the ticket. This can occur for both the initial trig gering tickets that create the security inci dent, as well as aggregated tickets.
Initial comments posted back to Secure works ticket	When a security incident is created, the ticket is automatically updated in Secureworks CTP with comments. You can modify the default text and use the ${field name}$ format to add or modify any fields available in the security incident form.
Close Secureworks tickets upon SIR Inci dent Closure	Select this option if you want to use the au tomated ticket closure option. This can oc cur for both the initial triggering tickets that create the security incident, as well as ag gregated tickets. When a security incident is closed, the corresponding ticket is automati cally closed in Secureworks CTP along with the same close code as the security incident and the default closure comments specified in the profile. **Note:** You cannot use this option to up date the Master Ticket status.
Closure comments posted back to Secure works ticket	The default closure comments are displayed here. You can edit the default text and use the ${field name}$ format to add or modify any fields available in the security incident form.

3. Click **Finish** to complete the configuration and move the profile to the **Waiting** state.
   A confirmation dialog is displayed. You have successfully set up the profile. Activate this profile to pull tickets from the Secureworks CTP portal based on your scheduling.

Optional: Copy a Secureworks CTP profile

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy profiles to save time.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.admin

About this task
As a user with the sn_si.admin role, if you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

Procedure
1. Navigate to **All** > **Secureworks Ticket Ingestion Integration** > **Secureworks Profile**.
2. In the Secureworks Profiles list that is displayed, select a profile that you want to copy, and, from the **Actions on selected rows** choice list, click **Copy**.
   The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains (copy). Although the original profile is enabled (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.

   You have successfully copied the settings from an existing profile to a new profile. Note that the **Active** column status is set to false as the profile needs to be activated.

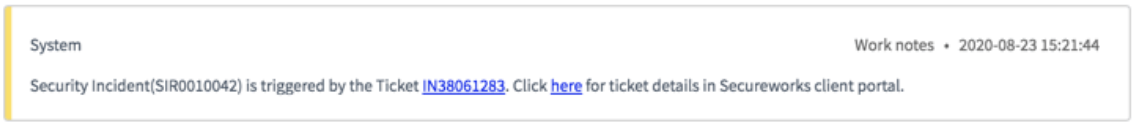
What to do next
You are prompted to activate (enable) the new profile after you complete the configuration steps.

Security Incident Response form changes after ticket ingestion

After a Secureworks CTP ticket has been ingested, a security incident is created and the corresponding updates are made to the security incident record.

Worknotes

A worknote is posted with details of the ticket that triggered the security incident.



Click on the ticket link to navigate to the internal Secureworks Ticket to Task record. The **Click here** hyperlink takes you to the Secureworks CTP dashboard where you can view the ticket details.

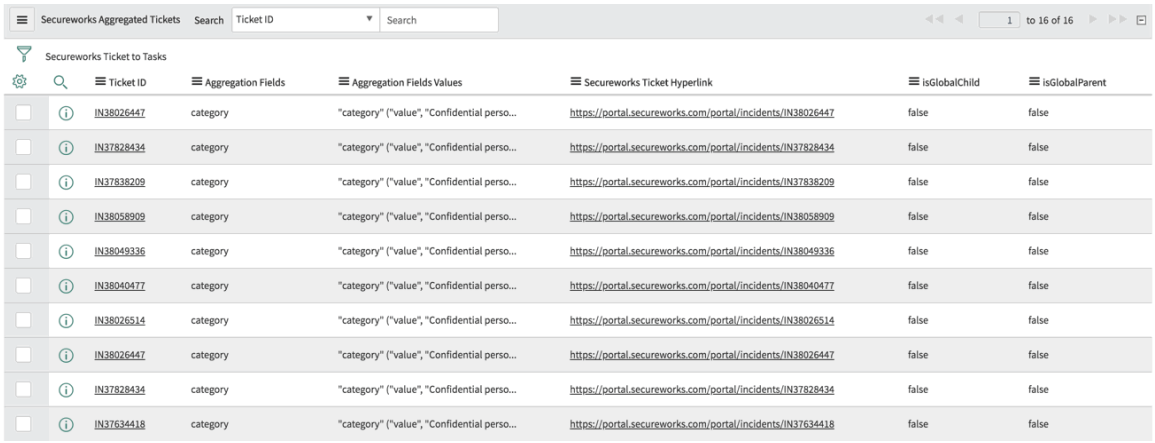
If you had selected the **Log work note for new ticket** option in the Ticket Aggregation Criteria as described in the Create Profile: Mapping page, a worknote is posted when the ticket is aggregated.



Aggregated tickets

Click **Related Lists** > **Secureworks Aggregated Tickets** to view the ticket aggregated to the security incident. Click the ticket hyperlink to view the ticket in the Secureworks CTP dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



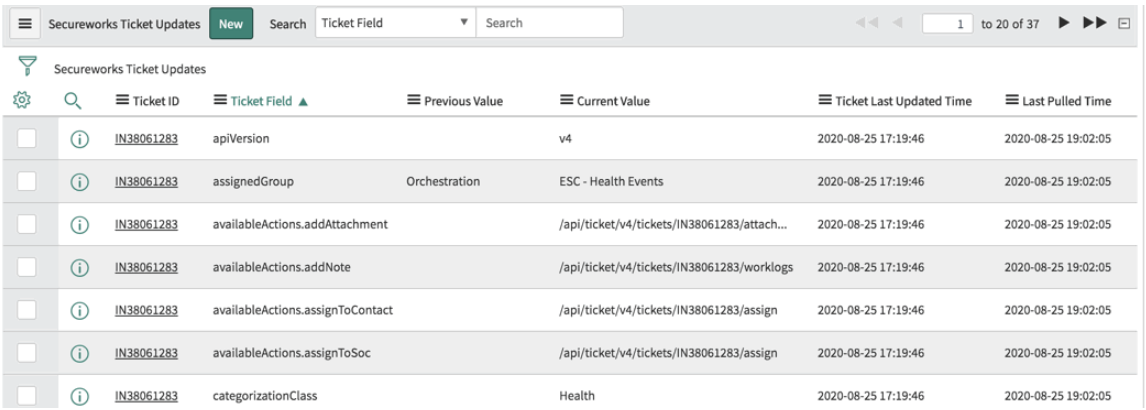
Ticket ID	Aggregation Fields	Aggregation Fields Values	Secureworks Ticket Hyperlink	isGlobalChild	isGlobalParent
IN38026447	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026447	false	false
IN37828434	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37828434	false	false
IN37838209	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37838209	false	false
IN38058909	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38058909	false	false
IN38049336	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38049336	false	false
IN38040477	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38040477	false	false
IN38026514	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026514	false	false
IN38026447	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026447	false	false
IN37828434	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37828434	false	false
IN37634418	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37634418	false	false

Create security incident: Select a ticket from the list, click the **Actions** menu and click **Create security incident**. This option creates a new security incident for the ticket and this ticket is de-aggregated from the parent security incident.

Delete ticket record: Select a ticket from the list, click the **Actions** menu and click **Delete**. This option deletes the ticket record.

Secureworks Ticket updates

This shows the standard ticket fields and tracks changes to the tickets during every polling interval. This is helpful as you can view any ticket updates directly without navigating to the Secureworks CTP dashboard. Any changes to the values are displayed in the Previous Value and Current Value fields.

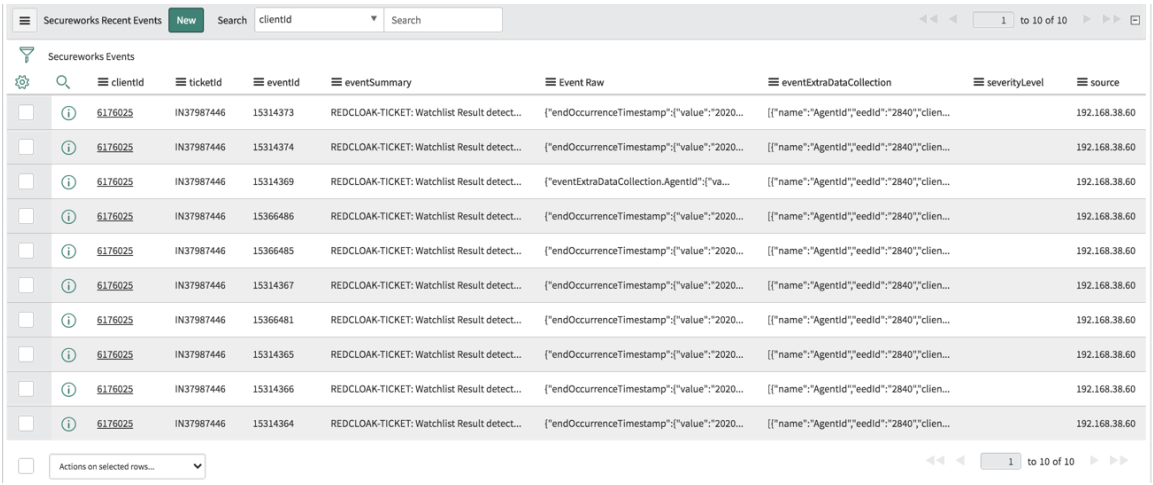


Ticket ID	Ticket Field	Previous Value	Current Value	Ticket Last Updated Time	Last Pulled Time
IN38061283	apiVersion		v4	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	assignedGroup	Orchestration	ESC - Health Events	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addAttachment		/api/ticket/v4/tickets/IN38061283/attach...	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addNote		/api/ticket/v4/tickets/IN38061283/worklogs	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToContact		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToSoc		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	categorizationClass		Health	2020-08-25 17:19:46	2020-08-25 19:02:05

Secureworks Recent Events

Click the **Fetch Recent Secureworks Events** option under the **Related Links** to view the most recent Secureworks events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



By default, a maximum number of 50 events will be displayed. You can modify this default setting in the Secureworks Integration Settings.

View the Secureworks tickets and the corresponding security incidents

The imported Secureworks CTP tickets are initially stored in the Ticket Import table. View all the Secureworks CTP tickets that have been imported before any filter conditions are applied.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Secureworks Ticket Ingestion Integration** > **Secure Ticket Import**.
2. You can view all the Secureworks CTP tickets that have been imported before they are aggregated or any filter conditions are applied.
3. Click on a Ticket ID to see the raw ticket data.
4. Navigate to **Secureworks Ticket Ingestion** > **Secureworks Ticket to Task**.
   The Secureworks CTP tickets with their corresponding security incidents are displayed.

Secureworks CTP Master Ticket Closure Notice

Before you close a security incident created by a Secureworks CTP master ticket, you must verify that all child tickets associated with the master ticket are closed.

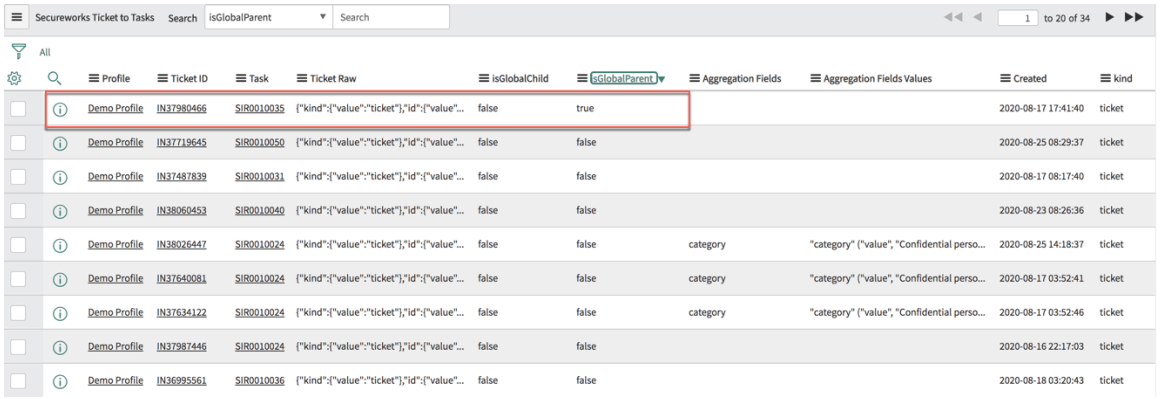
Before you begin

Role required: sn_si.admin

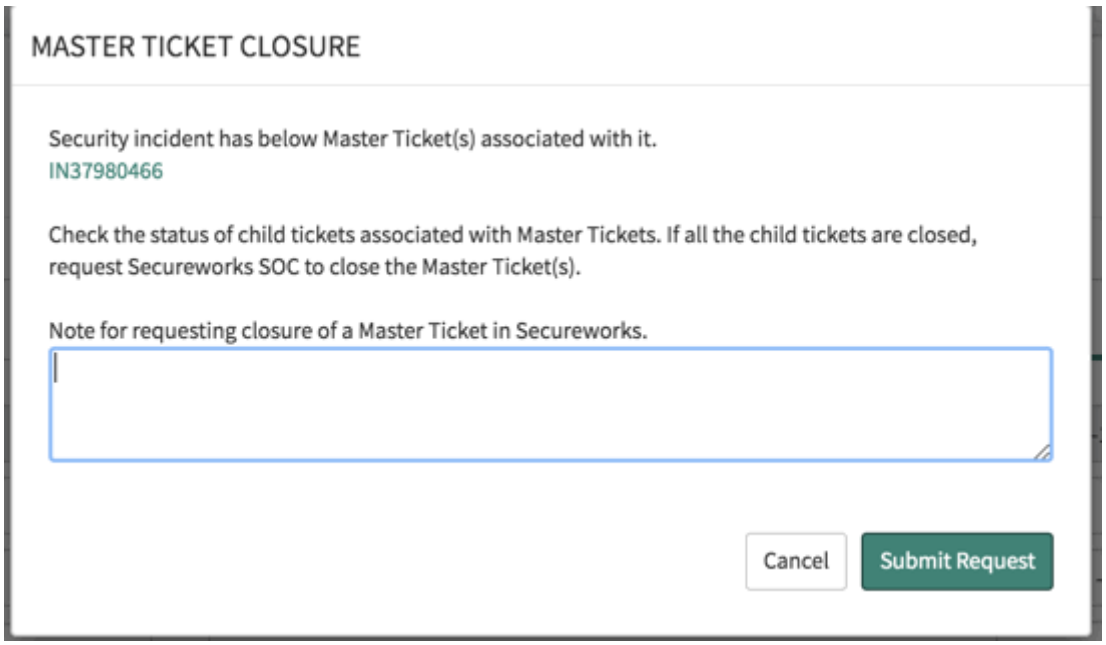
Procedure

1. Navigate to **All** > **Secureworks Ticket Ingestion** > **Secureworks Ticket to Task**.
   The Secureworks CTP tickets with their corresponding security incidents are displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Click on the security incident with the **isGlobalParent** field set to **true.**
3. Change the security incident State to **Closed**, specify the close codes and click **Save**. The following dialog box is displayed.



This security incident is associated with a Secureworks Master Ticket. A Master Ticket may have one or more child tickets associated with it. Before the Master Ticket can be closed, you must first verify if all the child tickets associated with this Master Ticket are closed.

4. Add a note requesting closure of the Master Ticket in Secureworks and click **Submit Request**. The Master Ticket is now reassigned to the Secureworks SOC team.
5. Once the request has been submitted, you can close the security incident.
6. Navigate to **Application** > **Module**.

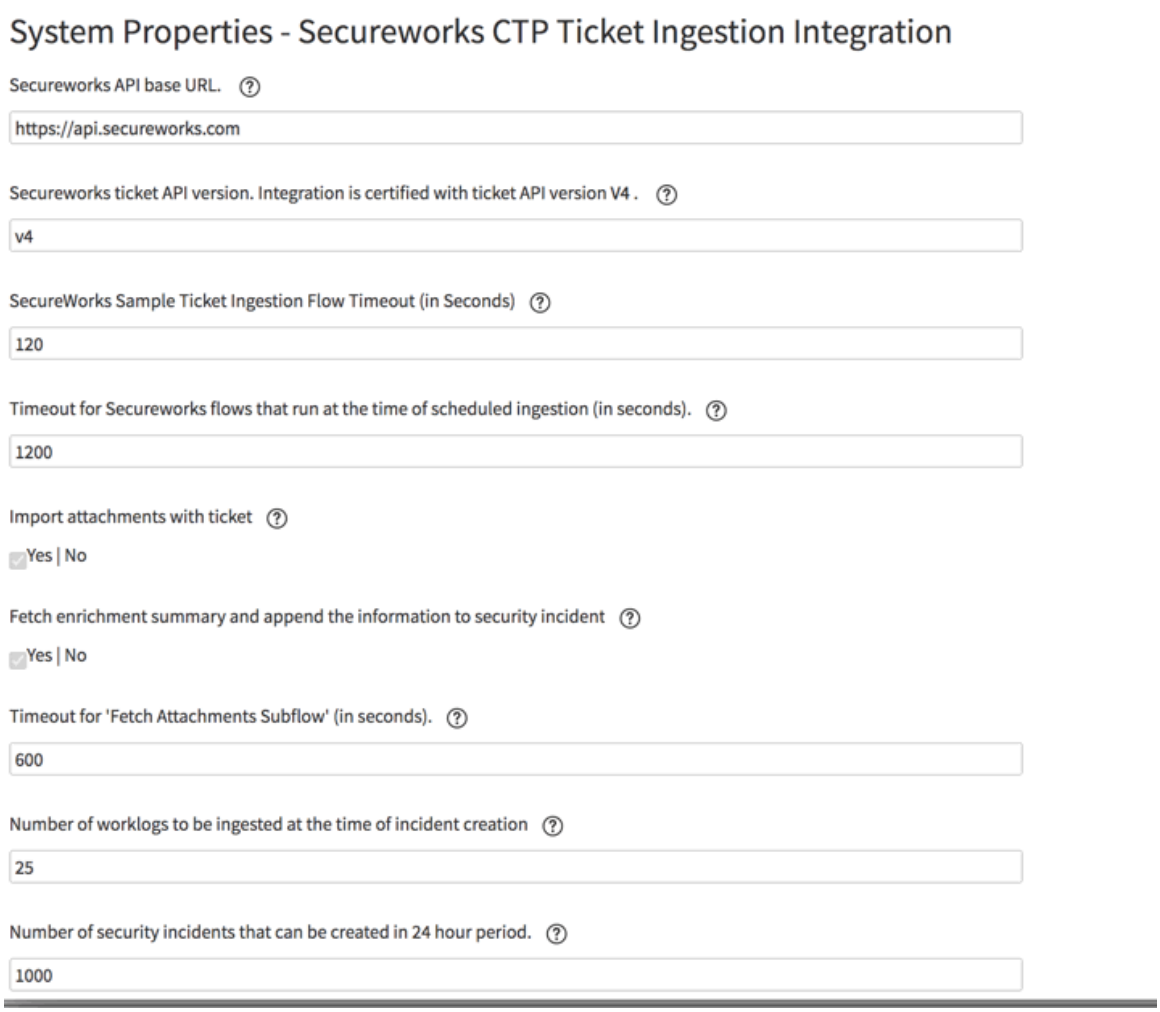
Secureworks CTP integration configuration settings

Use this option to modify the Secureworks CTP ticket ingestion integration default system properties.

To modify the system properties, log in as a user with the *sn_si.admin* role and navigate to **Secureworks Ticket Ingestion Integration** > **Secureworks Integration Settings**.

The default configuration settings are displayed. You can modify these settings if required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Any modified integration settings will be applied during the next polling interval as defined in the profile.

Security Incident Response Integration with Cortex XSIAM by Palo Alto Networks

Security Incident Response Integration with Cortex XSIAM by Palo Alto Networks ingests Alerts and Incidents from Cortex XSIAM into ServiceNow®'s Security Incident Response platform, enabling seamless post-incident management while maintaining bi-directional status and work note synchronization.

Request apps on the Store

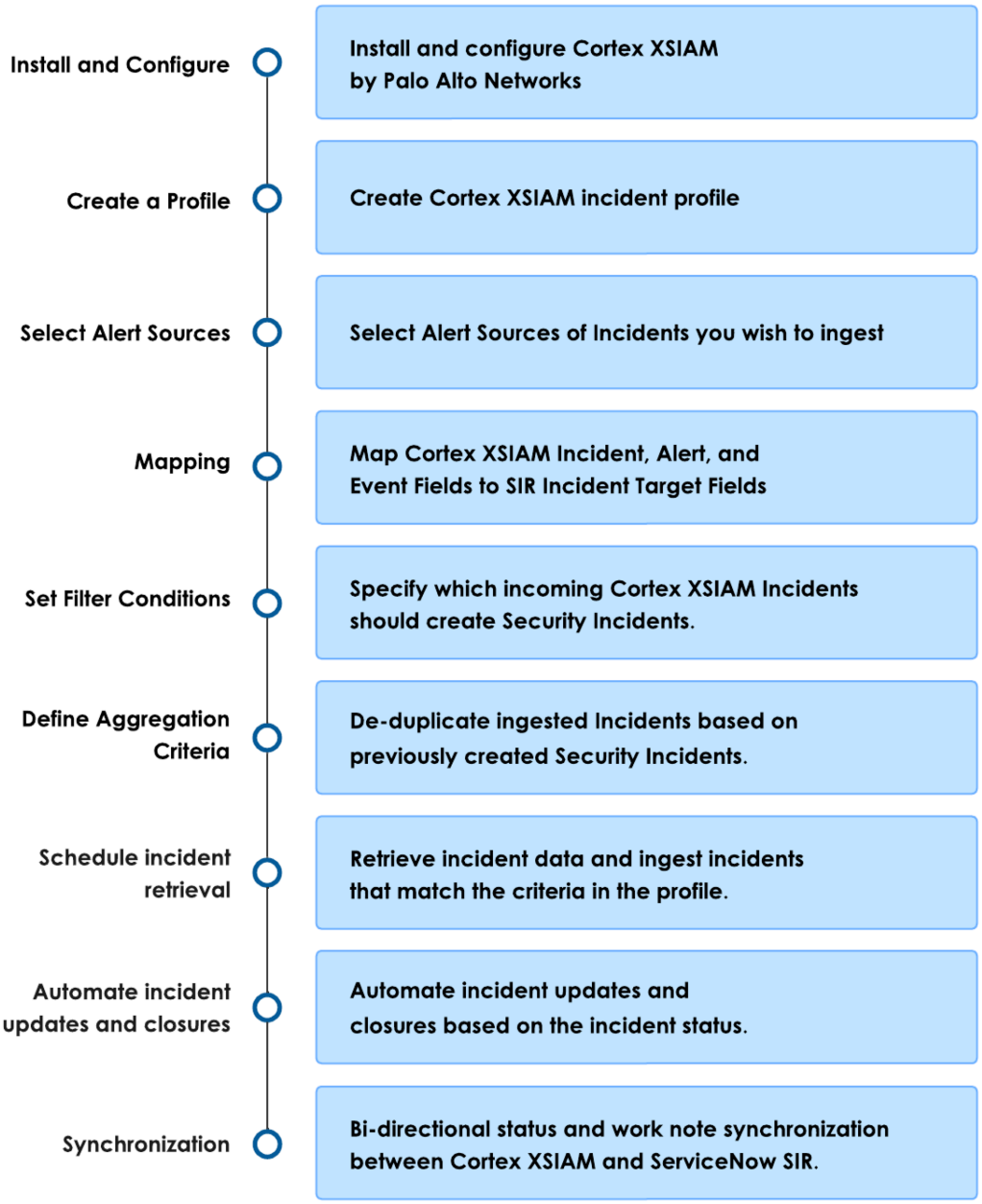
Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview of Cortex XSIAM integration

Security teams can leverage XSIAM's detection capabilities alongside ServiceNow®'s workflow Orchestration without manual updates or context switching for a rapid issue resolution.

See the following graphic to learn how Cortex XSIAM integrates with the ServiceNow AI Platform Security Operations applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Key Features

Use the key features of this integration to do the following actions:

- Create profiles for incident ingestion.
- Filter out noisy alerts and ingest only the actionable cases into ServiceNow® SIR.
- Map Cortex XSIAM Incident, Alert, and Event Field to SIR security incident fields.
- Correlate incidents to existing open security incidents so that you don't have to create duplicate security incidents.
- Bi-directional synchronization of status, priority, and work notes between Cortex XSIAM and ServiceNow® SIR.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install and Configure

Install and configure Palo Alto Networks XSIAM integration for Security Operations application from the ServiceNow Store on your ServiceNow AI Platform® instance.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin because this role inherits the required permissions by default.

Procedure

1. Download **Security Incident Response Integration with Palo Alto Networks XSIAM** integration from the ServiceNow® Store and install it.
2. Navigate to **All** > **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for **Security Incident Response Integration with Palo Alto Networks XSIAM** tile, and select **Configure**.
4. On the form, fill in the fields.

Security Incident Response Integration with Palo Alto Networks XSIAM form

Field	Description
Name	Name of the Cortex XSIAM integration.
Authorization Key	Secret API key to authenticate XSIAM API requests. The Authorization Key should have Instance Administrator role.
Key ID	API key ID associated with the authorization key.
API URL	URL of the XSIAM tenant.

5. Select **Submit**.
   The configured integration tile displays.

What to do next

Create an incident profile

Create an incident profile

Determine the Cortex XSIAM incidents that are suitable for creating security incidents by creating an incident profile in your ServiceNow AI Platform® instance.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Procedure

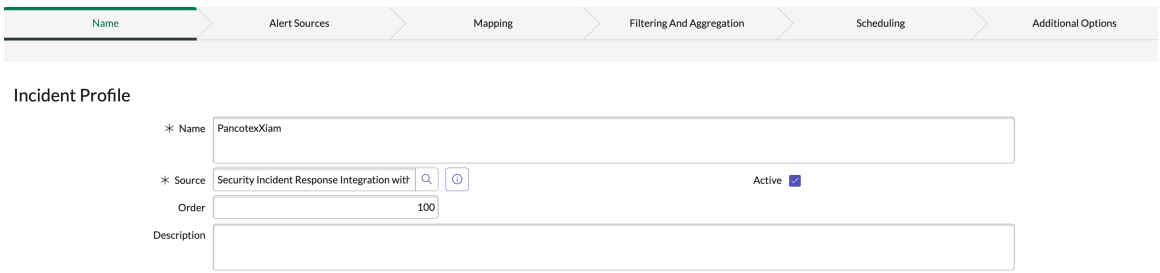
1. Navigate to **All** > **Palo Alto Networks XSIAM** > **XSIAM Profile**.
2. Select **New** to create a new profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the form, fill in the fields.

Incident Profile form

Field	Description
Name	Name of the profile. This name is also the default name for the security tag associated with this profile.
Active	Option to make the profile active. When a profile is active, the ServiceNow AI Platform® actively polls XSIAM incidents and corresponding security incidents are created in ServiceNow AI Platform® when the filtering conditions are matched.
Source	XSIAM tenant that you configured to ingest incidents. If you have multiple tenants configured, select the appropriate tenant for the incident types you are planning to ingest for the profile.
Order	Priority in which the profiles are executed when two or more profiles share triggering conditions. Priority values are provided as 100 (the default value), 200, 300, and so on. The profile with the lowest number has the highest priority.
Description	Optional description of the profile.



4. Select **Continue**.

   The initial incident profile is created with basic information. Saving the profile at this point enables you to continue with defining the profile in case you're interrupted.

5. **Optional:** Continue with the profile definition process immediately.
   a. Select the profile you created.
   b. Select **Alert Sources** in the progress bar.

What to do next

Set Alert Sources

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set Alert Sources

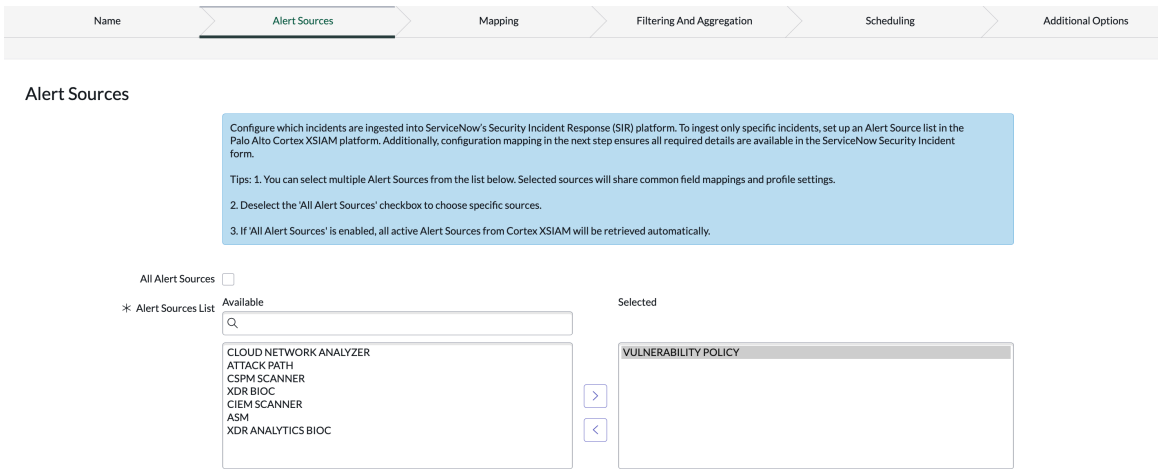
Select Alert Sources to map corresponding incidents to a security incident. Alert Sources are refreshed every time a profile is opened and new rules are available for selection. The Cortex XSIAM integration supports multiple profiles.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Procedure

1. If you are not continuing from the previous section of the incident profile definition process, access the profile you are defining.
   a. Navigate to **All** > **Palo Alto Networks XSIAM** > **XSIAM Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Alert Sources** in the progress bar.
2. Clear the **All Alert Sources** check box to select specific Alert Sources.
   Selecting this check box will retrieve all active Alert Sources from XSIAM.
3. In the Alert Sources List search field, enter the Alert Source name created in the XSIAM portal.
4. Select the Alert Source.
5. Use the right arrow **(>)** to move the rule from **Available** to **Selected** column.



6. Select **Continue**.

What to do next

Map incident fields

Map incident fields

Map Cortex XSIAM Incident, Alert, and Event Fields to SIR Incident Target Fields.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Select one of the Sample Ingestion Methods in the Field Mapping section.

Sample Ingestion Methods

Field	Description
All default Incident and Alert Fields	Use this ingestion method to view the static list of all the Incident, Event, and Alert fields. This method contains only default field names without any values.
Retrieve Recent Incidents	Use this ingestion method to import the most recent Incidents and alerts. If the XSIAM incident contains multiple alerts, the earliest alert that is part of the incident is shown in the mapping section. During ingestion as well the earliest security alert field values will be used. You can ingest 5 sample incidents. The sample field values populate when the profile ingests the sample incidents. You can map these incidents to the **SIR Incident Target Fields**. The Incident fields and values appear as individual tabs.

2. To add fields to the default fields that are displayed on the security incident, do the following actions:

   a. Select ⊕ Map another field in the SIR Incident Target Fields section.
   It shows a list of SIR fields, from which you can select a new field.

   b. In the Security Incident column, expand the list that is displayed and then select a field.

   > **Note:** Multiple observables can be displayed on the same security incident. For example, the **Observable** field can be mapped multiple times with different values. Similarly, the **Configuration Item** and **Work notes fields** support multiple values. If you try to map two values to a field that can't support multiple values, you see an error message that this field does not support multiple values. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field does not populate on the security incident.

   c. From the Incident and Alert Fields section, drag and drop your field to map it to your new field.

   d. When you select the check box that corresponds to a field, any new or updated changes made in XSIAM will automatically update the respective SIR incident data with the new incident data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: In the base system, the system property sn_sec_pan_xsiam.incident_updates is by default set to False to receive the XSIAM updates related to new alerts that are linked to SIR.

- By default, the Affected Users, Configuration items, and Observables fields are checked. This means that whenever there are new observables or associated configuration items, or affected users that gets added to the incident then that information is automatically extracted and populated in the respective related lists in the Security Incident Response (SIR) during that polling interval.
- For any other fields, you must select the check box that corresponds to a field for any new or updated changes made in the XSIAM incident record within XSIAM. This will automatically replace the respective SIR incident data with the new incident data.

Important: Due diligence is required to be done before selecting this functionality as overriding the existing data may result in unstable data for the analyst to work with and any other automation that is set even by the field values of security incident may also get affected. So, it is very important to do the due diligence before you select any override functionality.

3. To remove a field, use the Remove item button next to the input expression field in the SIR Incident Target Fields section.
4. To map a field value from the Incident and Event Fields section to a field on the SIR incident Target Fields section, use one of the following actions:

   a. Drag the Incident field name (for example, id) and drop it next to a field name in the SIR incident Target Fields column.

      You can match any value from the Incident, Event, and Alert fields section to a field on the SIR incident Target Fields section. Fields are color-coded so that you do not overlook or duplicate incident fields in the mapping process. Light blue fields indicate that an incident field is not yet selected and mapped on the security incident. You may prefer to associate an incoming incident fields with more than one field on a security incident. A gray field indicates that a field has been selected and mapped to a field on the security incident. This way, you can visualize which field values have been added to the security incident and if any remaining important incident information remains unmapped.

   b. You can add a combination of text and field.
   For example, `Incident name is ${Incidents: name}$`. Here `Incident name is` can be manually entered while `${Incidents: name}$` is mapped from the Incident and Event Fields section.

   c. You can manually enter and map a source Incidents or Events fields to a target field.

      - To manually map a source incident field use the ${field name}$ format. For example, to map an incident field Severity, the format is`${Incidents: severity}$`.
      - To manually add Incident, Event, and Alert fields, use the `${Source: field}$` format. For example, `${Incidents: incident_name}$`.

   This integration classifies certain observable sub-types. When you map a Cortex XSIAM field with the SIR observable field, the auto-classifies the observable. If you want to generically map the incoming Cortex XSIAM observable to the observable type in, then drag and drop the Incident and Event field in the Observable field. However, if you aware of the observable type for the incoming Cortex XSIAM observable, then map specifically to the Observable type

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

field. Some examples of specific observable types in include Observable(Domain name), Observable(Email address), Observable(IP address (V4)), and Observable(Host name).

Sometimes, incident field values in Cortex XSIAM may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical.

5. To format a field translation for a new field from a Cortex XSIAM Incident to match a field value on a Security Incident, select the **Click here** link in the **SIR Incident Target Fields** header.

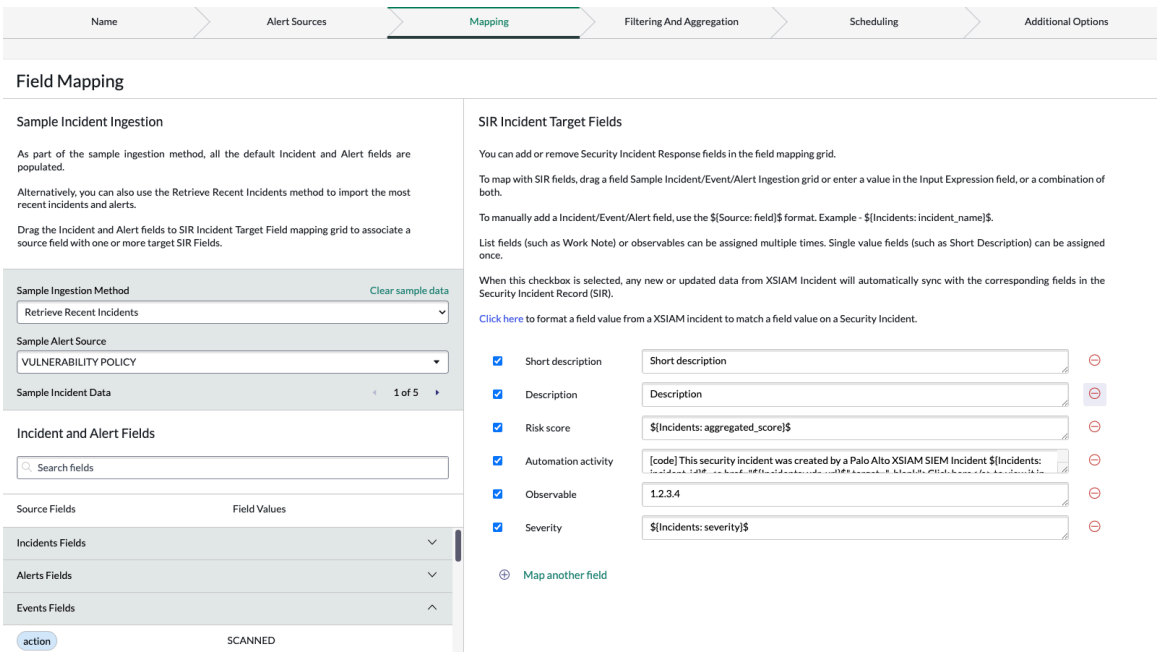
6. To modify the fields which support field translation, select the  script format field translation icon.
The fields that support field translation are **Affected user**, **Configuration Item**, and **Priority**.
For example, click on  icon next to the Category. The Cortex XSIAM Field Translation script editor opens.

7. Enter any changes to the script and select **Update** to save the changes and return to the Mapping page.
For example, for Category define the following in the script editor:

```
"<Incoming Cortex XSIAM Field Value>":"<Category to assign to
 the Security Incident>".
```

This mapping ensures that a profile uses only configured categories.

8. Continue mapping by adding or removing field values.
You can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming Incident must satisfy to create a security incident.



9. Select **Continue**.

What to do next

Define and set filter conditions to specify which incidents should create security incidents.
You can use the same field values (defined in the Mapping section) in the incident Generation Conditions builder (in the Filtering and Aggregation section) to define additional criteria that an incoming incident must satisfy to create a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see Define filter and aggregation criteria

Define filter and aggregation criteria

Define and set filter conditions to specify which incoming Cortex XSIAM Incidents should create security incidents. You can also define additional Incident field criteria that allows an incoming Incident to be appended to an open security incident instead of creating an incident.

Set filtering conditions

Set filter conditions for which Palo Alto Cortex XSIAM incidents create security incidents in ServiceNow.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

About this task

Filtering helps you isolate security incidents and limits the number of security incidents that you create. If you set additional filtering criteria, only the required incidents are ingested without having to change the query or the triggered incident configuration.

Procedure

Select **Filter based on conditions** to define the criteria that an incoming XSIAM incident must satisfy so that a security incident is created.

The options in the first field in the Filter Conditions match the fields that are displayed on the Cortex XSIAM Sample Incident Ingestion section for the Incident that you ingested. These fields are dynamic and change depending on the Incident that you ingest. The criteria that you enter is case-sensitive. Verify that the criteria that you define matches the values of the Incident.

Use the filter condition *`incident_id`* for the following fields with multiple values:

- Severity
- creation_time
- alert_categories
- alert_count

Because the filter condition can retrieve only strings, you must use the *`incident_id`* filter condition for the above fields to ensure that the data is filtered correctly.

Define aggregation conditions

Select Aggregation Conditions to define additional incident field criteria that allows an incoming incident to be appended to an open security incident instead of creating a new one.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Procedure

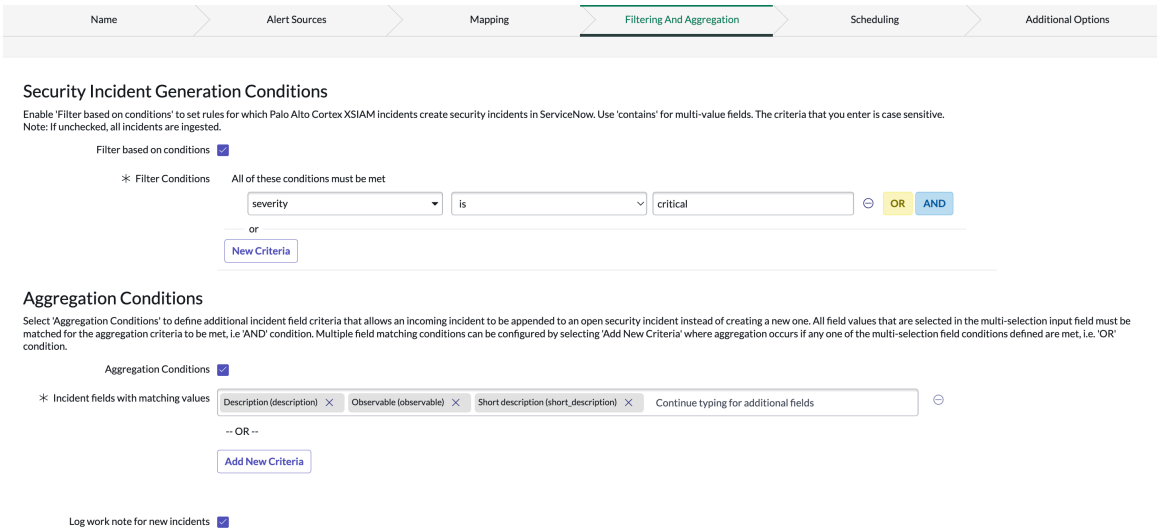
1. Select **Aggregation Conditions** check box.
2. In the **Incident fields with matching values** field, enter the field values that you want to match on existing security incidents in your ServiceNow AI Platform instance.
   All field values that you selected in the multi selection input field must match so that the aggregation criteria is met and that this incoming incident can be appended to an existing security incident. This selection implies it is an *AND* condition where fields, such as Observables and Configuration Items that may have multiple field values, are mapped to them.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If only a subset of the values is matched, the Cortex XSIAM Incident aggregation conditions are not met and a new security incident is created.

3. Select **Add New Criteria** to add multiple field matching conditions.
   The aggregation occurs if any one of the multi selection field conditions that you define are met. This selection implies the *OR* condition.
4. Select **Log work note for new Incident** to update the work note for a new incident when it is added to a security incident.

   The work note logs that a new incident is added and includes a link to the incident details. The log work note also updates more details that you add to the work note field in your mapping section.



5. Select **Continue**.

What to do next

Set a schedule to retrieve the incident data and ingested incidents that match the criteria in the profile. For more information, see Schedule incident retrieval.

Schedule incident retrieval

Configure a schedule to define how and when you pull incidents from Cortex XSIAM tenant.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Procedure

1. If you are not continuing from the previous section of the Filtering and Aggregation criteria, access the profile you are defining.
   a. Navigate to **All** > **Palo Alto Networks XSIAM** > **XSIAM Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Scheduling** in the progress bar.
2. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduling form

Field	Description
Ongoing incident ingestion	Option to set ongoing incident ingestion that the ServiceNow AI Platform instance pulls from the Cortex XSIAM tenant for new incidents. Security incidents are created if triggered incidents are found and the incident generation filtering criteria matches.
Polling increment (minutes)	Polling frequency defined in minutes.
Set incident ingestion time	Option to add Date and time for the initial ingestion.
Initial incident ingestion time	Date and time that you specify for the incident ingestion.
One-Time Retrieval	Option to enable one-time retrieval of historical Cortex XSIAM incidents and followed by the reconciliation of the data. When processing the data, both ongoing incidents and historical data are pulled. **Note:** The retrieved historical Cortex XSIAM incidents undergo de-duplication checks to avoid any duplicates within the Security Incident Response application.
Since date	The date since historical incidents were ingested from Cortex XSIAM.

3. Select **Continue**.

What to do next

Automate incident updates and closures

Automate incident updates and closures

Automate incident updates and closures based on the incident status. The Cortex XSIAM integration enables incidents to create security incidents and also to update the incidents after they are created or closed.

Before you begin

Role required: sn_si.admin, sn_si.ingestion_profile_admin

Procedure

1. If you are not continuing from the previous section of the Scheduling process, access the profile you are defining.
   a. Navigate to **All** > **Palo Alto Networks XSIAM** > **XSIAM Profile**.
   b. Select the profile you are continuing to define.
   c. Select **Additional Options** in the progress bar.
2. On the form, fill in the fields.

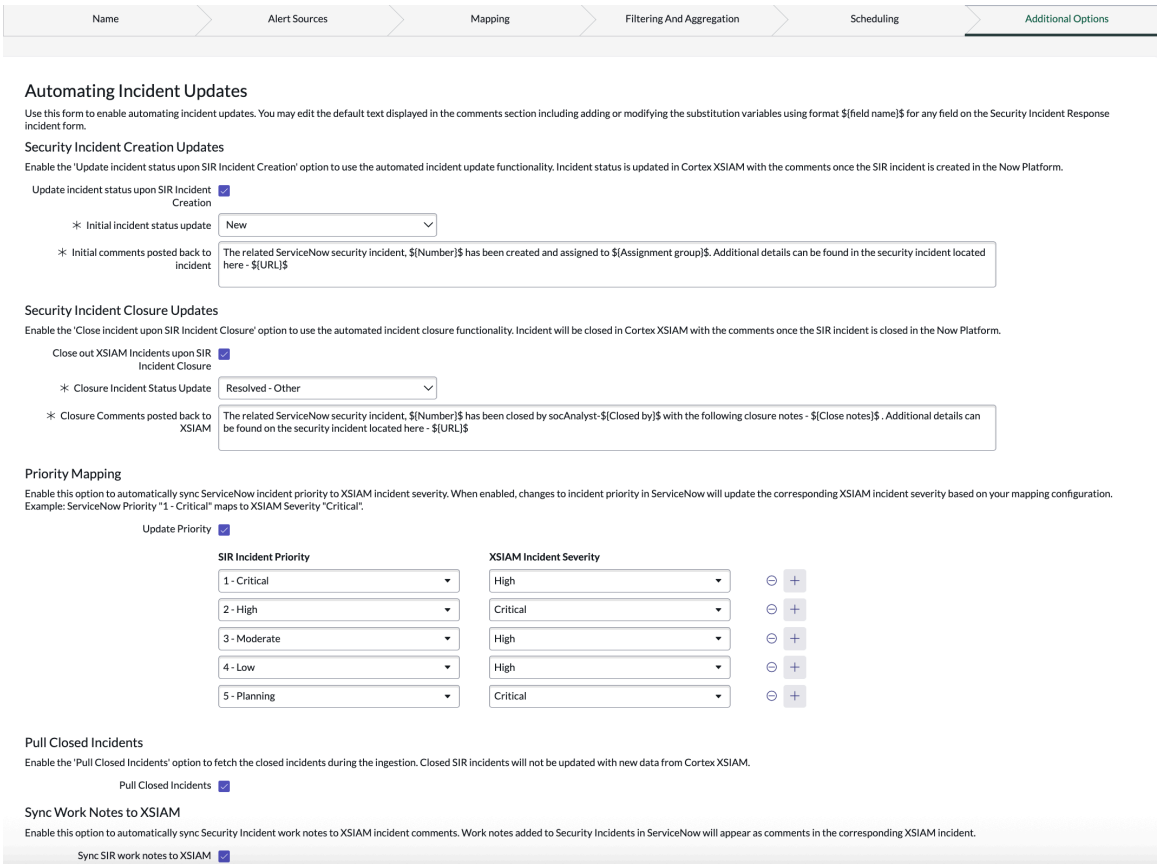
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Automating Incident Updates form

Category	Field	Description
Security Incident Creation Updates	Update incident status upon SIR Incident Creation	Option to use the automated incident update functionality. The Cortex XSIAM incident status is updated with the comments after the SIR incident is created in the ServiceNow AI Platform.
	Initial incident status update	Initial incident status that is updated in the Cortex XSIAM environment, either New or In Progress.
	Initial comments posted back to incident	Initial comments that are posted to the incident in the Cortex XSIAM environment.
Security Incident Closure Updates	Close out XSIAM incidents upon SIR Incident Closure	Option to use the automated incident status update functionality. Incidents will be closed in XSIAM with the comments given after the SIR incident is closed in the ServiceNow AI Platform.
	Closure Incident Status Update	Status update in the Cortex XSIAM incident when the security incident is closed in SIR.
	Closure Comments Posted back to XSIAM	Comments posted to the incident in the Cortex XSIAM incident when the security incident is closed in SIR.
Priority Mapping	Update Priority	Option to sync ServiceNow Incident priority to XSIAM Incident severity. When enabled, changes to incident priority in ServiceNow will update the corresponding XSIAM incident severity based on your mapping configuration. For example, ServiceNow Priority "1 - Critical" maps to XSIAM Severity "Critical".
Pull Closed Incidents	Pull Closed Incidents	Option to fetch closed incidents during ongoing ingestion and one-time retrieval. Closed SIR incidents will not be updated with new data from XSIAM.
Sync Work Notes to XSIAM	Sync SIR work notes to XSIAM	Option to sync Security Incident work notes to XSIAM incident comments. Work notes added to Security Incidents in ServiceNow® will

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Category	Field	Description
		appear as comments in the corresponding XSIAM incident.



3. Select **Finish**.
4. Activate the profile.
   a. Select the **Name** section of the progress bar.
   b. Select the **Active** check box.
   c. Select **Continue**.

Security Incident Response integration with Zscaler

You can use the Security Incident Response integration with Zscaler product to connect your Zscaler Internet Access server (ZIA) logs with the ServiceNow AI Platform. This integration enables you to view dashboards, create custom alerts, and help you investigate security incidents.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview

The Zscaler internet and web gateway product is delivered from the cloud. It provides you with the key data points and insights into your enterprise security environment. Security Incident

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Response integration with Zscaler connects the Zscaler Internet Access product with your ServiceNow AI Platform instance. By using the Zscaler product on the ServiceNow AI Platform, you get more insights into your organization's internet usage.

Key features of the integration

This integration includes the following key features:

- Reputation lookup of observables against the global threat library that the Zscaler product maintains.

  Note: The Zscaler global threat library lists threats by trends, country of origin, target destination, volume, and various threat categories. This global threat library enables you to investigate your observables against the global threat landscape.

- Maintenance of observables in a block list or allow list on the Zscaler product.
- Ability to fetch and review sandbox reports from the Zscaler product for an MD5 hash. The Cloud Sandbox feature in the Zscaler product runs and analyzes files in a virtual environment to detect malicious behavior.
- Security alerts from Patient 0 events that are generated in the Zscaler product when a user downloads an unknown malicious file.
- Multiple URL category lists that act as block lists or allow lists as defined in the Zscaler product.
- ServiceNow AI Platform security incidents that can be tagged to identify the URL category that the observables are added to.
- Expiration periods that maintain the size of the URL category list entries by automatically expiring or removing the older entries.
- Approval workflow for adding and removing observables from the URL category lists.
- URL category entries that can be linked to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

Learn about this integration

Document identifier	Document title
Zscaler product documentation website	ZScaler Product Documentation website
ServiceNow product documentation website	ServiceNow Product Documentation website

Getting started with Security Incident Response integration with Zscaler

Activate and set up the Zscaler Internet Access product to interface with your ServiceNow AI Platform instance and Security Incident Response product.

Checklist

Setup task	Description
Assign and verify the required ServiceNow AI Platform and Security Incident Response roles.	These roles are required for configuration and verification of the expected results:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description

	• The admin role installs the integration from the ServiceNow Store and assigns the sn_si.admin role.
	• The sn_si.admin role performs the following tasks:
	  ○ Configures the integration.
	  ○ Creates, activates, and removes the URL Category lists.
	  ○ Assigns the sn_si.analyst role.
	• The sn_si.analyst role creates entries and works with security incidents.

Verify that the ServiceNow core applications are installed and activated before you configure this integration.	The ServiceNow Integration Hub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] plugin is required. The Security Incident Response plugin (com.snc.security_incident) is required. This plugin automatically installs all the dependencies for the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications for the integration. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If these applications are not already installed, install and activate each application one at a time in the following order: **1.** Security Incident Response Dependency (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Security Support Orchestration **5.** Threat Intelligence Support Common **6.** Trusted Security Circles **7.** Security Operations Setup Assistant **8.** Security Incident Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description

Verify the Zscaler versions.	• This integration is supported on Zscaler Internet Access version 1.0 or later.
	• This integration is tested with the following Zscaler versions:
	  ○ Zscaler Client Connector for Windows - 3.0
	  ○ Zscaler Client Connector for macOS - 3.0
	  ○ Zscaler Client Connector for Linux - Beta
	  ○ Zscaler Cloud Connector - 6.1

Verify that you have the required Zscaler permissions and have configured access to the Zscaler Internet Access APIs.	• You must have the admin credentials for Zscaler Internet Access. • You must have a valid cloud service API subscription. Zscaler Support must provide your key. • You must have Zscaler Internet Access admin credentials (user name and password). API authentication is based on a combination of the API key and Zscaler Internet Access admin credentials. **Note:** For more information on managing the Zscaler Internet Access API keys, see the Zscaler documentation.

Configure access to Zscaler Internet Access APIs

Configure access to the Zscaler Internet Access server to authenticate the secure connection between the ServiceNow AI Platform instance and the Zscaler server.

Before you begin

Role required: Zscaler Internet Access admin

ServiceNow supports the following API role configurations for the Zscaler integration.

- **Service Admin Role**:

  Create the API key using a role with Service Admin privileges.

  This configuration provides full functionality and is recommended for environments without strict role-segregation requirements.

- **Least-Privilege Role (Supported)**:

  For users who require reduced privilege, ServiceNow supports a least-privilege configuration.

  Create a custom role with the following permissions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Security: Custom**
- **Malware Protection, Sandbox, & Advanced Threat Protection: Full**

When configured with these permissions, the integration runs as expected.

About this task

After Zscaler enables your API subscription for your organization's cloud service, it is available in the Zscaler Internet Access API key management page with the base URL. Your organization can only have one API key or token. Delete the existing key or token before you add a new one.

The base URL for the API is `${Cloud_Name}/api/v1`. Check the Zscaler cloud name that was provisioned for your organization and use it to replace `{Cloud_Name}` in the base URI. Some examples of the base URL are:

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Note: For more information about the Zscaler Internet Access administration portal, see the Zscaler API key management documentation and the Zscaler Portal documentation.

Procedure

1. Log in as an admin to the Zscaler Internet Access administration portal.
2. Navigate to **Administration** > **Cloud Service API Security**.
3. Select **Add API Key**.
   If you do not see the **Add API Key** option, delete the existing key.
   The new API key is immediately valid and is displayed in the tab.

Result

You have retrieved the base URL and the API key to configure access to Zscaler from the ServiceNow AI Platform instance.

Install and configure Security Incident Response integration with Zscaler

Install and configure the Security Incident Response integration with Zscaler internet Access product from the ServiceNow Store to start using the integration on your ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.admin

Procedure

1. Download the Security Incident Response integration with Zscaler product from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the Security Incident Response integration with Zscaler tile and select **Configure** > **Create new configuration**.
4. On the form, fill in the fields.

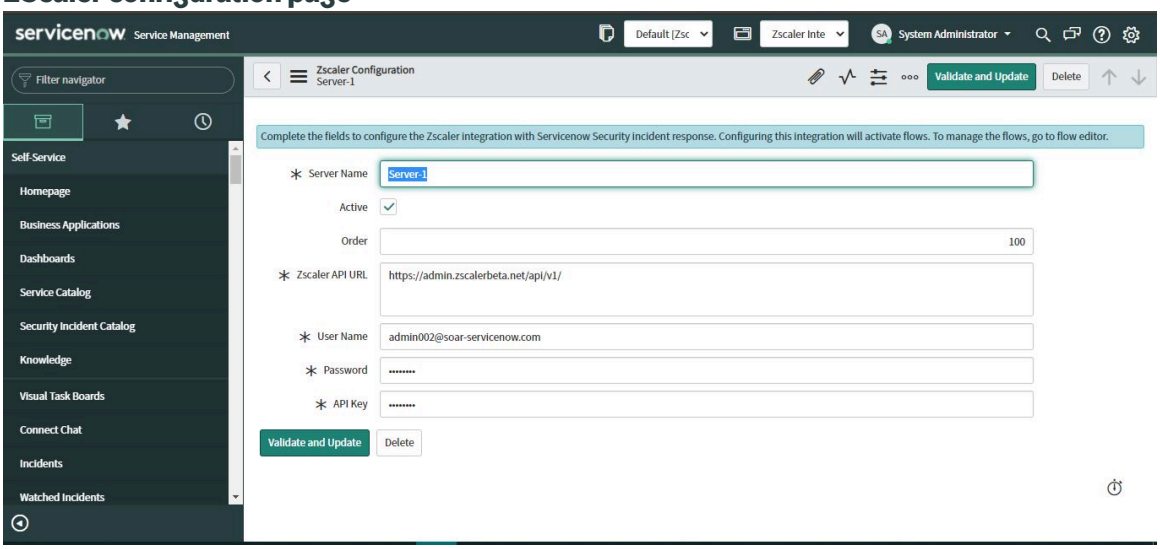
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Zscaler Configuration form

Field	Description
Server Name	Zscaler server name. For example, ZSserver.
Active	Indicator that the profile is active.
Order	Flow priority. The value for this field indicates the order of the workflows when two or more profiles share triggering conditions. The flow with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, 400. The default is 100.
Zscaler API URL	Base URL that hosts the Zscaler API. For example, https://example.zscalerbeta.net
User Name	User name for the Zscaler Internet Access admin account.
Password	Password for the Zscaler Internet Access admin account.
API Key	API key that you obtained from the Zscaler Internet Access administration portal. **Note: The user must have sn_si.admin role to setup the integration.**

The following example shows the Zscaler configuration page.

ZScaler configuration page



5. Select **Validate and Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
After you validate and save this configuration, return to the Zscaler Configurations page.

Add Zscaler Internet Access URL category lists

Add the URL categories that are available in the Zscaler Internet Access product to the ServiceNow AI Platform instance to specify an action for each URL so that you have easy access for granular filtering and policy creation.

Before you begin
Role required: sn_si.admin

About this task
The Security Incident Response integration with Zscaler provides a default allow list and deny list URL category lists to help filter content.

The URL categories that you add in the ServiceNow AI Platform instance should already be in your Zscaler Internet Access environment. You can't use Security Incident Response integration with Zscaler to create URL categories on Zscaler.

Note: For more information on URL category lists in the Zscaler product, see the Zscaler documentation on URL Categories.

Procedure
1. Navigate to **All** > **ZScaler Integration** > **ZScaler URL Category Lists**.
2. Click **New**.
3. On the form, fill in the fields.

Zscaler URL Category Lists form

Field	Description
Source	Name of the server. You can view only the previously configured Zscaler Internet Access servers from the URL category list.
Active	Indicator that the URL category list is active.
URL Category	Field that is enabled after you select the source. You can view the list of URL categories that are created in Zscaler.
Expiration Period (days)	Expiration period of the URL category list. 0 (by default) indicates that the URL category list entry never expires. By changing this value, any observable that was added to this URL category is active for the number of days that you enter. You can enter a minimum value of 1. For example, if you set the expiration period to 30 days, the entries are removed from the category list after 30 days.
Display Tag	Security tag that appears on the SIR security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	When you enable the **Display Tag** option, the Zscaler Tag for observables field is available on the form.
Create Change Request	Change request and change tasks in your ServiceNow AI Platform instance for the records that are attached to the URL category list. When you enable the **Create Change Request** option, the **Change Request** field is available on the form.
Require Approval	List of approver groups. After you submit a request, an approval is required from the group to complete the request. When you enable the **Require Approval** option, the **Approvers for adding observables** and **Approvers for removing observables** fields are available on the form. ○ **Approvers for adding observables**: Select the approvers using the look up to add the observables from the **Zscaler URL Category List** page. This option will allow you to add the user group(s) for approvals. ○ **Approvers for removing observables**: Select the approvers for removing the observables using the look up from the **Zscaler URL Category List** page. This option will allow you to remove the user group(s) from the approval list.
Description	Description of the Zscaler URL category list. Use this field for adding more details about the URL category record.

4. Click **Submit**.
   A successful submission triggers an email notification to the approval group.

Submit observables from a security incident record to a URL category list

Submit observables that are attached to a security incident record to a configured URL category list by using the allow or block request. Adding observables to the allow or block list for security scans allows users to review content from these URLs and gain access to trusted content.

Before you begin
Role required: sn_si.analyst

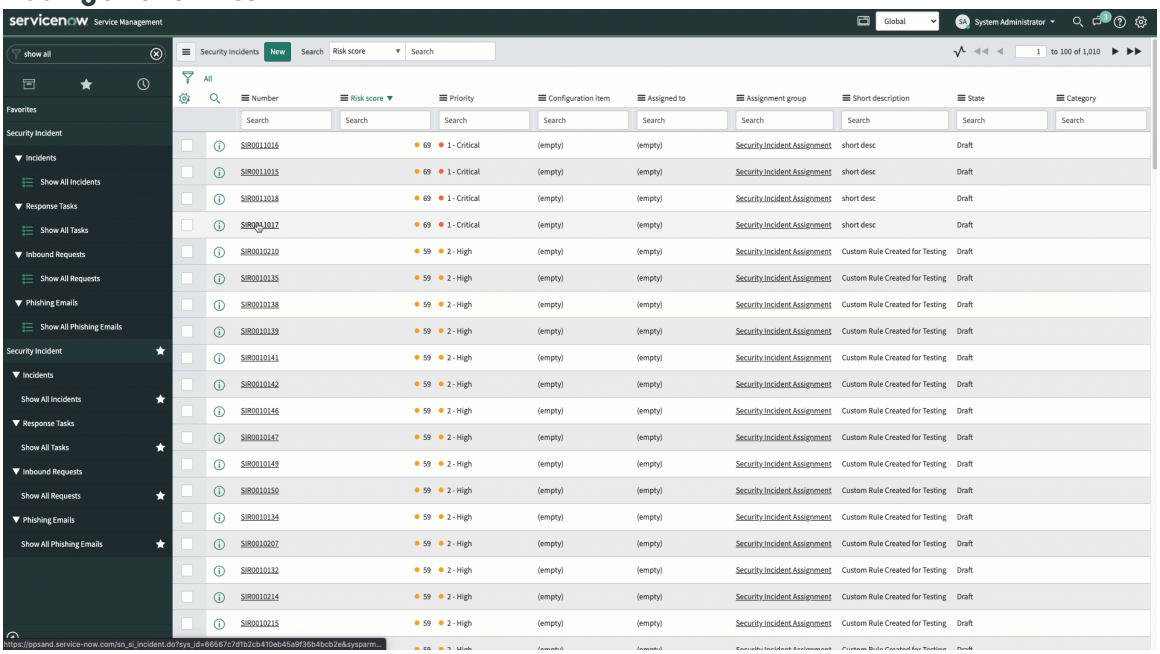
About this task
You submit observable entries by using the allow or block request action from the Associated Observables related list. Observables are artifacts found on a network or operating system that are likely to indicate an intrusion. Use the list of URL Categories configured previously to select the observable that you want to submit. After you submit the request, an approval request is sent to your approval group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**.
   In this example, you see how to select a security incident and an observable, and how to add an allow list.

Adding an allow list



2. Select the security incident that you want to associate with the Zscaler allow or block request.
3. Click **Show All Related Lists** and the **Associated Observables** tab.
   If you do not find any observables, click **New**.
4. Select an observable and then from the actions menu, click **Allow/Block Request**.
5. In the Allow/Block Request dialog box, select whether to perform the allow or block request on the observable.
6. Click **Submit**.
7. View the Work notes to see the status of your submission and the security tags.
   Click the links in the Work notes for more information about the status or to analyze the details on the Workflow Studio. Security tags are metadata on the responding record and define who should have access to specific types of security content.
8. To view the status of the observable that you selected, navigate to **Zscaler Integration** > **Zscaler URL Category List Entries**.
9. In the Zscaler URL Category List Entries page, click the observable to view the record.

Approve observables to URL category lists

Approve observables that are added to a URL Category List so that observable entries are in the appropriate allow or deny lists.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Zscaler Integration** > **Zscaler Approvals**.
2. Select the record to approve.
3. Click **Approve**.
   The approvers group receives an email notification for the approval request. After the approvers click the **Approve/Reject** link in the email, the status changes to approved.

Submit the security incident to the Zscaler URL category list

Submit entries directly for observables that are not associated with a specific ServiceNow AI Platform security incident record so that observable entries are in the appropriate allow or deny lists.

Before you begin
Role required: sn_si.admin

About this task
You can also add observables to the URL category list directly from the Observable record.

Procedure

1. Navigate to **All** > **Zscaler Integration** > **Zscaler URL Category List Entries**.
2. Click **New**.
3. On the form, fill in the fields.

Zscaler URL Category Lists Entries form

Field	Description
Entry Value	Observable name. If a matching observable is found, the rest of the form is automatically filled. If no matching observable is found, you must fill in the rest of information manually.
Observable	Value (for example, IP address or hash) that is associated with the observable.
Observable Type	Observable classification, such as an IP address or file hash.
URL Category List	URL category. For example, if an organization uses example.com for Office 365 services, then Zscaler categorizes example.com as Professional Services and Office 365.
Source	Name of the server. You can view only the previously configured Zscaler servers from the URL category list.
Incident count	Number of incidents that this observable appears in. This value is automatically updated when the observable is added to another incident manually or through a workflow.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	Indicator that the URL category list is active.
Status	Status if the observable is approved or rejected.
Expiration Period (days)	Expiration period of the URL category list. 0 (by default) indicates that the URL category list entry never expires. By changing this value, any observable that you add to this URL category is active for the number of days that you enter. You can enter a minimum value of 1. For example, if you set the expiration period to 30 days, the entries are removed from the category list after 30 days. **Note:** If you change the default expiration period of the URL category list entry, you see a warning that the period differs from the period that is configured in the selected URL category list.
Additional Information	Field where you can add more details about the observable.

4. Click **Submit**.

Run a threat lookup by using the Zscaler global threat library

Run a threat lookup on an observable by using the Zscaler Internet Access product's global threat library. Zscaler supports lookups against observables type IPs, URLs, and domains.

Before you begin
Role required: sn_si.admin

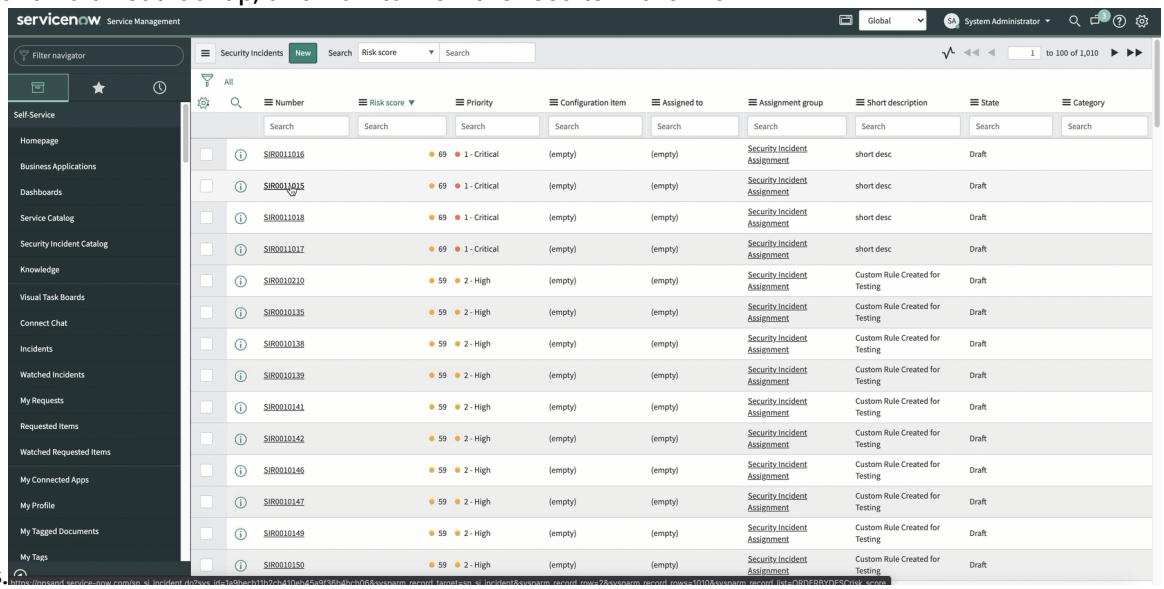
About this task
You can perform threat intelligence lookups on one or more observables to determine whether they are associated with known security threats. When an observable is associated with a security incident for the first time, all the active threat lookup implementations in the ServiceNow AI Platform perform an auto-threat lookup. You can view the results against the Threat Look Up Results related list.

By default, the configuration with the least order is picked to perform the threat lookup against Zscaler Internet Access product's global threat library. You can also perform the threat lookup manually.

Procedure
1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**.
2. Select the security incident that you want to run the threat lookup on.
3. Click **Show All Related Lists** and the **Associated Observables** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select the observable and then from the Actions menu, click **Run Threat Lookup**.
   In this example, you see how to select a security incident and an observable, how to run a threat lookup, and how to view the results in the Work notes.



Result

After you initiate the threat lookup, you can view the Work notes to see the status of your submission.

Submit to Zscaler Sandbox analysis

Use the Zscaler Internet Access products sandbox service to analyzes files in a virtual environment to detect malicious behavior.

Before you begin

Role required: sn_si.admin

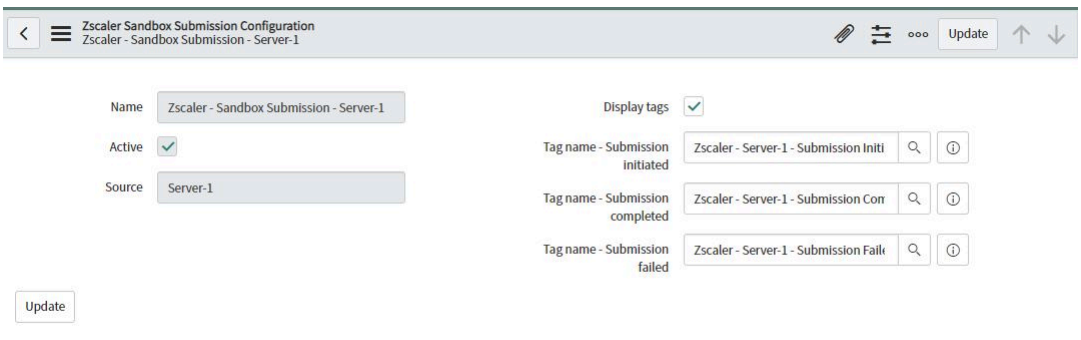
About this task

When you create a Zscaler configuration, a Zscaler sandbox submission is created by default in the Zscaler Sandbox Configuration module.

The name and source fields are auto-filled, and the configuration is enabled by default. You can edit only the display tag and the active options. Zscaler Internet Access product enables you to fetch only the sandbox report for the MD5 hash type observables.

The analysis for the file that is associated with the MD5 hash should be complete and the corresponding report should be in the Zscaler sandbox. If the MD5 hash that you send does not have a report in Zscaler, you get an error message.

Zscaler Sandbox Submission



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show All Incidents**.
2. Select the security incident that you want to run the sandbox analysis on.
3. Click **Show All Related Lists** and the **Associated Observables** tab.
4. Select an MD5 hash type observable and then from the Actions menu, select **Submit to Sandbox**.
   Create an MD5 hash type observable if you do not find an existing MD5 hash type observable.
5. In the File Submission dialog box, select the **Zscaler - Sandbox Submission - Server** option in the Submission configuration and click **Submit to sandbox**.
   After you initiate the sandbox submission, you can view the Work notes to see the status of your submission. A tag is also appended to the security incident.
6. In the Work notes, click the link in the Sandbox Submission Result post.

Result

You can also view the results from the Show All Related Lists and Sandbox Submission Results tab.

Set up email alerts for Patient 0 events

Configure Zscaler Internet Access product to identify and scan for unknown, potentially malicious files, such as Patient 0 events so that you can protect your network from malicious files.

Before you begin

Role required: sn_si.admin, Zscaler Internet Access admin

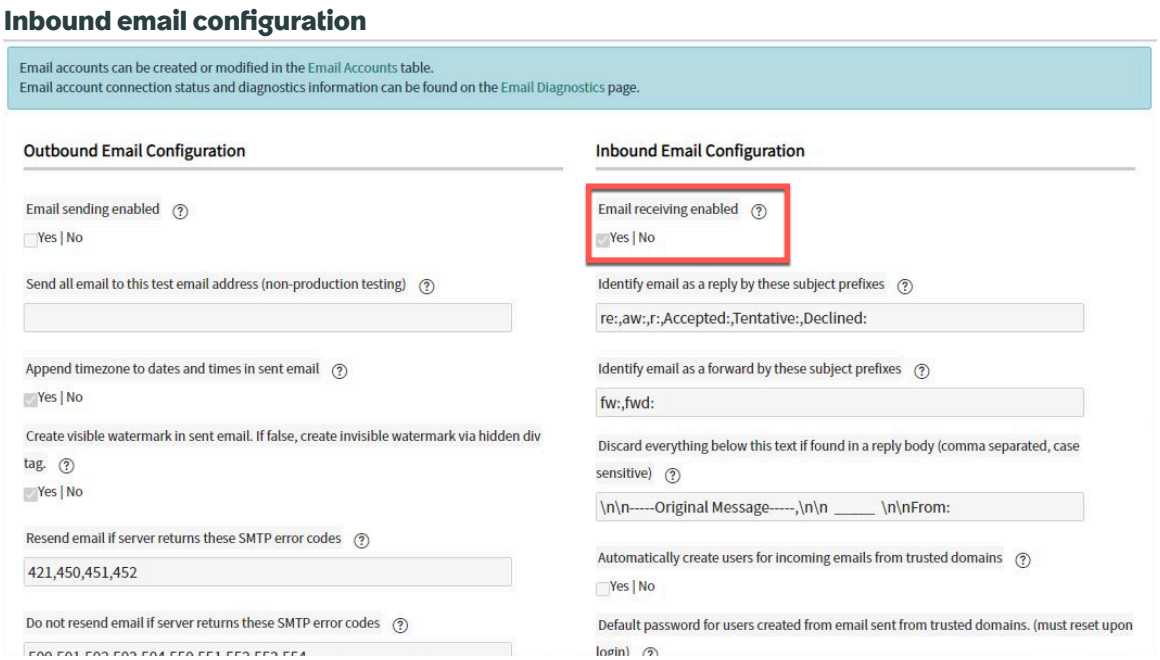
About this task

Patient O is an alert class that includes an unknown file that has been permitted to download but is found to be malicious. The patient 0 event is classified as critical. You can set up the ServiceNow AI Platform to receive email alerts at regular intervals for Patient 0 events.

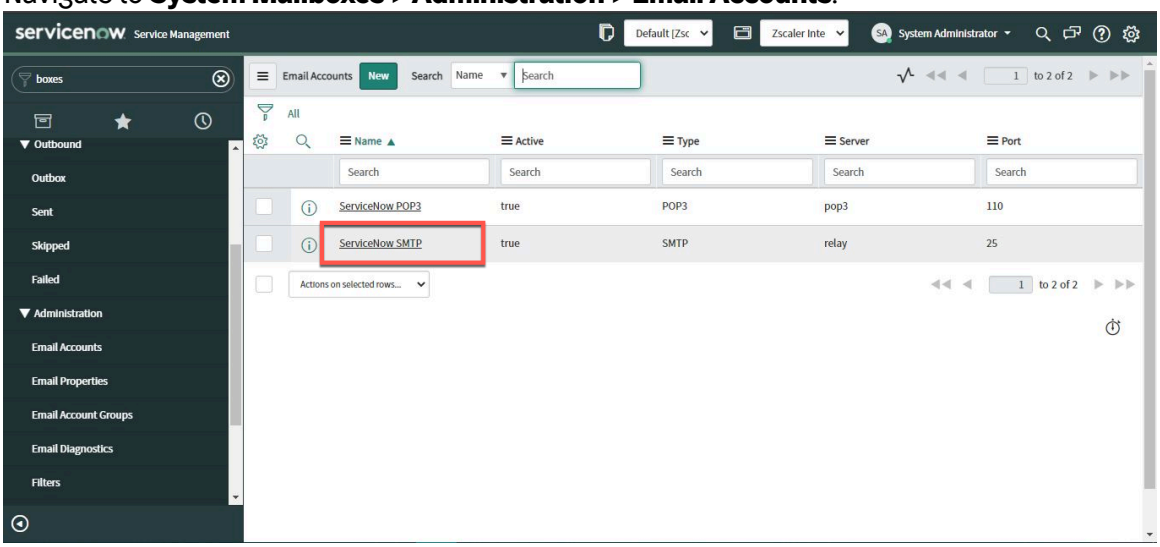
Procedure

1. Navigate to **All** > **System Mailboxes** > **Administration** > **Email Properties**.
2. In the Inbound Email Configuration section, select the **Email receiving enabled** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



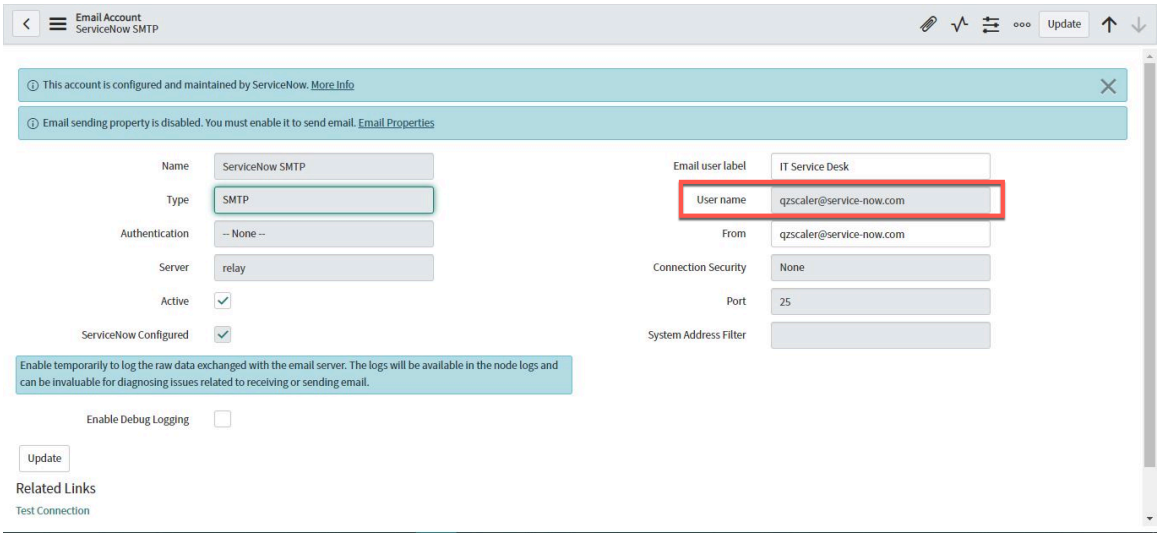
3. Click **Save**.
4. Navigate to **System Mailboxes** > **Administration** > **Email Accounts**.



5. Select the **ServiceNow SMTP** email account.
   Note the user name. The user name that is identified here is the ServiceNow AI Platform email address that you use to configure in Zscaler for Patient 0 alerts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User name for the ServiceNow AI Platform SMTP account



6. Log in to the Zscaler Internet Access administration portal.

   Note: For more information on the Zscaler Internet Access administration portal, see the Zscaler documentation.

7. Navigate to **Administration** > **Alerts** > **Publish Alerts**.
8. Click **Add Alert Subscription**.
9. On the form, fill in the fields.

Add Alert Subscription form

Field	Description
Email	ServiceNow AI Platform SMTP account email address.
Description	Field for adding more details about the Patient 0 alerts.

10. Click **Save**.

ServiceNow Security Operations add-on for Splunk overview

The ServiceNow Security Operations add-on for Splunk allows a Splunk software administrator to collect data and create incidents and events in the ServiceNow AI Platform.

The add-on is installed from Splunkbase.

Important: Splunk is also supported for Managed Service Provider (MSP) environment.

Setup Splunk environment

Configure Application Registry on the ServiceNow instance

Using ServiceNow Security Operations Integration add-on

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk integration setup

Setup procedures for the ServiceNow Security Operations add-on for Splunk include downloading the add-on file in Splunk, installing the add-on, and setting up the ServiceNow instance where security incidents and events are created.

Required role

Before performing Splunk integration setup procedures, be sure to define an integration user with the sn_si.integration_user and sn_si.analyst roles on your ServiceNow instance. Additionally, in order to perform imports, you need the import_transformer role to obtain read and write permission to the security tables. The sn_si.integration_user role should be defined with the import_transformer portion of the role.

Download the ServiceNow Security Operations application

The first step in setting up the ServiceNow-to-Splunk integration is to download the ServiceNow Security Operations application from Splunkbase.

Before you begin

Role required: admin

Procedure

1. Open Splunkbase.
2. Search for ServiceNow Security Operations Integration.
3. Download the application.

Install the ServiceNow Security Operations add-on for Splunk

Install the **ServiceNow Security Operations add-on for Splunk** to link Splunk to ServiceNow.

Before you begin

Role required: admin

Procedure

1. Open Splunk.
2. Click either the **Apps** gear icon, or the **Manage Apps** shortcut menu item.
3. Click **Install app from file**.
4. Click **Choose File**, select sn_sec_ops.spl, and click **Upload**.
5. If prompted, restart Splunk.
   The ServiceNow Security Operations add-on for Splunk is installed and ready to be set up.

Setup Splunk environment

ServiceNow Security Operations Integration enables seamless integration between Splunk and ServiceNow Security Operations. To set up or change the ServiceNow instance where new security incidents and security events are created, use the setup action in the application list.

Before you begin

Install **Event Management** plugin to access the em_event table.

Role required: sn_si.integration_user, sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Note: You're not required to have a profile for this addon. It directly creates the security event or the security incident.

If you want to export events manually and on-demand from your Splunk Enterprise console for the integration, download, install, and set up the ServiceNow Security Operations Integration add-on from Splunkbase in your Splunk Enterprise console.

This ServiceNow extension addon is required so that security incidents can be created from manually exported events in your ServiceNow AI Platform instance. This ServiceNow ServiceNow Security Operations Integration add-on is available on splunkbase.

Procedure

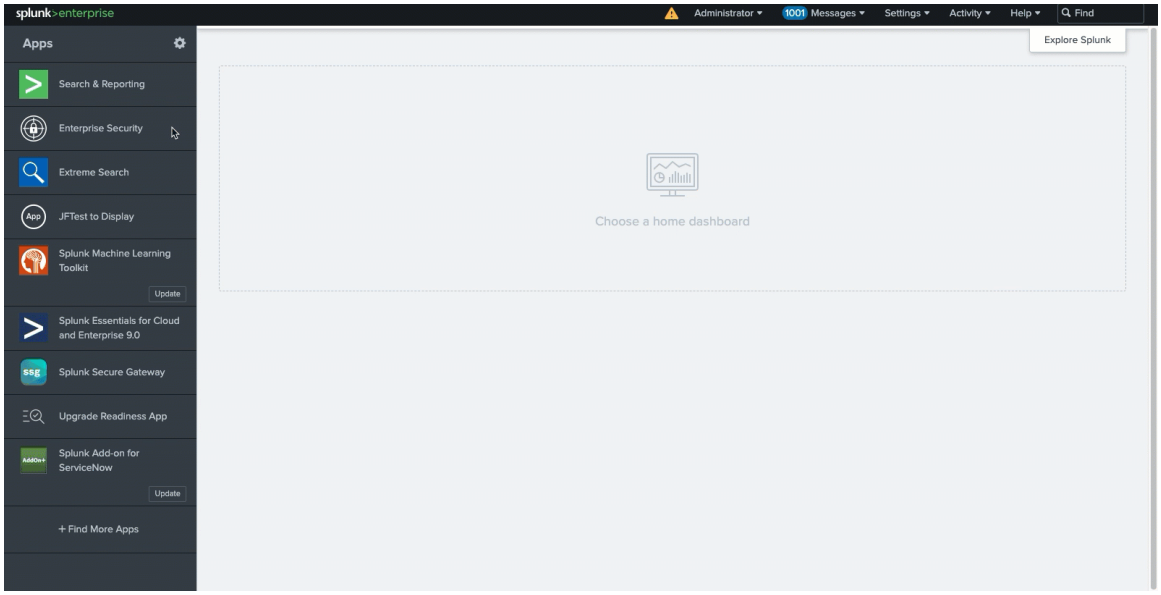
1. Log in to Splunk Enterprise.
2. Select **Manage Apps** gear icon on the menu drop-down list.
3. In the list of applications, search for **ServiceNow** apps using the filter.
4. Look for the **ServiceNow Security Operations Integration** add-on, and select the corresponding **Set up** action.
5. On the form, fill in the fields.

Field	Description
URL	URL of the ServiceNow instance for your Splunk Enterprise Security console or Splunk Cloud instance.
Auth type	Authentication method to be used for API re quests. The available options include: ○ **Basic Authentication**: Uses username and password to authenticate requests. ○ **OAuth 2.0 Authentication**: Uses access to kens to authenticate requests.
Basic Authentication	
Username	Username of the user. User with the (sn_si.integration_user, sn_ si.analyst) role should be present in the Ser viceNow instance specified in the preceding URL field.
Password	Password of the user. User with the (sn_si.integration_user, sn_ si.analyst) role should be present in the Ser viceNow instance specified in the preceding URL field.
Confirm Password	Renter the password to confirm it.
OAuth 2.0 Authentication	
Client ID	Client ID of the app created on the Service Now Server. For information on how to get the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Client ID, see Configure Application Registry on the ServiceNow instance
Client Secret	Client Secret of the app created on the ServiceNow Server. For information on how to get the Client Secret, see Configure Application Registry on the ServiceNow instance
Redirect URL	The URL to be redirected to. Copy and paste this URL in the redirect URL field of the Application Registries record.
Optional Proxy	
Proxy URL	Proxy URL for your Splunk Enterprise Security console or Splunk Cloud instance.
Port	Address of the port.
Username	Username that you created for the Proxy account on the Splunk Enterprise Security console.
Password	Password that you created for the Proxy account on the Splunk Enterprise Security console.
Confirm Password	Renter the password to confirm it.
Logging Level Setup	
Logging Level	The level of reporting logs generated by the integration, meaning the name of the type of information. You can also update the value to the following options: ○ **info** ○ **error** ○ **warn** ○ **debug** By default, the value is **info**.
API Selection	
API Selection	Select one of the following APIs: ○ Table API ○ Import Set API

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Select **Save**.

What to do next

Using ServiceNow Security Operations Integration add-on

Configure Application Registry on the ServiceNow instance

Register the application with the instance to use OAuth authorization.

Before you begin

Role required: admin

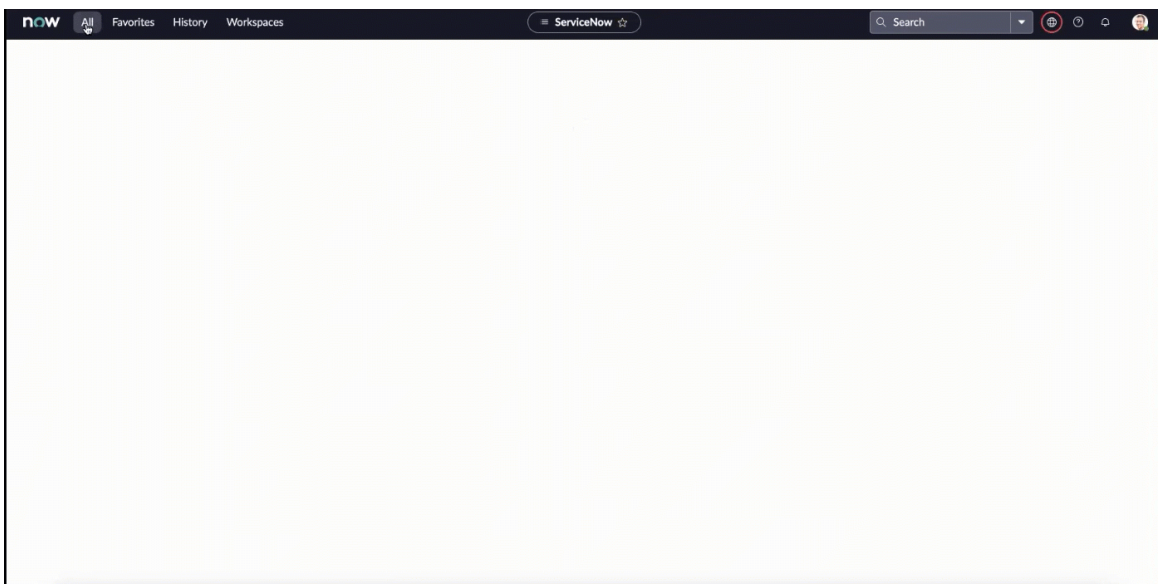
Procedure

1. Navigate to **All** > **System OAuth** > **Application Registry**.
2. Click **New**.
3. Click **Create an OAuth API endpoint for external clients**.
4. On the form, fill in the fields.

Field	Description
Name	A unique name that identifies the application that you require OAuth access for.
Client ID	(Read-Only) The auto-generated unique ID of the application. The instance uses the client ID when requesting an access token.
Client Secret	The shared secret string that both the in stance and the client application or website use to authorize communications with one another. The instance uses the client secret when requesting an access token. Leave this field blank to have the instance auto-gener ate a client secret. To display existing client secrets, click the lock icon.
Redirect URL	The callback URL that the authorization serv er redirects to. Enter as many URLs as need

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	ed for all possible token consumers. The in stance matches the URL of the incoming re quest to one of the redirect URLs. If no match is made, the instance uses the first redirect URL.
Logo URL	The URL that contains an image to use as the application logo. The logo appears on the ap proval page when the user receives a request to grant a client application access to a re stricted resource on the instance.
Application	The name of the application.
Accessible from	Define the application scope. Select one of the following: ○ **All application scopes** ○ **This application scope only**
Active	Select the check box to make the application registry active.
Refresh Token Lifespan	The number of seconds that a refresh token is valid. The instance uses the lifespan value when requesting a refresh token. By default, refresh tokens expire in 100 days (8640000 seconds).
Access Token Lifespan	The number of seconds that an access token is valid. The instance uses the lifespan value when requesting an access token. By default, access tokens expire in 30 minutes (1800 sec onds).
Comments	Additional information to associate with the application.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Right-click on the form header, and click **Save**.
6. Click **Submit**.

Using ServiceNow Security Operations Integration add-on

Create security events and incidents directly from Splunk alerts after setting up ServiceNow Security Operations Integration add-on.

Before you begin

Role required: sn_si.integration_user, sn_si.analyst

Procedure

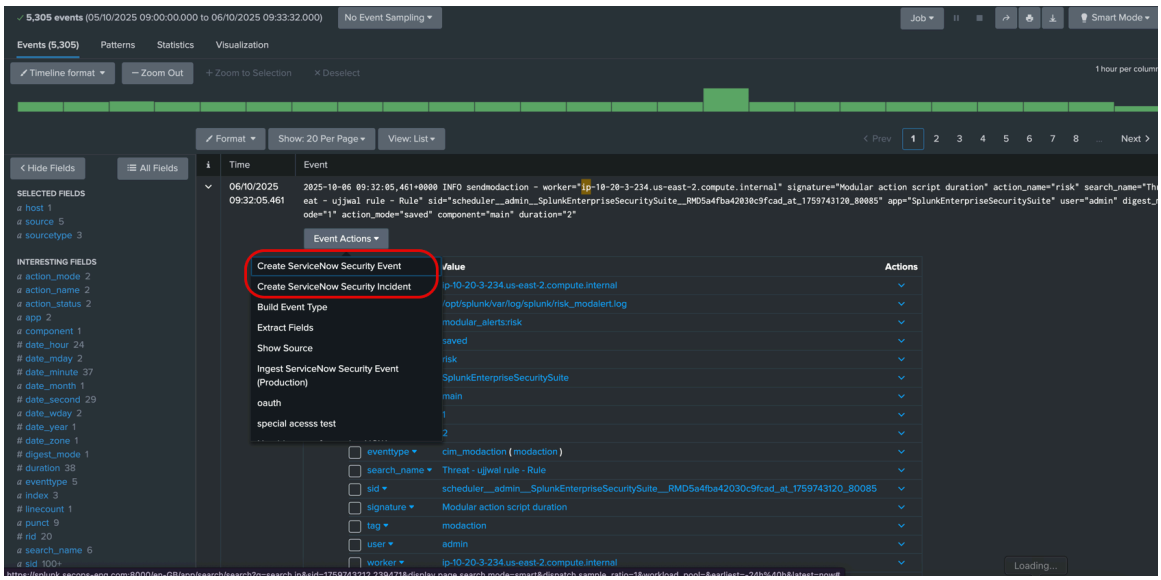
1. Log in to Splunk Enterprise.
2. Navigate to **Apps** > **Search & Reporting**.
3. Enter a keyword in the New Search field.
   A list of events with the keyword show up.
4. Expand any of the events using **(>)** icon.
5. Select **Event Actions**.
   - **Create ServiceNow Security Event**: Events are stored in the em_event table.

     Note:

     Install **Event Management** plugin to access the em_event table.

   - **Create ServiceNow Security Incident**: Incidents are stored in the sn_si_incident table.

     Note: The mapping is pre defined as we don't have a profile for this add-on.



Manual search commands

Manual search commands are entered from any Search window. You can create a security incident or event. After the command, there are pairs of field names and values used to create the desired record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security event

The security event command, **snsecevent**, creates an event in ServiceNow with the Security classification.

These events can be reviewed on their own, or alert rules within ServiceNow or manual actions can turn an event or collection of events into a security incident.

If the event becomes a security incident and each parameter is sent into the event, this data is used to populate the security incident as follows:

Security event

Parameter Name	Required	Use	Use in Security Incident
node	Yes	The node represents the server or configuration item for the event. Ideally, this node maps to an existing CI within ServiceNow.	Use in Security Incident
type	Yes	The category of event.	Short description
resource	Yes	The configuration item.	Short description
source	No	The origination of this data. By default, the Splunk server generates the data.	Activity log
external_url	No	The drilldown URL to use in ServiceNow to get back to the Splunk data regarding this event. By default, this URL contains the result link for any alert, or a link to the default Splunk search page.	External URL accessed via the **Drilldown** button on the Security Incident form
time_of_event	No	The time that the event was logged in Splunk.	N/A
All other values (category, subcategory in the example)	No	Any field that is not part of the information field in the event. If a security incident is created, it is used.	If the field exists, and is not populated, the security incident uses that value. For example, the category passed through the Event becomes the category of the new security incident. If a field with this name does not exist, the value is placed in the activity log.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security incident

The Security Incident command, **snsecincident**, creates a Security Incident in your ServiceNow instance.

Security incident

Parameter	Required	Use
short_description	Yes	A short, one line description of the incident.
category	No	The category of the security incident. If this category does not exist, it is created.
subcategory	No	The subcategory. If this subcategory does not exist, it is created.
cmdb_ci	No	The configuration item for the security incident. Ideally, this item maps to an existing CI within ServiceNow.
description	No	The longer, detailed description of the incident.

There are many possible useful columns – anything in the Security Incident transform map can be used. If new columns are added to the security incident, they too are used, as long as they are in the transform map. Some useful columns: location, priority, assignment_group, assigned_to, affected_user, attack_vector, and watch_list.

Splunk event actions

When reviewing Splunk logs, you can rapidly create security events and security incidents from any item in the log using the Event Actions.

Clicking either of these actions creates a manual search command populated with the data in the log entry, and run it to generate the new record.

These actions are easily configured to add fields in your normalized data. Within Splunk, using **Settings** > **Fields** > **Workflow Actions**, you can select and edit either of these actions using the manual search fields.

You can choose where the action is shown, for what fields, and modify the search string that contains a search command to create your record.

Single-record Splunk alerts

Within any alert, you can specify security events or security incidents to be created when the alert is fired.

Open or create your alert, and when editing actions, select the type of record you want, and fill in the alert dialog box.

Multiple-record, custom field Splunk alerts

Multi-record alerts (defined using the **Create Multiple ServiceNow Security Incidents** and **Create Multiple ServiceNow Security Events** trigger actions) can automatically create records with any set of fields supported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These act differently from the other alert actions in that default values are provided. However, most of the data comes from the search result for that alert.

Note: In previous versions of the add-on and this documentation, scripted alerts were supported. That feature has been deprecated and replaced by these instructions.

Create a multi-record, custom field Splunk alert

To create a multiple record Splunk alert with custom fields, you must build a search that is designed to match the ServiceNow columns you want to populate.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **Search**.
2. In the **Search** box, create a search that generates your record data.
   See the examples for recommended search criteria.
3. Click **Save As** and select **Alert**.
4. Set the name, permissions, and schedule, as needed.
5. Click **Add Actions**.
6. Make one of the following selections.
   - To create one event per result from your search, select **Create Multiple ServiceNow Security Events**.
   - To create one incident per result from your search, select **Create Multiple ServiceNow Security Incidents**.
7. Set any defaults, as needed.
   If the field in the search result is blank or not present, the defaults are used. If there is a value in the result, the defaults are overwritten.

Multi-record, custom field Splunk alert examples

When you are creating multiple record Splunk alerts with custom fields, you need to define search criteria for generating alert data. Examples of search criteria for security incidents and security events are shown.

Security incident search

For a security incident, this criteria builds a search to fill in columns in the security incident table.

```
host=Development
 source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Security event search

For a security event, this is the same search, but it populates Event fields instead. If this event is turned into a security incident, and any fields that do not exist in the event are populated, they

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

are transferred to the security incident. Otherwise, they remain in the additional information field of the event and alert.

```
host=Development
 source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Note: The search criteria you use will add as many records as are found in the search. It may add 5 or 10,000,000,000 records. So this is NOT a recommended method for the bulk tranfer of data. The intent of this method is to add one record per REST call into the ServiceNow instance.

Splunk error reporting

Whenever a connectivity issue with your ServiceNow instance occurs, an error is logged in Splunk with information describing the problem.

Error messages are stored in a new index named **servicenow** with sourcetype **servicenow**.

To search for error logs, ensure you are specifying the **servicenow** index in your search. Alternatively, refer to the current Splunk documentation on how to add the new **servicenow** index to the default search indexes.

Splunk Enterprise Event Ingestion integration for Security Operations by ServiceNow

The Splunk Enterprise event and alert data integration with the Security Incident Response (SIR) product allows security incident analysts to collect and process security logs and related event data.

Overview

Data is collected in real-time, and it is used by analysts to identify and report on potential cyber threats. The security events that are collected can be processed into triggered alerts that are ingested automatically with this integration. Also, individual security events can be manually forwarded on-demand from the Splunk Enterprise search and reporting interface into the Security Incident Response product of the ServiceNow AI Platform to create security incidents. You can retrieve notable events from Splunk Enterprise search with the search head cluster configuration. You can achieve this by using the URL and API port of any search head that is a part of the cluster.

This integration provides a security operations center (SOC) analyst with visibility to events and related alert data. This data can be integrated into ServiceNow AI Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles for Splunk ongoing ingested alerts and forwarded events are created in your ServiceNow AI Platform instance. These profiles customize how different Splunk alert and event fields are displayed on SIR security incidents. A default mapping of alert fields is provided that can be edited and augmented to meet customer-specific needs.

Key features

This integration includes the following key features:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Create multiple alert ingestion profiles to create SIR security incidents for specific types of threats such as phishing and malware.
- Create multiple event profiles for on-demand event forwarding from your Splunk console to create SIR security incidents.
- Drag-and-drop mapping of Splunk alert and event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample alerts or events to validate profile configuration.
- Ingest historical alerts as well as ongoing, future alerts on configurable intervals.
- Aggregate events or alerts to existing SIR security incidents based on matching field values to avoid duplicate security incidents.

Supported ServiceNow AI Platform versions

The com.snc.si_dep plugin is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Support Orchestration
4. Security Incident Response

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

ServiceNow Addons

The ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise is required only if you prefer to forward events manually from your Splunk Enterprise console into your ServiceNow AI Platform instance. This ServiceNow addon is available in splunkbase.

This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise application in splunkbase is not required for the automated alert ingestion that is supported by the integration.

Splunk Supported versions

This integration supports version 6.0 or later of Splunk Enterprise. The integration also supports the Splunk Enterprise Cloud service.

MID Server

This integration requires an installed and configured MID Server in your ServiceNow AI Platform® instance to connect to the Splunk service if the Splunk server is deployed within your corporate network. If you are using the Splunk Cloud service, a MID Server is not required. For more information about MID Servers, see MID Server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration architecture and systems connection

For more information about the architecture of the integration including key terms and external systems connection details, see Integration architecture and external systems connection for the Splunk Enterprise Event Ingestion integration.

Checklist

For a printable checklist of these topics, see Checklist for the Splunk Enterprise Security Notable Event Ingestion integration. You can use this list to monitor your progress as you work through the tasks of the integration.

The images used in the following topics were generated for the Kingston release of the ServiceNow AI Platform. For information about the San Diego user interface, see Manage security threats using the Security Analyst Workspace.

The following topics are numbered. Follow the topics listed below in the order that they are presented for a smooth installation and configuration of the application.

Set up your ServiceNow AI Platform® instance for the Splunk Enterprise Event Ingestion integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the application from the ServiceNow Store.

Before you begin

Role required: admin

About this task

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

Procedure

1. Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.

   The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform® instance.

   - A user with the ServiceNow AI Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.
   - If you want to forward events manually from Splunk Enterprise for this integration, a user with the ServiceNow AI Platform® admin role assigns a user with the (sn_sec_splunk_v2.api_account_access) role in the ServiceNow AI Platform®. This role permits a user with the Splunk Enterprise administrator role to access the API in the ServiceNow AI Platform® that is required for manual event forwarding for this integration.

     The (sn_sec_splunk_v2.api_account_access) role is not required for the integration if you are ingesting alerts automatically from Splunk Enterprise into your ServiceNow AI Platform® instance.

   - A user with the sn_si.admin role oversees the following tasks in the ServiceNow AI Platform®:
     - Names, creates, and edits alert and event profiles.
     - Selects and maps values from alerts and events to ServiceNow AI Platform® security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Previews security incident details for accuracy prior to finalizing the configuration.
- Schedules on-going alert ingestion.
- Assigns the security incident analyst (sn_si.analyst) role.
- Users with the sn_si.analyst work with security incidents.

For more information about roles and assigning roles to users, see Managing roles.

2. Verify that you are using version 6.0 or later of the Splunk API.

   If you have access to the Splunk Enterprise console, you have access to the API that is required for this integration. There is no other special setup required for the API.

3. Verify that you have installed and configured a MID Server.

   A MID Server in your ServiceNow AI Platform® instance is required to connect to the Splunk service if the Splunk server is deployed within your corporate network. For more information about MID servers, see MID Server

   If you are using the Splunk Cloud service, a MID Server is not required.

4. Verify that the ServiceNow core applications required to support the integration are installed and activated.

   The Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration.

   Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.

   a. Security Incident Response
   b. Security Integration Framework
   c. Security Support Common
   d. Security Support Orchestration

   For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

What to do next

You have successfully set up your ServiceNow AI Platform® instance for the integration. The next step is to install the Splunk Enterprise Event Ingestion application from the ServiceNow Store for the integration. For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration.

If you have not saved searches in your Splunk Enterprise console for ingestion, or if you are performing the initial setup for this integration in your Splunk Enterprise console and the Security Operations product of your ServiceNow AI Platform® instance simultaneously, see Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration for more information.

If you want to export events manually and on-demand from your Splunk Enterprise console for the integration, see Set up ServiceNow Event Ingestion Integration add-on for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration

Before you run the integration on your ServiceNow AI Platform® instance, complete these installation and configuration steps so the application properly integrates with the Security Incident Response and Security Operations products on your ServiceNow AI Platform® instance.

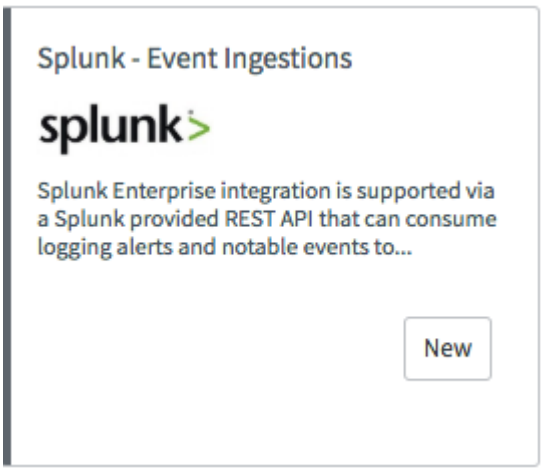
Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

1. If you have not installed the Splunk Enterprise Event Ingestion application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **Integrations** > **Integrations Configurations** and locate the Splunk Event Ingestions tile.
3. To configure the application, click **New**.



4. Alternatively, if a **Configure** button is displayed on a tile, click it to edit an existing configuration.
5. In the Event Ingestions Configuration dialog that is displayed, fill in the fields.

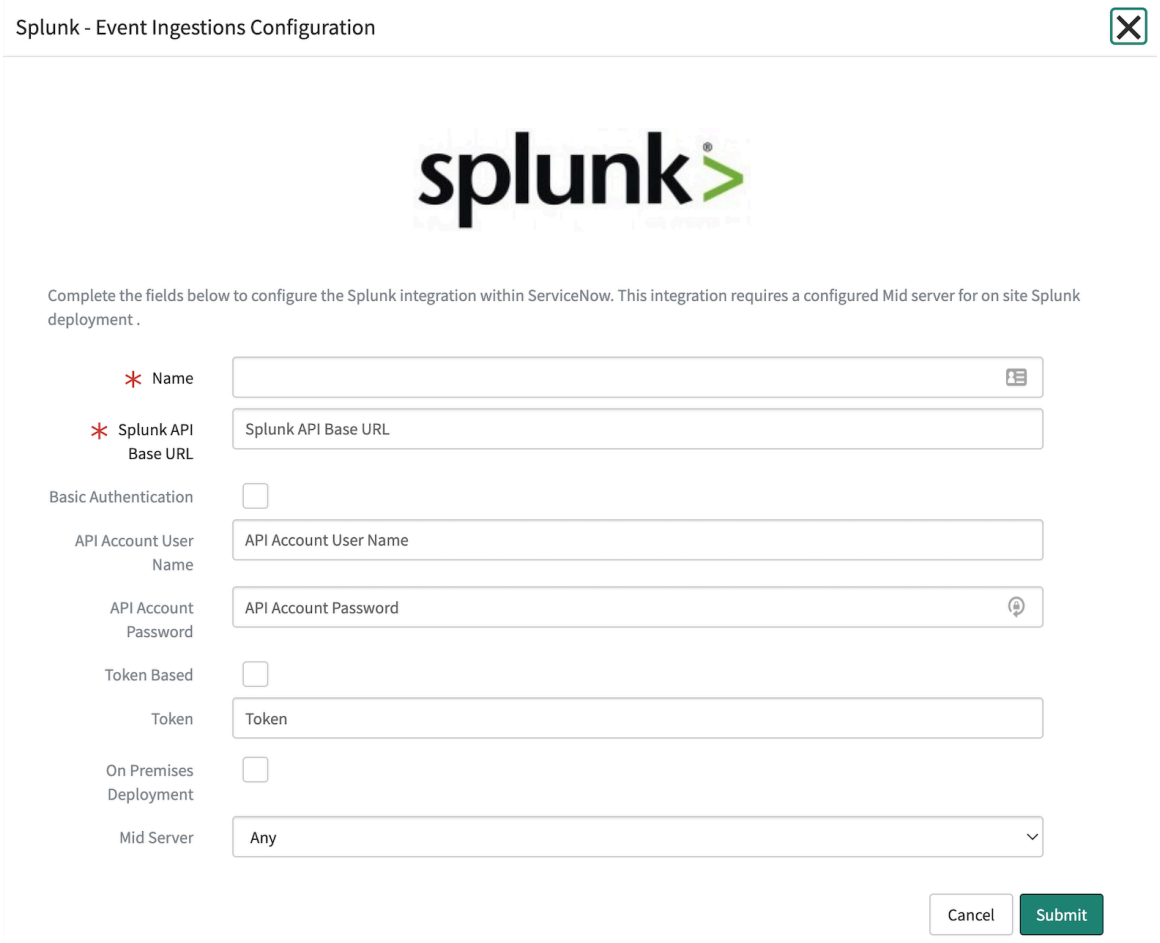
Field	Description
Name	Name of the Splunk Enterprise console or Splunk Cloud instance used for the integra tion. Spaces are supported for names, but paren theses are not supported. For example, enter HQ - USA, or HQ USA.
Splunk API Base URL	URL for your Splunk Enterprise console or Splunk Cloud instance.
Basic Authentication	Default is disabled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If you are using API Account User Name and API Password for configuration, enable the check box.
API Account User Name	User name that you created for your individ ual user account on the Splunk Enterprise console.
API Password	Password that you created for your individual user account on the Splunk Enterprise con sole.
Token Based (available from version 12.0.0)	Token based authentication that you created for your API user account on the Splunk Enter prise console.
Token	Token that you created for your API user ac count on the Splunk Enterprise console.
MID Server	Specific MID Server that is set up in your en vironment. Only MID Servers that are active and validated are available from this choice list.
On Premises Deployment	Default is disabled. If you are using the cloud-based version of Splunk Enterprise, verify that the check box is cleared. If this option is enabled, the MID Server choice list is displayed. If you are using an on-premises version of Splunk Enterprise, follow these steps to select a MID Server. **a.** Select the check box. A choice list is displayed. Default is **Any**. **b.** Select **Any** only if this MID server is config ured for the Splunk Enterprise Event Inges tion integration. **c.** From the choice list, select the ServiceNow AI Platform® MID server that you config ured in your instance for this specific inte gration.

The following figure is an example of a completed form for a configuration of an on-premises version of Splunk Enterprise with a MID Server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Each Splunk Enterprise alert that you ingest from your Splunk Enterprise console requires a unique event profile in your ServiceNow AI Platform® instance. However, the source that you configure on the Event Ingestions Configuration form can be reused for multiple ServiceNow AI Platform® profiles as long as each profile ingests unique Splunk triggered alerts.

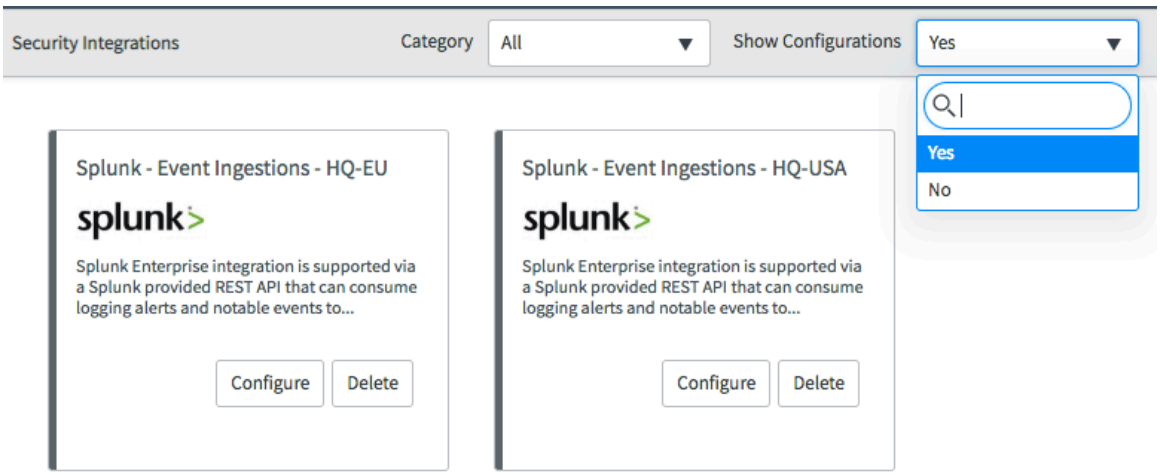
6. Click **Submit**.
   After validation is successfully completed, the Security Integrations page is displayed with each of your configurations. On each valid configuration tile, **Configure** and **Delete** buttons are displayed as shown in the following figure.

   Note: You have to use either Basic Authentication or Token Based Authentication only. Enable one of the authentications and enter the corresponding authentication details. Enabling both will display an error.

   After it is successfully validated and submitted, each Event Ingestions Splunk server configuration is saved on the Security Integrations page as a tile. If your saved configuration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

tiles are not displayed on the Security Integrations page, on the top right corner of the page, from the Show Configurations choice list, click **Yes**.



Trouble?

If an error message is displayed after you click **Submit**, enter your information again and click **Submit**.

What to do next

You have successfully installed and configured the application. The next step is to create an event profile.

Configure Splunk Enterprise Event Ingestion settings

Use the Splunk Enterprise Event Ingestion settings to modify the preset configurations and their values as per your requirements.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

1. Navigate to **All** > **Splunk Integration** > **Splunk Integration Settings**.
2. On the form, fill the fields.

Splunk Integration Settings

Field	Description
Maximum number of alerts to be displayed in the profile creation. sn_sec_splunk_v2.max_alerts_to_display	Option to define the maximum number of alerts that you want to display while creating an event profile. By default, the value is set as 500.
Maximum number of security incidents to be created in one day. sn_sec_splunk_v2.max_si_per_day	Option to define the maximum number of security incidents that can be created in one day.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	By default, the value is set as 1000.
Maximum number of events to fetch from Splunk per call. sn_sec_splunk_v2.max_events_per_call	Option to define the maximum number of events to retrieve from Splunk for each call. By default, the value is set as 100.
The number of days an item remains in the queue table after completing/erroring for information or debugging purposes. sn_sec_splunk_v2.queue_item_expire	Option to define the number of days for an item to remain in the queue table after completion or error occurrence due to information or debugging purposes. By default, the value is set as 14.
Number of days to retain the event import, event to task and fired alerts data. sn_sec_splunk_v2.retention_period	Option to determine the number of days that you want to retain the event import, event to task, and fired alerts data. By default, the value is set as 30.
Activate this setting to update existing Splunk source configurations for token based authentication support. You will need to update the integration configuration with token details once this setting is enabled. sn_sec_splunk_v2.upgrade_existing_tile	Option to update existing Splunk source configuration to token based authentication support from an existing version. **Note:** After you upgrade to the new version, the token field would become unavailable. You need to enable this setting to get the token based authentication, after which you need to update the integration configuration with token details. By default, the value is set as No.
Logging level - debug, info, warn, error. sn_sec_splunk_v2.logging.verbosity	Option to set the logging level (debug, info, warn, or error)
Splunk search time to live in seconds. sn_sec_splunk_v2.sid_ttl	Option to set the time in seconds that Splunk search results are retained. By default, the value is set as 14.
Number of overlap minutes to add while fetching the events from Splunk(to overcome indexing delay from Splunk). sn_sec_splunk_v2.overlap_time	Option to specify additional minutes to overlap when fetching events from Splunk, helping to account for indexing delays. By default, the value is set as 0.
Alert rule batch size to be used for firing Splunk search queries during ingestion. sn_sec_splunk_v2.rules_batch_size	Option to set the batch size for firing Splunk search queries during ingestion. By default, the value is set as 50.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Events Limit per triggered alert to handle spike. sn_sec_splunk_v2.spike_events_limit	Option to limit the number of events processed per triggered alert, helping to manage spikes in event volume. By default, the value is set as 1000.
The delimiter character to split the values in field mappings. sn_sec_splunk_v2.delimiter	Option to specify the delimiter character used to split values in field mapping.

3. Select **Save**.

Create and name an event profile for the Splunk Enterprise Event Ingestion integration

Create an event profile in your ServiceNow AI Platform instance and determine which Splunk alerts create security incidents.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

Before ServiceNow AI Platform Security Incident Response (SIR) security incidents are created from ingested alerts, the field values from alerts are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident is displayed.

From an integration perspective using available APIs, Splunk events are forwarded individually and manually as discreet events, or they are combined into triggered alerts that are automatically ingested into the Security Operations environment of your ServiceNow AI Platform instance. The integration workflows ingest different types of alerts such as unauthorized access attempts and malware, for example.

These alerts are ingested based on the profiles that you configure in the Security Operations environment of your instance. All alerts are initially ingested for a configured alert type in a profile. Ingested alerts can then be further filtered to specify which alerts create security incidents. For example, you may prefer filters that create security incidents only for alerts that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested alerts, individual field values on the filtered alerts are mapped to corresponding fields on a layout of security incident for a preview.

Alert names for event profiles in your ServiceNow AI Platform instance must be unique and can only be mapped to one active event profile at any given time. These are the triggered alert names that you configured in your Splunk service as part of the setup for the integration. For more information about configuring alerts in your Splunk Enterprise environment, see Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration.

The ServiceNow AI Platform ingests specific alerts using the workflows of the integration. All alerts that meet the selection criteria in your Splunk enterprise console are initially ingested into your ServiceNow AI Platform instance.

A profile in your ServiceNow AI Platform is an encapsulation of a Splunk alert in your Splunk enterprise console. There is a one-to-one relationship between alerts that are ingested with a profile and connections to your Splunk enterprise console: one alert for one connection. There

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

is a single https connection to a search head in your Splunk Enterprise console. Multiple alerts can come from a single search head. If you connect to multiple search heads in your Splunk Enterprise console, you must create multiple profiles in your ServiceNow AI Platform instance to ingest these alerts.

Steps to create profiles for scheduled alert ingestion

Procedure

1. To create an event profile for an alert, in your ServiceNow AI Platform instance, navigate to **Splunk ES Integration** > **Splunk ES Event Profiles**.
2. If the Splunk Event Profile form is not displayed, click **Name** in the Progress bar.
3. Click **New**.
4. Fill in the fields.

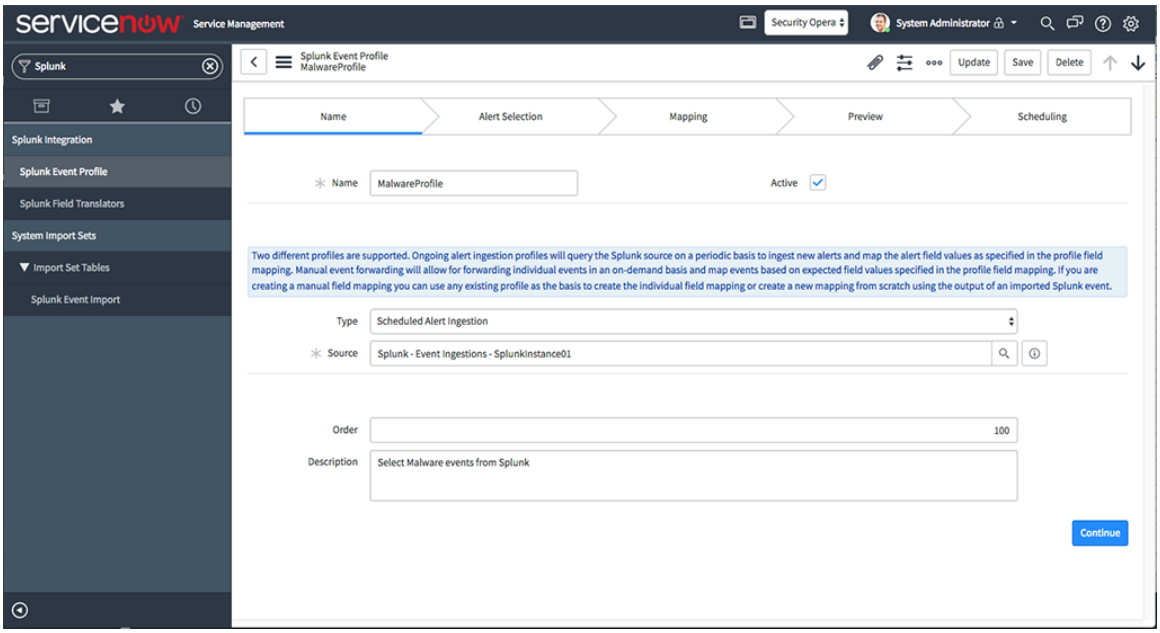
   An example of a completed form follows the table.

Field	Description
Name	Unique name for the profile. If names are not unique, duplicate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Active	Check box is cleared by default. The Active option is disabled and not available for selection till you complete all the profile configuration steps and click **Finish**.
Type	Select the profile type from the choice list. ○ Scheduled Alert Ingestion - This type of profile supports triggered alerts that are ingested on a schedule that you configure. Fill in the fields and click **Continue** to proceed to the Alert Selection step of the profile. ○ Manual Event Forwarding - This type of profile supports individual events that are forwarded manually from your Splunk Enterprise console on demand. See the following steps to fill out the form for these types of profiles.
Source Type	Splunk server or search end that you configured to ingest alerts. If you have multiple Splunk servers configured, select the appropriate server for the alert types that your are planning to ingest for the profile. You are required to enter a value.
Order	Default is 100. Leave this setting at the default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Text to help you distinguish this profile from other profiles.

The following figure is an example of a completed form for a scheduled alert.



5. For a profile with a scheduled alert, choose one option to continue with the profile configuration.

Option	Description
Continue	Save the profile and progress to the Alert Selection step.
Update	Save updates to this profile and return to the Splunk Event Profiles list.
Save	Save this profile and remain on the page.
Delete	Delete this profile record and return to the Splunk Event Profiles list.

Steps to create profiles for manual event forwarding

6. To create a profile that supports manual event forwarding, follow these steps.

   For events that you forward on-demand from your Splunk enterprise console, you can base the individual field mapping on any existing profile. Alternatively, you can create a new mapping grid for exported attachment data. Events that you forward manually are not scheduled in the event profile.

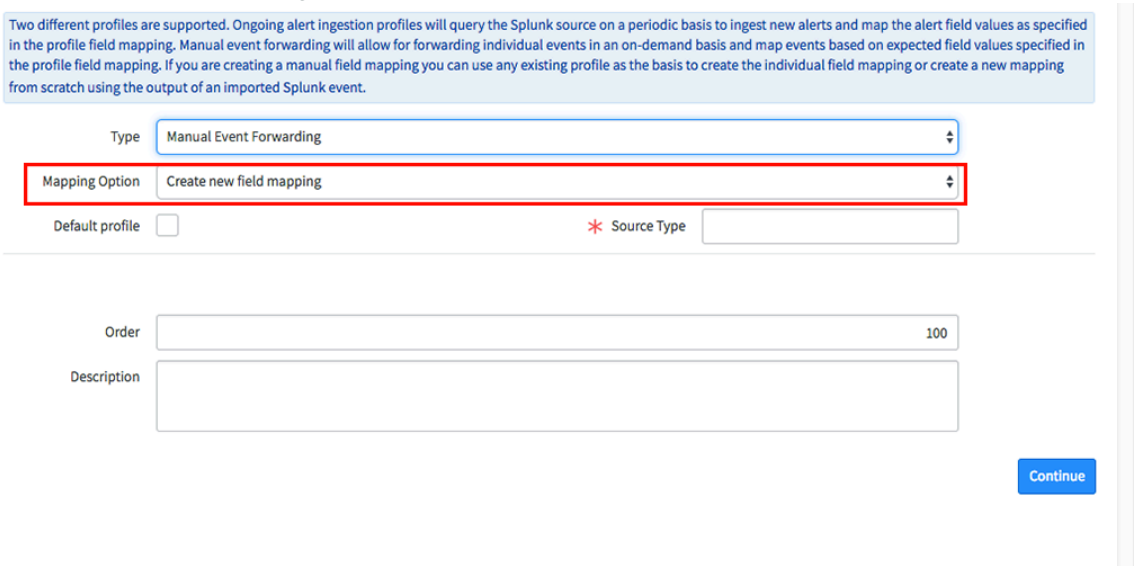
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. If not already selected, in the choice list for the Type field, select **Manual Event Forwarding**.

b. In the Mapping Option field that is displayed, from the choice list, choose one mapping option to continue.

Refer to the following figures and tables for more information about the available mapping options in the Mapping Options choice list.

Create new field mapping option



Create New field mapping option

Option or field	Description
Create new field mapping option	New field mapping for your event. If you do not have an existing field mapping that is similar to the profile that you are creating, select this option to create a new map.
Default profile	Default event forwarding profile for all Splunk events. Default is cleared (disabled). When this option is enabled, this profile becomes the default profile for manual event forwarding. This profile is the only profile that is active and used for every Splunk event field mapping to a SIR security incident. One profile fits all forwarded events. The Source field is unavailable if the default profile option is enabled.
Source type	Splunk server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or field	Description
	This field is unavailable if the default profile option is enabled. If available, the Source Type option permits unique event field mapping to security incident fields based on the Splunk source type. If you want to manage firewall log events differently than endpoint detection events, and they have different Splunk source types, you can create different event profiles based on source types to accomplish this requirement.
Order	Default is 100. Leave this setting at the default. If you have created a large number of profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Text to help you distinguish this profile from other profiles.

For a profile with a new field mapping, verify that you have entered a value in the Source type field and click **Continue** to proceed to the mapping step of the configuration.

For a profile with an existing field mapping, refer to the following figure and table for more information.

Select existing profile for field mapping option



Select existing profile for field mapping option

Option or field	Description
Select existing profile for field mapping	An existing field mapping for your event. The Copy from profile field is displayed. Follow these steps to copy an existing field mapping for this profile. i. To the left of the Copy from profile field that is displayed, click the search icon. ii. In the Splunk Event Profiles list that is displayed, click the profile name that has the map that you want to copy. The profile name is displayed in the Copy from profile field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or field	Description
Default profile	Default event forwarding profile for all Splunk events. Default is cleared (disabled). When this option is enabled, this profile becomes the default profile for manual event forwarding. This profile is the only profile that is active. It is used for every Splunk event field mapping to a SIR security incident. One profile fits all forwarded events. The Source field is unavailable if the default profile option is enabled.
Source type	Splunk server. This field is unavailable if the default profile option is selected. If available, the Source Type option permits unique event field mapping to security incident fields based on the Splunk source type. If you want to manage firewall log events differently than endpoint detection events, and they have different Splunk source types, you can create different event profiles based on source types to accomplish this requirement.
Order	Default is 100. Leave this setting at the default. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Text to help you distinguish this profile from other profiles.

At the bottom of the form for selecting an existing mapping for your profile, click **Finish** to complete the profile configuration.

What to do next

You have successfully completed the steps to create profiles for both scheduled alerts and manual event forwarding. For profiles for manual event forwarding, you have completed the profile configuration. The next step is to load attachment data in the mapping step.
For profiles for scheduled alerts, the next step is to select alerts for automatic ingestion.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select scheduled alerts for the Splunk Enterprise Event Ingestion integration

After you have created a profile for a scheduled alert, select a Splunk alert for this profile that you want to map to a ServiceNow AI Platform Security Incident Response security incident.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

View the available alerts in your ServiceNow AI Platform instance so you know which field values are available for mapping. Select an alert to verify that you receive the expected results on the basic form layout before you map the values to fields on SIR security incidents. You can only select one alert from the list in this form.

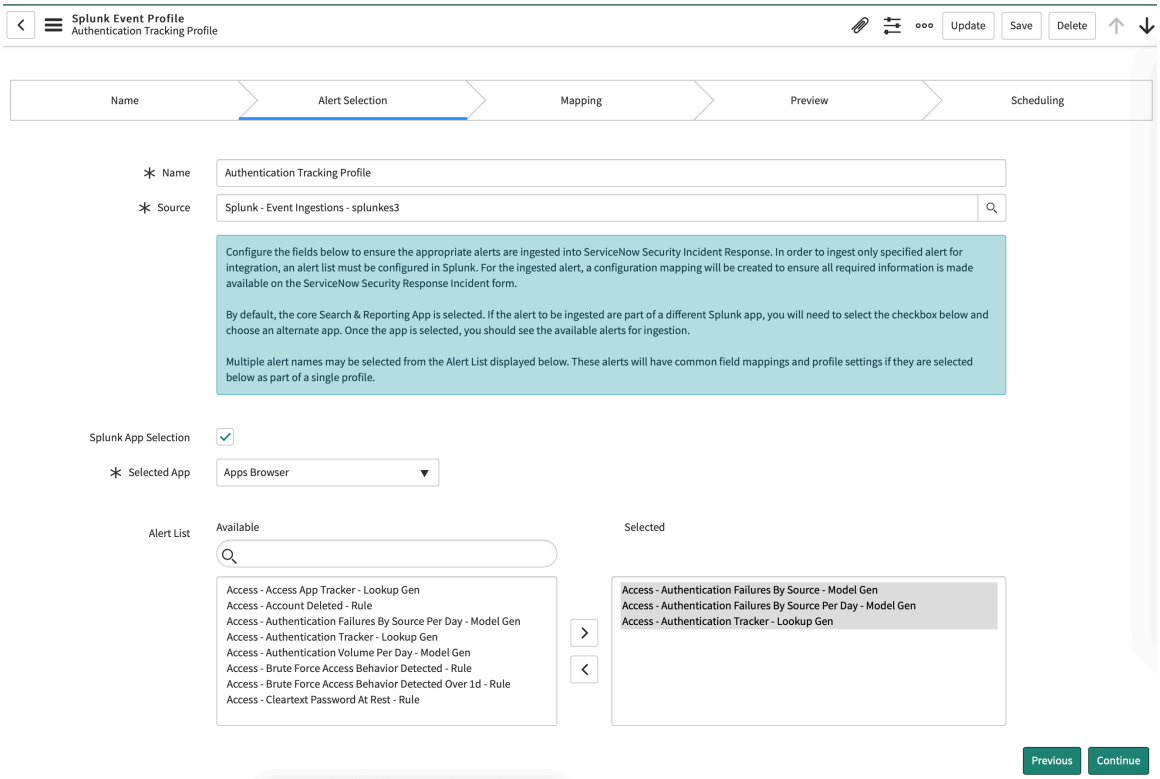
Procedure

1. If the Alert Selection page is not displayed, select it on the progress bar to display it.
   By default, the core Search & Reporting App is selected.
2. If the alert to be ingested is part of a different Splunk app, select **Splunk App Selection** and choose your Splunk app from the **Selected App** list.
3. From the **Alert List**, choose an alert and move it to from the **Available** column to the **Selected** column.
   You can also choose multiple alerts. If the alerts are selected as part of a single profile, then the alerts will have common field mappings and profile settings.

   The list of alerts on this form matches the list of alerts in your Splunk console. Up to 500 alerts are displayed on this form. If there are more than 500 alerts listed in your Splunk console on the Alerts page, only the first 500 alerts are displayed on this form in your ServiceNow AI Platform instance.

Option	Description
In the Alert List search field, enter text.	The column below the search field is filtered with available options based on the text that you enter. Select an alert, and with the arrow keys, move the selected alarm from **Available** to **Selected**.
In the Alert List, double-click an Alert.	The **Selected** column is populated with your selection.
In the Alert List, single-click an alarm rule.	The alarm is selected. With the arrow keys, move the selected alert from **Available** to **Selected**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Choose one option to continue.

Option	Description
Continue, or alternatively, click Mapping in the progress bar	The Mapping form is displayed. **Mapping** is selected on the progress bar. The next step is to map alert fields to a SIR securi ty incident.
Update	Your data is saved and the Splunk Event Pro files list is displayed.
Previous	The **Name** step is displayed.
Delete	Delete this event profile and the Splunk Event Profiles list is displayed.

What to do next

You have successfully selected an alert for a scheduled alert profile. The next step is map alert values to fields on a security incident.

Mapping alerts and events for the Splunk Enterprise Event Ingestion integration

After you identify the sources for scheduled alert ingestion or manual event forwarding, the next step is to map individual event fields to the fields on a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Overview of Mapping alerts and events

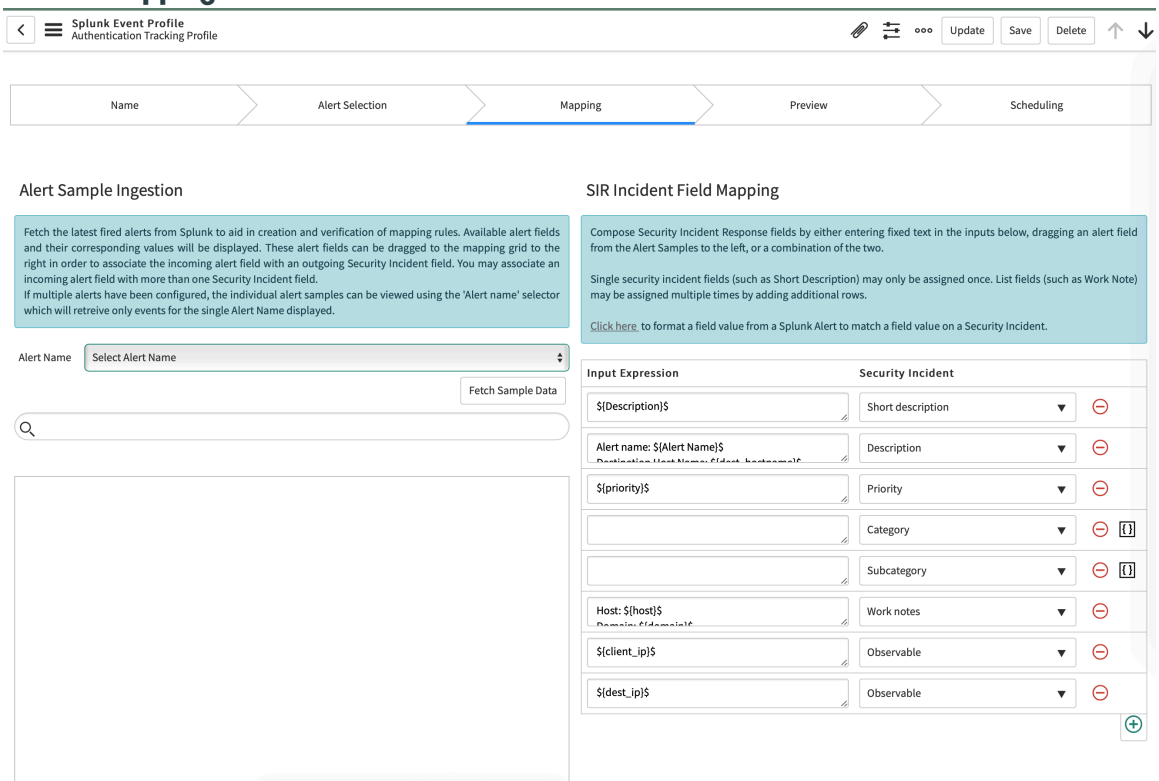
For the mapping step, as a user with the **sn_si.ingestion_profile_admin** role, you ingest sample alerts from your Splunk Enterprise console, or you export event data for a Splunk Enterprise event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figures are examples of the default mapping grids that are provided for each type of event profile. This default mapping can be edited. This modification allows you to customize the fields that populate the security incident. With the mapping step, you can visualize how adding or removing event fields impacts the SIR security incident field values.

Select the **Alert Name**, and after you click to **Fetch Sample Data**, the Splunk alert field values are populated on the left side of the form when sample alerts are ingested by the profile. These are the Splunk alert fields that you map to the SIR security incident fields.

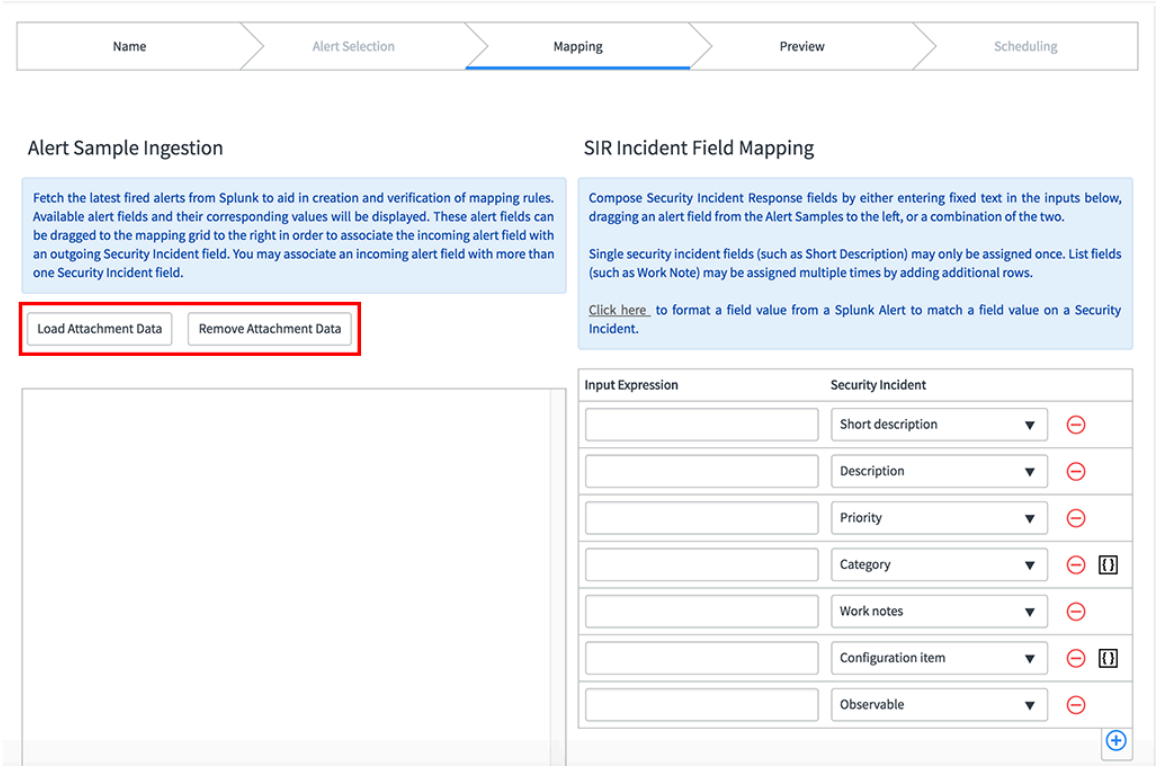
Default mapping form for alerts



After you click to load attachment data for forwarded events, the Splunk event fields are populated on the left side of the form. These are the Splunk data fields that are mapped to the SIR security incident fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Default mapping form for forwarded events



You may prefer to review a few sample alerts on your Splunk console to ingest for the field mapping configuration step. This step is labeled, **Mapping** on the progress bar. If this page is not displayed, click **Mapping** on the progress bar.

Mapping alerts and exporting events on-demand from your Splunk enterprise console includes the following concepts and tasks:

- Fetch Sample data for automatically ingested alert profiles. After data is fetched (pulled) from a fired alert on the Splunk Enterprise console, available alert fields and their corresponding values are displayed in a default mapping layout on the left side of the mapping form. Tabs are displayed for you to view the values for an alert ID that you pulled. Verify that all the critical fields from the Alert Sample Ingestion section on the left of the form are mapped to the grid on the right of the form.
- If required, load event sample data for any manually forwarded event profiles. Sample data for these events is exported in a `.xml` file from the Splunk Enterprise console and loaded into your ServiceNow AI Platform® instance. The imported data is displayed in the Alert Sample Ingestion section on the left of the form.
- Edit the mapping configuration by dragging alerts from the left side and dropping them on the mapping grid on the right. The mapping grid on the right associates the incoming alert field with an outgoing security incident field.
- Customize the mapping grid by adding or removing fields. Track overlooked or duplicated fields with the color coding that is provided.
- Set filter conditions so that you can specify which alerts are ingested into the SIR application, and which alerts are filtered out.
- Define additional incident field criteria that aggregates an incoming alert to an existing SIR security incident to prevent duplicate incidents. This additional filtering can reduce the number of active, overlapping security incidents by placing all related security event data on a single security incident.
- In certain cases, event field values in the Splunk Enterprise console may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format

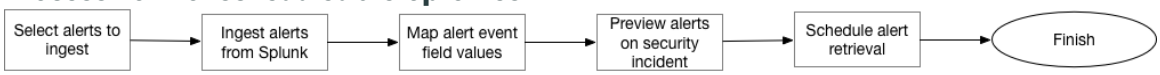
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, the Malware Alert and Virus Infection field values in the Splunk console both translate to Malicious Code Activity in the Category field on the SIR security incident.

Scheduled alert profiles

After creating a scheduled alert profile, the process flow for the configuration is shown in the following figure.

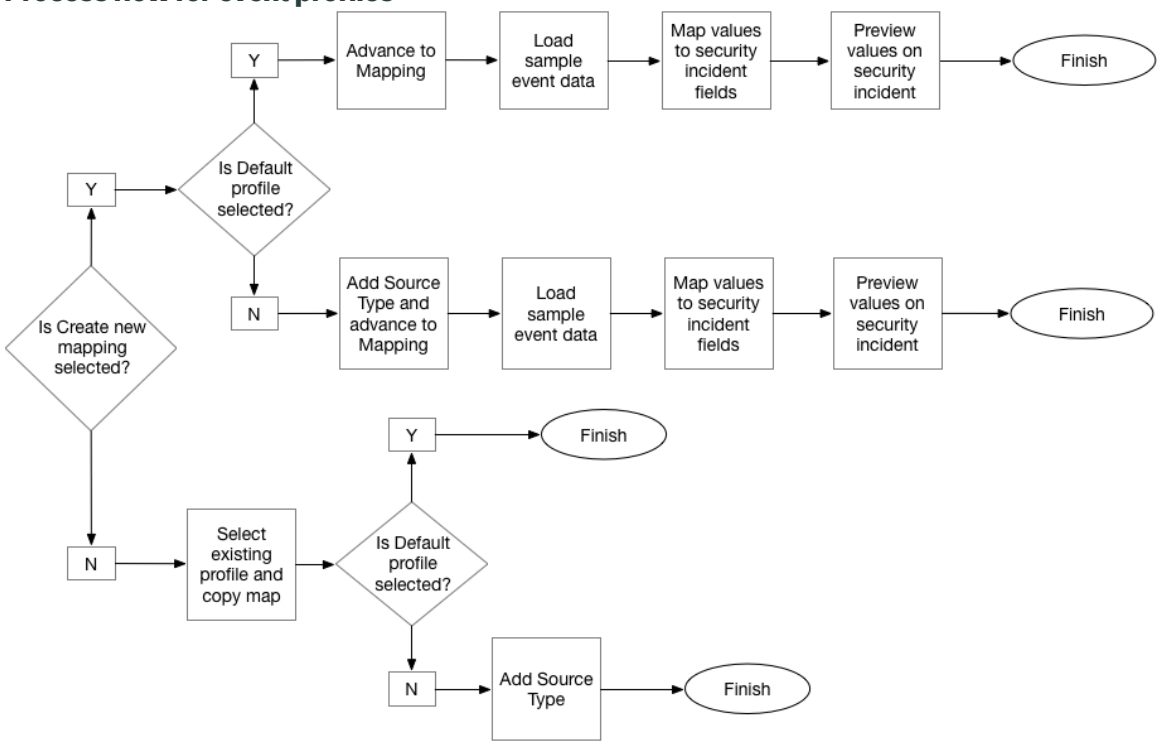
Process flow for scheduled alert profiles



Manual Event forwarding profiles

After creating a profile for an event, the process flow for the configuration is shown in the following figure.

Process flow for event profiles



The next step is to ingest triggered alerts or export data and map values to the SIR security incident fields.

Map alerts for the Splunk Enterprise Event Ingestion integration

During the event field-mapping step, you map individual event fields from triggered alerts or imported event data to fields on a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Before you begin
Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The preconfigured mapping grid of the default security incident fields can be edited. The color-coding of the event fields helps you monitor the field values that you have already mapped. This step helps you visualize how your edits impact the fields on the security incident.

Map up to five alerts from the Alert Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.

Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default-mapping grid on the SIR security incident.

Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. For a profile with a scheduled alert, below Alarm Sample Ingestion, select the alert in the **Alert Name** and click **Fetch Sample Data** to pull the latest instance of a fired alert from the Splunk Enterprise console.

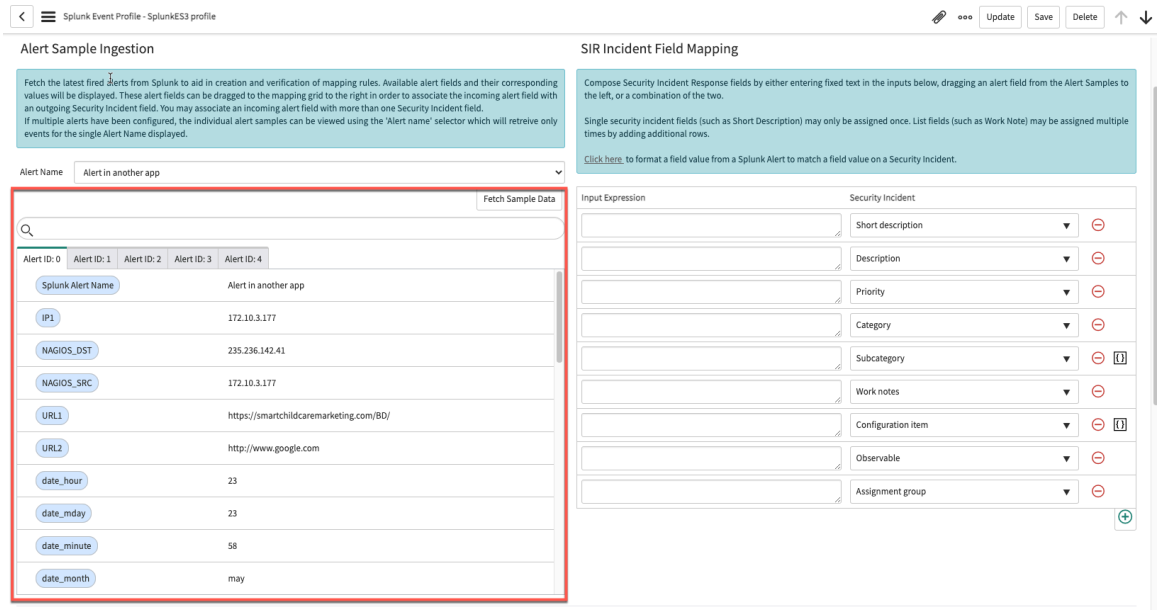
   The alerts are displayed as tabs. You can ingest up to five of the most recent alerts.

   The pull for sample events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

   Note: An additional mapping field, **Splunk Alert Name**, is added by the integration to allow for tracing an event to the source alert rule in Splunk. This may be helpful in scenarios where multiple Splunk alerts are combined into a single profile.

   When a single field contains multiple values, those values are parsed and mapped to individual field entries on the SIR incident field mapping section. For example, the source IP addresses, asset names, or URLs may have multiple observable field entries or multiple CIs, those are parsed and mapped to individual field entries on the SIR incident field mapping section.

   In the following figure, the field-name value pairs for the ingested alert, or the imported sample event, are displayed on the left side of this form after the pull is completed. These values are the values that you map to the security incident fields on the SIR Incident Field Mapping side of the form.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. For scheduled alert profiles, proceed to step five to map the values.
4. Alternatively, for a profile for an event type that you want to export from your Splunk Enterprise console, follow these steps to upload attachment data in your ServiceNow AI Platform® instance.

   a. If not already logged in, log in to your Splunk Enterprise console.

   b. Navigate to the Search tab and enter a name for a search that has the event data that you want to export.

      For example, malware is a search term used for all malware events that you can forward with the workflow of this integration.

   c. Expand the event, and in the Field column, select the fields that you want to import.

      These fields are the field-value pairs that are exported and displayed on the Mapping page in your ServiceNow AI Platform® instance.

   d. In your Splunk Enterprise console, in the upper right of the Search page, click the **Export** icon.

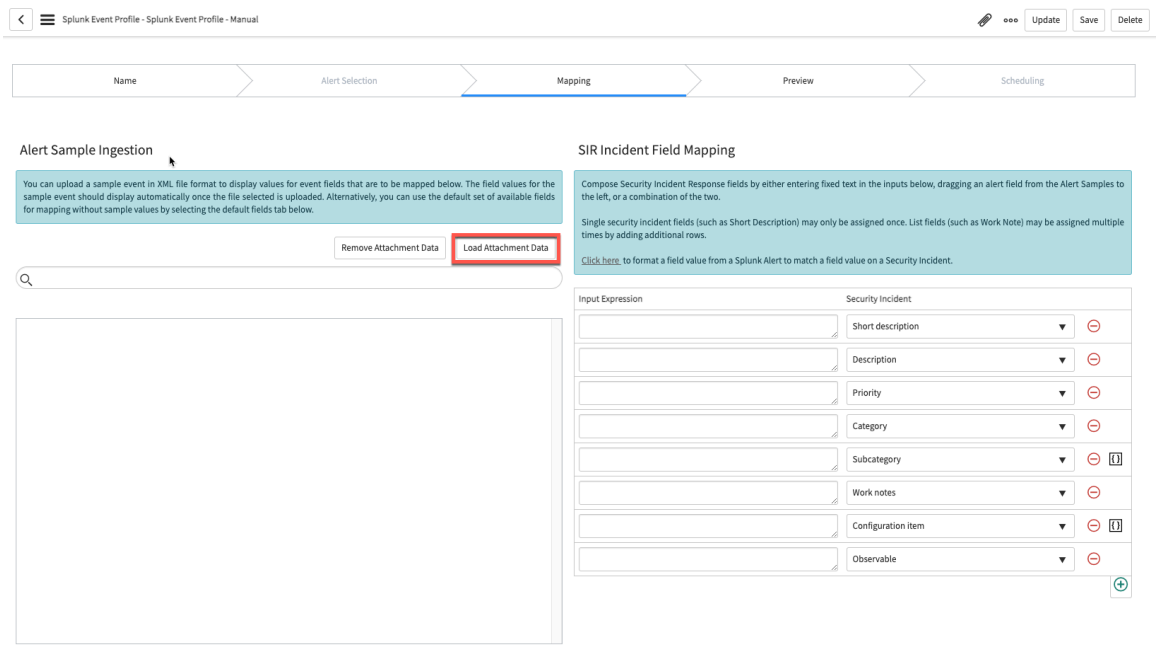
   e. In the list for the Format field in the dialog that is displayed, click **XML Format**.

   f. **Optional:** Enter a new filename.

   g. Click **Export**.
   The file is downloaded to your ServiceNow AI Platform® instance.

   h. If the Mapping page is not already displayed in your ServiceNow AI Platform® instance, click **Mapping** in the progress bar.

   i. In the Alert Sample Ingestion column, click **Load Attachment Data**.

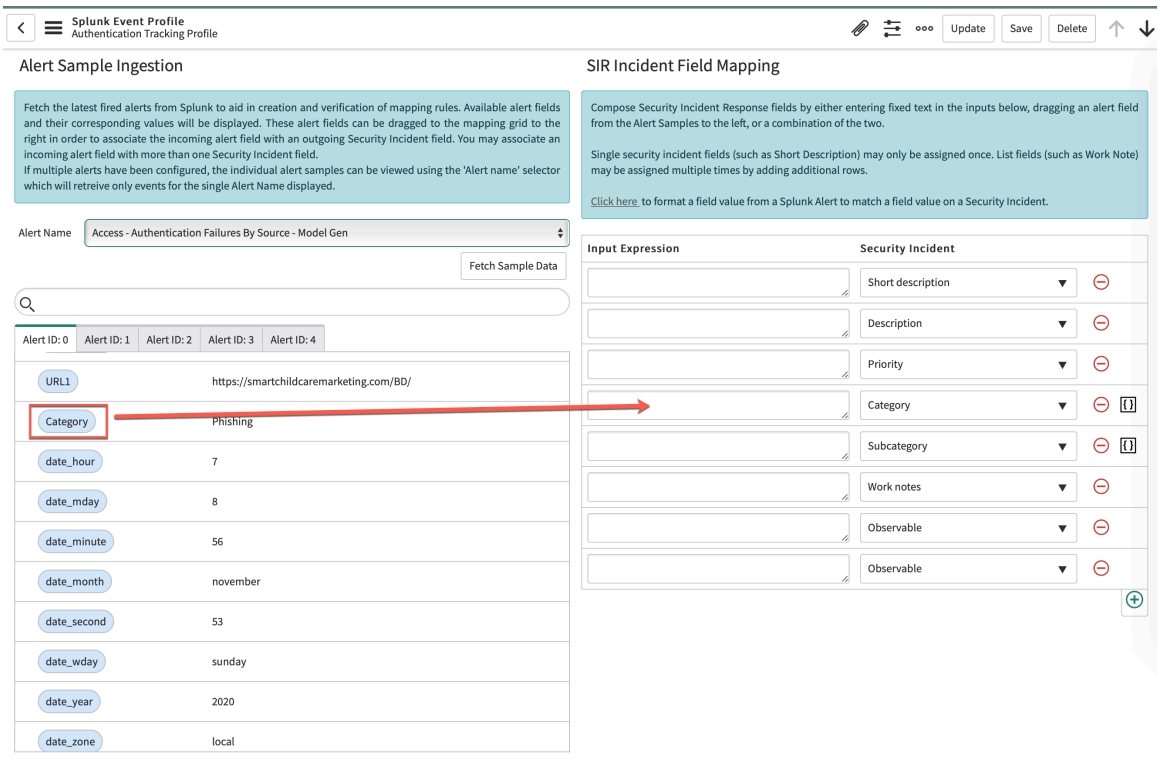


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

j. In the dialog that is displayed, click **Choose files** and navigate to the `.xml` file that you exported and click **Open**.
The value pairs for the fields that you exported for the event are displayed on the left side of the mapping form.

In the following figure, the data pairs for an ingested scheduled alert are displayed on the left side of this form. Value pairs for imported events are also displayed on this side of the form. These values are the field values that you map to the security incident fields on the Sir Incident Field Mapping side of the form.

5. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
6. Drag the field name, for example, `category`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

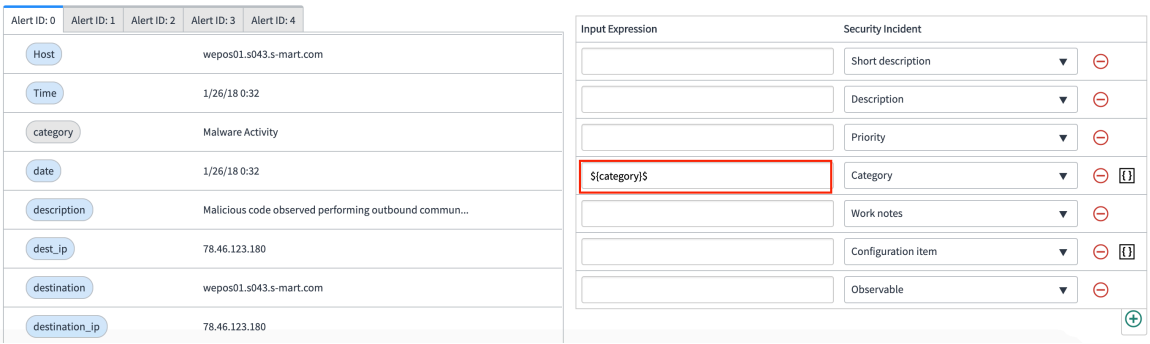


The field value is displayed in the Input Expression column. In the following image, `category` is mapped to the `category` field on the security incident. However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no events are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a field is not yet selected and mapped on the security incident. You may prefer to associate an incoming alert field with more than one field on a security incident.

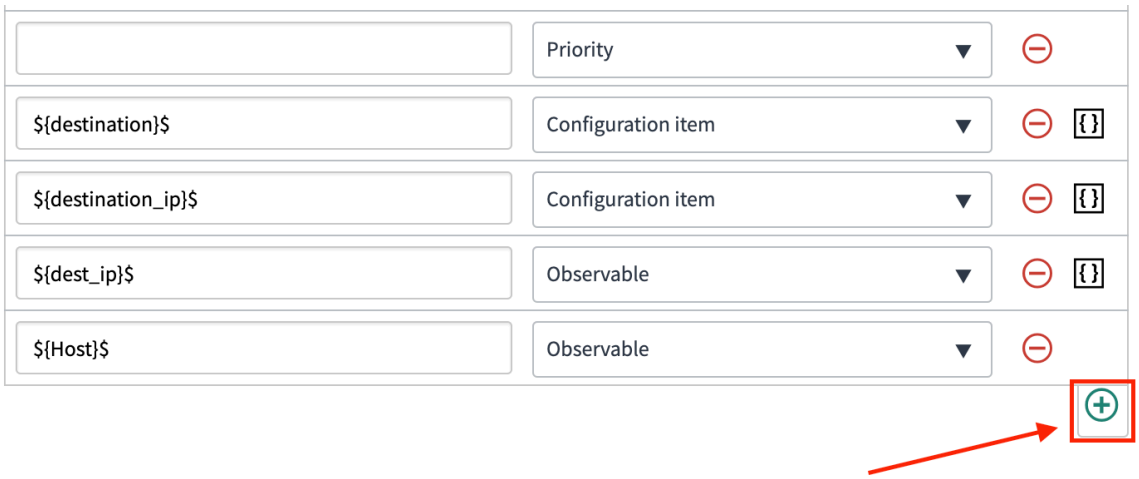
A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping, because in certain cases, alert event fields may only be assigned once. For instance, you can only assign values to fields such as Short Description once. However, you can assign list fields such as Work Note multiple times by adding additional rows to the mapping grid.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. To add fields to the default mapping of the security incident on the right side of the form, follow these steps.

   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon.

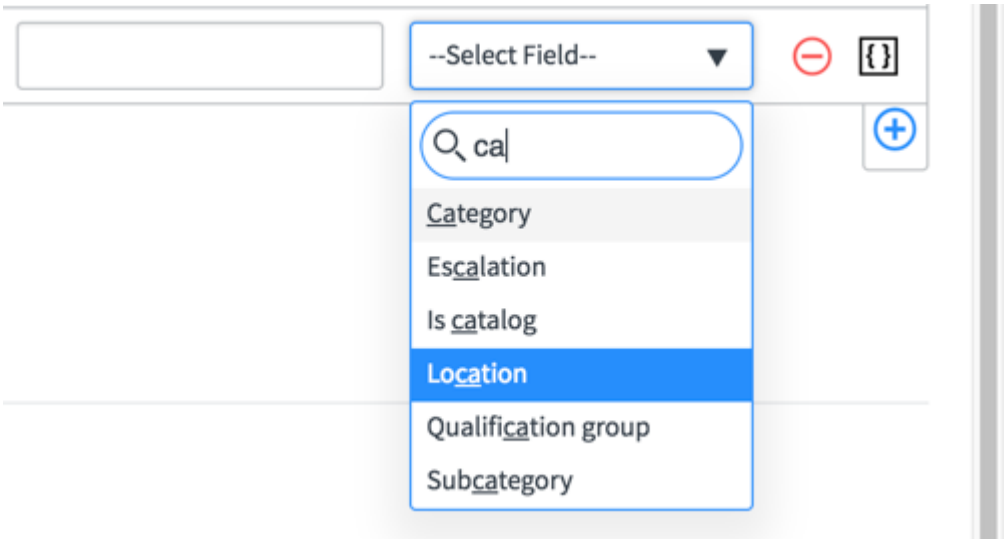


   A new field is displayed.

   b. In the Security Incident column, expand the list that is displayed, and select a field.

   In the expanded list for the new field, some fields are shaded. In the following figure, `Category` has a gray background, because it has been mapped in the security incident. Similar to the color-coding for alert fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the mapping.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

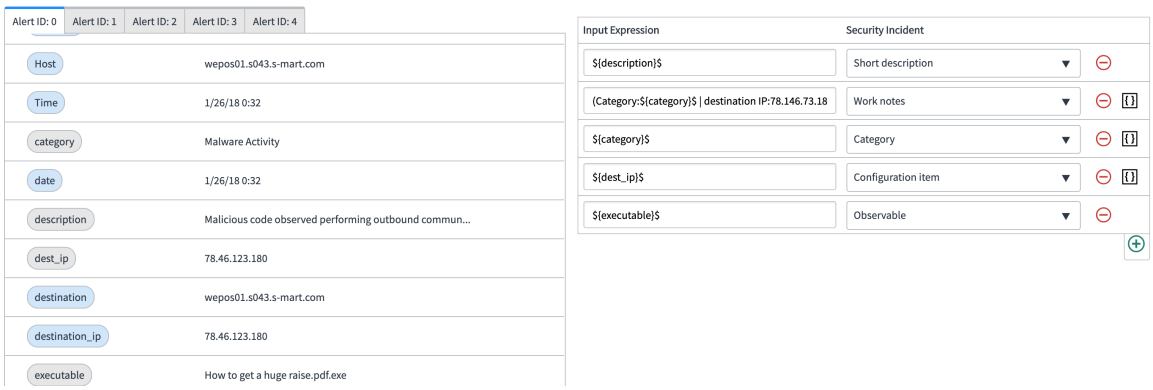


Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the **Alert ID** that you want in the Input Expression field.
With the drag feature, map it next to your new field.

8. Continue mapping by adding or removing fields and adding values to the map.
The following figure is an example of an edited mapping grid. In the bottom field on the right, the Work notes field is added, and it has more than one value. The values are separated by spaces and punctuation marks (`Category:${category} | destination IP:78.146.73.180`).



In the preview, these values are displayed in the Work notes on the security incident. Because the value is for a field that you added to the grid, and there are multiple values mapped to the Work notes field, the values are displayed as entered. In this example, the spaces and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

punctuation marks that you entered in the field are displayed on the Related Items section as a work note on the preview of the security incident.

The following image is an example of how the values in the preceding image are displayed on the security incident.



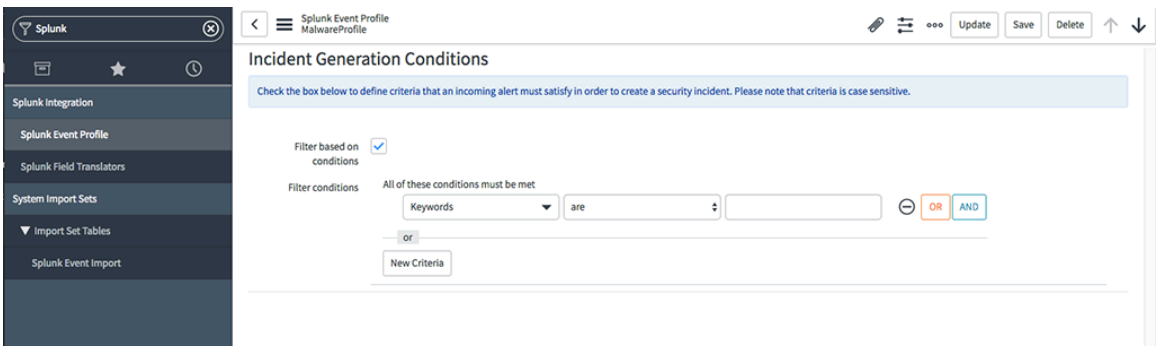
Incident generation filtering conditions

9. **Optional:** After you have completed the preceding field-level mapping steps, you can use the same field values in the Filter conditions builder to define additional criteria that an incoming alert must satisfy to create a SIR security incident.
To set filtering conditions, follow these steps.

   a. Scroll to the Incident Generation Conditions section on the form and select the **Filter based on conditions** check box to enable the option.

      (Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

      The options in the lists for the first field in the Filter conditions builder match the fields that are displayed on the Alert Sample Ingestion section for the alert you ingested. These fields are dynamic and change depending on the Splunk alert that you ingest, or the event that you manually forward. Criteria that you enter are case-sensitive, and they must match exactly the values of the Splunk Enterprise alert or event. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Splunk Enterprise console and review your alerts and events for the keywords.



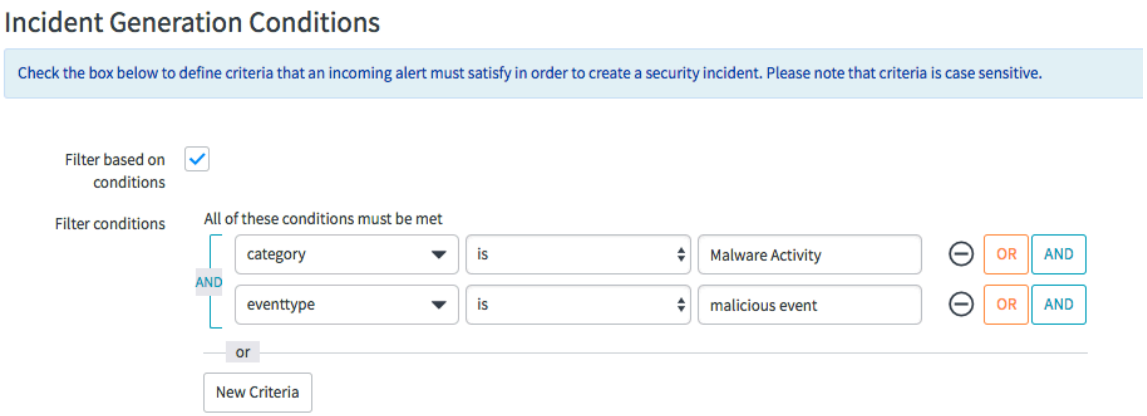
   b. Using the lists and fields of the conditions builder, set filters for the first row.

   c. To add more conditions, to the right of the fields, click **AND** or **OR**.
   If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

   d. **Optional:** In the second row, set a second filter condition.

      (Optional) The following image is an example with two conditions that must be matched before security incidents are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



(Optional) You have set the triggering conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

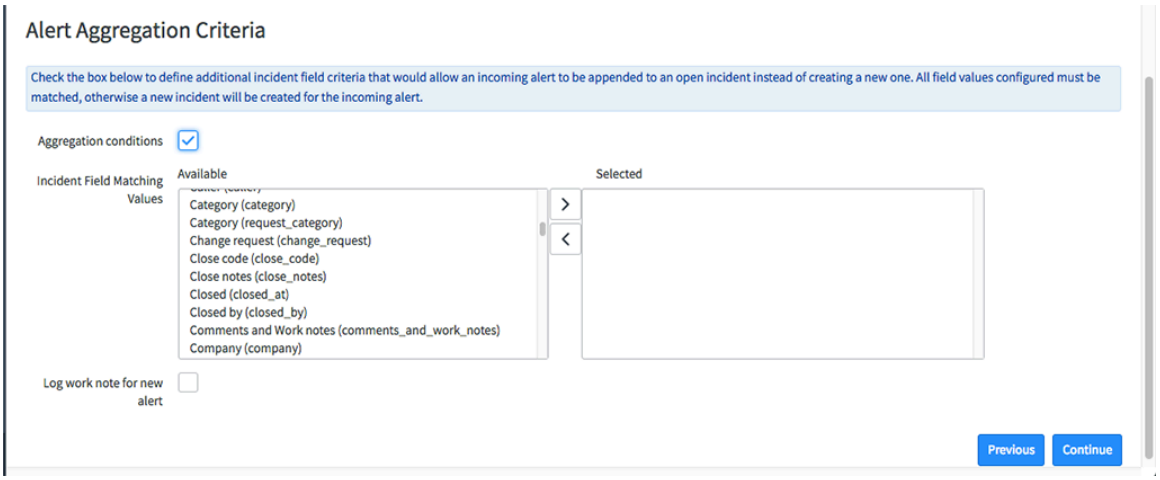
This type of filtering helps you isolate security events, and it limits the number of security incidents that you create. If additional filtering criteria are set, only alerts that are required are ingested without having to change the Splunk query or the triggered alert configuration.

Aggregation Alerts to Prevent Duplicate Incidents

10. **Optional:** To avoid potentially creating duplicate security incidents, define additional incident field criteria so incoming alerts are aggregated to an open security incident.
To set this criteria, follow these steps.

    a. Scroll to the Alert Aggregation Criteria section on the form and select the Aggregate conditions check box to enable this option.

    (Optional) The Incident Field Matching Values columns are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

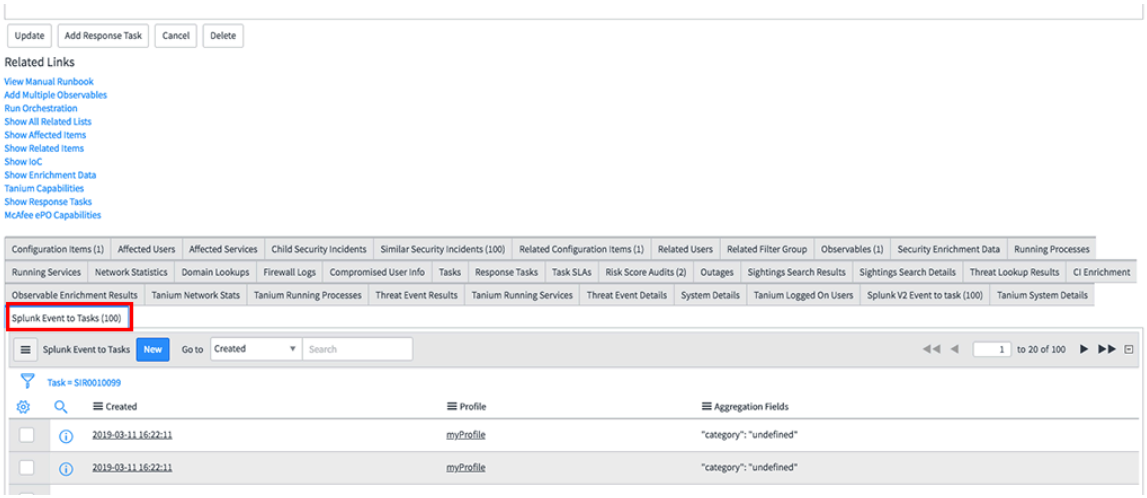


    b. From the Available list, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform and move them to the Selected list.

    (Optional) All the field values that you select must be matched to append this incoming alert to an existing security incident. If you prefer to review field values on security incidents to use for this criteria, navigate to **Incidents** > **Show all incidents**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a new alert matches all the values that are selected in the aggregation field conditions in the mapping step, the alert is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate alerts on a related list on a security incident. All of the aggregated alerts on a security incident are displayed on the Splunk Event to Tasks related list. This list details associated timestamps and aggregated field values. This information helps you understand why alerts are added to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the **Show All Related Lists** link.



c. **Optional:** To log a work note for a new alert that is recently added on the security incident, select the check box to enable this option.
The work note logs that a new alert has been added along with a link to the alert details.

You have successfully mapped values from a Splunk alert or event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with filtering criteria. You also appended alerts or events to existing SIR security incidents.

11. **Optional:** Open the script editor and continue editing.

(Optional) For more information about the script editor, see Use the script editor to format alert values for the Splunk Enterprise Event Ingestion integration.

12. Choose one to continue with the profile configuration.

Option	Description
Continue	The Mapping form is displayed. **Preview** is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.
Update	Your data is saved and the Splunk Event Pro files list is displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Previous	The Alert Selection form is displayed.
Delete	Delete this event profile and the Splunk Event Profiles list is displayed.

What to do next
The next step is to preview the values that you mapped on the security incident.

Preview the security incident for the Splunk Enterprise Event Ingestion integration

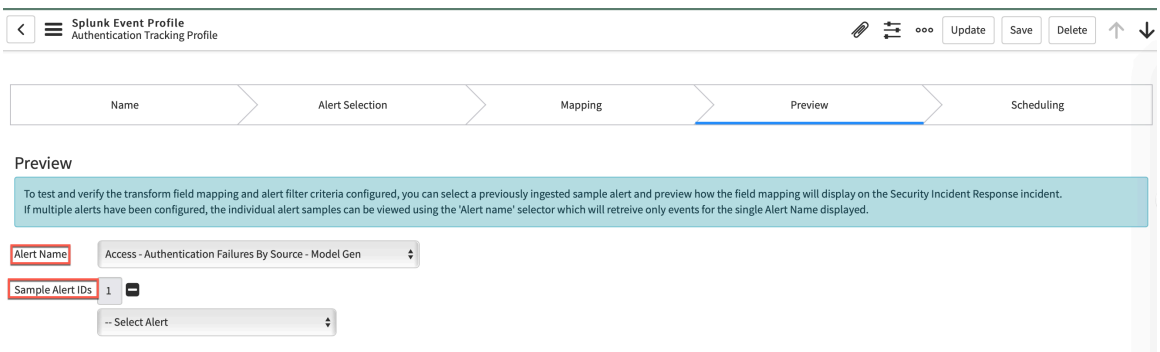
After you complete the mapping step, preview the values that you mapped in a ServiceNow AI Platform® Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the alert fields that you want displayed on the security incident.

Before you begin
Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task
Preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the SIR product.

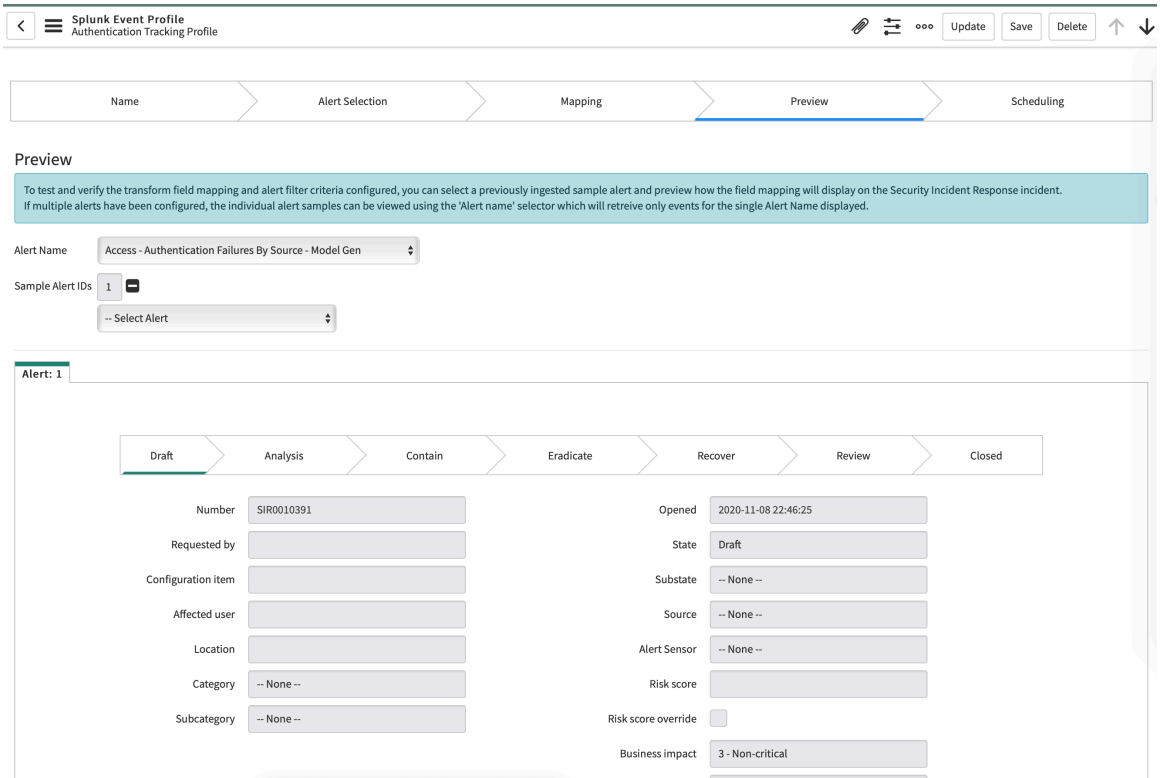
Procedure
1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. Select the **Alert Name** and then select an item from the **Sample Alert IDs** list.



   The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.

3. Review the field mapping of the alert values on the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

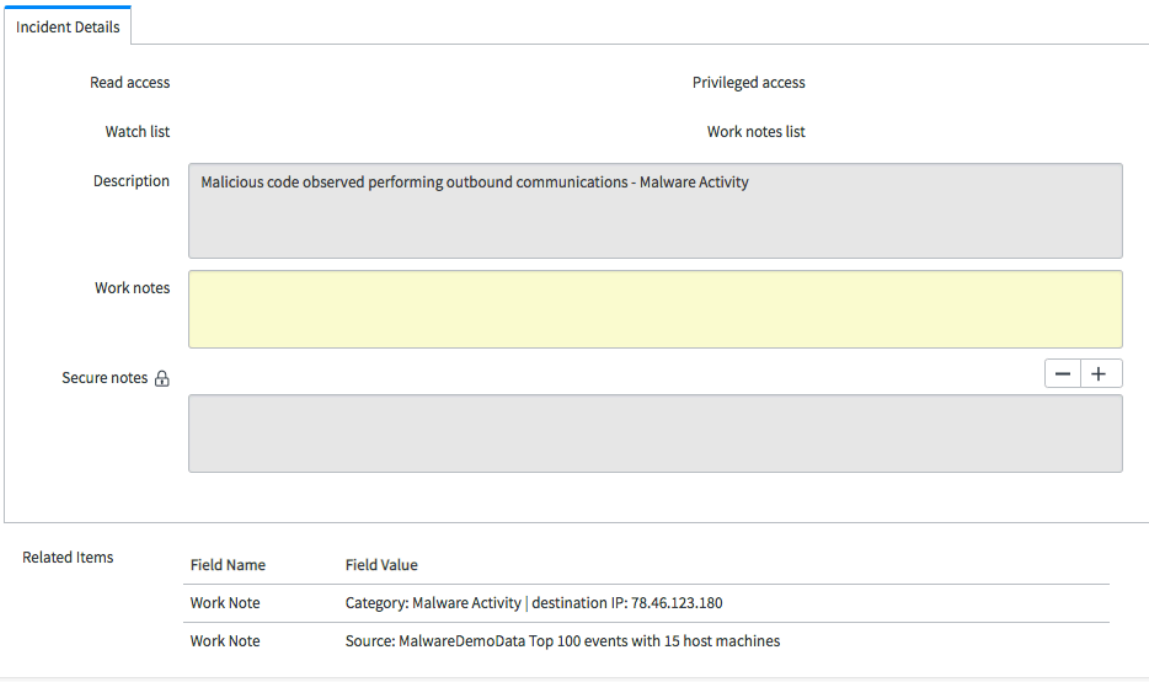


The preceding image is an example of a preview with a mapping error. In this example, a field on the security incident does not exist for a value, or the field does not support the value that you mapped. An error message is displayed that indicates an input value was not found for the `Configuration item` field.

4. To resolve this error, click **Mapping** in the progress bar.
5. Edit the mapping to fix incorrect values or populate any missing data.
6. Preview the mapping again and continue to fix any errors that are described in error messages.

   The following figure is an example of the Incident Details tab on the bottom half of a SIR security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the Splunk Enterprise console. The first Work notes field has no value. This field was left empty on the mapping grid during the mapping step. The additional Work Note fields that have values were added to the mapping grid during the mapping step.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. After you have fixed any errors and verified that the fields are the way you want them, choose one option to continue.

Option	Description
Continue	The Scheduling form is displayed for profiles with scheduled alerts. **Scheduling** is selected on the progress bar.
Finish	For profiles with configured for manual event forwarding, click **Finish**. There is no schedul ing step for profiles with event data that are exported on-demand directly from the Splunk Enterprise console.
Update	Your data is saved, and you are returned to the Splunk Event Profiles list.
Previous	The Mapping step on the progress bar is dis played.
Delete	Delete this event profile and the Splunk Event Profiles list is displayed.

What to do next

If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.

Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration

For automated alert ingestion profiles, this step is final step of the event profile configuration. During this step, you can verify the default settings for alert retrieval or modify the scheduling as needed. This step permits you to filter your alert retrieval based on a date range.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

After you have completed all the steps in the progress bar for the profile configuration as shown in the following figure, you have completed the configuration for profiles for manual event forwarding. There is no scheduling available for events forwarded manually from your Splunk Enterprise console. For profiles for automated alert ingestion, you choose whether you want to ingest any historical alerts during the Scheduling step. You also choose how often you will poll for future alerts that match the alert profile configuration.

Progress bar



For automated alert ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This step is the final step of the event profile configuration process for scheduled alert profiles.

Configure these polling intervals on a per-profile basis. The performance of the Splunk event ingestion integration is impacted by the different polling intervals. When scheduling, you may prefer to balance system load against incident urgency. A five-minute default value is set for any profile, but you may prefer to modify this setting based on the urgency of the incident and the anticipated load on your system.

In the Splunk Enterprise console, you set an alert to trigger that is based on increments or on a specific time. Use this setting to help you configure the scheduling in your ServiceNow AI Platform instance so the time increments in your Splunk Enterprise console synchronize with the scheduling that you set up in your ServiceNow AI Platform instance.

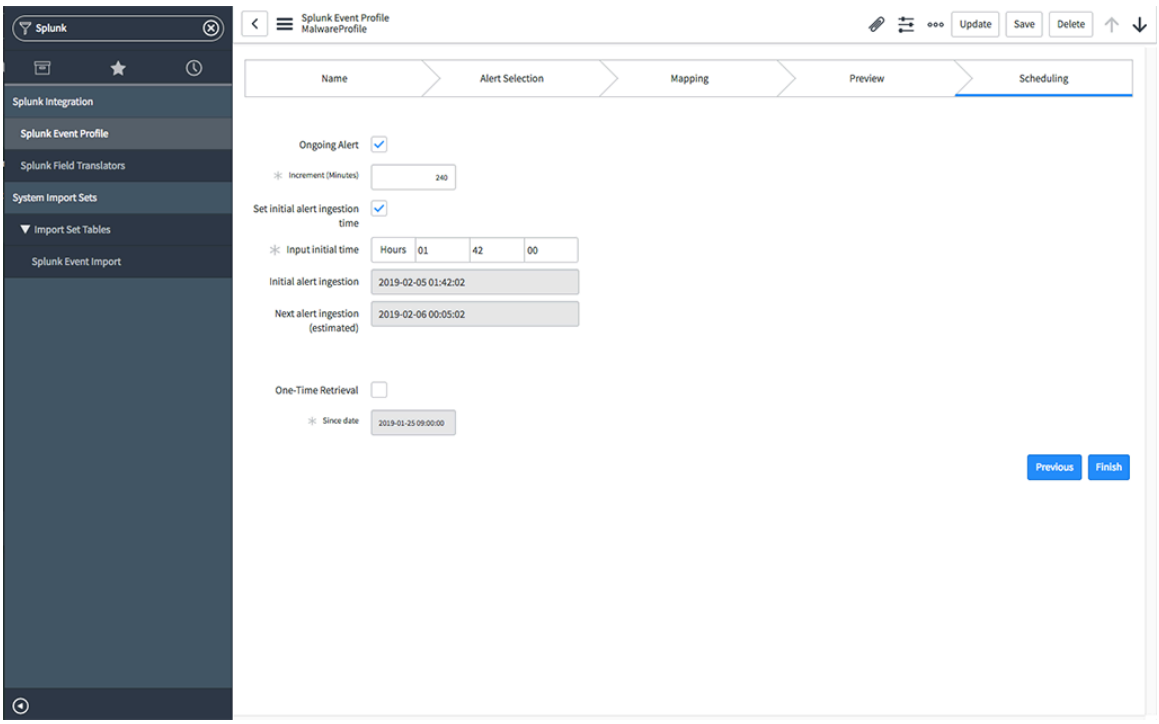
Procedure

1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when alerts are pulled from the Splunk Enterprise console.

Option	Description
○ **On-going Alert field selected** ○ **One-Time Retrieval field cleared**	On-going Alert Based on the default setting, the ServiceNow AI Platform instance pulls from the Splunk Enterprise server for new alerts every five minutes. Security incidents are created if trig gered alerts are found and filtering criteria are matched. To balance alert ingestion against server load, and to pull the most current da ta, five minutes is the setting you may prefer. However, this value can be modified as need ed.
○ **On-going alert field cleared** ○ **One-Time Retrieval field selected**	One-time retrieval Use this configuration if you want a one-time pull to ingest alerts based on historic events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	When configured, a profile is used once to re trieve triggered alerts including alerts from historical events that are based on a date range. To the right of the **Since date** field, click the calendar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the **Since date** value, triggered alerts are retrieved up through the current date. After the alerts are pulled, this setting will not retrieve triggered alerts for this profile going forward from the current date. This setting populates the security incident with all the alerts that are found for the range you enter.



As an example for scheduling, if you have a daily Splunk alert that runs once a day at 4 AM local time, you can set up the corresponding alert profile in your ServiceNow AI Platform instance to run at 4:05 AM local time to capture the alert right away and create a security incident. Enter `04 05 00` in the **Initial alert ingestion** field. In the **Increment (Minutes)** field, enter `1440` (24 hours) to schedule the next alert ingestion for 24 hours from the initial alert ingestion. Both the initial alert ingestion time and next alert ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

   a. With the Scheduling page displayed, select the **Ongoing alert** check box to enable this option.

   b. In the **Increment (minutes)** field, enter `1440` (24 hours).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Click the **Select Initial alert ingestion** check box to enable editing for the Initial alert ingestion and Next alert ingestion fields.

d. In the Initial alert ingestion field, enter `04 05 00`.
In the **The Next alert ingestion (estimated)** field, the time of the next alert ingestion is displayed.

4. Click **Finish** to complete the configuration.
A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. This profile is activated, and it pulls alerts from the Splunk Enterprise console based on your scheduling. There is a limit of 1,000 security incidents that can be created in a 24-hour period. Up to 100 events are per fired alert. Subsequent events will be ignored after the limits are reached.

Integration architecture and external systems connection for the Splunk Enterprise Event Ingestion integration

The following topic outlines the integration architecture developed to support the ingestion of triggered alerts from the Splunk Enterprise console. This information clarifies, at a high level, the conceptual operation of the integration. It also explains why there are setup steps that are required prior to installing the application from the ServiceNow Store.

Key terms used for this integration

The following key terms are used during the installation and configuration. For more information about these terms, see the ServiceNow Product Documentation website and the Splunk website and resources on Splunk Resources page.

ServiceNow AI Platform

An enterprise ServiceNow product. The ServiceNow AI Platform is the base upon which individual components such as Security Incident Response (SIR), IT Service Management (ITSM), and other products are built.

ServiceNow Splunkbase Addon

A ServiceNow application that is installed on your Splunk Enterprise console that supports the manual event forwarding option of the integration. Manual event forwarding is an optional feature of the integration. This ServiceNow Splunkbase addon is not required for the automated alert ingestion that is provided by the integration.

Security Incident Response (SIR)

A ServiceNow AI Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

Splunk Enterprise

An automated security incident event management (SIEM) product or cloud service that collects data used for incident analysis and management. This service is on a host that is sometimes also referred to as a Splunk console in this guide.

Splunk alert

A search that you configure and save in Splunk to scan for specific data based in the parameters you set up in the Splunk Enterprise service. When you pull alerts from Splunk, you also pull all the events associated with that alert.

Splunk triggered alert

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A configured search in the Splunk Enterprise console that returns results and flags these results as triggered alerts. The triggered alerts are ingested from the Splunk console into your ServiceNow AI Platform instance for this integration. Triggered alerts have one or more Splunk events.

Splunk event

One or more data elements that result in the triggered alerts of the Splunk service. From your ServiceNow AI Platform instance, you can look up which Splunk events triggered ServiceNow AI Platform security incidents.

MID Server

This application facilitates communication and movement of data between the ServiceNow AI Platform and external applications, data sources, and services. This application is typically required for integration with on-premises technologies, and, for this Splunk Enterprise Event Ingestion integration, the MID Server facilitates communication between the ServiceNow AI Platform and the on-premises instance of Splunk Enterprise. A MID Server is not required if you are integrating your ServiceNow AI Platform instance with a Splunk Cloud instance.

Security incident admin (sn_si.admin)

The user with this role oversees the configuration of the integration with the SIR product in your ServiceNow AI Platform instance.

Security incident analyst (sn_si.analyst)

The user with this role interacts with and analyzes security incidents in the ServiceNow Security Incident Response product.

Security incident profile admin (sn_si.ingestion_profile_admin)

The user with this role configures the plugin, create, edit, delete and maintain ingestion profiles for Azure Sentinel, Splunk and Splunk ES Integration for the SIR product in your ServiceNow AI Platform instance.

External systems connection

An event profile is a container that you create, name, and configure for a singular connection and call to the Splunk service to pull the most current triggered alerts that match specific criteria. After triggered alerts that match your profile have been pulled from Splunk, you select which of these alerts you want displayed as a ServiceNow AI Platform Security Incident Response SIR security incident. A default view of the Splunk Enterprise alert fields is available, and you edit this mapping of alert fields to the fields on a SIR security incident to meet your needs. You preview your mapping to verify that you have all the required alert field values populated on the SIR security incident. To complete the configuration of the alert profile, you schedule the retrieval of alerts and then activate the profile. After you activate the profile in the ServiceNow AI Platform, you are ready to ingest historical and on-going Splunk alerts automatically.

As a user with the sn_si.admin role, if you determine that a new triggered alert is similar to alerts previously ingested, you can aggregate new triggered alerts to existing SIR security incidents. You set criteria to specify matching target field values in the Splunk Enterprise alert profile that define when an existing security incident is updated and when a new security incident is created. If the aggregation feature is enabled in your event profile, when the import set is transformed, your ServiceNow AI Platform instance checks for an existing record in the target table that has the same value in the target and source fields. If an existing record with a matching value in the target table is found, that record is updated. If no matching record is found, a new record is created in the target table. If enabled, the aggregation option updates existing security incidents with new triggered alerts, and you avoid creating multiple security incidents. For more information about updating records using aggregation options, see Updating records using coalesce.

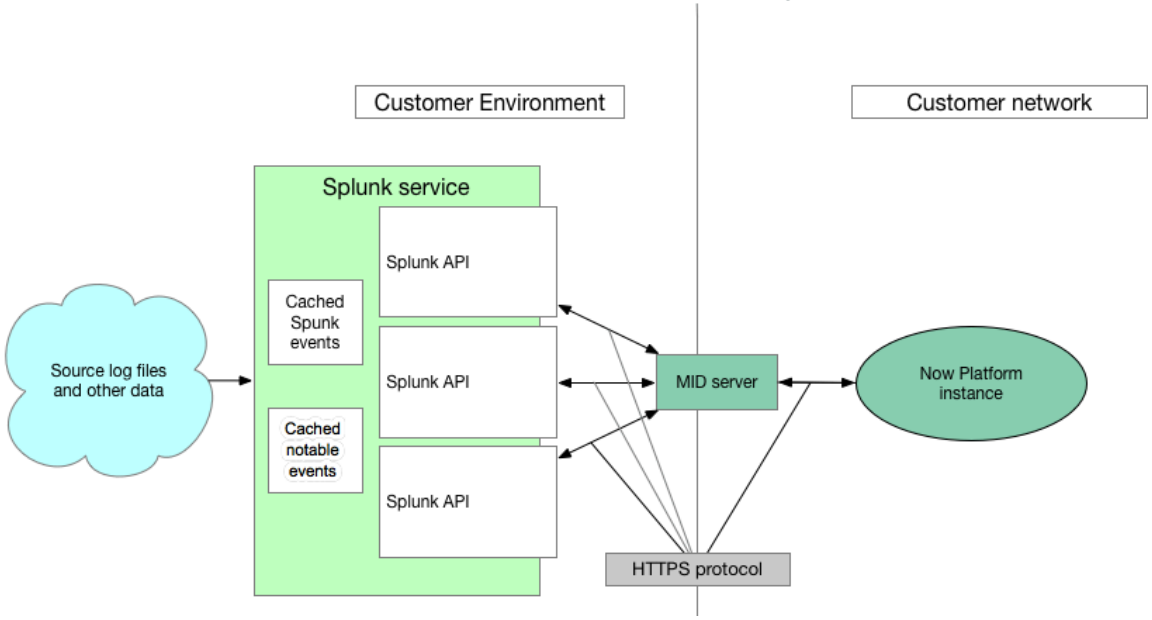
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This application uses the Splunk API service to retrieve information from the Splunk service. An outbound HTTPS connection from the MID server to this environment is necessary for the integration to work properly.

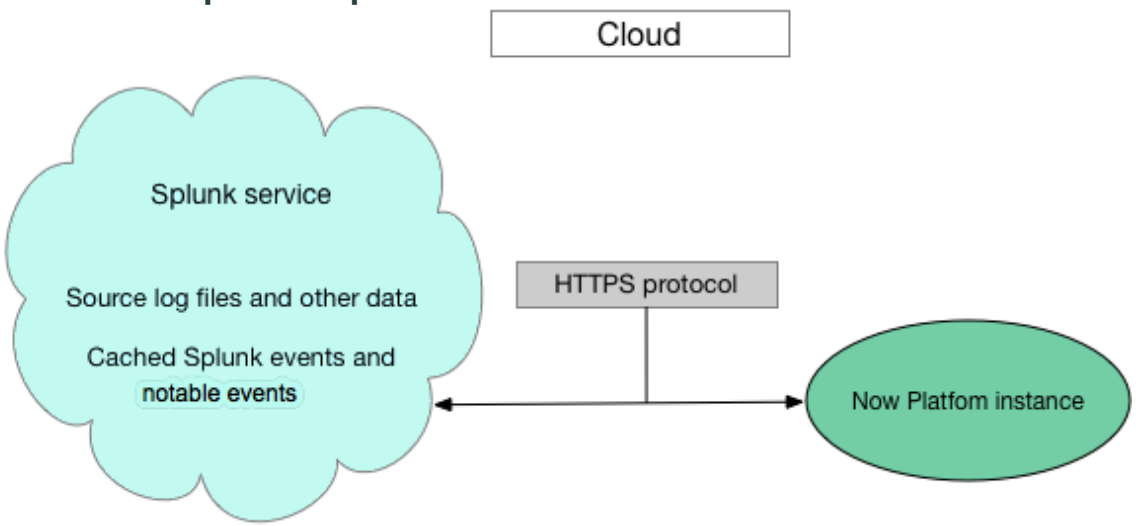
After it is connected to the Splunk service, the integration supports the pulling and ingestion of triggered alerts and events that trigger security incidents.

The basic data flow is illustrated in the following figures. In each figure, your ServiceNow AI Platform is pulling (ingesting) data. Splunk is not pushing data for scheduled alerts.

Connection to on premises Splunk enterprise service with single MID server

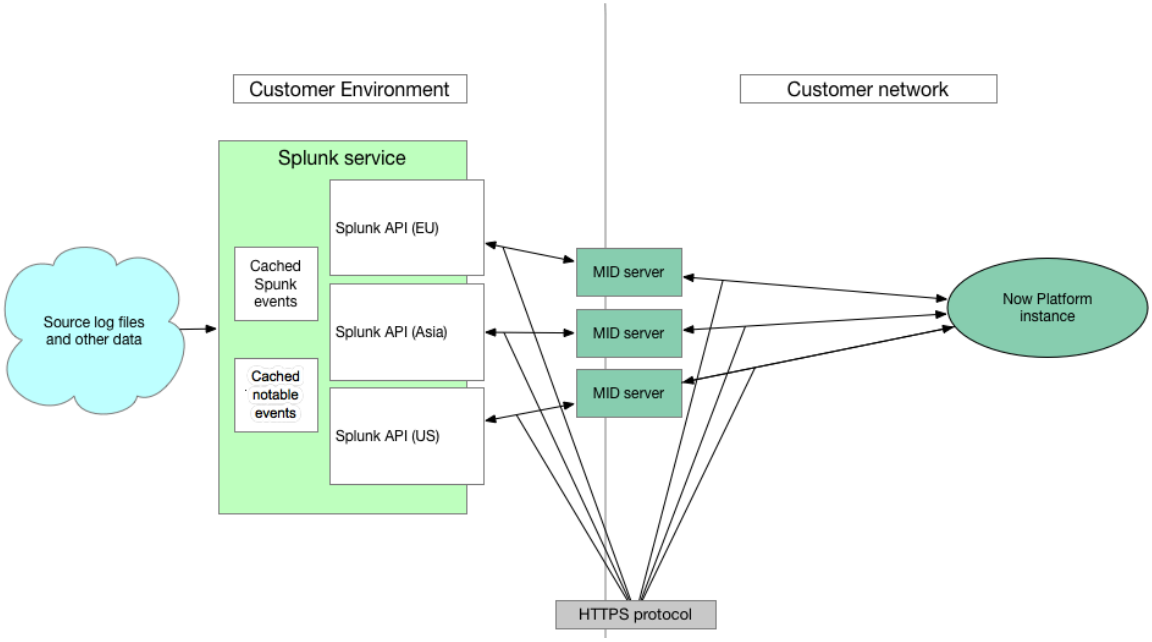


Connection to a Splunk enterprise cloud instance



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Multiple connections to the Splunk enterprise service using multiple MID servers



Copy Splunk Enterprise Event Ingestion profiles from one instance to another using export/import functionality

You can export and import Splunk Enterprise Event Ingestion profiles settings from one ServiceNow AI Platform instance to a different ServiceNow AI Platform instance.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

This functionality allows the security administrator to copy profiles that have been tested and verified on one ServiceNow AI Platform instance, for example on non-production, to another ServiceNow AI Platform instance, for example production, without the need to redo all configuration settings. The settings that are exported and imported include profile name, correlation rules, mappings, filters, aggregation criteria, field translations, fetched sample data, scheduling, and configuration tile source information.

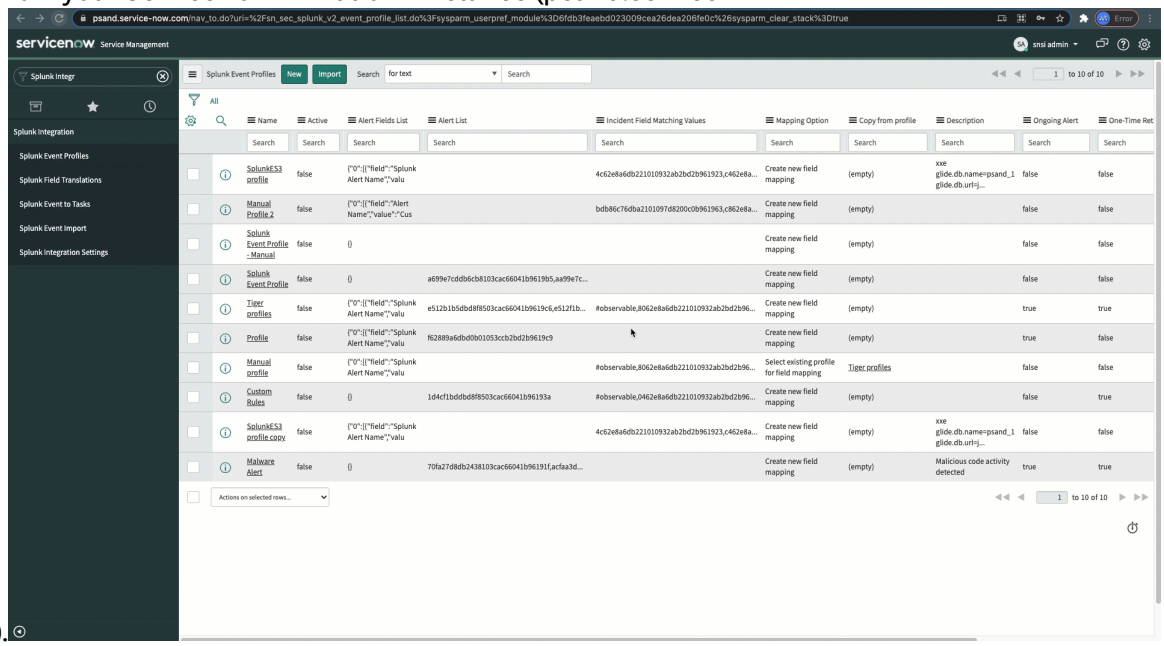
Note: When you export a manual event forwarding profile type, the attachment data used for the sample field mapping is copied, however, the attachment file itself is not exported.

Procedure

1. Navigate to **All** > **Splunk Integration** > **Splunk Event Profiles**.
2. Select a profile that you want to export to another ServiceNow AI Platform instance. You can select multiple profiles for export.
3. From the Actions menu, click **Export**.
4. Once the export complete message appears, click **Download**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows exporting a Splunk profile (Manual Profile 2) from your ServiceNow AI Platform instance (psand.service-now.com).

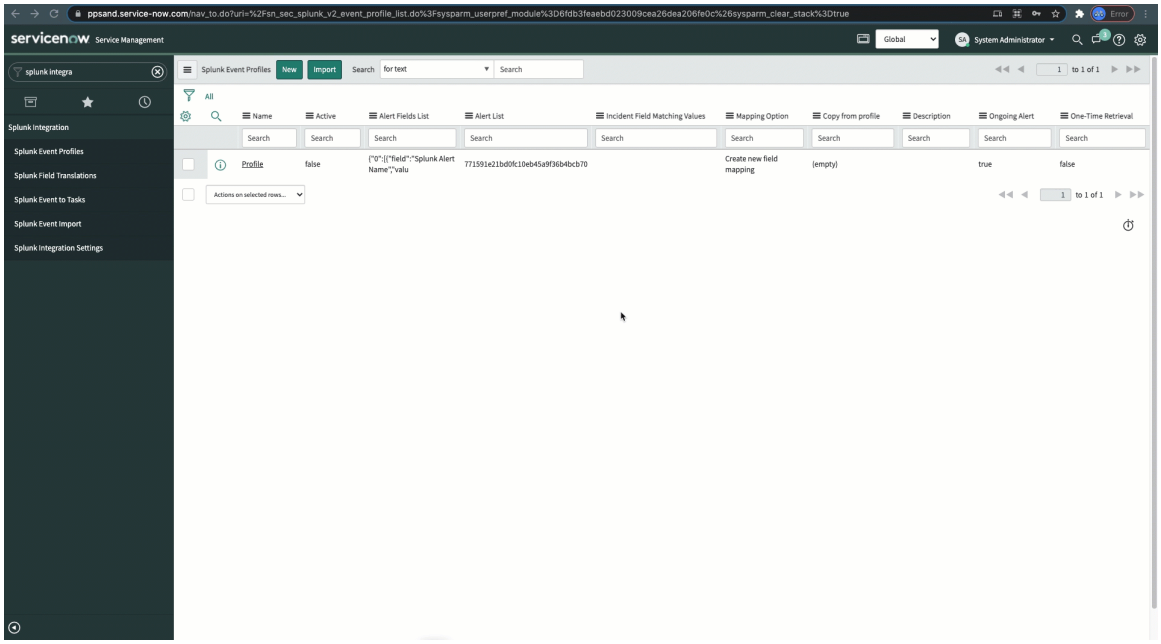


The exported payload.xml file is downloaded on your computer. The file contains the profile name, correlation rules, mappings, filters, aggregation criteria, field translations, fetched sample data, scheduling, and configuration tile source information. When you select and download multiple profiles, they appear in the same payload.xml file.

You can now proceed to import the profile in another ServiceNow AI Platform instance.

5. Navigate to **Splunk Integration** > **Splunk Event Profiles**.
6. Click **Import**.
7. Click **Choose file** and select the xml file on your computer.
8. Click **Upload**.
9. Click **Close and Reload Profiles**.
   The following illustration shows importing a Splunk profile (Manual Profile 2) from the ServiceNow AI Platform instance (psand.service-now.com) to another ServiceNow AI Platform instance (ppsand.service-now.com).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You have successfully imported the profile from another ServiceNow AI Platform instance.

Verify that the exported Source (Splunk API account and Splunk server URL) and MID Server configuration settings are valid and available in imported ServiceNow AI Platform instance. Update your Splunk Enterprise Event Ingestion configuration if required.

10. **Optional:** Verify the MID Server settings after your import a profile.
11. **Optional:** Navigate to **Security Operations** > **Integration Configurations**.
12. **Optional:** Select the Splunk Enterprise Event Ingestion configuration tile, and click **Update**.
13. **Optional:** Review and update the Source and MID Server details as required.

Copy an event profile for the Splunk Enterprise Event Ingestion integration

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you might prefer to copy alarm profiles to save time.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

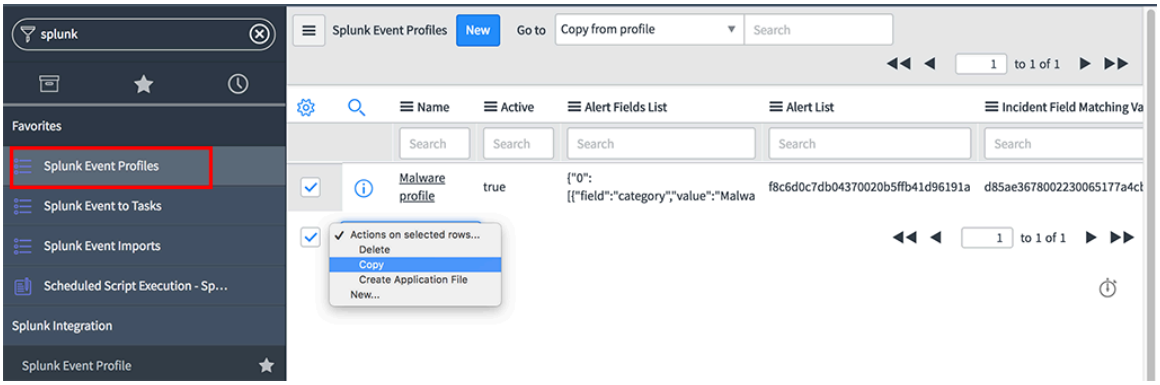
Copying an existing profile and its associated settings is optional.

If you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is disabled (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

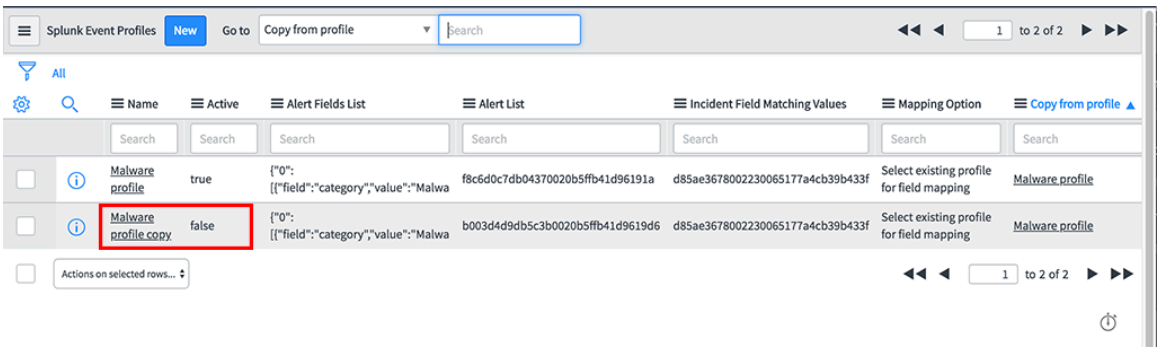
Procedure

1. Navigate to **All** > **Splunk Integration** > **Splunk Event Profile**.
2. In the Splunk Event Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is enabled (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.



You have successfully copied the settings from an existing profile to a new profile.

What to do next

You are prompted to activate (enable) the new profile after you complete the configuration steps.

Set up ServiceNow Event Ingestion Integration add-on

Install and set up the ServiceNow Event Ingestion Integration add-on in your Splunk enterprise console or Splunk Cloud instance.

Before you begin

Important:

Create a **Manual event forwarding** profile to forward alerts on-demand from your splunk console to create a Security Incident Response (SIR) on the ServiceNow instance. For more information, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration and implement same for Splunk V2.

This add-on setup is necessary to enable manual event forwarding for the Splunk profile. Up-to two configurations can be created for a particular add-on. (**Splunk Primary** and **Splunk Secondary**)

Verify that you have installed the application for this integration from the ServiceNow Store before installing the add-on plugin from splunkbase that is required for manual event ingestion. If you have not installed the application for the integration from the ServiceNow Store, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration and follow the instructions to install it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: ServiceNow AI Platform administrator (admin)

About this task

If you want to export events manually and on-demand from your Splunk console for the integration, download, and set up the ServiceNow Event Ingestion Integration add-on from Splunkbase in your Splunk console.

This ServiceNow extension add-on is required so that security incidents can be created from manually exported events in your ServiceNow AI Platform instance. This ServiceNow Event Ingestion Integration add-on is available on splunkbase.

For manual event forwarding, you can identify up to two different ServiceNow AI Platform endpoints (instances) in your Splunk Enterprise console. You forward the events to the endpoint or endpoints manually to create security incidents. For example, you can specify both a staging (development) instance and a production instance. By specifying separate instances and naming primary and secondary workflows for each instance, you can choose where you want to forward different events.

Procedure

1. If you have not already installed the **ServiceNow Event Ingestion Integration** add-on, follow these steps to install and configure it.

   a. Download **ServiceNow Event Ingestion Integration** add-on from Splunkbase.

   b. If prompted, restart the Splunk Enterprise.
   The **ServiceNow Event Ingestion Integration** add-on is installed in your Splunk Enterprise enterprise console. The next step is to set up the Add-on.

2. To set up the Addon, follow these steps.

   a. In the Splunk Enterprise, select **Manage Apps** gear icon on the menu drop-down list.

   b. On the list of applications that is displayed, in the **Actions** column, select **Set up** for **ServiceNow Event Ingestion Integration**.

   The ServiceNow Event Ingestion Integration add-on is configured into three different tabs.

   - **Splunk Primary**: The default or primary Splunk configuration.
   - **Splunk Secondary**: (Optional) The backup or second Splunk configuration.
   - **Logging Level**: The level of reporting logs generated by the integration, meaning the name of the type of information.

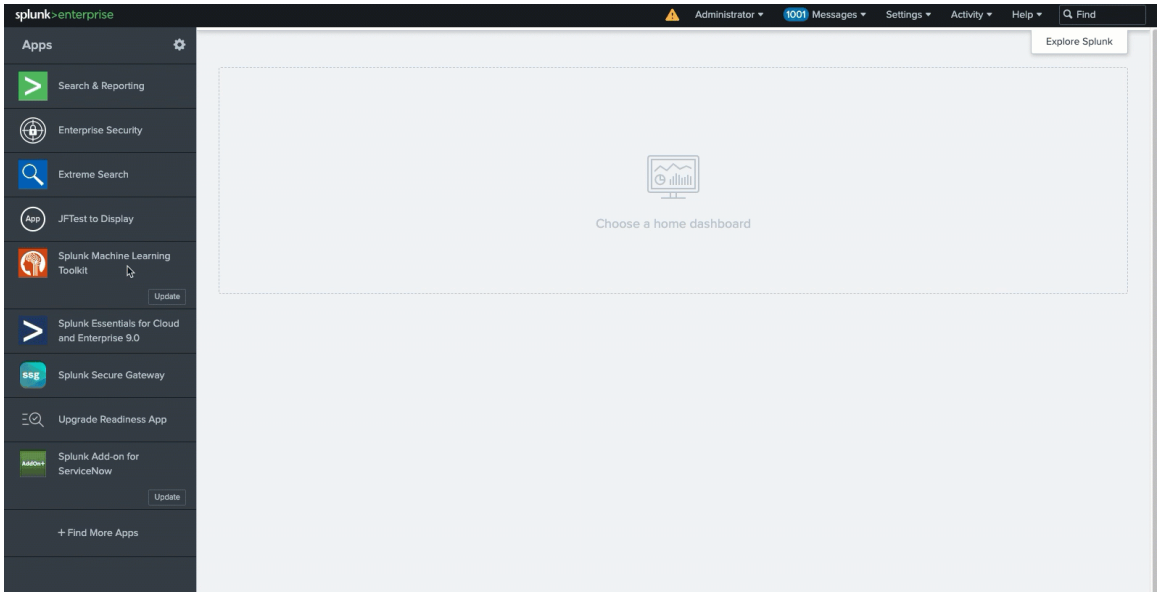
   c. On the form, fill in the fields.

Field	Description
Workflow action label	Name of the instance. This will be an action in the drop-down of **Event Actions** for alerts in the Splunk console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
URL	URL of the ServiceNow instance you entered in the preceding workflow action label field.
Endpoint	Base API path. Default for this field is: `/api/sn_sec_splunk_v2/event_ingestion`.
Auth type	Authentication method to be used for API requests. The available options include: ▪ **Basic Authentication**: Uses username and password to authenticate requests. ▪ **OAuth 2.0 Authentication**: Uses access tokens to authenticate requests.
Basic Authentication	
Username	Username of the user. User with the (sn_sec_splunk_v2.api_account_access) role should be present in the instance specified in the preceding URL field for manual event forwarding.
Password	Password of the user. User with the (sn_sec_splunk_v2.api_account_access) role should be present in the instance specified in the preceding URL field for manual event forwarding.
OAuth 2.0 Authentication	
Client Id	Client ID of the app created in the ServiceNow instance. For information on how to get the Client ID, see Configure Application Registry on the ServiceNow instance.
Client Secret	Client Secret of the app created in the ServiceNow instance. For information on how to get the Client Secret, see Configure Application Registry on the ServiceNow instance.
Redirect URL	Copy and paste this URL in the redirect URL field of the Application Registries record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



d. Select **Save**.

e. Select the **Splunk Secondary** tab.

f. On the form, fill in the fields.
Fields are same as in the Splunk Primary tab.

g. Select **Save**.

> **Note:** Up-to two configurations can be created for a particular add-on.(**Basic Authentication** and another **OAuth 2.0 Authentication**)

h. Select the **Logging Level** tab.

i. On the form, fill in the fields.

Logging level

Field	Description
Log Level	The level of reporting logs generated by the integration, meaning the name of the type of information. You can also update the value to the following options: ▪ **info** ▪ **error** ▪ **warn** ▪ **debug** By default, the value is **info**.

j. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Using ServiceNow Event Ingestion Integration add-on

Using ServiceNow Event Ingestion Integration add-on

Map alerts from Splunk console to create a Security Incident Response (SIR) on the ServiceNow instance.

Before you begin

Role required: sn_sec_splunk_v2.api_account_access

Procedure

1. Log in to Splunk Enterprise.
2. Navigate to **Apps** > **Search & Reporting**.
3. Select **Alerts**.
   A list of alerts generated in the Splunk console on the basis of correlation rule configured previously show up.
4. Select any **Configured Alert** from the list.
   Trigger History of the configured alert show up.
5. Select **View Results** against the alert.
6. Expand any of the alerts using **(>)** icon.
7. From the drop down, select the **Workflow action label** configured while setting up the add-on.
   For more information on Workflow action label, see Set up ServiceNow Event Ingestion Integration add-on
   Alerts will go in **Splunk Import** table followed by **Splunk Event to Tasks** table.

Result

A Security Incident Response (SIR) record is created on the ServiceNow instance as per the mapping specified in the Manual event forwarding profile. For instructions on how to set up a Manual event forwarding profile, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration

Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration

The following steps for saving searches in your Splunk Enterprise console are provided for a user with the Splunk Enterprise administrator role.

Before you begin

If you already have existing saved searches and triggered alerts in your Splunk Enterprise console, you are not required to modify these searches for this integration.

The integration of the ServiceNow AI Platform® Security Operations product with the Splunk event notification service pulls event and alert information from Splunk.

Prior to ingesting alerts into your Security Operations environment, configure searches in your Splunk Enterprise console so that you automatically pull the relevant security events in Splunk Enterprise that you want to save as alerts.

If you do not have saved searches and triggered alerts established for notification when important security events occur in your Splunk Enterprise console, follow these steps to save searches.

Role required: Splunk Enterprise administrator

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Log in to your Splunk Enterprise account.
2. Click the **Search** tab.
3. In the New Search field that is displayed, enter a value for the alert, for example, Malware.
4. To view the events related to your search, to the right of the New Search field, click the search icon or press enter.
   The search results with events are displayed.
5. To save the search as an alert, in the upper right of the page, expand the Save As choice list and select **Alert**.
6. In the form that is displayed, fill in the fields.

Field	Description
Title	Descriptive name for the alert, for example, Malware Events. After you save this search as an alert, events from a fired alert in the Splunk service are automatically processed into trig gered alerts using this search data. This trig gered alert title is used in the event profile that you create in your ServiceNow AI Plat form instance to identify which events are in gested into your instance for ServiceNow AI Platform® Security Incident Response SIR se curity incident creation.
(Optional) Description	Text to help you distinguish this alert from oth er alerts.
Alert type	In the fields that are displayed, select **Sched uled** to search for this alert on a schedule, or **Real-time** to search continuously for this alert.
Trigger results	You may prefer to set one of the following fil ter conditions: ○ Number of Results is greater than or less than ○ One-time (once) for each result
Trigger actions	Add actions to trigger this alert. Expand the Add choice list and click **Add to Triggered Alerts** so that it is displayed on the form. You may prefer this setting for the alerts that you ingest into your ServiceNow AI Platform in stance.

7. Click **Save**.
   Your alert is saved, and it is displayed under the Alerts tab on the Search page.
   The Splunk service pulls in the events by matching the criteria that you configured in the alert. It caches the events, and you then request these events from your profiles that you set up in your ServiceNow AI Platform instance. Because the ingestion pull of events occurs from a cache in the Splunk service, this ingestion from your ServiceNow AI Platform does not impact performance on your Splunk platform.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

You have successfully completed the required setup for the integration in your Splunk Enterprise console. If you have not already installed the application for the integration from the ServiceNow Store, the next step is to install the application for the integration and configure it.

Use the script editor to format alert values for the Splunk Enterprise Event Ingestion integration

Use the script editor to format field values on the security incident during the mapping step.

Before you begin

In addition to the directly mapped fields from the pulled alert values, and the alert values you enter manually, you can optionally use the script editor to format field values on the security incident during the mapping step. The script editor changes the values of a Splunk alert so that values that are supported by the ServiceNow AI Platform® Security Incident Response security incident are mapped to the Category, Configuration item (CI), and Observable fields.

Role required: sn_si.ingestion_profile_admin

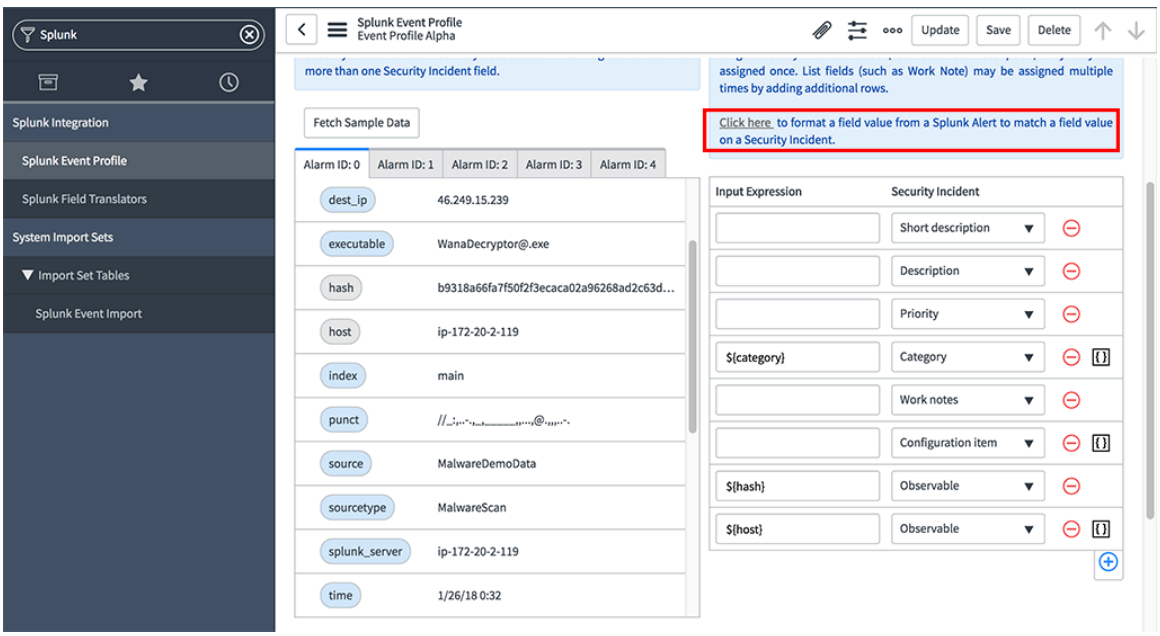
Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

In certain cases, Splunk Enterprise alert values are mapped to the Category, Configuration item (CI), and Observable fields on the SIR incident and are not supported. You might prefer to edit the mapped values. If you want to translate the value of a Splunk Enterprise alert to a value that is supported by these fields on the SIR security incident, use the script editor.

Procedure

1. With the mapping form displayed, click the link to open the script editor.



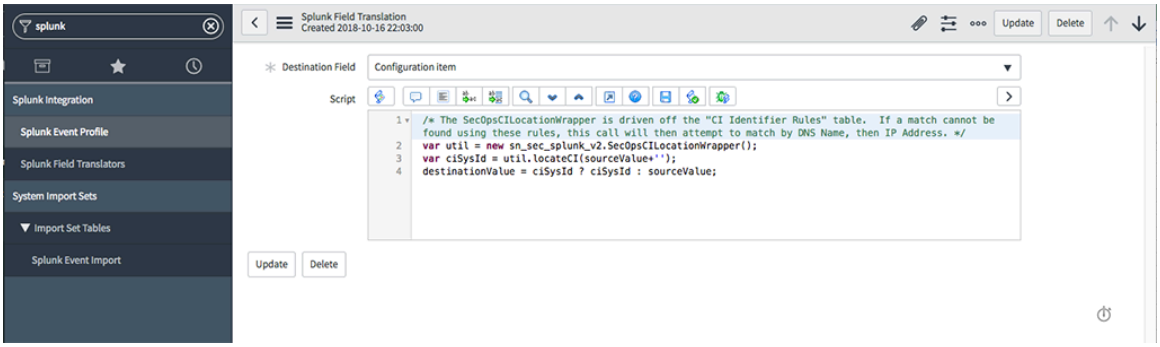
2. From the choice list, select a destination field for the value that you want to edit.
3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon [{ }] next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For an alert, for example, a value for the Configuration item may not be matched.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As shown in the following figure, if a match for a host name cannot be found in the ServiceNow AI Platform® CMBD for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field. If there is no value for the alarm, the field on the security incident is set to null.

The editor opens with the field displayed in Destination Field. The following image shows the editor with the `Configuration item` field as the Destination Field.



4. Enter any changes to then script, and click **Update** to save your changes.
   The Splunk Field Translations table is displayed.
5. Close the table to return to the Mapping form.

Checklist for the Splunk Enterprise Event Ingestion integration

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

Before you begin

Role required: admin

About this task

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.

Roles required: Roles are listed for each step below.

Procedure

1. As a user with the ServiceNow AI Platform admin role, set up your ServiceNow AI Platform instance.
   - Assign users with the sn_si.admin and sn_si.analyst roles as required.
   - Install and configure a MID Server if the Splunk server is deployed within your corporate network.
   - Verify that the ServiceNow Security Incident Response plugins are activated for your release of the ServiceNow AI Platform.
   - If you want to forward events manually from your Splunk Enterprise console into your ServiceNow AI Platform instance, verify that you have assigned the (sn_sec_splunk_v2.api_account_access) role to a user with the Splunk Enterprise enterprise administrator permission.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see Set up your ServiceNow AI Platform instance for the Splunk Enterprise Event Ingestion integration.

You have successfully completed the set up steps and verified expected results for the integration.

2. As a user with the ServiceNow AI Platform admin role, install and configure the Splunk Enterprise Event Ingestion application from the ServiceNow Store.
   a. Download and install the application on your ServiceNow AI Platform instance.
   b. Configure the application and connect to your Splunk Enterprise console.

   For more information, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration.

3. **Optional:** If you intend to export events manually from your Splunk Enterprise console to your ServiceNow AI Platform instance, perform the following tasks:

   a. As a Splunk Enterprise administrator, install, set up, and enable the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise from splunkbase in your Splunk Enterprise console.

   b. As a Splunk Enterprise administrator, if not already configured, save searches as alerts in your Splunk Enterprise console.

      (Optional) For more information, see Set up ServiceNow Event Ingestion Integration add-on and Save searches in your Splunk Enterprise console for the Splunk Enterprise Event Ingestion integration.

4. As a user with the ServiceNow AI Platform sn_si.admin role, create and name an event profile.

   Select the profile type from the choice list. Options are a scheduled alert profile that you use to ingest sample data, or, an event profile that you use to export attachment data manually from your Splunk Enterprise console.

   - For a scheduled alert, select an available alert.
   - For profile for manually exported data, create a new map or copy an existing map.

   For more information, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration.

5. As a user with the ServiceNow AI Platform sn_si.admin role, map values ingested or attachment data that is exported from Splunk Enterprise to ServiceNow AI Platform security incidents.
   a. Fetch sample data for a scheduled alert.
   b. Export attachment data manually from Splunk Enterprise for an event.
   c. Edit the default mapping configuration.
   d. Optionally add filtering criteria, append an alert to an existing security incident, and use the script editor.

   For more information, see Mapping alerts and events for the Splunk Enterprise Event Ingestion integration and Map alerts for the Splunk Enterprise Event Ingestion integration.

6. As a user with the ServiceNow AI Platform sn_si.admin role, preview the data from Splunk Enterprise that is displayed on a ServiceNow AI Platform security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Fix any errors or add any missing data so that no error messages are displayed.

For more information, see Preview the security incident for the Splunk Enterprise Event Ingestion integration.

7. As a user with the ServiceNow AI Platform sn_si.admin role, schedule alert retrieval for a profile with a scheduled alert.

   For more information, see Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.

Splunk Enterprise Security event ingestion integration

The Splunk Enterprise Security notable event ingestion integration with the Security Incident Response (SIR) product allows security incident analysts to collect and process notable event data (referred to as notables).

Overview of Splunk Enterprise Security event ingestion integration

Data is ingested continually based on a configured polling schedule and it is used by analysts to identify and respond to potential cyber threats. Security events that are collected can be correlated into notable events in Splunk Enterprise Security and then ingested automatically with this integration. Also, individual notable events can be manually forwarded on-demand from the Splunk Enterprise Security Incident Review console and reporting interface into the Security Incident Response product of the ServiceNow AI Platform to create security incidents.

This integration provides a security operations center (SOC) analyst with visibility to notable events and related contributing event data. This data can be integrated into ServiceNow AI Platform Security Incident Response (SIR) security incidents for further investigation and remediation. Profiles are created in your ServiceNow AI Platform instance to handle different notable event types that are created via correlation searches in Splunk Enterprise Security. These profiles customize how different Splunk event fields are displayed on SIR security incidents.

Key features

This integration includes the following key features:

- Create multiple notable event ingestion profiles to create SIR security incidents for specific types of threats such as phishing and malware and unauthorized access attempts.
- Create multiple event profiles for on-demand event forwarding from your Splunk ES incident review console to create SIR security incidents.
- Drag-and-drop mapping of Splunk notable event field values to associated SIR security incident fields.
- A preview of the SIR security incident layout based on sample notable events to validate event mapping details.
- Ingest historical notable events as well as ongoing, new, and updated notable events on configurable intervals.
- Filter out notable events that do not meet SIR incident generation criteria, for example, low priority events, events that have yet to achieve a specific status, and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Aggregate events or alerts to existing SIR security incidents based on matching field values to avoid duplicate security incidents.
- Update notable events based on SIR incident creation and/or closure conditionals via a bi-directional interface to keep Splunk ES notable event updates in sync with the ServiceNow SIR incident status.

Supported ServiceNow AI Platform versions

The com.snc.si_dep plugin is required for this integration. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before installing and activating the other Security Operations applications.

The following Security Operations applications must be installed and activated from the ServiceNow Store. Install and then activate one application at a time in the order listed below to ensure a smooth installation:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response

For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

ServiceNow Addons

The ServiceNow Security Operations Event Ingestion Addon for Splunk ES is required only if you prefer to forward events manually from your Splunk Enterprise Security Incident Review console into your ServiceNow AI Platform instance. This ServiceNow addon is available in splunkbase.

This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise application in splunkbase is not required for the automated alert ingestion that is supported by the integration.

Splunk Supported versions

This integration has been tested with:

- Splunk Enterprise version 10.0.0 and earlier.
- Splunk Enterprise Security application version 8.3.0 and earlier.

MID Server

This integration requires an installed and configured MID Server in your ServiceNow AI Platform® instance to connect to the Splunk service when the Splunk server is deployed within your corporate network. If you are using the Splunk Cloud service, a MID Server is not required. See MID Server for more information about MID Servers.

References

Reference	Document Identifier	Document Title
1	Splunk product website	Splunk Enterprise Security product website.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist

For a printable checklist of these topics, see Checklist for the Splunk Enterprise Security Notable Event Ingestion integration. You can use this list to monitor your progress as you work through the tasks of the integration.

Key terms used in this integration

This section describes some of the key terms used in this integration.

The following key terms are used during the installation and configuration. For more information about these terms, see the ServiceNow Product Documentation website and the Splunk website and resources on Splunk Resources page.

ServiceNow AI Platform

An enterprise ServiceNow product. The ServiceNow AI Platform is the base upon which individual components such as Security Incident Response (SIR), IT Service Management (ITSM), and other products are built.

ServiceNow Splunkbase Addon

A ServiceNow application that is installed on your Splunk Enterprise Security console that supports the manual event forwarding option of the integration. Manual event forwarding is an optional feature of the integration. This ServiceNow Splunkbase add-on is not required for the automated notable event ingestion that is provided by the integration which pulls events from Splunk.

Security Incident Response (SIR)

A ServiceNow AI Platform application that tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review and closure.

Splunk Enterprise Security

Splunk Enterprise Security helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk. Splunk Enterprise Security is a premium security solution requiring a paid license. This service is on a host or a Splunk cloud offering that is referred to as a Splunk console in this guide.

Splunk Enterprise Security notable event

When a correlation search identifies an event or a pattern of events, it creates a notable event. Correlation searches filter the security data and correlate across events to identify a particular type of incident (or pattern of events) and then create notable events.

Splunk event

One or more data elements that result in the notable events of the Splunk service. From your ServiceNow AI Platform instance, you can look up which Splunk events triggered ServiceNow AI Platform security incidents.

MID Server

This application facilitates communication and movement of data between the ServiceNow AI Platform and external applications, data sources, and services. This application is typically required for integration with on-premises technologies, and, for this Splunk Enterprise Security event ingestion integration, the MID Server facilitates communication between the ServiceNow AI Platform and the on-premises instance of Splunk Enterprise Security. A MID Server is not required if you are integrating your ServiceNow AI Platform instance with a Splunk Cloud instance.

Security incident admin (sn_si.admin)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The user with this role oversees the configuration of the integration with the SIR product in your ServiceNow AI Platform instance.

Security incident analyst (sn_si.analyst)

The user with this role interacts with and analyzes security incidents in the ServiceNow Security Incident Response product.

Set up your ServiceNow AI Platform® instance for the Splunk Enterprise Security integration

The following section lists the setup tasks that you are required to complete in your ServiceNow AI Platform® instance prior to installing the application from the ServiceNow Store.

Role required: sn_si.ingestion_profile_admin.

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Refer to the following table and verify that you have completed all the listed tasks before you download and install the application to ensure a smooth installation and configuration.

1. Verify that you have assigned the required ServiceNow AI Platform® and Security Incident Response (SIR) roles.

   The following roles are required for the installation, setup, and use of the integration in your ServiceNow AI Platform® instance.

   - A user with the ServiceNow AI Platform® administrator role (admin) installs the application from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) role.
   - If you want to forward notable events manually from Splunk Enterprise Security for this integration, a user with the ServiceNow AI Platform® admin role assigns a user with the (sn_sec_splunkes.api_account_access) role in the ServiceNow AI Platform®. This role permits a user with the Splunk Enterprise Security administrator role to access the API in the ServiceNow AI Platform® that is required for manual event forwarding for this integration.

     The (sn_sec_splunkes.api_account_access) role is not required for the integration if you are ingesting notable events automatically from Splunk Enterprise Security into your ServiceNow AI Platform® instance.

   - A user with the **sn_si.ingestion_profile_admin** role oversees the following tasks in the ServiceNow AI Platform®:
     - Names, creates, and edits event profiles.
     - Selects and maps values from Splunk Enterprise Security to ServiceNow AI Platform® security incidents.
     - Previews security incident details for accuracy prior to finalizing the configuration.
     - Schedules on-going notable event ingestion.
     - Enables notable event updates when a SIR incident is created and closed.
     - Assigns the security incident analyst (sn_si.analyst) role.
     - Users with the sn_si.analyst work with security incidents.

   For more information, see Managing roles.

2. Assign the Splunk user role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign a Security Analyst (ess_analyst) user role in Splunk ES to perform all integration-related activities on the Splunk server.

3. Verify that you are using version 7.2.6 or later of the Splunk API. Earlier versions are not supported.

   If you have access to the Splunk Enterprise Security console, you have access to the API that is required for this integration. There is no other special setup required for the API.

4. Verify that you have installed and configured a MID Server.

   A MID Server in your ServiceNow AI Platform® instance is required to connect to the Splunk service if the Splunk server is deployed within your corporate network. For information, see MID Server.

   If you are using the Splunk Enterprise Security Cloud service, a MID Server is not required.

5. Verify that the ServiceNow core applications that are required to support the integration are installed and activated.

   The Security Incident Response Dependency plugin (com.snc.si_dep) is required. This plugin automatically installs all the dependencies that are required to support the Security Incident Response product. Install and activate this plugin before you install and activate the other Security Operations applications required by the integration.

   Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation.

   a. Security Incident Response
   b. Security Integration Framework
   c. Security Support Common

   For more information about installing the Security Operations core applications, see Get entitlement for a Security Operations product or application and Activate a ServiceNow Store application.

You have successfully set up your ServiceNow AI Platform® instance for the integration. The next step is to install the Splunk Enterprise Security Notable Event Ingestion application from the ServiceNow Store for the integration. For more information, see Install and configure Splunk Enterprise Security Notable Event Ingestion integration.

If you want to export notable events manually and on-demand from your Splunk Enterprise Security console for the integration, see Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration for more information.

Install and configure Splunk Enterprise Security Notable Event Ingestion integration

Install and configure Splunk Enterprise Security Notable Event Ingestion integration for Security Operations application from the ServiceNow Store on your ServiceNow AI Platform® instance.

Before you begin
Role required: ess_analyst

Assign a Security Analyst (ess_analyst) user role in Splunk ES to perform all integration-related activities on the Splunk server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

https://player.vimeo.com/video/1147269492?h=9386cf9f7d&badge=0&autopause=0&%E2%80%A6

Procedure

1. If you have not installed the Splunk Enterprise Security Event Ingestion application from the ServiceNow Store for the integration, see Install a Security Operations integration and follow the steps to install it.
2. After you have successfully installed the application, navigate to **All** > **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for **Splunk Enterprise Security- Event Ingestion** tile, and select **Configure**.
4. On the form, fill in the fields.

Field	Description
Name	Name of the Splunk Enterprise Security con sole or Splunk Cloud instance used for the inte gration. Spaces are supported for names, but paren theses are not supported. For example, enter `SplunkES2`.
Splunk API Base URL	URL for your Splunk Enterprise Security con sole or Splunk Cloud instance. The URL should include the API port, for example: `https://mysplunkserver.com:8089`
Basic Authentication	Default is disabled. If you are using API Account User Name and API Password for configuration, enable the check box.
API Account User Name	User name that you created for your API user account on the Splunk Enterprise Security con sole.
API Password	Password that you created for your API user ac count on the Splunk Enterprise Security con sole.
Token Based (available from version 12.0.0)	Token that you created for your API user ac count on the Splunk Enterprise Security con sole.
Token	Token that you created for your API user ac count on the Splunk Enterprise Security con sole.
On Premises Deployment	Default is disabled. If you're using an on-premise based version of Splunk Enterprise Security, verify that this check box is selected.
MID Server	Option to choose a particular MID Server to set up in your environment, which will be used by

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	this integration to pull notable events into ServiceNow. You can select a specific MID Server from the list or select **Any** to enable an auto-selection of a valid MID Server from the list for this integration. **Note:** ○ The MID Server selected during this configuration time applies throughout this integration. ○ Only MID Servers that are active and validated are displayed on this list. By default, the value is set to **Any**. For example, there are three MID Servers A, B, and C. If you select **Any**, then one of these MID Servers is auto-selected and applies throughout this integration. If you select a specific MID Server, say C, then the selected MID Server C applies throughout this integration. If you want to change the MID Server, then you have to reconfigure it from the App Configuration tile.

Each Splunk Enterprise Security notable event type that you ingest from your Splunk Enterprise Security incident review console requires a unique event profile in your ServiceNow AI Platform® instance. However, the source that you configure on the Event Ingestion Configuration form can be reused for multiple ServiceNow AI Platform® profiles as long as each profile ingests unique notable event types.

5. Select **Submit**.
   The configured integration tile displays.

What to do next

Create and name an event profile for the Splunk Enterprise Security event ingestion integration

Configure Splunk Enterprise Security settings

Use the Splunk Enterprise Security (ES) settings to modify the preset configurations and their values as per your requirements.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

1. Navigate to **All** > **Splunk ES Integration** > **Splunk ES Settings**.
2. On the form, fill the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk ES Settings

Field	Description
Enforce a limit on the number of notable events that can be aggregated to a single incident.	Option to enforce a limit on the number of your notable events that you want to aggregate to a single incident. By default, the value is set as 100.
Enforce a limit on the number of security incidents that can be created in a 24-hour period.	Option to enforce a limit on the number of security incidents that can be created in a period of 24 hours. By default, the value is set as 1000.
Enforce a limit on the number of values to parse in each field received from Splunk.	Option to enforce a limit on the number of values that you want to parse for each field received from Splunk. By default, the value is set as 1000.
Number of correlation rules to pull from Splunk.	Option to define the number of correlation rules to retrieve from Splunk. By default, the value is set as 500.
The Time-to-Live parameter for Splunk search job in seconds.	Option to define the Time-to-Live parameter for the Splunk search in the form of seconds. By default, the value is set as 600.
Number of notable types to batch in one search.	Option to define the total number of notable types that you want batch in a single search. By default, the value is set as 20.
Number of days to retain the Splunk search job metadata in ServiceNow	Option to define the number of days that you want to retain the Splunk search job metadata in ServiceNow. By default, the value is set as 30.
The delimiter character to split the values in field mappings.	Option to define the delimiter character to split the values in field mappings. By default, the value is set as (,).
Number of overlap minutes to add while fetching the events from Splunk (to overcome the indexing delay from Splunk)	Option to define the number of overlap minutes to add while retrieving the events from Splunk to overcome the indexing delay from Splunk. By default, the value is set as 30.
Pull updated notable events	Option to retrieve updated notable events. By default, the value is set as No.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Activate this setting to update existing Splunk source configurations for token based authentication support. You must update the integration configuration with token details after this setting is enabled.	Option to update existing Splunk source configuration to token based authentication support from an existing version. **Note:** After you upgrade to the new version, the token field would become unavailable. You must enable this setting to get the token-based authentication, after which you must update the integration configuration with token details. By default, the value is set as No.
Enable the check box to pull Closed Notables during ingestion.	Option to pull the closed events into the ServiceNow Splunk ES instance. If unchecked, only active events are pulled into the instance. By default, the value is set as No.

3. Click **Save**.

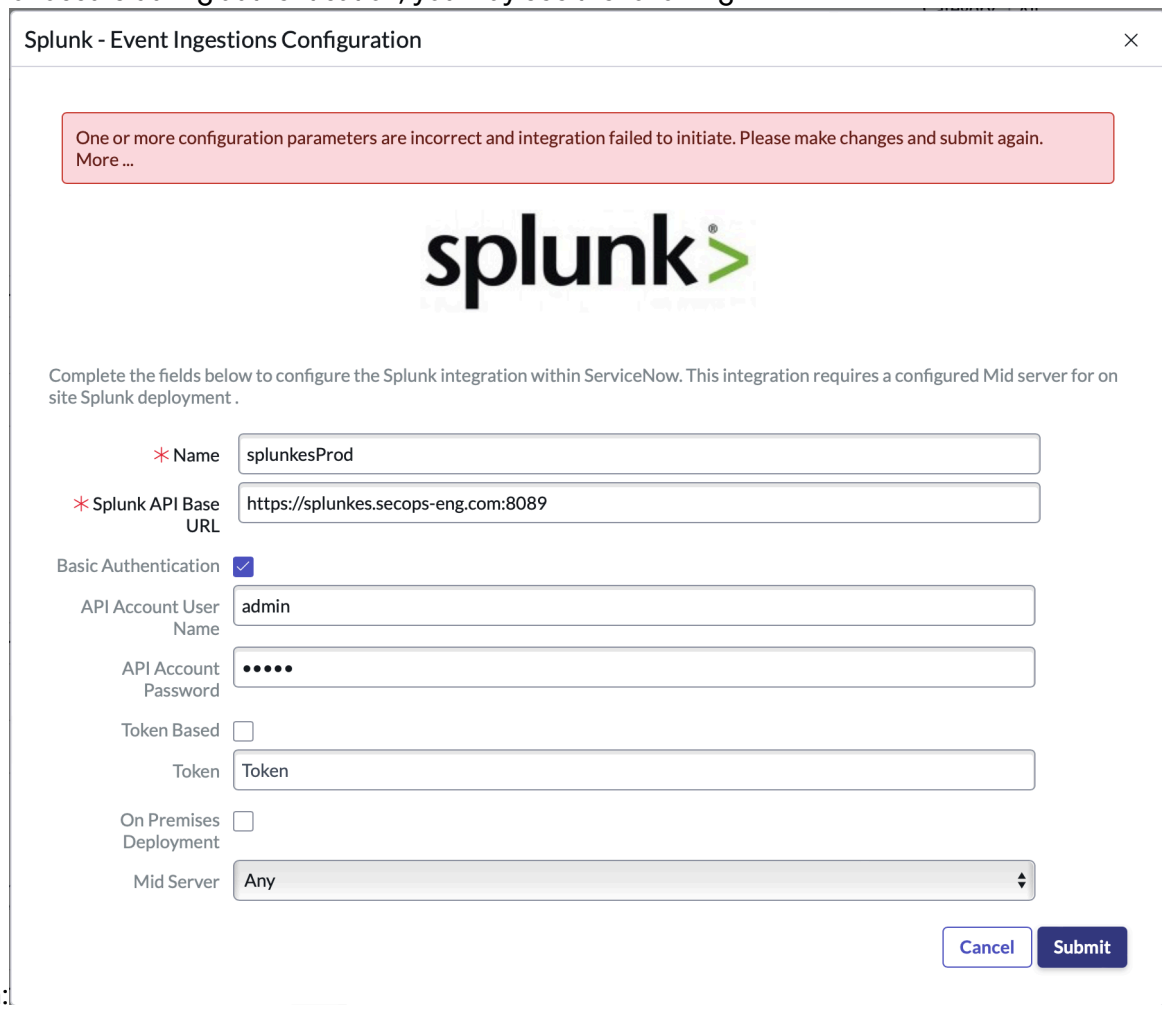
Authentication errors

This section describes some common authentication errors and how they can be resolved.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

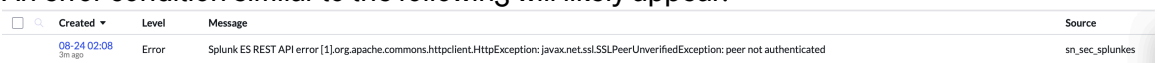
Certificate validation issue

If an error occurs during authentication, you may see the following screen:



If you have verified that your API account credentials and the Splunk Base URL information are correct, this error may be due to an issue with the Splunk certificate for the port 8089 communication. ServiceNow® instance requires a valid certificate with a common name that matches the server host name to establish secure connections. For more information, see Certificates. If you see this error, you can verify that the issue is due to a certificate problem by viewing the system logs.

An error condition similar to the following will likely appear:



To proceed with the authentication, you must replace the Splunk default certificate that is provided for API access on port 8089. For detailed instructions on how to replace the SSL certificate, see KB0778285.

Create and name an event profile for the Splunk Enterprise Security event ingestion integration

You create an event profile in your ServiceNow AI Platform instance and determine which Splunk notable events create security incidents.

Before you begin

Role required: sn_si.ingestion_profile_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

Before ServiceNow AI Platform Security Incident Response (SIR) security incidents are created from ingested notable events, the field values from alerts are displayed on a layout of a ServiceNow AI Platform security incident so that you can preview how the actual security incident will be created.

From an integration perspective using the available APIs, Splunk ES notable events are forwarded individually and manually as discrete notable events, or they're automatically ingested into the Security Operations environment of your ServiceNow AI Platform instance depending on the profile type defined.

The integration workflows ingest different types of notable events such as unauthorized access attempts and malware, for example. These notable events are ingested based on the profiles that you configure in the Security Operations environment of your instance.

All notables are initially ingested for a configured correlation search type in a profile. Ingested notables can then be further filtered to specify which notables create security incidents. For example, you may prefer filters that create security incidents only for notable events that are identified as high-risk. Before a profile is activated, and it creates security incidents from ingested notable events, individual field values on the notable events are mapped to corresponding fields on a layout the security incident for a preview.

Procedure

1. Names for the event profiles in your ServiceNow AI Platform instance must be unique and can only be mapped to one active event profile at any given time.
2. The ServiceNow AI Platform ingests specific notables using the workflows of the integration. All notable events that meet the selection criteria in your Splunk ES console are initially ingested into your ServiceNow AI Platform instance.
3. A profile in your ServiceNow AI Platform is an encapsulation of a notable event in your Splunk ES console.
   There's a one-to-one relationship between notable events that are ingested with a profile and connections to your Splunk ES console: one notable event type for one connection.
4. To create profiles for scheduled notable events, see Set up a profile for scheduled notable event ingestion.
5. To create profiles for manual event forwarding, see Set up a profile for manual event forwarding.

Set up a profile for scheduled notable event ingestion

Depending on the profile defined, Splunk ES notable events are automatically ingested into the Security Operations environment of your ServiceNow AI Platform instance.

The following table shows the list of tasks you need to follow to set up a profile for scheduled ingestion of notable events:

Steps to set up a profile for scheduled notable event ingestion

Task	Section
Create an event profile	See Create profiles for scheduled notable event ingestion

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Steps to set up a profile for scheduled notable event ingestion (continued)

Task	Section
Select notable events based on correlation search name	See Select notable events based on correlation rule name for the profile for Splunk ES Event Ingestion integration
Map notable event fields	See Mapping notable event fields for the Splunk Enterprise Security integration
Create custom mappings	See Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion)
Preview the security incident	See Preview the security incident for the Splunk Enterprise Security Event Ingestion integration
Schedule and retrieve new and updated notable events	See Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration
Automate notable event updates and closure based on SIR incident status	See Automate notable event updates and closure based on SIR incident status

Create profiles for scheduled notable event ingestion

You can set up a profile so that notable events are automatically ingested.

Before you begin

Role required: sn_si.admin

Procedure

1. To create an event profile for a notable event or correlation rule type in your ServiceNow AI Platform instance, navigate to **Splunk Integration** > **Splunk Event Profile**.
2. If the Splunk Event Profile form is not displayed, click **Name** in the Progress bar.
3. Click **New**.
4. Fill in the fields.

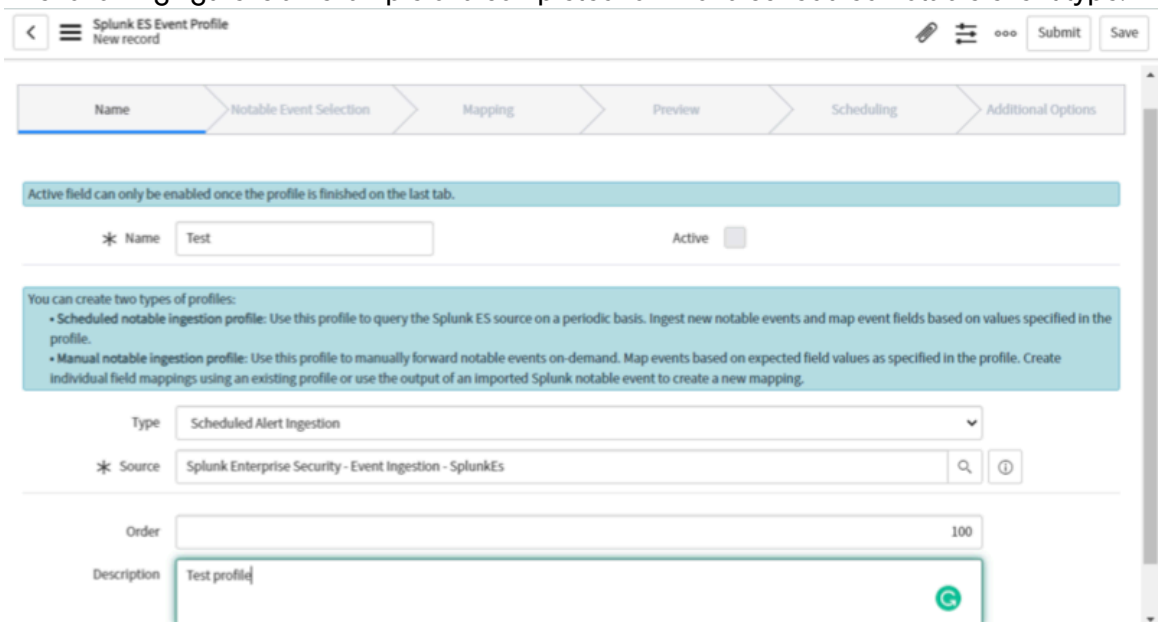
   An example of a completed form follows the table.

Field	Description
Name	Unique name for the profile. If names are not unique, an error will be displayed and duplicate profile names are not saved. Profile names in your ServiceNow AI Platform instance must be unique.
Active	Check box is cleared and disabled by default. You should complete all sections in the profile before making it active.
Type	Select the profile type from the choice list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Scheduled Event Ingestion: This type of profile supports notable events that are ingested on a configured schedule. Fill in the fields. ○ Manual Event Forwarding: This type of profile supports notable events that are forwarded manually from your Splunk Enterprise Security Incident Review console on demand. See the following steps to fill out the form for these types of profiles.
Source	Splunk server or search end that you configured to ingest notable events. If you have multiple Splunk servers configured, select the appropriate server for the notable event types that will be ingested for the profile. You are required to enter a value.
Order	Default is 100. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share the same triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Additional text to help you distinguish this profile from other profiles.

The following figure is an example of a completed form for a scheduled notable event type.



5. For a profile with a scheduled notable event, choose one option to continue with the profile configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Continue	Save the profile and progress to the Event Selection step.
Update	Save updates to this profile and return to the Splunk Event Profiles list.
Save	Save this profile and remain on the page.
Delete	Delete this profile record and return to the Splunk Event Profiles list.

What to do next
The next step is to select notable events for automatic ingestion.

Select notable events based on correlation rule name for the profile for Splunk ES Event Ingestion integration

After you have created a profile for a scheduled notable event type ingestion, select a Splunk Enterprise Security correlation rule name for this profile for which you want to map corresponding notable events to a ServiceNow AI Platform Security Incident Response security incident.

Before you begin
Role required: sn_si.admin

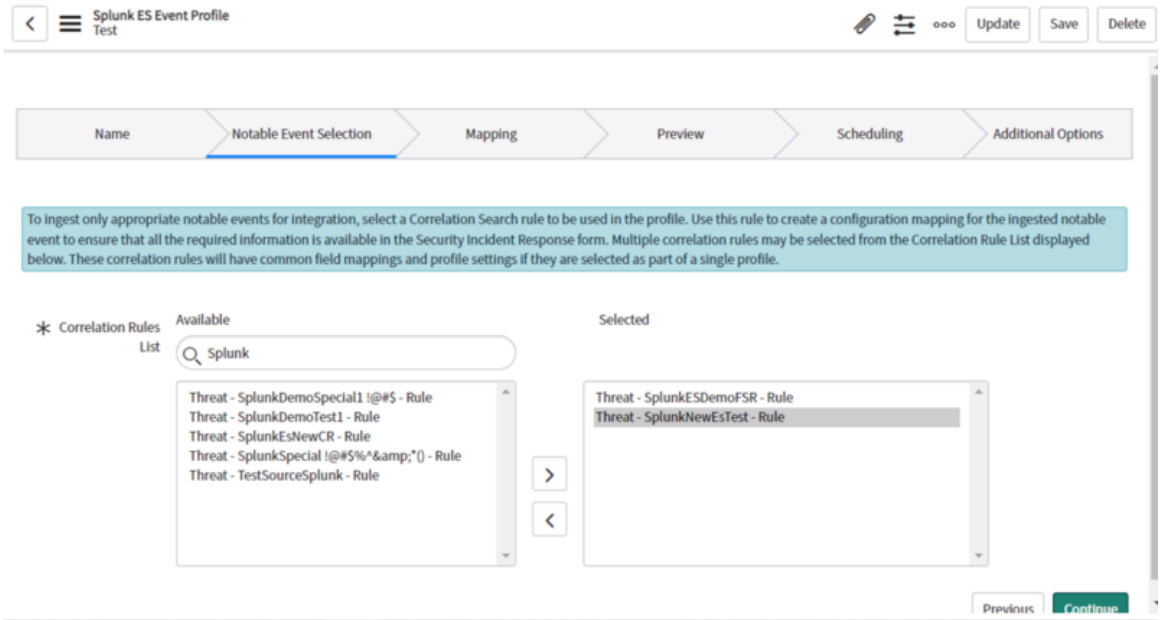
About this task
View the available correlation rules in your ServiceNow AI Platform instance so you know the notable event types for which you want to ingest and create security incidents. Select a correlation rule. You can select one or more notable event from the list in this form.

Procedure
1. If the Notable Event Selection page is not displayed, select it on the progress bar to display it.
2. From the Correlation Rule List, choose one of the following options to select a single correlation rule or multiple correlation rules and move them and move it to from the Available column to the Selected column.

   The list of correlation rules on this form matches the list of correlation rules in your Splunk ES Incident Review console. Up to 500 correlation rules are displayed on this form. If there are more than 500 correlation rules listed in your Splunk ES, only the first 500 notable events are displayed on this form in your ServiceNow AI Platform instance.

Option	Description
In the Correlation Rule List search field, enter text.	The column below the search field is filtered with available options based on the text that you enter. Select an correlation rule, and with the arrow keys, move the selected alarm from **Available** to **Selected**.
In the Correlation Rule List, double-click a Correlation Rule.	The **Selected** column is populated with your selection.
In the Correlation Rule List, single-click a Correlation Rule.	The correlation rule is selected. With the arrow keys, move the selected correlation rule from **Available** to **Selected**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Choose one option to continue.

Option	Description
Continue, or alternatively, click Mapping in the progress bar	The Mapping form is displayed. **Mapping** is selected on the progress bar. The next step is to map notable event fields to a SIR security incident.
Update	Your data is saved and the Splunk Notable Event Profiles list is displayed.
Previous	The **Name** step is displayed.
Delete	Delete this event profile and the Splunk No table Event Profiles list is displayed.

What to do next

You have successfully selected a correlation rule for a scheduled Splunk Enterprise Security profile. The next step is map notable event values to fields on a security incident.

Mapping notable event fields for the Splunk Enterprise Security integration

After you identify the specific correlation rule and notable event type for the profile, the next step is to map individual notable event fields to the fields on a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Overview

For the mapping step, you can ingest sample notable events for the selected correlation rule or export notable event data for manually forwarded notable events. The event mapping process is identical regardless of the profile type you are creating.

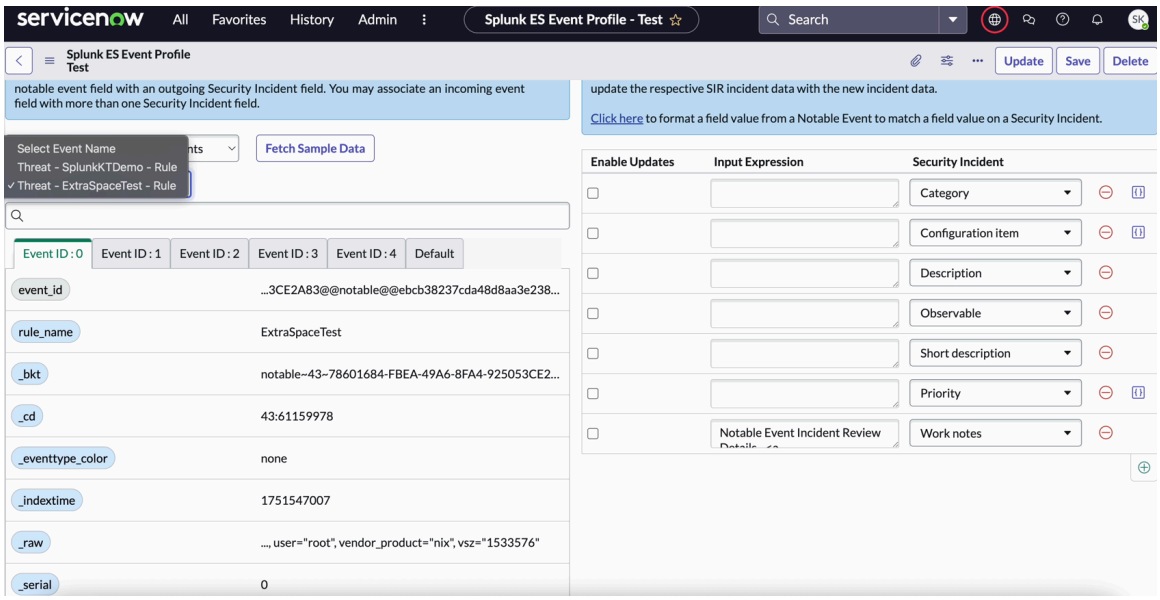
The following figures are examples of the default mapping configurations that are provided for each type of event profile. You can customize the fields that populate the security incident. During this mapping phase, you can ensure all relevant notable event field data is mapped to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the appropriate place on the SIR incident form and then visualize the SIR incident in the preview section.

If Multiple correlations are used, then notable events can be fetched by selecting required Event. Use **Alert Name** to choose your alert if you have configured multiple alerts for ingestion.

After you click to fetch data, the Splunk notable event field names and corresponding values are populated on the left side of the form. These are the Splunk notable event fields that are available to map to the SIR security incident fields. Some fields can be mapped multiple times to the SIR security incident fields.



You may prefer to review a few sample notable events on your Splunk console to ingest for the field mapping configuration step. This step is labeled Mapping on the progress bar. If this page is not displayed, click **Mapping** on the progress bar. You can ingest up to five sample notable events from Splunk Enterprise Security to assist with the notable event field mapping process. There are options to either ingest the five most recent notable events for the correlation rule selected or ingest up to five specific notable events based on the notable event IDs.

Below is a summary of the steps required to map notable events:

- Scheduled Notable Event Sample Data Ingestion: For sample data that is used for automatically ingested notable event profiles, available notable event fields and their corresponding values are displayed in a default mapping layout on the left side of the mapping form once the sample data is retrieved. Tabs are displayed for you to view the values for a specific notable event ID that you pulled. Verify that all the critical fields from the notable event sample ingestion section on the left of the form are mapped to ServiceNow security incident fields on the right of the form.
- Field Mapping: Edit the mapping configuration by dragging notable event fields from the left side and dropping them on the ServiceNow SIR incident mapping section on the right. The mapping on the right associates the incoming notable event field with an outgoing security incident field.
- Mapping Experience: Customize the mapping grid by adding or removing fields using the + icon at the bottom of the SIR incident field mapping section. Track overlooked or duplicated fields with the color coding that is provided (mapped fields are greyed out, blue fields are unmapped).
- Incident Generation Conditions: Once the mapping section is complete, you can set filter conditions so that you can specify which notable events should create security incidents versus which notable events should be filtered out, for example, low priority notable events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This is done in the Incident Generation Conditions section located below the Notable Event Mapping section.

- Event Aggregation Criteria: Define additional Event Aggregation criteria that aggregates an incoming notable event to an existing SIR security incident instead pf creating similar, potentially duplicate incidents. Using field matching value criteria for each profile, this additional aggregation capability can reduce the number of active, overlapping security incidents by placing all related security notable event data on a single security incident.
- Format Field Translation: In certain cases, event field values in the Splunk Enterprise notable events may not translate directly to the fields on the SIR security incident. For these values, you can use a script editor to format field values on the security incident during the mapping step. Use the script editor if you want to format values that are similar, but not identical. For example, with the script editor, a category value of Malware Alert and Virus Infection may have different field values for the source category but both values can be translated to a common Malicious Code Activity in the Category field on the SIR security incident using the Format Field Translation functionality.

The next step is to ingest notable events and map values to the SIR security incident fields.

Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion)

During the notable event field-mapping step, you map individual event fields from notable events to fields on a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

The mapping grid can be customized for the notable event type selected in the correlation rule selection. Color-coding of the event fields helps you keep track of the event values that you have already mapped as they become grayed out while all remaining unmapped fields appear in blue. This helps you better visualize which field values have been added to the security incident and if any remaining important event information remains unmapped.

Map up to five notable events from the Notable Event Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.

Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Default fields that are typically important field to populate on the security incident response form are displayed. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default-mapping grid on the SIR security incident.

Procedure

1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. For a profile with a scheduled ingestion, below Notable Event Sample Ingestion, click **Fetch Sample Data** to pull the latest sample notable events from the Splunk Enterprise console for the correlation rule selected.

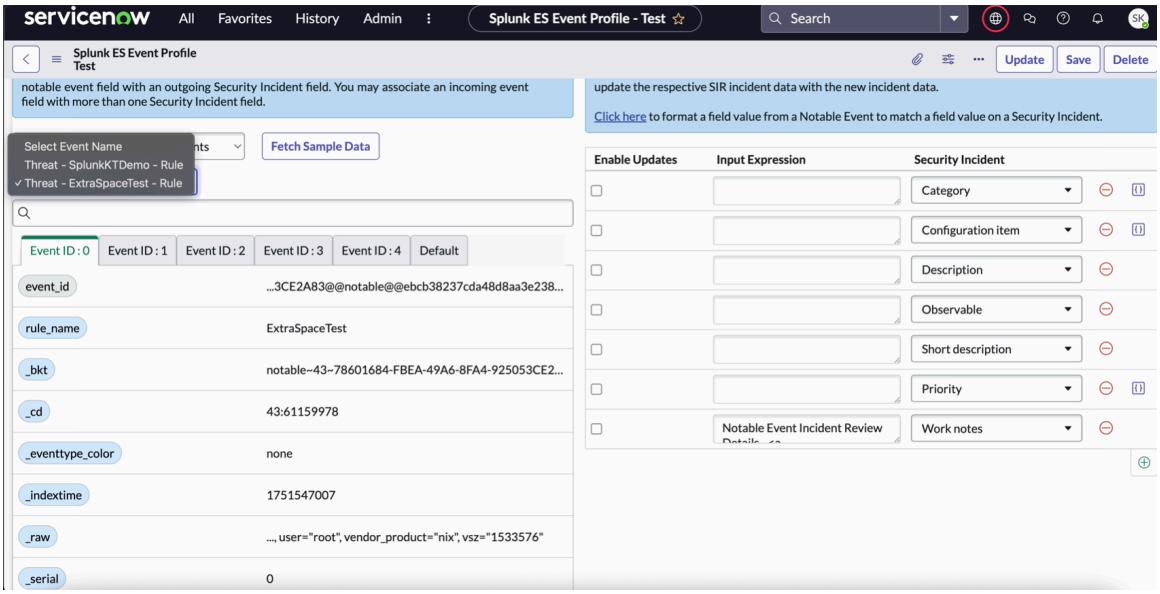
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can either pull the most recent sample notable events or provide the unique notable event IDs for the specific notable events that you want to use for your notable event mapping experience.

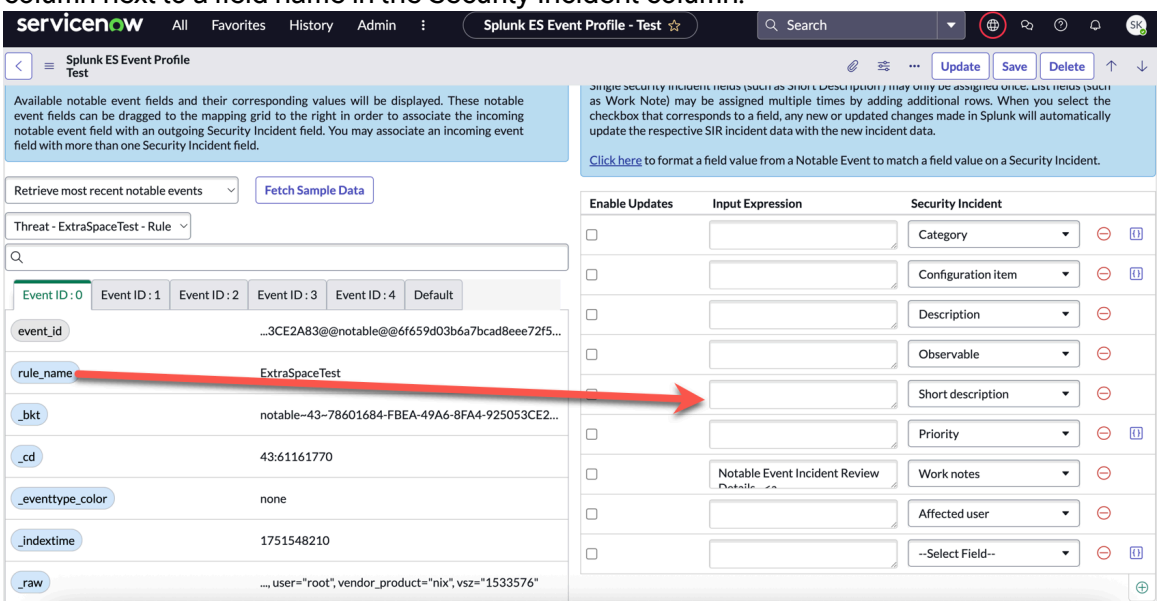
The notable event fields and values results are displayed as individual tabs. You can ingest up to five notable events.

The pull for sample notable events may take a few moments. A message indicating that the transaction is working is displayed at the top of the screen.

In the following figure, the field-name value pairs for the ingested notable event, or the imported sample events, are displayed on the left side of this form after the ingestion pull is completed. These values are the values that you map to the security incident fields on the SIR Incident Field Mapping side of the form.



3. To map a field value from the left side of the form to a field on the security incident on the right side of the form, click-hold a blue field name on the left side of the form.
4. Drag the field name, for example, `rule_name`, and drop it on a field in the Input Expression column next to a field name in the Security Incident column.

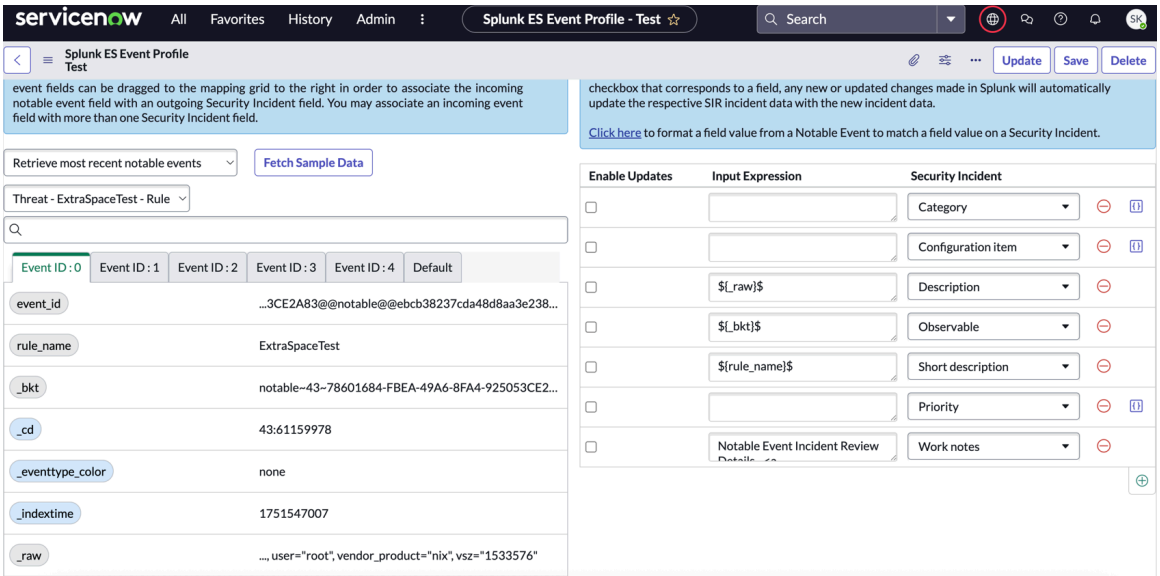


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The field value is displayed in the Input Expression column. In the following image, `rule_name` is mapped to the `Short description` field on the security incident. However, you can match any value from the left side to a field on the right. Verify that the value is mapped correctly on the security incident during the preview step.

To help you ensure that no event fields are overlooked or duplicated in the mapping process, fields are color-coded. Light blue fields on the left indicate that a notable event field is not yet selected and mapped on the security incident. You may prefer to associate an incoming notable field with more than one field on a security incident.

A gray field indicates that a field has been selected and mapped to a field on the security incident. This color-coding helps you track the mapping.



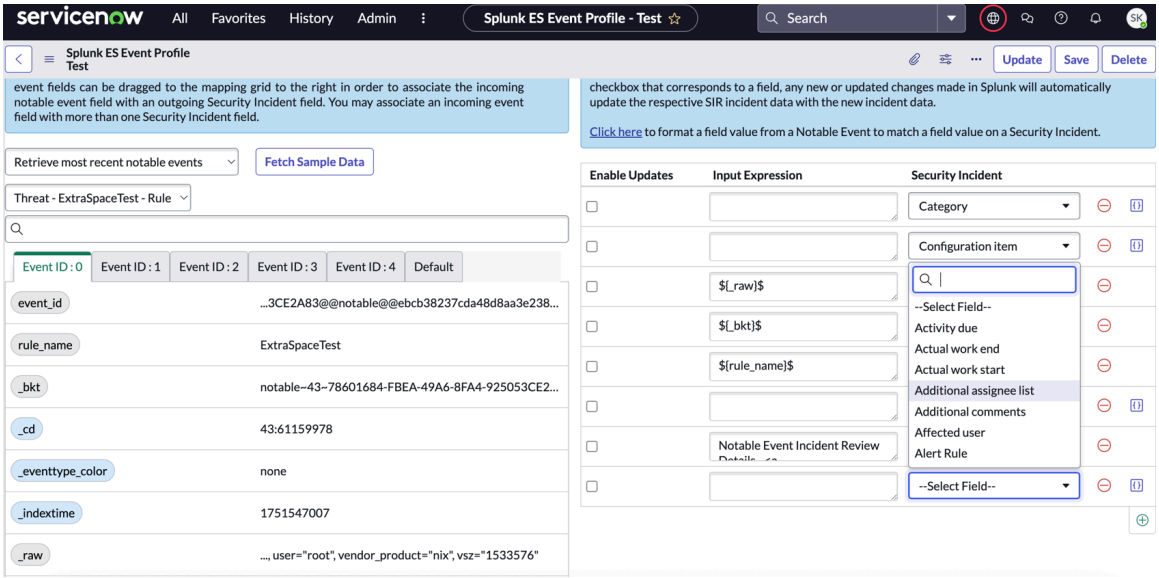
5. To add fields to the default fields displayed on the security incident on the right side of the form, follow these steps.

   a. On the right of the form in the SIR Incident Field Mapping section, at the bottom of the grid, click the plus icon.
   A new field is displayed.

   b. In the Security Incident column, expand the list that is displayed, and select a field.

      In the expanded list for the new field, some fields are shaded. In the following figure, `rule_name` has a gray background, because it has been mapped in the security incident. Similar to the color-coding for the notable events fields on the left side of the form, this color-coding for the security incident fields on the right helps you track the already mapped SIR incident fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



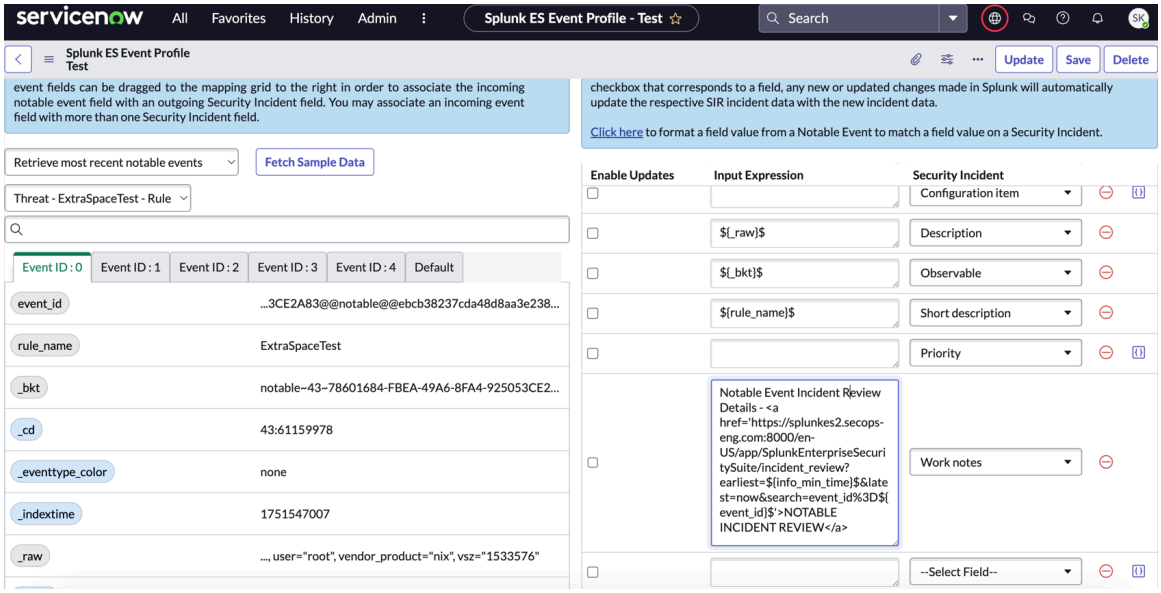
Note: So that multiple observables can be displayed on the same security incident, the Observable field can be mapped multiple times with different values. Similarly, the Configuration Item and Work notes fields support multiple values. If you try to map two values to a field that cannot support multiple values, when you preview the incident, an error message is displayed that there is no value for the field. Similarly, if a field on a security incident has a list from which you can choose multiple options, and you try to map an option to that field that is not displayed on the list, the field is not populated on the security incident.

c. Alternatively, type a value in the Search field for the new row.

d. From the left side of the form, left-click to select the **Event ID** that you want in the Input Expression field.

6. Continue mapping by adding or removing field values to the mapping.
The following figure is an example of an edited mapping. In the bottom field on the right, the Work notes field is added, and it has more than one value. Note that for long text string field, you can expand the mapping field to see the full string and re-size as needed by pulling the lower right corner of the field as indicated in screen shot below with the added Work notes field:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Warning: Please note that in the **SIR Incident Field Mapping** section, the URL and port number mentioned in the **Input Expression** field is just an example and not the URL or port number provided out-of-the-box.

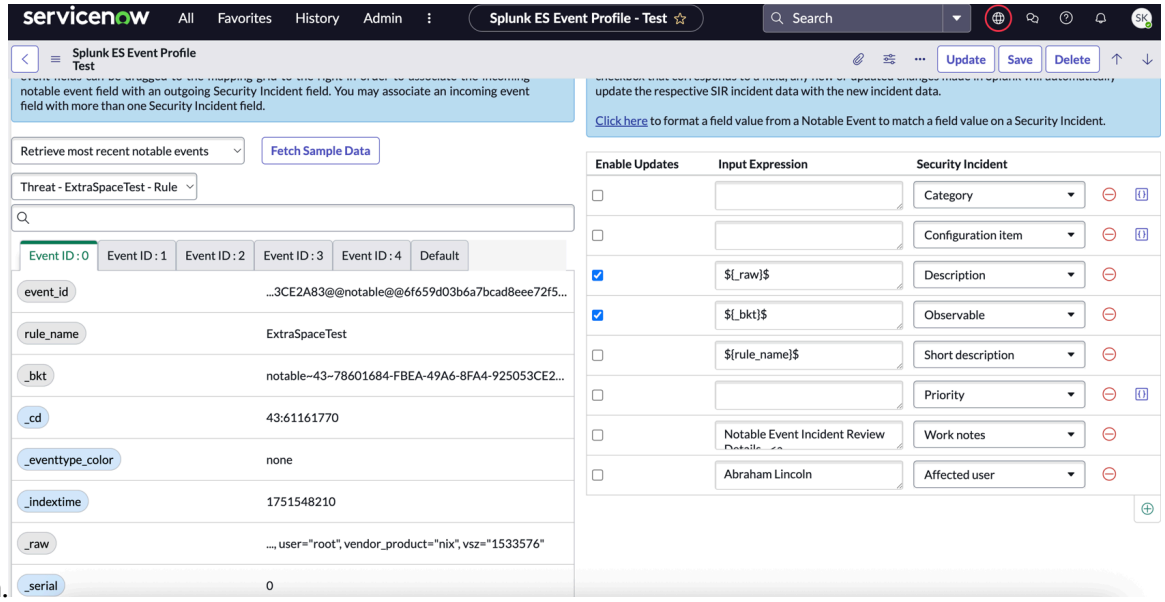
In the preview, these values are displayed in the Work notes on the security incident. Because the value is for a field that you added to the mapping section, and there are multiple values mapped to the Work notes field, the values are displayed as entered. In this example, the spaces and punctuation marks that you entered in the field are displayed on the Related Items section as a work note on the preview of the security incident.

The following image is an example of how the values in the preceding image are displayed on the security incident.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. To receive updates for the mapped fields in SIR, select the **Enable Updates** check box against the Input Expression.



8. **Optional:** After you have completed the preceding field-mapping steps, you can use the same field values in the Incident Generation Conditions builder to define additional criteria that an incoming notable event must satisfy to create a SIR security incident.
To set incident generation conditions, follow these steps.

   a. Scroll to the Incident Generation Conditions section on the form and select the **Filter based on conditions** check box to enable the option.

      (Optional) The Filter conditions builder is displayed. Use these filters to create security incidents that match the specific conditions described by the fields.

      The options in the lists for the first field in the Filter conditions builder match the fields that are displayed on the Notable Event Sample Ingestion section for the events you ingested. These fields are dynamic and change depending on the Splunk notable events that you ingest, or the event that you select for the manually forwarded notable event samples. Criteria that you enter are case-sensitive, and they must match exactly the values of the Splunk Enterprise Security notable event. If you are not sure about the values to enter in the filter fields, you may prefer to return to your Splunk Enterprise Security console and review your notable events for the keywords.



   b. Using the lists and fields of the conditions builder, set filters for the first row.

   c. To add more conditions, to the right of the fields, click **AND** or **OR**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched.

d. Optional: In the second row, set a second filter condition.

(Optional) The following image is an example with two conditions that must be matched before security incidents are created.



(Optional) You have set the incident generation conditions so that security incidents are created only when both of the filtering conditions that you entered are matched.

This type of incident generation condition filtering helps you narrow down the security events, and limit the number of unnecessary security incidents that you create without modifying the underlying correlation search or filters in Splunk. If additional filtering criteria are set, only notable events that match all criteria are mapped to incidents.

Note: If any of the event field names have special characters such as quotes (“), hyphens (‘), underscores (-), at (@), or ampersands (&), these characters may must be replaced for mapping translation purposes and possibly create a duplicate event name. The mapping can be done appropriately but a numerical suffix is appended to differentiate fields with duplicate event names. For example, if the first event field is `alerts.alert` and the second event field is `alerts@alerts`, these fields cannot be uniquely identified as the remaining standard text characters are the same. In this case, a suffix is added to the second event field and the field is renamed to `alerts@alert(1)`.

(Optional) Event Aggregation Criteria to Handle Similar Notables and Prevent Duplicate Incidents

9. **Optional:** To avoid creating duplicate security incidents, define additional event aggregation criteria so that incoming notable events are aggregated to an open security incident. To set the criteria, follow these steps below.

a. Scroll to the Event Aggregation Criteria section on the form and select the **Aggregate Conditions** check box to enable this option.

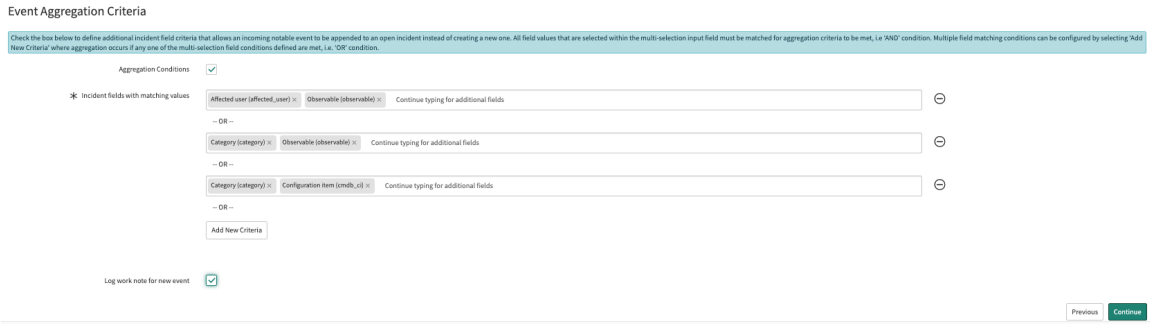
(Optional) The Incident fields with matching values are displayed. These field names are the fields on the security incident that include any custom fields that are configured on the SIR security incident.

b. From the multi-select input field, select the field values that you want to match on existing security incidents in your ServiceNow AI Platform.

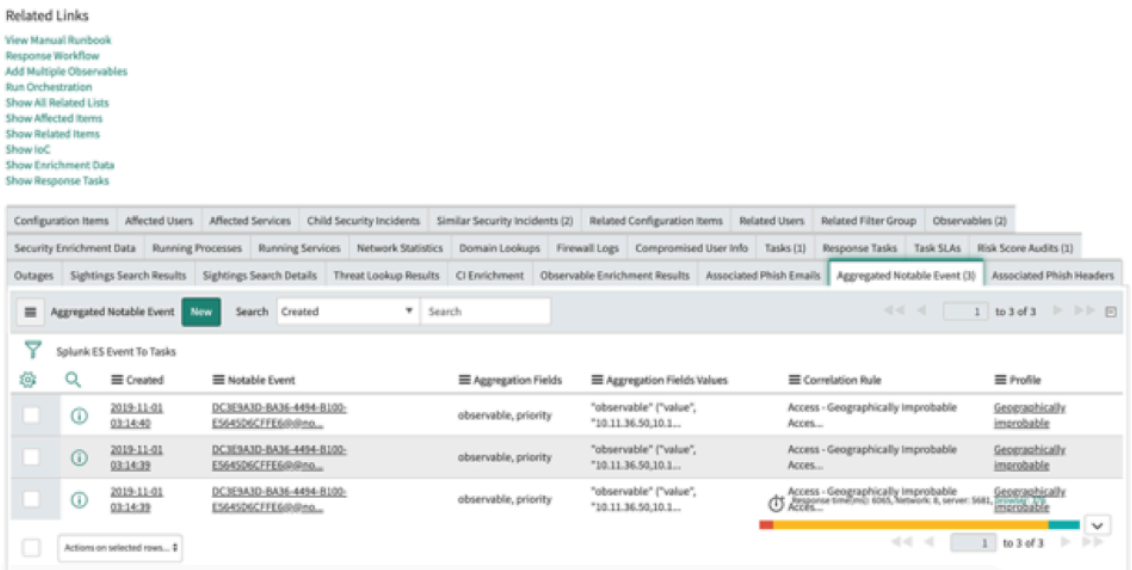
c. Use the **Add New Criteria** to select multiple field matching conditions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

All the field values that you select in the multi-selection input field are matched for aggregation criteria using the AND condition. Click **Add New Criteria** to select multiple field matching conditions where aggregation occurs if any one of the multi-selected field conditions that are defined are met using the OR condition.



If a new notable event matches all the values that are selected in the aggregation field conditions in the mapping step, the new notable event is automatically added to the most recently opened security incident with the same field values. As a user with the sn_si.analyst role working with security incidents, you can view all the added aggregate notable events on a related list on a security incident. All of the aggregated notable events on a security incident are displayed on the Splunk Event to Tasks related list. This list details associated timestamps and aggregated field values. This information helps you understand why these notable events are being aggregated to existing security incidents. If this tab is not displayed, scroll to the left side of the record under Related Links and click the **Show All Related Lists** link.



d. **Optional:** To log a work note for a new notable event that is recently added on the security incident, select the check box to enable this option.
The work note logs that a new notable has been added along with a link to the alert details and any other details that may have been added to the work note field in your mapping section.

You have successfully mapped values from a Splunk notable event to fields on a SIR security incident. Also, you have configured additional conditions to limit the creation of security incidents with incident generation filtering criteria. You also appended notable events to existing SIR security incidents when event field values match the configured aggregation criteria.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Choose one to continue with the profile configuration.

Option	Description
Continue	The Mapping form is displayed. **Preview** is selected on the progress bar. The next step is to preview the fields you mapped on a SIR security incident.
Update	Your data is saved and the Splunk Event Pro files list is displayed.
Previous	The Notable Event Selection form is dis played.
Delete	Delete this event profile and the Splunk Event Profiles list is displayed.

What to do next
The next step is to preview the values that you mapped on the security incident.

Preview the security incident for the Splunk Enterprise Security Event Ingestion integration

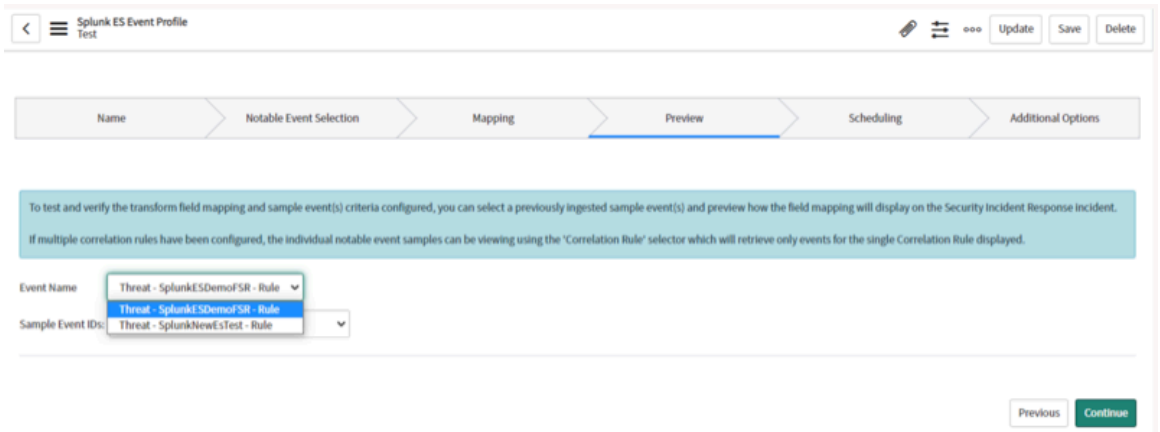
After you complete the mapping step, preview the values that you mapped in a ServiceNow AI Platform® Security Incident Response (SIR) security incident. This preview step permits you to verify that you have mapped all the notable fields that you want displayed on the security incident.

Before you begin
Role required: sn_si.admin

About this task
Preview a security incident and edit the mapping again as required to fix fields with errors or to populate any missing data. If the preview is not successfully completed, you cannot proceed to the scheduling step. Previews of SIR security incidents are not saved as actual incidents in the SIR product.

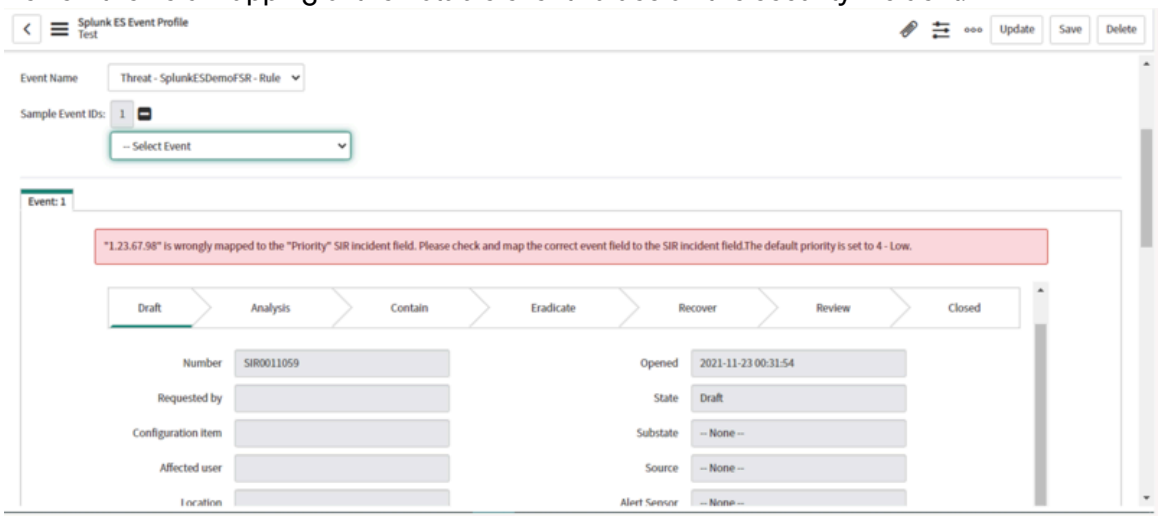
Procedure
1. If the security incident preview is not displayed, click **Preview** in the progress bar.
2. From the Event Name choice list, select an item if multiple Events were used.
3. Select event IDs from the Sample Notable Event IDs choice list.
4. From the Sample Notable Event IDs choice list, select an item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The security incident is displayed. Do not change any information in the fields. This view is a read-only view, and a record of this security incident is not saved.

5. Review the field mapping of the notable event values on the security incident.

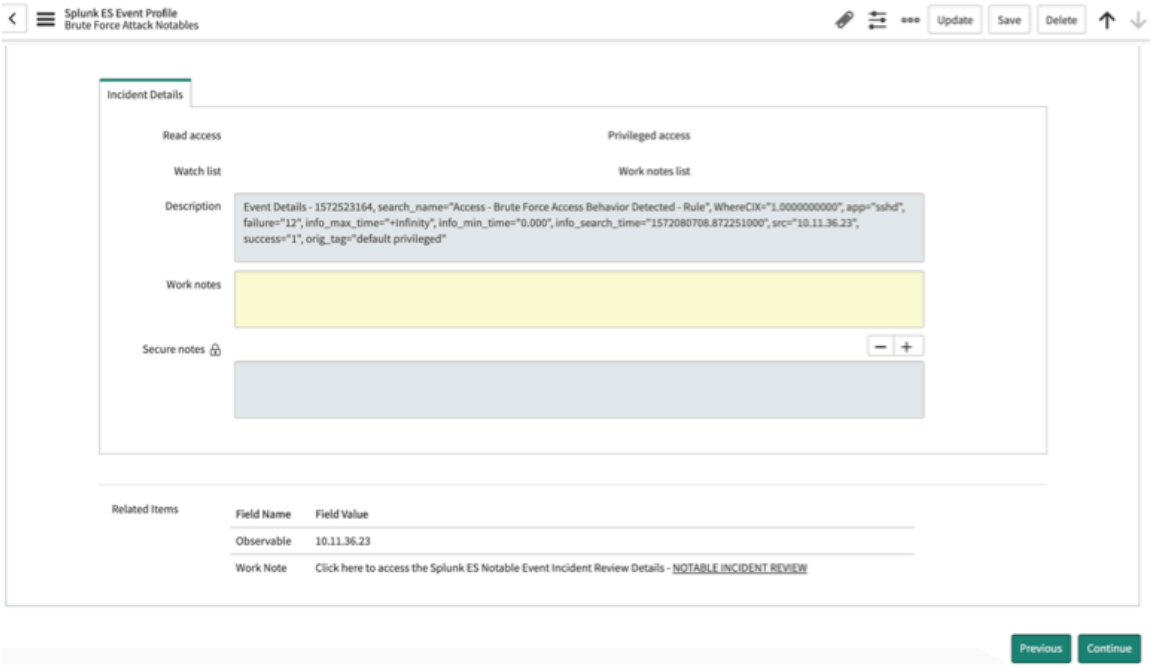


The preceding image is an example of a preview with a mapping error. In this example, a field value from the notable event does not have an acceptable value for the reference field on the SIR incident form. An error message is displayed that indicates an input value was not found for the `Configuration item` field in the ServiceNow® customer management database (CMDB). As a result, this mapped field value will not appear on the SIR security incident form without further modification.

6. To resolve this error, click **Mapping** in the progress bar.
7. Edit the mapping to fix incorrect values or populate any missing data.
8. Preview the mapping again and continue to fix any errors that are described in error messages.

   The following figure is an example of the Incident Details tab on the bottom half of a SIR security incident after all error messages are resolved. For this example, the Description and Work notes fields were mapped, and these fields are populated with the values from the value pairs pulled from the Splunk Enterprise Security notable event samples. The first Work notes field has no value. This field was left blank on the mapping grid during the mapping step. The additional Work Note fields that have values were added to the mapping section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. After you have fixed any errors and verified that the fields are the way you want them, choose one option to continue.

Option	Description
Continue	The Scheduling form is displayed for profiles with scheduled notable events. **Scheduling** is selected on the progress bar.
Finish	For profiles with configured for manual event forwarding, click **Finish**. There is no schedul ing step for profiles with event data that are exported on-demand directly from the Splunk Enterprise Security console.
Update	Your data is saved, and you are returned to the Splunk Event Profiles list.
Previous	The Mapping step on the progress bar is dis played.
Delete	Delete this event profile and the Splunk Event Profiles list is displayed.

What to do next

If no error messages are displayed, and you are satisfied with the field mapping on the security incident, the next step is to Schedule and retrieve alerts for the Splunk Enterprise Event Ingestion integration.

Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration

For automated notable event ingestion profiles, this step is required in the event profile configuration. During this step, you can verify the default settings for notable event retrieval or modify the scheduling as needed. This step also permits you to retrieve historical notable events using a date range.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.admin

About this task
For profiles for automated notable event ingestion, you choose whether you want to ingest any historical notable events during the Scheduling step. You also choose how often you will poll for future new notable events and updated notable events that match the alert profile configuration.

For automated notable event ingestion profiles, before the profile is activated, you verify and modify the scheduling and alert retrieval. This is a required step for all event profile configuration process for scheduled alert profiles.

You configure these polling intervals on a per-profile basis. The performance of the Splunk event ingestion integration may be impacted by the different polling intervals. When scheduling, you may prefer to balance reducing polling overhead on the Splunk Enterprise Security server against a desire to be notified as soon as possible when a notable event is created or updated. A five-minute default value is set for any profile, but you may prefer to modify this setting to as low as one minute if required.

Pulling new and updated notable events

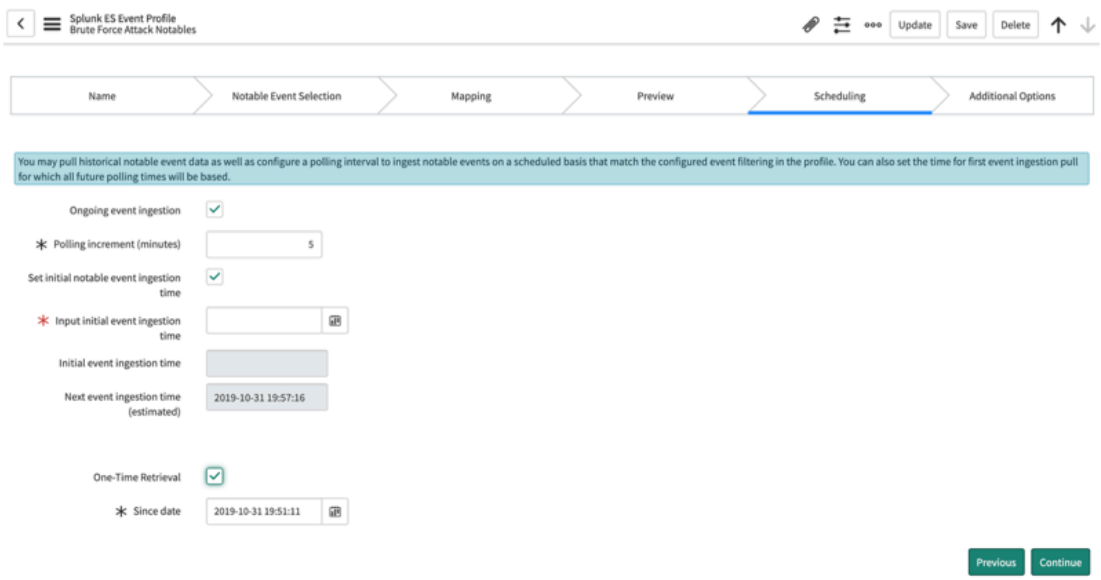
When the polling schedule is set, the scheduled job pulls both new and updated notable events that were pulled previously but did not meet the incident filtering criteria. This provides you with the flexibility to create incidents based on criteria that may not be present when a notable event is first created but becomes available after an update occurs, for example, during the investigation phase. Once an incident is created for a specific notable event, its subsequent updates are ignored since it is expected that the notable is now being treated as an active ServiceNow® security incident. However, all other notables that have been previously ingested but failed to meet the incident generation criteria, will continue to be pulled and checked against the incident generation criteria until they become part of an active incident.

Procedure
1. If the Scheduling page on the progress bar is not displayed, select **Scheduling**.
2. Choose one to schedule how and when notable events are pulled from the Splunk Enterprise Security console.

Option	Description
○ **On-going Event Ingestion field selected** ○ **One-Time Retrieval field cleared**	On-going Event Based on the default setting, the ServiceNow AI Platform instance pulls from the Splunk En terprise Security server for new and updated notable events every five minutes. Security incidents are created if notable events are found and incident generation filtering crite ria are matched. To balance ingestion polling overhead desire to get the most current data, five minutes is the default setting. However, this value can be modified to as low as one minute if needed.
○ **On-going Notable Event field cleared** ○ **One-Time Retrieval field selected**	One-Time Retrieval Use this configuration if you want a one-time pull to ingest historical notable events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	When this setting configured, a profile is used once to retrieve notable events from histori cal events that are based on a date range. To the right of the Since date field, click the cal endar icon. In the calendar that is displayed, select the date that you want to start pulling alerts. Starting with the Since date value, no table events are retrieved up through the cur rent date. Note that you can pull as far back as seven days from the current date. This functionality is not intended to retrieve signifi cant amounts of historical events from Splunk Enterprise Security for archival reasons but rather a minimal amount of in-flight events that are being actively worked at the time of profile activation. After the notable events are pulled, this set ting will not retrieve more notable events for this profile going forward from the current date. This setting populates the security inci dent with all the notable events that are found for the range you enter.



As an example for scheduling an initial notable event ingestion time, if you have a daily Splunk security check that runs once a day at 4 AM local time, you can set up the corresponding notable event profile in your ServiceNow AI Platform instance to run at 4:05 AM local time to capture the security failure event right away and create a security incident. Enter `04 05 00` in the Initial event ingestion field. In the Increment (Minutes) field, enter `1440` (24 hours) to schedule the next event ingestion for 24 hours from the initial event ingestion. Both the initial event ingestion time and next event ingestion time are displayed in the fields.

3. To configure the settings for this example, follow these steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. With the Scheduling page displayed, select the **Ongoing event ingestion** check box to enable this option.

b. In the Increment (minutes) field, enter `1440` (24 hours).

c. Click the **Select Initial event ingestion** check box to enable editing for the Initial event ingestion and Next event ingestion fields.

d. In the Initial event ingestion field, enter `04 05 00`.
In the The Next event ingestion (estimated) field, the time of the next event ingestion is displayed.

4. Click one of the following to continue with the profile configuration.

Option	Description
Continue	The Additional Options form is displayed. **Additional Options** is selected on the progress bar. The next step is to update the notable events when the SIR incident is created and/or closed.
Update	Your data is saved and the Splunk Event Security Profiles list is displayed.
Previous	The Scheduling form is displayed.
Delete	Delete this event profile and the Splunk Enterprise Security Event Profiles list is displayed.

Automate notable event updates and closure based on SIR incident status

Security incidents can be created and updated after they are created with a bi-directional interface with the Splunk Enterprise Security integration.

Before you begin

The Splunk Enterprise Security integration has a bi-directional interface that allows notable events to create security incidents as well as update the notable events after the security incident is created and/or closed.

Relevant incident details include SIR incident number, assignment group, SIR incident URL. This section is the final portion of the profile configuration set-up that provides optional capabilities to update the Splunk Enterprise Security notable events.

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

Procedure

1. If the Additional Options page on the progress bar is not displayed, select **Additional Options**.
2. Follow the instructions below to complete the configuration for updating notable events based on security incident updates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

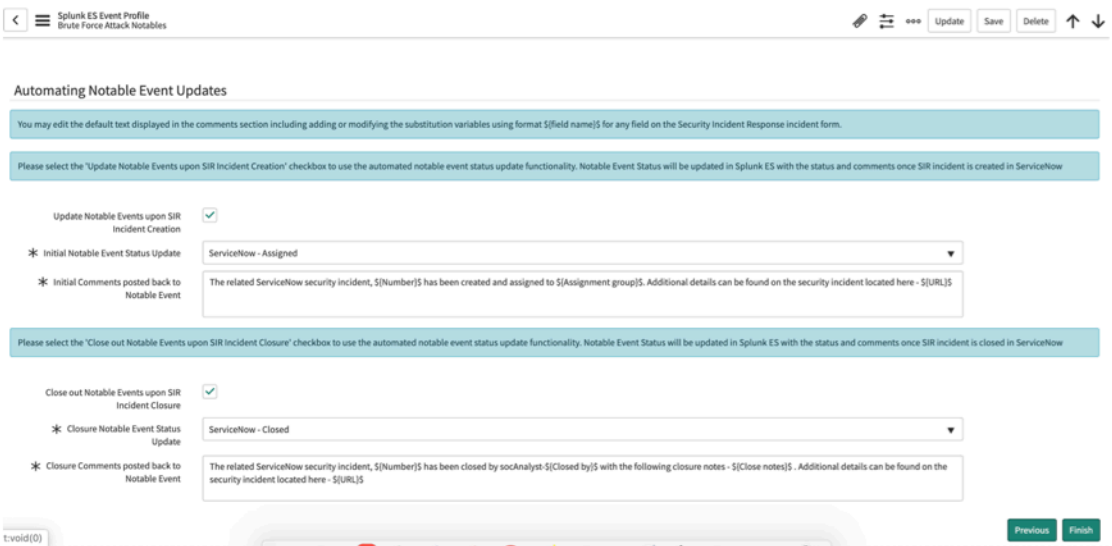
Option or Field	Description
Update Notable Events upon SIR Incident Creation	Select this option if you want to update the notable event status and add additional com ments when a security incident is created from the notable event. This can occur for both the initial triggering notable events that create the security incident, as well as aggre gated events.
Initial Notable Event Status Update	You must select a status option from the menu that displays all available status values retrieved from the Splunk Enterprise Security server. This may include a custom created sta tus, such as ServiceNow - Assigned as shown in the screen shot below. Select the status val ue to be set for all notable events when a se curity incident is created for an ingested no table event. This includes notables that cre ate new incidents and notables that are in gested and aggregated to an existing open in cident.
Initial Comments posted back to Notable Event	In addition to updating the notable status val ue, you can also post comments to the no table event incident review history. As indi cated in the instructions, you may edit the de fault text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response inci dent form.
Close out Notable Events upon SIR Incident Closure	Select this option if you want to update the notable event status and add additional com ments when a security incident is closed from the notable event. This will occur for both the initial triggering notable events that create the security incident, as well as aggregated events.
Closure Notable Event Status Update	You must select a status option from the list menu that displays all available status val ues that are retrieved from the Splunk Enter prise Security server. This may include a cus tom created status, such as ServiceNow - As signed as shown in the screen shot below. Select the status value to be set for all no table events when a security incident is cre ated for an ingested notable event. This in cludes notables that create new incidents as well as notables that are ingested and aggre gated to an existing open incident.
Closure Comments Posted back to Notable Event	In addition to updating the notable status val ue, you can also post closure comments to the notable event incident review history. As indicated in the instructions, you may edit

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or Field	Description
	the default text displayed in the comments section including adding or modifying the substitution variables using format ${field name}$ for any field on the Security Incident Response incident form.
Update SIR Automation Activity with Splunk Event comments	Option to update your Splunk Event com ments in the SIR Automation Activity. The comment in the SIR Automation Activity appears with the prefix *`Comment from Splunk`*. **Note:** Starting from Splunk Enterprise Secu rity version 8.0.x, the comments field has been deprecated, and therefore our application can no longer retrieve com ments from Splunk Enterprise Security.
Update Splunk comments with SIR work notes	Option to update your SIR work notes in the Splunk Event comments. The comment in Splunk Event appears with the prefix *`Comment from ServiceNow`*.

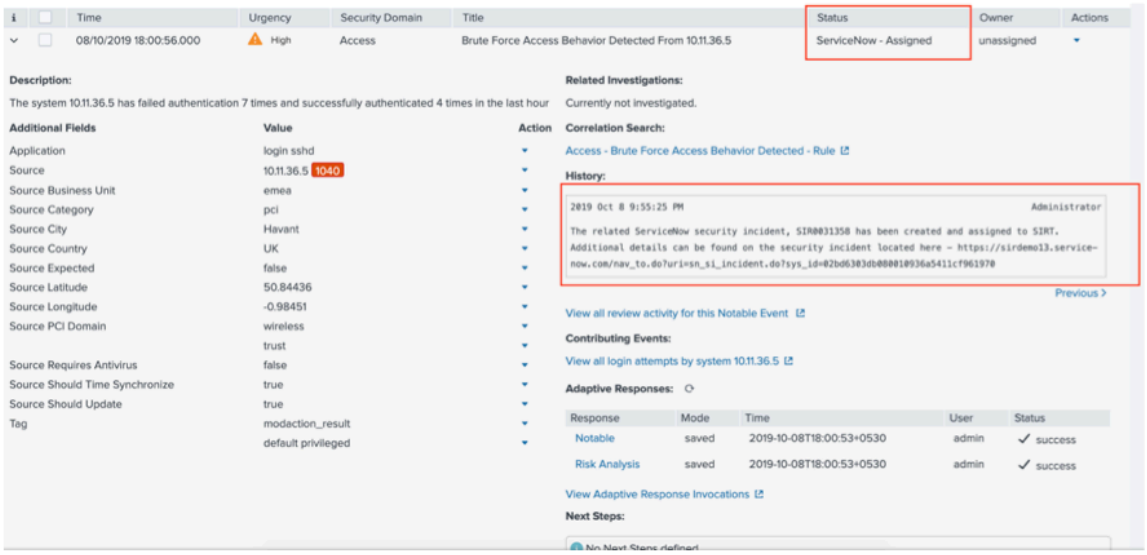
3. Click **Finish** to complete the configuration.
   A confirmation dialog is displayed. You have successfully completed the setup and configuration for the integration. Activate this profile to pull notable events from the Splunk Enterprise Security console based on your scheduling. There is a limit of 1,000 security incidents that can be created in a 24-hour period. Up to 100 notable events are per fired alert. Subsequent notable events will be ignored after the limits are reached.

   The following image shows the Additional Options tab with default values populated:



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With the Additional Options configuration enabled, the notable event incident review shows the status change and an update to the history comments:



Set up a profile for manual event forwarding

Depending on the profile defined, Splunk ES notable events are forwarded manually as discrete notable events into the Security Operations environment of your ServiceNow AI Platform instance.

To set up a profile for manual forwarding of notable events:

Task	Section
Create an event profile	See Create profiles for manually forwarded events
Map notable event fields	See Mapping notable event fields for the Splunk Enterprise Security integration
Create custom mappings	See Create mappings for Splunk ES notable event incident review and contributing event details (manual forwarding)
Preview the security incident	See Preview the security incident for the Splunk Enterprise Security Event Ingestion integration
Set up your Splunk environment for manual ingestion	See Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration
Automate notable event updates and closure based on SIR incident status	See Automate notable event updates and closure based on SIR incident status

Create profiles for manually forwarded events

You can set up a profile for manual forwarded events.

Before you begin

Role required: sn_si.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

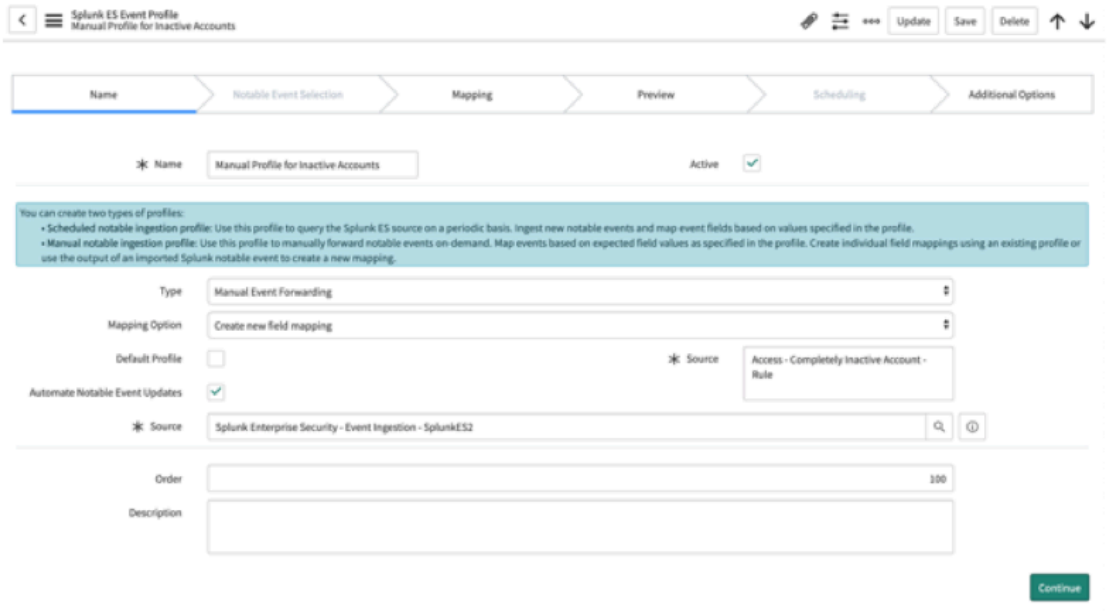
To create a profile that supports manual event forwarding, follow these steps.

For events that you forward on-demand from your Splunk Enterprise Security console, you can base the individual field mapping on any existing profile. Alternatively, you can create a new mapping grid for exported attachment data. Events that you forward manually are not scheduled in the event profile.

a. If not already selected, in the choice list for the Type field, select **Manual Event Forwarding**.

b. In the Mapping Option field that is displayed, from the choice list, choose one mapping option to continue.

Refer to the following figures and tables for more information about the available mapping options in the Mapping Options choice list.



Create New field mapping option

Option or field	Description
Create new field mapping option	New field mapping for your event. If you do not have an existing field mapping that is similar to the profile that you are creating, select this option to create a new map.
Default profile	Default event forwarding profile for all Splunk events. Default is cleared (deactivated). When this option is enabled, this profile becomes the default profile for manual event forwarding. This profile is used when there is no match on source from the manually forwarded event. It becomes the default profile for all events with unknown sources.

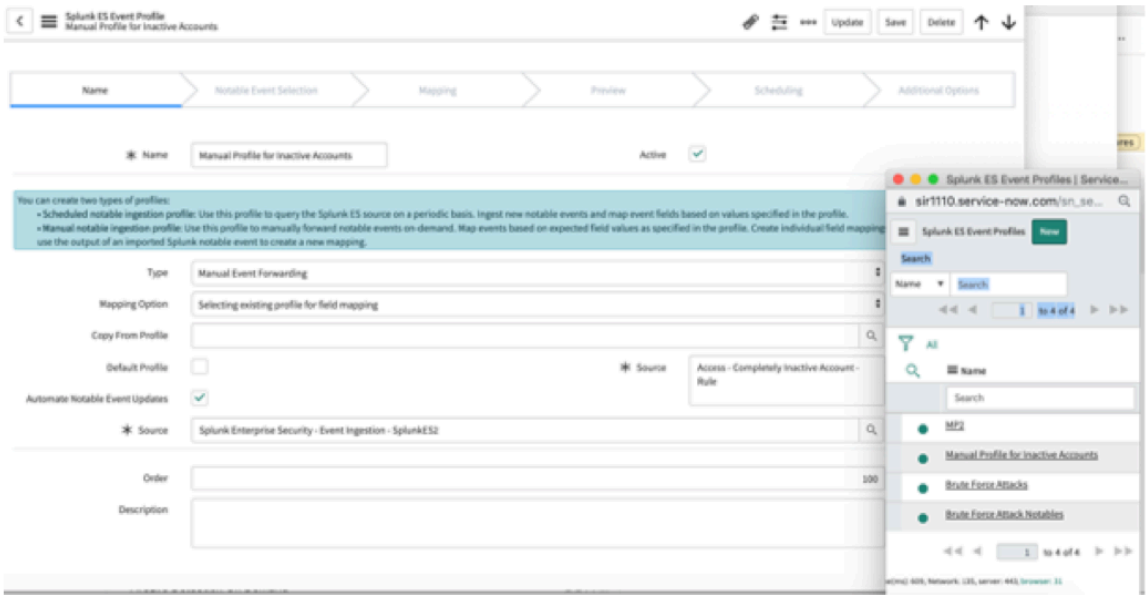
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or field	Description
	The Source field is unavailable if the default profile option is enabled.
Source (Notable Event field)	This is a field that typically defines the correlation rule that triggered the notable, for example, Brute Force Attacks. This field is unavailable if the default profile option is enabled. If available, this field permits unique event field mapping to security incident fields based on the splunk correlation rule that is typically different for different event types. If you want to manage different correlation rules separately, you can create different profile event profiles based on correlation rule to accomplish this requirement.
Automate Notable Event Updates	Select this check box if you want to update the notable event status and add additional comments when a SIR incident is created from the notable event and / or when the SIR incident is closed. This will occur for both the initial triggering notable events that creates the SIR incident, as well as aggregated events.
Source (Splunk Server)	The Splunk server that you configured as the source for notable events. If you have multiple Splunk servers configured, select the appropriate server for the notable event types that will be updated for the profile. You are required to enter a value.
Order	Default is 100. Leave this setting at the default. If you have created a large number of profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Text to help you distinguish this profile from other profiles.

For a profile with a new field mapping, verify that you have entered a value in the Source type field and click **Continue** to proceed to the mapping step of the configuration.

For a profile with an existing field mapping, refer to the following figure and table for more information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Select existing profile for field mapping option

Option or field	Description
Select existing profile for field mapping	Reuse an existing field mapping for your new notable event profile. The Copy from profile field is displayed. Follow these steps to copy an existing field mapping for this profile. i. To the left of the Copy from profile field that is displayed, click the search icon. ii. In the Splunk ES Event Profiles list that is displayed, click the profile name that has the map that you want to copy. The profile name is displayed in the Copy from profile field.
Default profile	Default event forwarding profile for all Splunk notable events with unmatched source. Default is cleared (disabled). When this option is enabled, this profile becomes the default profile for manual event forwarding. The Source field is unavailable if the default profile option is enabled.
Source (Notable Event field)	This is a field that typically defines the correlation rule that triggered the notable, for example, Brute Force Attacks. This field is unavailable if the default profile option is enabled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option or field	Description
	If available, this field permits unique event field mapping to security incident fields based on the splunk correlation rule that is typically different for different event types. If you want to manage different correlation rules separately, you can create different profile event profiles based on correlation rule to accomplish this requirement.
Automate Notable Events	Select this check box if you want to update the notable event status and add additional comments when a security incident is created from the notable event or when the security incident is closed. This occurs for both the initial triggering notable events that creates the security incident, as well as aggregated events.
Source (Splunk Server)	Splunk server or search end that you configured as the source for notable events. If you have multiple Splunk servers configured, select the appropriate server for the notable event types that will be updated for the profile. You are required to enter a value.
Order	Default is 100. Leave this setting at the default. If you have created multiple profiles, this value provides a run time execution priority when two or more profiles share triggering conditions. The workflow in the profile with the lowest number has the highest priority.
(Optional) Description	Text to help you distinguish this profile from other profiles.

At the bottom of the form for selecting an existing mapping for your profile, click **Finish** to complete the profile configuration.

Create mappings for Splunk ES notable event incident review and contributing event details (manual forwarding)

During the notable event field mapping step, you map individual event fields from notable events to fields on a ServiceNow AI Platform Security Incident Response (SIR) security incident.

Before you begin

Role required: sn_si.admin

About this task

Map up to five notable events from the Notable Event Sample Ingestion column on the left of the form to the security incident fields in the SIR Incident Field Mapping column on the right.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create custom mappings by adding or removing the fields on the mapping grid on the right side of the form. Default fields that are typically important field to populate on the SIR incident form are displayed. However, these fields can be removed and any additional fields can be displayed using the + and - buttons. Create custom maps by adding or removing the fields on the mapping grid on the right side of the form. Customizing the fields permits you to map Splunk fields that are not displayed on the default mapping grid on the SIR security incident.

Procedure

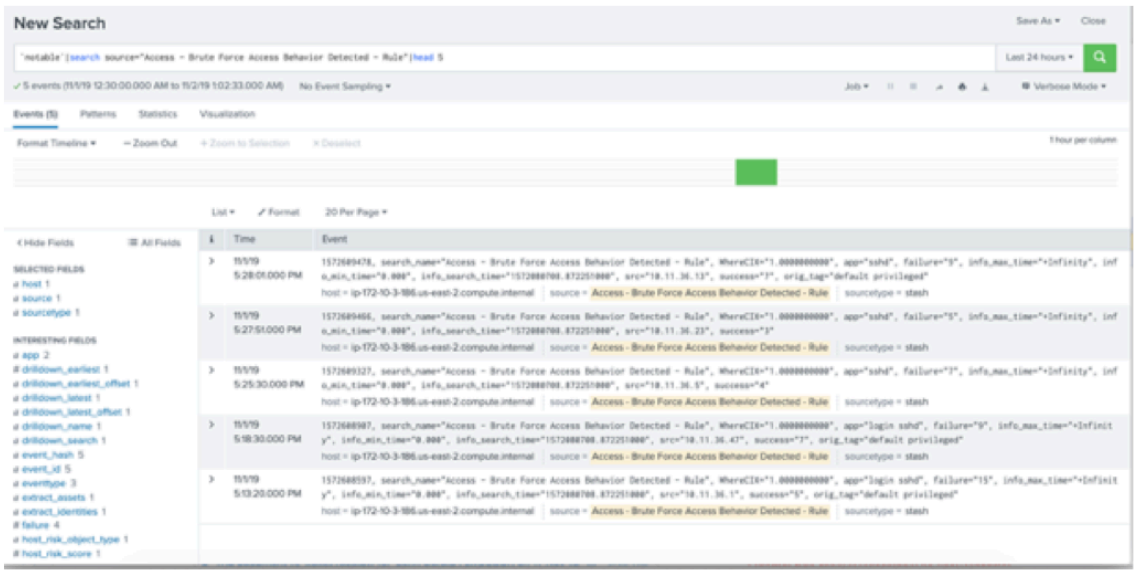
1. If the mapping form is not displayed, click **Mapping** on the progress bar.
2. Follow these steps to upload attachment data in your ServiceNow AI Platform® instance.

   a. If not already logged in, log in to your Splunk Enterprise console.

   b. Navigate to the Search tab and enter a name for a search that has the notable event data that you want to export.
   An example search format to retrieve notable events for the Brute Force Access Behavior correlation rule would be the following: `notable`|search source="Access - Brute Force Access Behavior Detected - Rule".

   c. Expand the notable event, and in the Field column, select the fields that you want to import.

   These fields are the field-value pairs that are exported and displayed on the Mapping page in your ServiceNow AI Platform® instance.



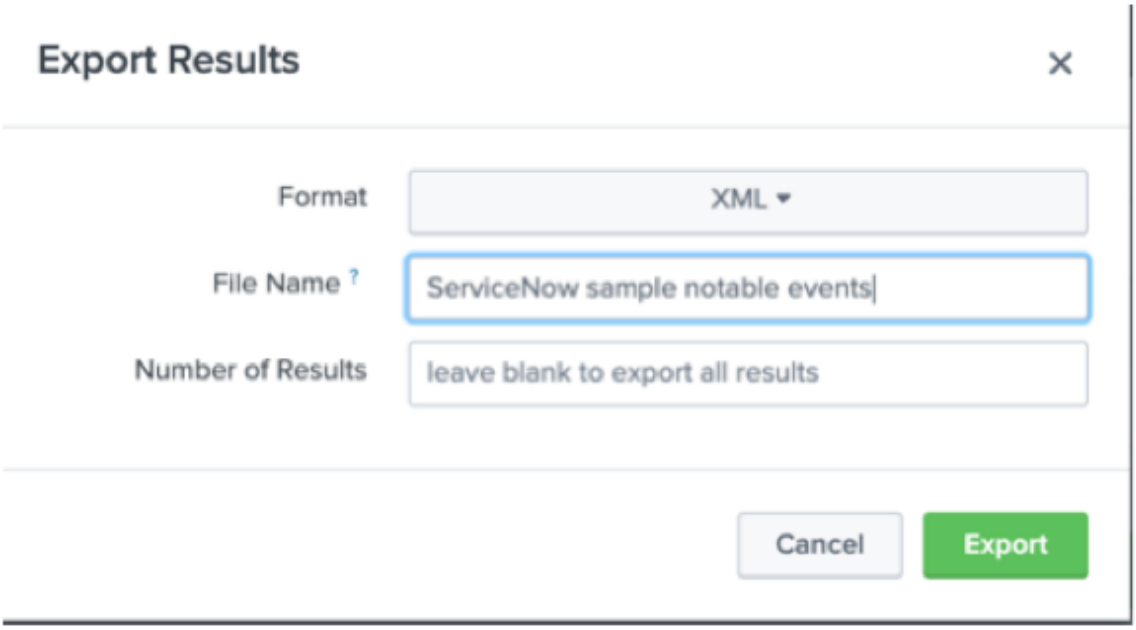
   d. In your Splunk Enterprise console, in the upper right of the Search page, click the **Export** icon.

   e. In the choice list for the Format field in the dialog that is displayed, click **XML Format**.

   f. **Optional:** Enter a new filename.

   g. Click **Export**.

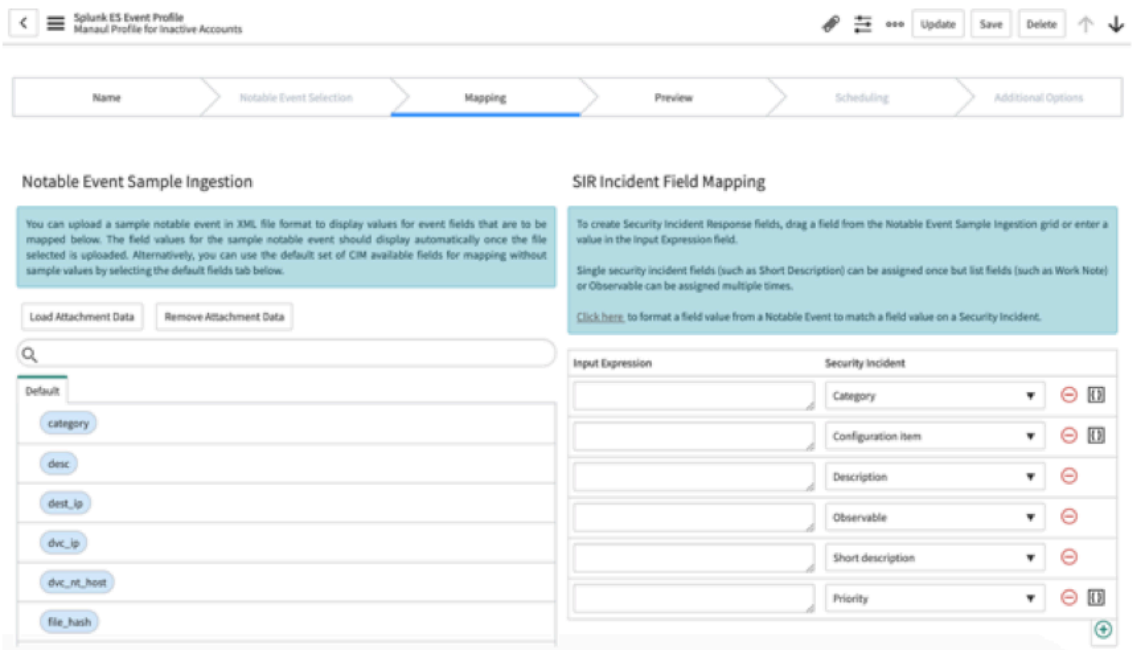
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The exported Splunk notable event XML file must now be uploaded to your ServiceNow AI Platform® instance.

h. If the Mapping page is not already displayed in your ServiceNow AI Platform® instance, click **Mapping** in the progress bar.

i. In the Notable Event Sample Ingestion column, click **Load Attachment Data**.



j. In the dialog that is displayed, click **Choose files** and navigate to the `.xml` file that you exported and click **Open**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you click to load attachment data for manually forwarded events, the Splunk ES notable event fields are populated on the left side of the form. These values are the field values that you map to the security incident fields on the Sir Incident Field Mapping side of the form. The value pairs for the fields that you exported for the event are displayed on the left side of the mapping form.

3. Follow steps 5 to 10 in the Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion) section.

Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration

Install and set up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security application in your Splunk enterprise console or Splunk Cloud instance if you want to export events manually and on-demand from your Splunk Enterprise Security console for this integration.

Before you begin

Installing and setting up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security application in your Splunk enterprise console or Splunk Cloud instance is optional.

Verify that you have installed the application for this integration from the ServiceNow Store prior to installing the addon plugin from splunkbase that is required for manual event ingestion. If you have not installed the application for the integration from the ServiceNow Store, see Install and configure Splunk Enterprise Security Notable Event Ingestion integration and follow the instructions to install it.

Role required: Splunk Enterprise Security administrator

About this task

If you want to export events manually and on-demand from your Splunk Enterprise console for the integration, download, install, and set up the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security from splunkbase in your Splunk Enterprise Security console. This ServiceNow extension addon is required so that security incidents can be created from manually exported events in your ServiceNow AI Platform instance. This ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security application is available on splunkbase.

For manual event forwarding, you can identify up to two different ServiceNow AI Platform endpoints (instances) in your Splunk Enterprise Security console. You forward the events to the endpoint or endpoints manually to create security incidents. For example, you can specify both a staging (development) instance and a production instance. By specifying separate instances and naming primary and secondary workflows for each instance, you can choose where you want to forward different events.

Procedure

1. If you have not already installed the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security, follow these steps to install and configure it.

   a. Navigate to splunkbase.

   b. Search for the ServiceNow Security Operations Security Operations Event Ingestion Addon for Splunk Enterprise Security.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

> **Note:** Verify that you have selected ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security. There are additional ServiceNow addons that are displayed in this list. These addons are for different ServiceNow Splunk integrations, and they are not required for this integration.

c. Download the application.

d. Open your Splunk Enterprise Security account.

e. On the Apps page, click the gear icon or the **Manage Apps** shortcut on the menu drop-down list.

f. On the upper left of the Apps page that is displayed, click **Install app from file**.

g. Click **Choose File**, select ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security, and click **Upload**.

h. If prompted, restart Splunk Enterprise.
The ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security is installed in your Splunk Enterprise Security console. The next step to set up the Addon.

2. To set up the Addon, follow these steps.

a. In Splunk Enterprise Security, click the **Apps** gear icon or **Manage Apps** on the menu drop-down list.

b. On the list of applications that is displayed, in the **Actions** column, click **Set up** for ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security.

c. Fill out the form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure is an example of a completed form in your Splunk Enterprise Security console.



Field on Specify ServiceNow Primary Instance section	Description
Workflow action label	Name of the ServiceNow AI Platform workflow for your production (primary) instance. This name is the name of a ServiceNow AI Plat form instance that your users who are moni toring Splunk events identify as a primary in stance, for example, Servicenow Event Inges tion (Production). Default for this field is Servicenow Event Ingestion (Production). In your Splunk Enterprise Security console, this workflow name is displayed for the pro duction (Primary) instance in the expand ed `Event Actions` drop-down list of a search. This name is the name of your produc tion instance. You can edit the name.
URL	The URL for the ServiceNow AI Platform in stance you entered in the preceding Work flow action label field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

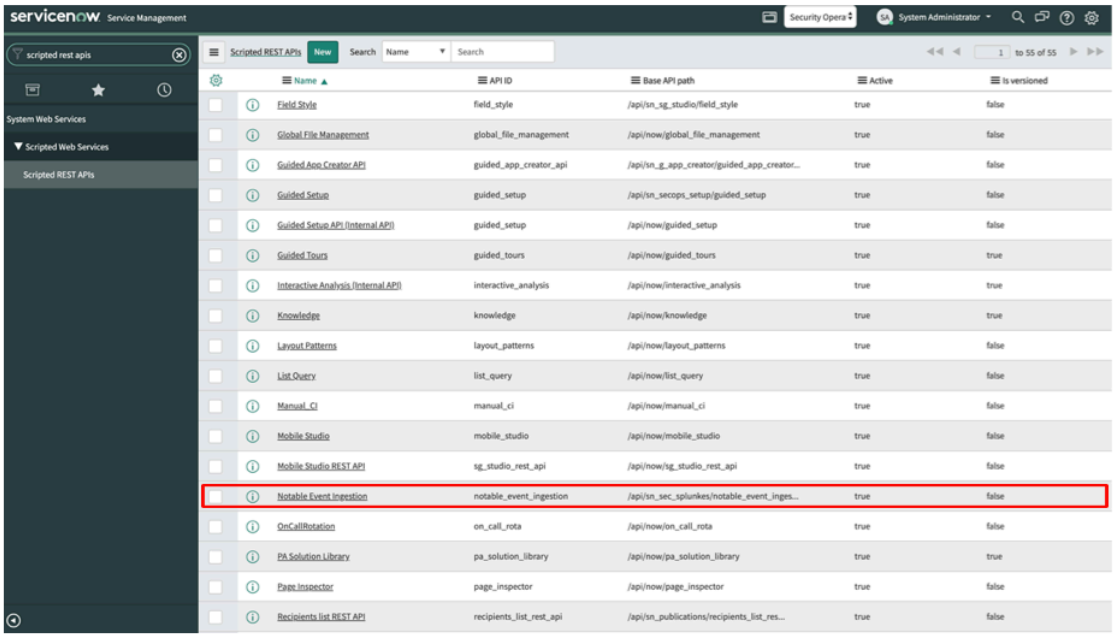
Field on Specify ServiceNow Primary Instance section	Description
	Copy the URL in your browser and paste it in this field in the form.
Endpoint	Base API path. For more information, refer to the figure that follows the table. If you do not have a value for the endpoint of your ServiceNow AI Platform production in stance, follow these steps. **a.** Log in to your ServiceNow AI Platform pro duction instance as a user with the system administrator (admin) role. **b.** Enter `Scripted REST APIs` in the navi gation panel. **c.** After the navigation panel is refreshed, se lect the **Scripted REST APIs** module that is displayed. **d.** If Event Ingestion is not listed in the Name column of the `Scripted REST APIs` list that is displayed, in the search field at the top, enter `Event Ingestion`. **e.** In the Base API path column on the re freshed page, copy this value and paste it in the Endpoint field on the form. An ex ample base api path is, `/api/sn_sec_s plunk_v2/event_ingestion`.
Username	User name for your ServiceNow AI Platform instance. This name is the user name for the ServiceNow AI Platform instance in which you assigned a user with the (sn_sec_splunk_ v2.api_account_access) role for manual event forwarding. For more information about assigning this role, see Set up your ServiceNow AI Platform instance for the Splunk Enterprise Event Ingestion integration.
Password	Password for your ServiceNow AI Platform in stance. This password is the password for the Ser viceNow AI Platform instance in which you assigned a user with the (sn_sec_splunk_ v2.api_account_access) role for manual event forwarding.
(Optional) Fields on Specify ServiceNow Se condary Instance section	Description

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field on Specify ServiceNow Primary Instance section	Description
	These fields are optional. You are not re quired to specify a secondary instance.
Workflow action label	Name of the ServiceNow AI Platform workflow for your secondary (staging) instance. This name is the name of a ServiceNow AI Plat form instance that your users who are monitor ing Splunk events identify as a secondary in stance, for example, ServiceNow Event Inges tion (Staging). In your Splunk Enterprise Security console, this workflow name is displayed for the stag ing (Secondary) instance in the expanded Event Actions drop-down list of a search. This ServiceNow AI Platform instance is your stag ing instance. You can edit the name.
URL	The URL for the ServiceNow AI Platform in stance you entered in the preceding Work flow action label field for the secondary Servi ceNow AI Platform instance. Copy the URL in your browser and paste it in this field in the form.
Endpoint	Base API path. This value for the Base API path for your secondary instance is the same value as the Base API path for your primary in stance. See the preceding figure of the form for more information.
Username	Username for your ServiceNow AI Platform staging instance. The user must have the (sn_ sec_splunk_v2.api_account_access) role.
Password	Password for your ServiceNow AI Platform staging instance. The user must have the (sn_ sec_splunkes.api_account_access) role.

The following figure is an example of the Scripted REST APIs list in your ServiceNow AI Platform. The list displays the location of the endpoint value of a ServiceNow AI Platform instance that you enter in the form as part of the set up for the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security extension in your Splunk Enterprise Security console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. In the setup form in your Splunk Enterprise Security console, click **Save** to save your edits.

   After a few moments, at the top left of the form in your Splunk Enterprise Security console, a message is displayed that the record is successfully updated.

   After you save the form, the names (Workflow action labels) for your ServiceNow AI Platform instance(s) that you created in the form are available from the Event Actions choice list on a selected event of a search in your Splunk Enterprise Security console.

What to do next

If you have not already save searches in your Splunk Enterprise Security console, the next step is to save searches as alerts in your Splunk Enterprise Security console.

Setup ServiceNow Security Operations Event Ingestion Addon for Splunk ES

The ServiceNow Security Operations Event Ingestion Add-on for Splunk ES enables seamless integration between Splunk and ServiceNow Security Operations, allowing you to send security-related events from Splunk to ServiceNow security incident. For detailed instructions on downloading and installing the Addon, follow the steps outlined in this guide.

Before you begin

Verify that you have installed the application for this integration from the ServiceNow Store prior to installing the addon plugin from splunkbase that is required for manual event ingestion. If you have not installed the application for the integration from the ServiceNow Store, see Install and configure the ServiceNow application for the Splunk Enterprise Event Ingestion integration and follow the instructions to install it.

Role required: ServiceNow AI Platform administrator (admin)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Important:

Create a **Manual event forwarding** profile to forward events on-demand from your Splunk Enterprise Security console to create a Security Incident Response (SIR) on the ServiceNow instance. For more information, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration.

This add-on setup is necessary to enable manual event forwarding for the Splunk profile. Up to two configurations can be created for a particular add-on. (**Splunk Primary** and **Splunk Secondary**)

For manual event forwarding, you can identify up to two different ServiceNow AI Platform endpoints (instances) in your Splunk Enterprise console. You forward the events to the endpoint or endpoints manually to create security incidents. For example, you can specify both a staging (development) instance and a production instance. By specifying separate instances and naming primary and secondary workflows for each instance, you can choose where you want to forward different events.

Procedure

1. If you have not already installed the **ServiceNow Security Operations Event Ingestion Add-on for Splunk ES**, follow these steps to install and configure it.

   a. Download the **ServiceNow Security Operations Event Ingestion Add-on for Splunk ES** from Splunkbase.

   b. If prompted, restart the Splunk Enterprise.
   The **ServiceNow Security Operations Event Ingestion Add-on for Splunk ES** is installed in your Splunk Enterprise enterprise console. The next step is to set up the Add-on.

2. To set up the Add-on, follow these steps.

   a. In the Splunk Enterprise, select **Manage Apps** gear icon on the menu drop-down list.

   b. In the list of applications, search for **ServiceNow** apps using the filter.

   c. Look for the **ServiceNow Security Operations Event Ingestion Add-on for Splunk ES**, and select the corresponding **Set up** action.

   The ServiceNow Security Operations Event Ingestion Add-on for Splunk ES is configured into three different tabs.

   - **Splunk Primary**: The default or primary Splunk configuration.
   - **Splunk Secondary**: (Optional) The backup or second Splunk configuration.
   - **Logging Level**: The level of reporting logs generated by the integration, meaning the name of the type of information.

   d. Select the **Splunk Primary** tab.

   e. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk Primary

Field	Description
Workflow action label	Name of the instance. This will be an action in the drop-down of the **Event Actions** in Enterprise Security.
URL	URL of the ServiceNow instance you entered in the preceding workflow action label field.
Endpoint	Base API path. Default for this field is: `/api/sn_sec_splunkes/notable_event_ingestion`.
Auth type	Authentication method to be used for API requests. The available options include: ▪ **Basic Authentication**: Uses username and password to authenticate requests. ▪ **OAuth 2.0 Authentication**: Uses access tokens to authenticate requests.
Basic Authentication	
Username	Username of the user. User with the (sn_sec_splunkes.api_account_access) role should be present in the instance specified in the preceding URL field for manual event forwarding. For more information about assigning this role, see Set up your ServiceNow AI Platform instance for the Splunk Enterprise Event Ingestion integration.
Password	Password of the user. User with the (sn_sec_splunkes.api_account_access) role should be present in the instance specified in the preceding URL field for manual event forwarding.
Confirm Password	Re enter the password to confirm it.
OAuth 2.0 Authentication	
Client Id	Client ID of the app created in the ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For information on how to get the Client ID, see Configure Application Registry on the ServiceNow instance.
Client Secret	Client Secret of the app created in the ServiceNow instance. For information on how to get the Client Secret, see Configure Application Registry on the ServiceNow instance.
Redirect URL	Copy and paste this URL in the redirect URL field of the Application Registries record.

f. Select **Save**.

g. Select the **Splunk Secondary** tab.

h. On the form, fill in the fields.
Fields are same as in the Splunk Primary tab.

i. Select **Save**.

Note: Up to two configurations can be created for a particular add-on.(**Basic Authentication** and another **OAuth 2.0 Authentication**)

j. Select the **Logging Level** tab.

k. On the form, fill in the fields.

Logging level

Field	Description
Log Level	The level of reporting logs generated by the integration, meaning the name of the type of information. You can also update the value to the following options: ▪ **info** ▪ **error** ▪ **warn** ▪ **debug** By default, the value is **info**.

l. Select **Save**.

What to do next

Using ServiceNow Security Operations Event Ingestion Add-on for Splunk ES

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using ServiceNow Security Operations Event Ingestion Add-on for Splunk ES

Forward events on-demand from your Splunk Enterprise Security console to create a Security Incident Response (SIR) on the ServiceNow instance.

Before you begin
Role required: sn_sec_splunkes.api_account_access

Procedure

1. Log in to Splunk Enterprise.
2. Navigate to **Apps** > **Enterprise Security**.
3. Select **Mission Control**.
   A list of notable events generated in the Splunk console on the basis of correlation rule configured previously show up.
4. Select any **Notable Event** from the list.
5. Select **Ellipsis icon** (⋮).
6. From the drop down, select the **Workflow action label** configured while setting up the add-on.
   For more information on Workflow action label, see Setup ServiceNow Security Operations Event Ingestion Addon for Splunk ES
   Events will go in **Splunk ES Event Import** table followed by **Splunk ES Event to Tasks** table.

Result
A Security Incident Response (SIR) record is created on the ServiceNow instance as per the mapping specified in the Manual event forwarding profile. For instructions on how to set up a Manual event forwarding profile, see Create and name an event profile for the Splunk Enterprise Event Ingestion integration

Copy an event profile for the Splunk Enterprise Security Event Ingestion integration

Copy an existing profile and its associated settings instead of creating new profiles. If you are creating multiple profiles, and you want to reuse the settings of an existing profile, you may prefer to copy alarm profiles to save time.

Before you begin
Role required: sn_si.ingestion_profile_admin

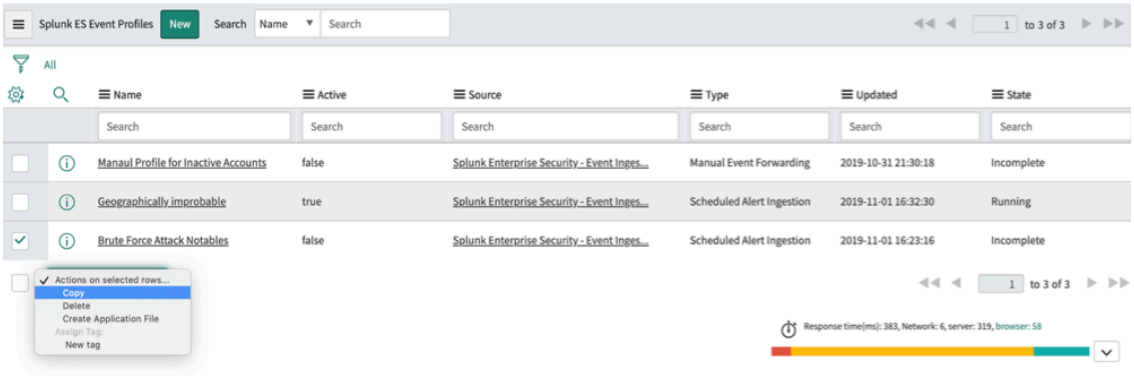
Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task
If you copy a profile, the profile name is initially modified to avoid duplicate profiles. In addition, the copied profile is deactivated (false) so it is not activated accidentally prior to completing the configuration. Copy profiles and use existing maps for security incidents that you have already previewed and verified.

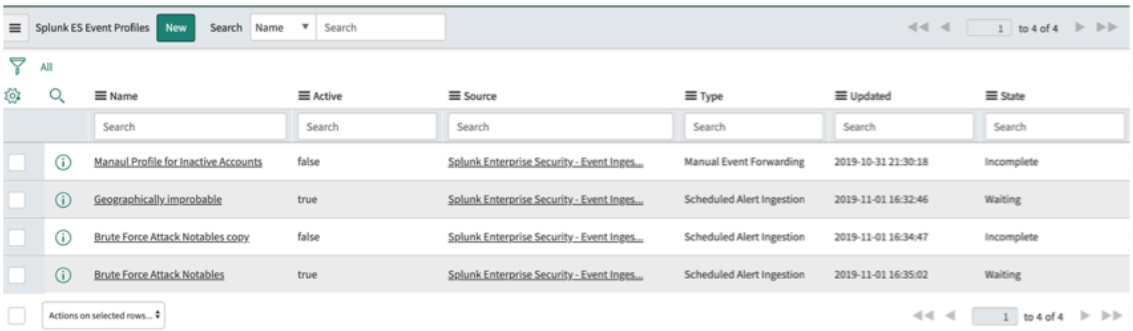
Procedure

1. Navigate to **All** > **Splunk Integration** > **Splunk Event Profile**.
2. In the Splunk Event Profiles list that is displayed, select a profile that you want to copy, and, from the Actions on selected rows choice list, click **Copy**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The profile is copied and displayed on the list. The copy has all the settings of the original profile including the mapping and scheduling configuration. The name of the profile contains copy. Although the original profile is activated (`true`), the copy is disabled at this point (`false`). You may prefer to edit values of the copied profile and rename it so the configuration settings apply to the new profile as required.



You have successfully copied the settings from an existing profile to a new profile.

What to do next

You are prompted to activate (enable) the new profile after you complete the configuration step.

Use the script editor to format alert values for the Splunk Enterprise Security Event Ingestion integration

In addition to the directly mapped fields from the ingested notable event values, and the values you enter manually, use the script editor to format field values on the security incident during the mapping step.

Before you begin

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

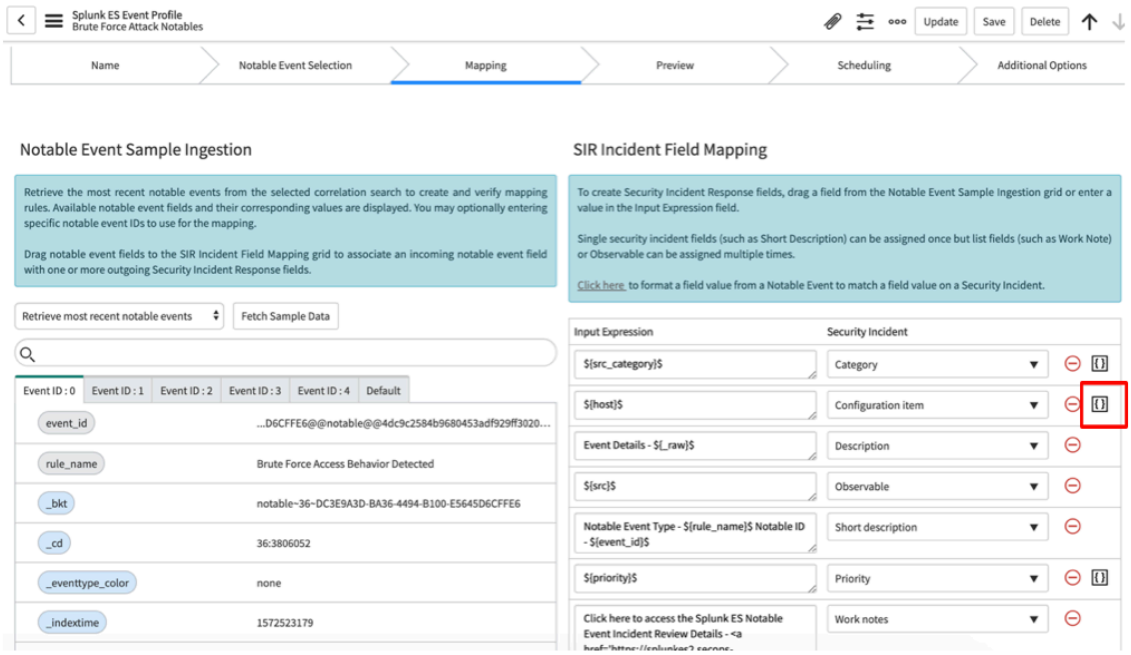
About this task

In certain cases, Splunk Enterprise Security notable event values are mapped to the Category, Configuration item (CI), and Observable fields on the SIR incident are not supported. You might prefer to edit the mapped values. If you want to translate the value of a Splunk Enterprise Security notable event to a value that is supported by these fields on the SIR security incident, use the script editor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. With the mapping form displayed, click the link to open the script editor.

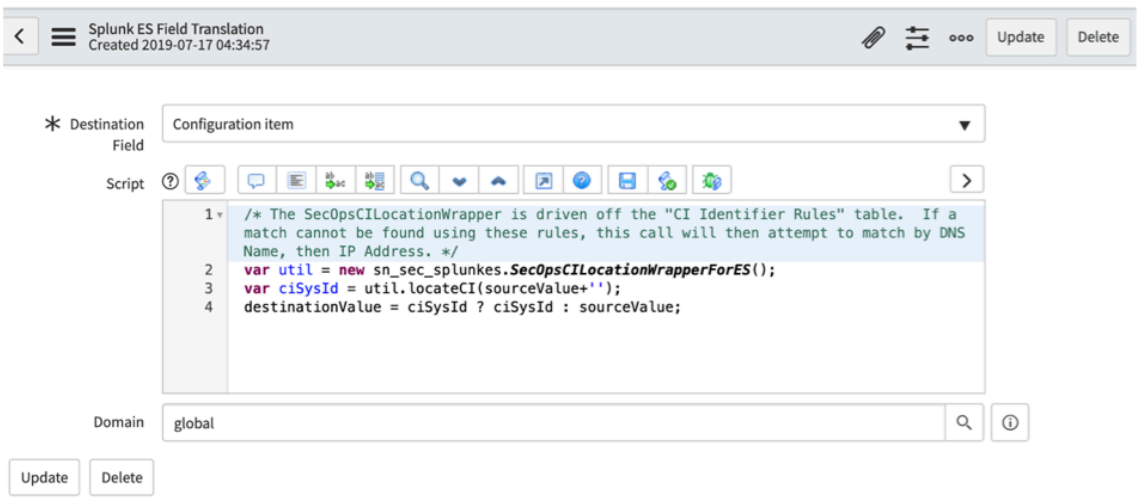


2. From the choice list, select a destination field for the value that you want to edit.
3. Alternatively, in the SIR Incident Field Mapping section, click the bracket icon [{ }] next to a field to open the script editor for that field.

   In certain instances, a script include may be appropriate for the Configuration item field. For an notable event, for example, a value for the Configuration item may not be matched.

   As shown in the following figure, if a match for a host name cannot be found in the ServiceNow AI Platform® CMDB for the Configuration item field, you can edit the rule so that if an IP address is found, it populates the Configuration item field. If there is no value for the alarm, the field on the security incident is set to null.

   The editor opens with the field displayed in Destination Field. The following image shows the editor with the `Configuration item` field as the Destination Field.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Enter any changes to then script, and click **Update** to save your changes.
   The Splunk Field Translations table is displayed.
5. Close the table to return to the Mapping form.

Copy Splunk Enterprise Security profiles from one instance to another using export/import functionality

You can export and import Splunk Enterprise Security profiles settings from one ServiceNow AI Platform instance to a different ServiceNow AI Platform instance.

Before you begin

The settings you can export and import include profile name, correlation rules, mappings, filters, aggregation criteria, field translations, fetched sample data, scheduling, and configuration tile source information.

Role required: sn_si.ingestion_profile_admin

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

This functionality allows the security administrator to copy profiles that have been tested and verified on one ServiceNow AI Platform instance, for example on non-production, to another ServiceNow AI Platform instance, for example production, without the need to redo all configuration settings. The settings that are exported and imported include profile name, correlation rules, mappings, filters, aggregation criteria, field translations, fetched sample data, scheduling, and configuration tile source information.

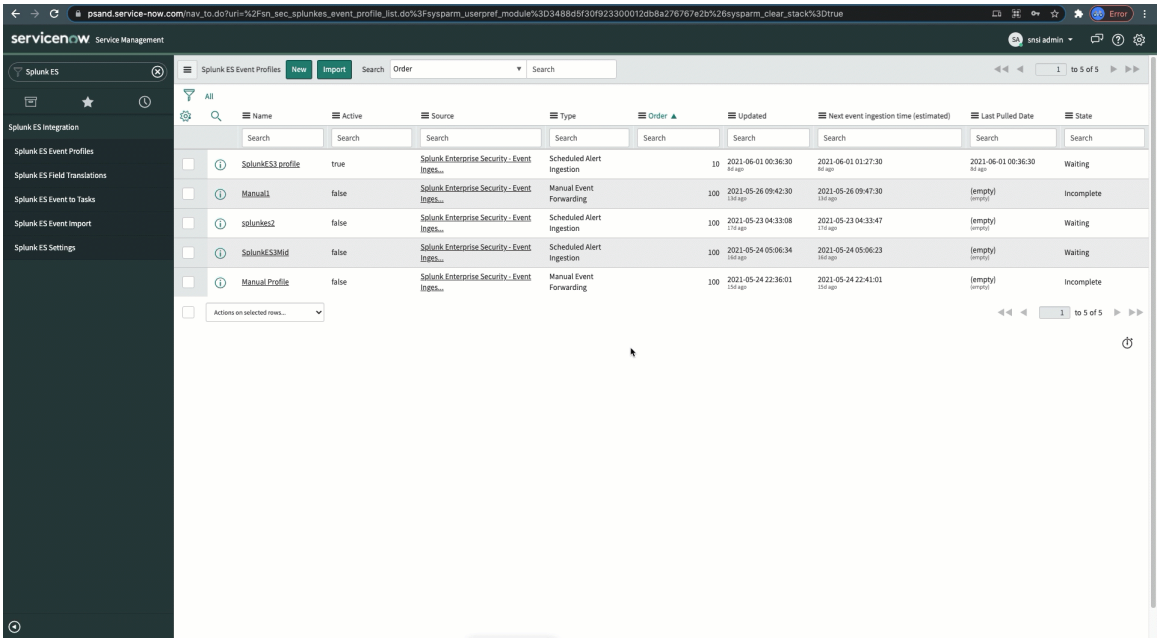
Note: When you export a manual event forwarding profile type, the attachment data used for the sample field mapping is copied, however, the attachment file itself is not exported.

Procedure

1. Navigate to **All** > **Splunk ES Integration** > **Splunk ES Event Profiles**.
2. Select a profile that you want to export to another ServiceNow AI Platform instance.
   You can select multiple profiles for export.
3. From the Actions menu, click **Export**.
4. Once the export complete message appears, click **Download**.

   The following illustration shows exporting a profile (SplunkES3profile) from the ServiceNow AI Platform instance (psand.service-now.com).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



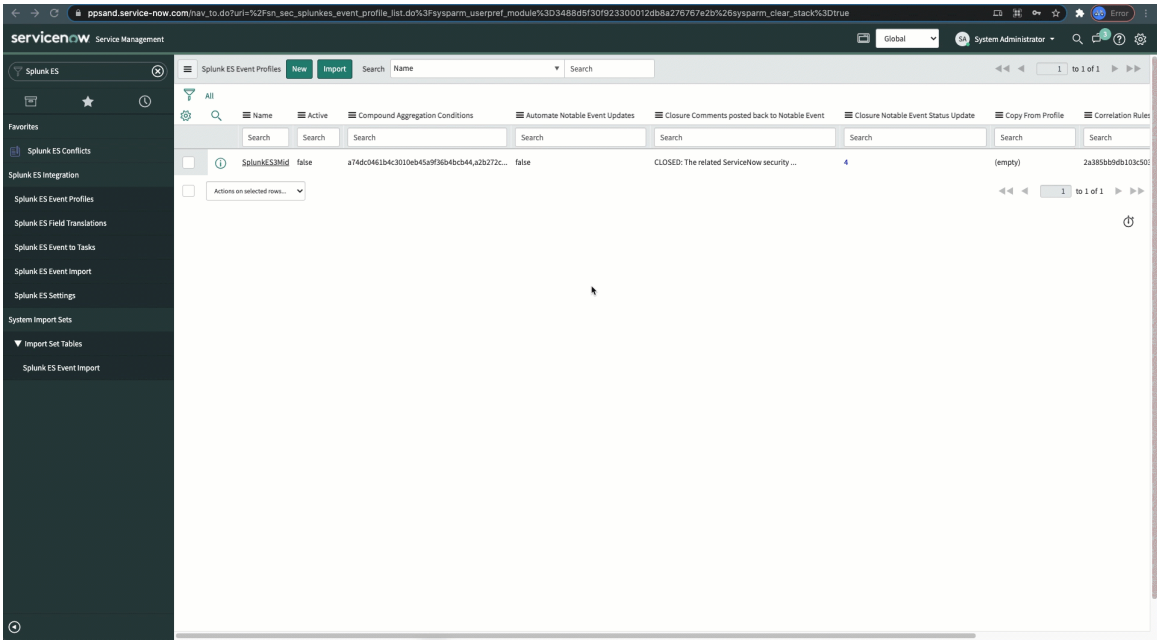
The exported payload.xml file is downloaded on your computer. The file contains the profile name, correlation rules, mappings, filters, aggregation criteria, field translations, fetched sample data, scheduling, and configuration tile source information. When you select and download multiple profiles, they appear in the same payload.xml file.

You can now proceed to import the profile in another ServiceNow AI Platform instance.

5. Navigate to **Splunk ES Integration** > **Splunk ES Event Profiles**.
6. Click **Import**.
7. Click **Choose file** and select the xml file on your computer.
8. Click **Upload**.
9. Click **Close and Reload Profiles**.

The following illustration shows importing a profile (SplunkES3profile) from the ServiceNow AI Platform instance (psand.service-now.com) to the ServiceNow AI Platform instance (ppsand.service-now.com).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You have successfully imported the profile from another ServiceNow AI Platform instance.

Verify that the exported Source (Splunk API account and Splunk server URL) and MID Server configuration settings are valid and available in imported ServiceNow AI Platform instance. Update your Splunk Enterprise Security configuration if required.

10. **Optional:** Verify the MID Server settings after your import a profile.
11. **Optional:** Navigate to **Security Operations** > **Integration Configurations**.
12. **Optional:** Select the Splunk Enterprise Security configuration tile, and click **Update**.
13. **Optional:** Review and update the Source and MID Server details as required.

Checklist for the Splunk Enterprise Security Notable Event Ingestion integration

Use this checklist to guide you through all the tasks of the integration. The following checklist includes setup and installation tasks and examples of use cases that include expected results for the integration.

Before you begin

Roles required: sn_si.ingestion_profile_admin, admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrator

Note: Users with the sn_si.admin role can perform all operations available to a profile admin, as the sn_si.admin role inherits the required permissions by default.

About this task

Track your progress with the setup, installation, and configuration of the integration with the following table. Complete all the tasks for a step before moving on to the next step. Each row of the table lists tasks and identifies the roles that are required to perform the tasks. Numbered topics of the installation and configuration guide are also referenced.

Roles required for each task are listed with each step in the following table.

Procedure

1. Track your progress with the setup, installation, and configuration of the integration. Complete all the tasks for a step before moving on to the next step.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Follow the steps in the table in the order that they are presented.

Checklist

☐	As a user with the ServiceNow AI Platform admin role, set up your ServiceNow AI Platform instance. ○ Assign users with the **sn_si.ingestion_profile_admin** (or sn_si.admin) and sn_si.analyst roles as required. ○ Install and configure a MID Server if the Splunk server is deployed within your corporate network. ○ Verify that the ServiceNow Security Incident Response plugins are activated for your release of the ServiceNow AI Platform. ○ (Optional) If you want to forward events manually from your Splunk Enterprise Security console into your ServiceNow AI Platform instance, verify that you have assigned the (sn_sec_splunkes.api_account_access) role to a user with the Splunk Enterprise Security administrator permission. For more information, see Set up your ServiceNow AI Platform instance for the Splunk Enterprise Security integration.
☐	As a user with the ServiceNow AI Platform admin role, install and configure the Splunk Enterprise Security application from the ServiceNow Store. **a.** Download and install the application on your ServiceNow AI Platform instance. **b.** Configure the application and connect to your Splunk Enterprise Security console. For more information, see Install and configure Splunk Enterprise Security Notable Event Ingestion integration.
☐	(Optional) If you intend to export events manually from your Splunk Enterprise Security console to your ServiceNow AI Platform instance, perform the following tasks: ○ As a Splunk Enterprise Security administrator, install, set up, and enable the ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security from splunkbase in your Splunk Enterprise Security console. ○ As a Splunk Enterprise Security administrator, if not already configured, save searches as notable events in your Splunk Enterprise Security console. For more information, see Set up your Splunk environment for manual event ingestion for the Splunk Enterprise Security Notable Event Ingestion integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

☐	As a user with the ServiceNow AI Platform **sn_si.ingestion_profile_admin** role, create and name an event profile. Select the profile type from the choice list. Options are a scheduled alert profile that you use to ingest sample data, or, an event profile that you use to export attachment data manually from your Splunk Enterprise Security console. ○ For a scheduled alert, select an available alert. ○ For profile for manually exported data, create a new map or copy an existing map. For more information, see Create and name an event profile for the Splunk Enterprise Security event ingestion integration.
☐	As a user with the ServiceNow AI Platform **sn_si.ingestion_profile_admin** role, map values ingested or attachment data that is exported from Splunk Enterprise Security to ServiceNow AI Platform security incidents. **a.** Fetch sample data for a scheduled alert. **b.** (Optional) Export attachment data manually from Splunk Enterprise Security for an event. **c.** Edit the default mapping configuration. **d.** Optionally add filtering criteria, append an alert to an existing security incident, and use the script editor. For more information, see Mapping notable event fields for the Splunk Enterprise Security integration and Create mappings for Splunk ES notable event incident review and contributing event details (scheduled ingestion).
☐	○ As a user with the ServiceNow AI Platform **sn_si.ingestion_profile_admin** role, preview the data from Splunk Enterprise that is displayed on a ServiceNow AI Platform security incident. ○ Fix any errors or add any missing data so that no error messages are displayed. For more information, see Preview the security incident for the Splunk Enterprise Security Event Ingestion integration.
☐	As a user with the ServiceNow AI Platform **sn_si.ingestion_profile_admin** role, schedule alert retrieval for a profile with a scheduled alert. For more information, see Schedule and retrieve new and updated notable events for the Splunk Enterprise Security Event Ingestion integration.

You have successfully completed the set up steps and verified expected results for the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk - Incident Enrichment integration

The Splunk - Incident Enrichment integration searches your logs and adds relevant sighting information to your security incidents.

Explore	Setup
Security Incident Response integrations	Get started with the Splunk Search integration for Security Operations
Use	**Develop**
• Run a Sightings Search • Security Operations Integration - Sightings Search Flow • Security Operations Integration - Splunk Sightings Search Flow • View Sightings Search Details • View Sightings Search Results	• ServiceNow Security Operations integration development guidelines • Tips for writing integrations • Developer training • Developer documentation • Find components installed with an application
Troubleshooting and Additional information	
• Integration troubleshooting • Ask or answer questions in the Security Operations community • Search the Known Error Portal for known error articles • Contact Customer Service and Support	

Get started with the Splunk Search integration for Security Operations

Splunk software searches, monitors, and analyzes machine-generated big data and integrates easily with Security Operations. Before you can use the Splunk - Incident Enrichment integration, you must download it from the ServiceNow Store and add the appropriate API Base URL and login credentials.

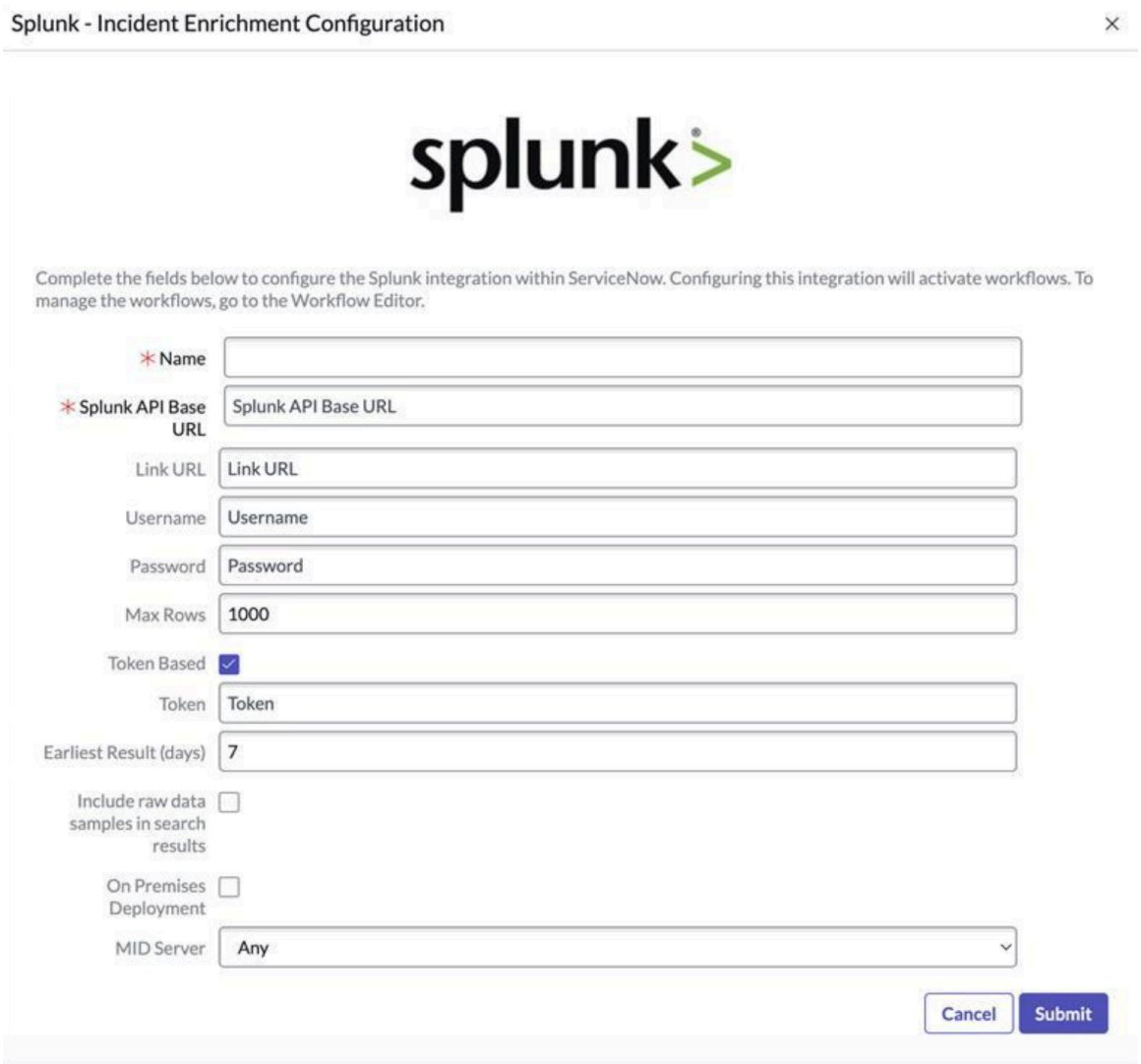
Before you begin

Role required: sn_si_admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access Splunk and obtain the API Key and API ID under your profile.
3. In your instance, navigate to **Security Operations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
4. In the Splunk - Incident Enrichment card, click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Fill in the fields, as needed.

Field	Description
Name	The name of this configuration.
Splunk API Base URL	The base URL you acquired from the Splunk site.
Link URL	[Optional] The Link URL that links to the Splunk web interface, when available.
Username	Your Splunk username.
Password	Your Splunk password.
Max Rows	The maximum number of rows you want to search.
Token Based	Enable this for token based authentication. **Note:** This field is optional.
Token	Your Splunk token.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the **number of rows of raw data** property in Security Incident Response properties.
On Premises Deployment	Enable this for on premises Splunk. **Note:** This field is optional.
MID Server	Select **Any** to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the **Workflow Editor**.

6. Click **Submit**.
   The integration configuration card displays.
7. When viewing the new configuration card, you can click **Configure** or **Delete** to change or delete the configuration, respectively.
8. To return to the original list of integration configuration cards, select **No** from the **Show Configurations** drop-down list.

Mobile Experience for Security Incident Response

Use your Android or iOS mobile device to manage your security operations center (SOC) tasks.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Security Incident Response

If you're unfamiliar with the basic concepts of the Security Incident Response (SIR) product on your ServiceNow AI Platform® instance, see Security Incident Response Overview dashboard for more information about threat intelligence and how this product can help you prioritize and resolve cyberthreats to your organization.

Mobile experience for SIR overview

As a security operations center (SOC) manager or a user with the ServiceNow AI Platform security analyst role (sn_si.analyst), you can log in to a ServiceNow AI Platform instance directly from your mobile device. With the Security Incident Response Mobile app, you can view, edit, and assign your most current and critical SIR security incidents and response tasks. Notifications inform you when critical security incidents assigned to you arrive.

With the Security Incident Response Mobile app, you can perform the following SIR -related tasks from your mobile device:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- View a list of critical security incidents and response tasks.
- Receive detailed notifications for security incidents and tasks that meet pre-defined notification criteria.
- View groupings of security incidents or tasks that are based on a pre-defined set of queries or filters.
- View the work notes and related lists of security incidents.
- Update security incidents and add work notes or attachments.
- Edit the fields on security incidents.
- Assign security incidents to yourself or to other members of your security team.

When they're populated, you can view the following related lists on SIR security incidents with the Security Incident Response Mobile app:

- Configuration Item
- Affected User
- Affected Services
- Child Security Incidents
- Similar Security Incidents (not support by ServiceNow AI Platform)
- Observables
- Response Tasks
- Tasks
- Task SLA
- Attachments (not support by ServiceNow AI Platform)

The following figure illustrates how you log into your ServiceNow AI Platform instance from your mobile device and the structure of the landing screen of the Security Incident Response Mobile app that is displayed after you log in.

For step-by-step instructions about how to set up your ServiceNow AI Platform instance and install the Security Incident Response Mobile app, see Set up checklist for the Security Incident Response Mobile app. For instructions about how to log in, see Log in to the Security Incident Response Mobile app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response Mobile app



Applications

Applications are the ServiceNow® software components such as Security Incident Response (SIR), Vulnerability Response (VR), Governance, Risk, and Compliance (GRC) that provide specific features and functionalities within your ServiceNow AI Platform instance. After you install the Security Incident Response core application and the Security Incident Response Mobile app on your ServiceNow AI Platform instance, the icon for the core application is displayed on the bottom of your Android or iOS mobile device after you log in.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response Mobile app (Security Incidents) icon

Folders

Each ServiceNow® mobile application contains folders that separate the applets by category. In the preceding image of the landing page, **Security Incidents** and **Incident Response Tasks** are folders.

Applets

Applets are the different options within the application. The icons under the **Security Incidents** and **Incident Response Tasks** sections are the available applets of the Security Incident Response Mobile app.

Set up checklist for the Security Incident Response Mobile app

The following checklist includes the set up tasks that you are required to complete in your ServiceNow AI Platform® instance and on your mobile device prior to using the Security Incident Response Mobile app.

Before you begin

As an option, print this checklist and use it to guide you through the set up tasks that are required for the Security Incident Response Mobile app. Verify that each item on the list is completed so that you can view and edit SIR security incidents on your mobile device.

The check list items are displayed in highlighted text. More information follows each item in the right column. Estimated time to complete this task: 15-20 minutes.

Roles required: admin, sn_si.analyst

Mobile checklist

Item	Description
☐	As a user with the admin role, verify that you have the Security Incident Response core application installed on a ServiceNow AI Platform instance. This is the ServiceNow AI Platform instance that you view on your mobile device. **Note:** The Security Incident Response core application and the ServiceNow AI Platform instance should be from the same family release. 1. To verify the core application is installed on your instance, navigate to **Plugins** and search for Security Incident Response. 2. If the Security Incident Response core application is not already installed, click **Install** to install it. For more information about installing the Security Incident Response core application, see Install and configure Security Incident Response. If the Security Incident Response core application is not visible in Plugins, for more information about installing core applications and entitlements to applications, see Security Operations and the ServiceNow Store.
☐	As a user with the admin role, verify that you have the Security Incident Response Mobile app installed on the ServiceNow AI Platform instance that you want to view on your mobile device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mobile checklist (continued)

Item	Description
	Note: the Security Incident Response Mobile app and the ServiceNow AI Platform instance should be from the same family release. Download and install the Security Incident Response Mobile app from the ServiceNow Store on your ServiceNow AI Platform instance. When you install the Security Incident Response Mobile app, its dependencies, com.glide.sg and com.glide.sg.agent_native_client, are also installed. To verify that these dependencies are installed: 1. Navigate to **Plugins**. 2. Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client). 3. If they are not activated, activate these plugins. These plugins are required for the Security Incident Response Mobile app. For more information about installing applications and entitlements to applications, see Security Operations and the ServiceNow Store.
☐	As a user with the ServiceNow AI Platform admin role, verify that you have assigned mobile users with the required roles in your ServiceNow AI Platform instance. 1. To view the roles that are assigned to a user, navigate to **Users and Groups** > **Users**. 2. Select the user name followed by the roles related list. All roles assigned to this user are displayed. 3. Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, update and close security incidents. Only users with the itil role can have tasks assigned to them. 4. Verify a user is assigned, or assign a user with the security analyst role (sn_si.analyst). Users with the sn_si.analyst role can read and edit security incident records. This role is automatically added when you assign the itil role. 5. Verify you have created any required assignment groups and assigned mobile users to these groups. **Note:** If you have a large number of users for the mobile application, you alternatively can assign the sn_si.analyst role to a group. Each user you add to the group inherits this role. For more information about security analysts, see Assigning security analysts. For more information on users and assigning roles to users and groups, see User administration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mobile checklist (continued)

Item	Description
☐	As a user with the sn_si.analyst role, download the most current ServiceNow® Agent app on your mobile device. The most current version of the Agent app is available on the Apple iOS App Store and the Google Play Store.
☐	As a user with the sn_si.analyst role, verify notifications are enabled on your mobile device and in your ServiceNow AI Platform instance. Notifications inform you when critical security incidents are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the Security Incident Response Mobile app to navigate directly to the security incident. To enable notifications in your ServiceNow AI Platform instance so they are displayed on your mobile device, follow these steps. **1.** Verify you have downloaded and installed the Security Incident Response Mobile app on your ServiceNow AI Platform instance. **2.** In System Settings in your ServiceNow AI Platform instance, under Notifications, verify you have enabled the **ServiceNow Mobile Application**. For more information about setting notifications, see Setting user notification preferences in Core UI. ServiceNow AI Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device.

You have successfully set up your mobile device and the ServiceNow AI Platform for the Security Incident Response Mobile app. The next step is to log in to your ServiceNow AI Platform instance with your mobile device.

Log in to the Security Incident Response Mobile app

Open the Security Incident Response Mobile app and add a ServiceNow AI Platform® instance with Security Incident Response to your mobile device.

Before you begin

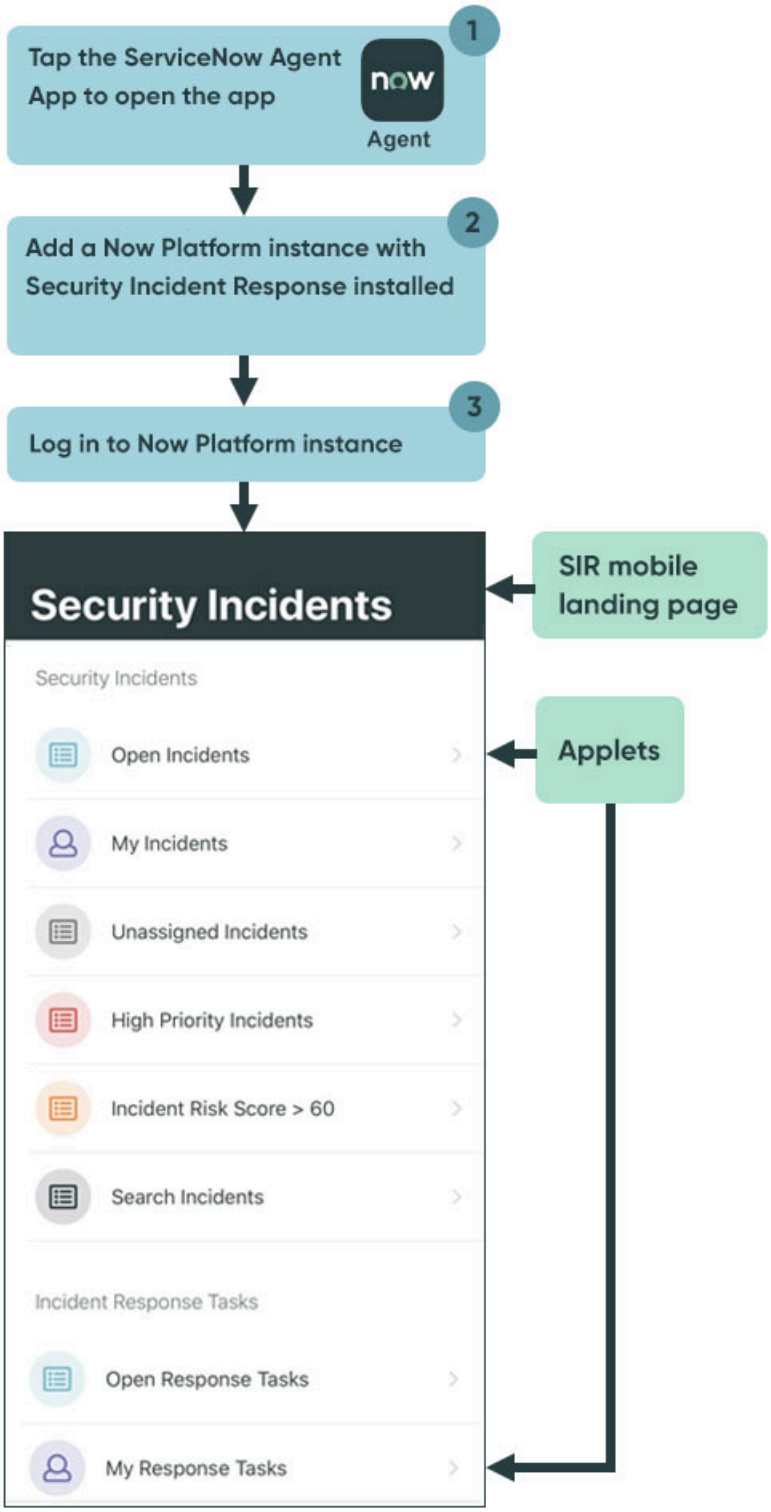
Role required: sn_si.analyst

About this task

Time to complete this task: 5-10 minutes.
Verify that you have completed the setup steps described in Set up checklist for the Security Incident Response Mobile app.

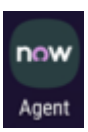
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response Mobile app



Procedure

1. On your mobile device, tap the **ServiceNow Agent** app to open it.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you are not already logged in to a ServiceNow AI Platform instance, the Instances screen is displayed.

2. If the ServiceNow AI Platform instance with the Security Incident Response core application is not already added to your mobile device, follow these steps to add it.

   a. On the Instances screen that is displayed, tap the  .
   A screen is displayed that prompts you to enter and save an address of a ServiceNow AI Platform instance.

   b. Fill in the fields.

Field	Description
Enter the instance address or scan a QR code.	Choose one to continue: ▪ Before the `.service-now.com`, enter the name of your ServiceNow AI Platform instance, for example, `sirmobileny`. ▪ Enter an address. This address is the URL of your ServiceNow AI Platform instance that you want to view on your mobile device, for example, https://sirmobileny.service-now.com. ▪ Scan a QR code.
(Optional) Enter nickname	Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a ServiceNow AI Platform instance.

   c. Tap **Save and Login**.

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the ServiceNow AI Platform instance that you want to add and tap **Login**.
   The Security Incidents landing screen is displayed. You have successfully logged in to the Security Incident Response Mobile app.
4. After you log in, verify notifications are enabled in the Security Incident Response Mobile app.

   a. On the landing screen on the bottom, tap **Notification**.

   b. On the Notifications screen, tap **Enable Notifications** if not enabled.
   Notifications from the ServiceNow AI Platform are displayed on the Notifications screen in the Security Incident Response Mobile app.

5. After you log in to an instance on your mobile device, it is the default ServiceNow AI Platform instance on the device.
   If you want to view another ServiceNow AI Platform on the device, you are required to log out of the default instance. To log out:

   a. Tap the settings icon.

   b. Tap **Logout**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Instances screen is displayed with any ServiceNow AI Platform instances you have added to the mobile device.

c. **Optional:** Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

If the instances screen for the Security Incident Response Mobile app is not displayed after you tap the **ServiceNow Agent** app on your device, verify that the **ServiceNow Agent** is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings and general device management on your device and tap the option (Trust app, etc.) to permit access.

If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the ServiceNow AI Platform instance is correct.

If you have problems viewing the landing screen, verify your network connection.

If you cannot view the Instances screen after you tap the **ServiceNow Agent** app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.

View, edit, and assign open security incidents with the Security Incident Response Mobile app

As a security incident analyst, view, edit, and assign open Security Incident Response (SIR) security incidents from your mobile device. View related lists and the audit trail of work notes for more details about incidents.

Before you begin

Role required: sn_si.analyst

About this task

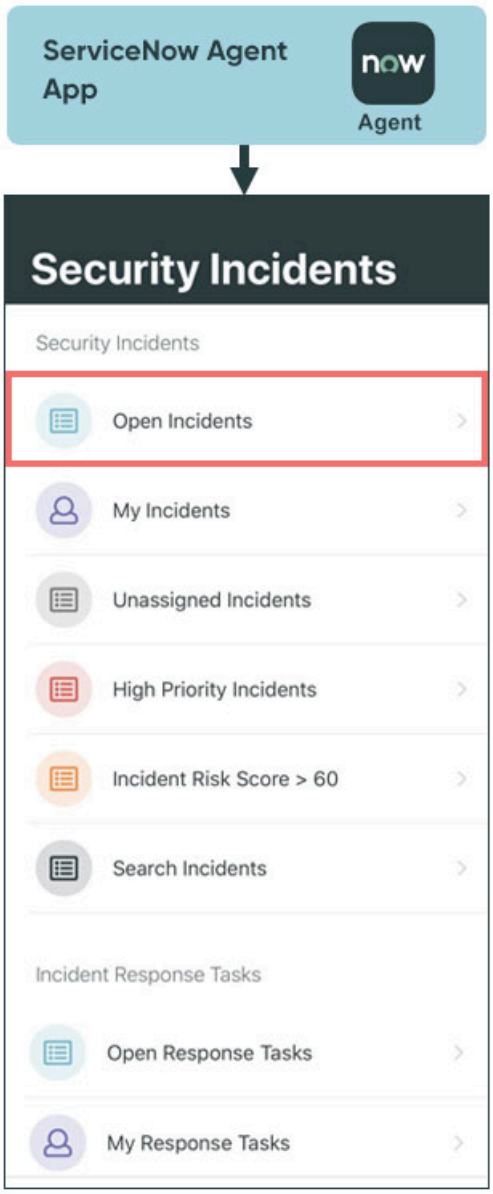
From the list of records, assign an open security incident to yourself, or reassign it. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing page displayed, tap **Open Incidents**.

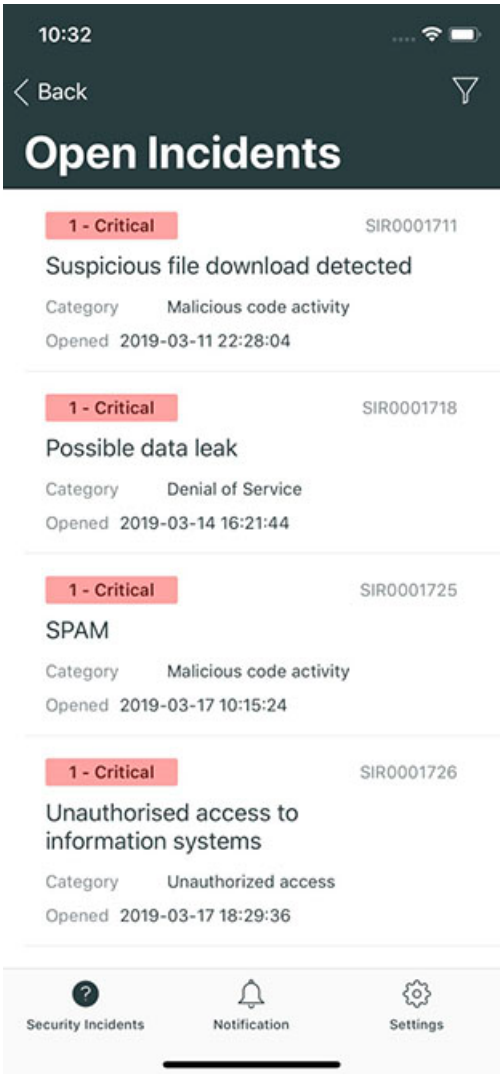
   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Open Incidents screen is displayed with a list of open security incident records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

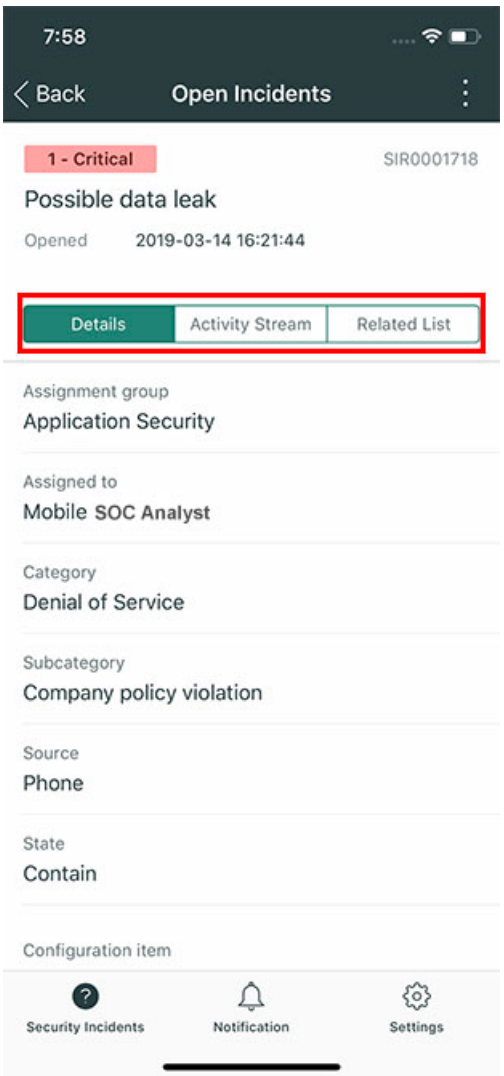
4. To assign an incident to yourself or reassign it directly from the list of open security incidents, swipe left on a record to open the menu.
5. Choose one from the menu that is displayed to continue.

Option	Description
Assign to Me	Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.
Reassign	To assign or reassign the assignment group: **a.** Tap **Assignment group**. **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	To assign or reassign the security incident to a member of the assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed, or enter text in the search field. Tap the send icon ( ) or **Submit** to save and submit your changes.

6. Alternatively, to view the details of an open security incident record and to see more associated records and related lists, with the Open Incidents screen displayed, tap a record on the list.
7. On the open record that is displayed, choose one option from the following table to continue.



Option	Description
Tap the menu icon ( ) on the upper right of the screen.	From the menu that is displayed, choose from the following options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text. ○ To reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions de scribed in the previous table. After you complete your edits, tap the send icon () or **Submit** to save your changes and update the security incident.
Activity Stream tab	With the Activity Stream tab selected, review the audit trail of work notes, activities, and ad ditional comments of the record. Tap the plus icon () to add a work note or attach a file.
Related List tab	With the Related List tab selected, view the items of any Related Lists of the security inci dent that are populated. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to con tinue to view the activity streams and related lists associated with the parent security inci dent.
Screen icons at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Security Incidents icon to return to the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Securi ty Incident Response Mobile app. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

View, edit, and reassign security incidents assigned to you with the Security Incident Response Mobile app

As a security incident analyst, view, edit, and reassign Security Incident Response (SIR) incidents that are assigned to you. View related lists and the audit trail of work notes for more details about incidents.

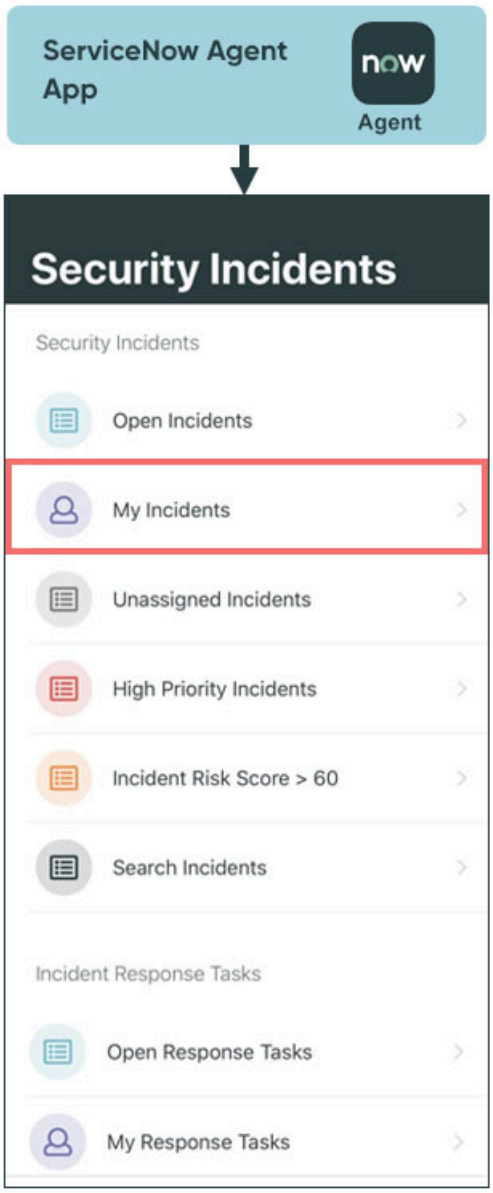
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.analyst

About this task
Reassign an open security incident to another analyst in your group from the list of records. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

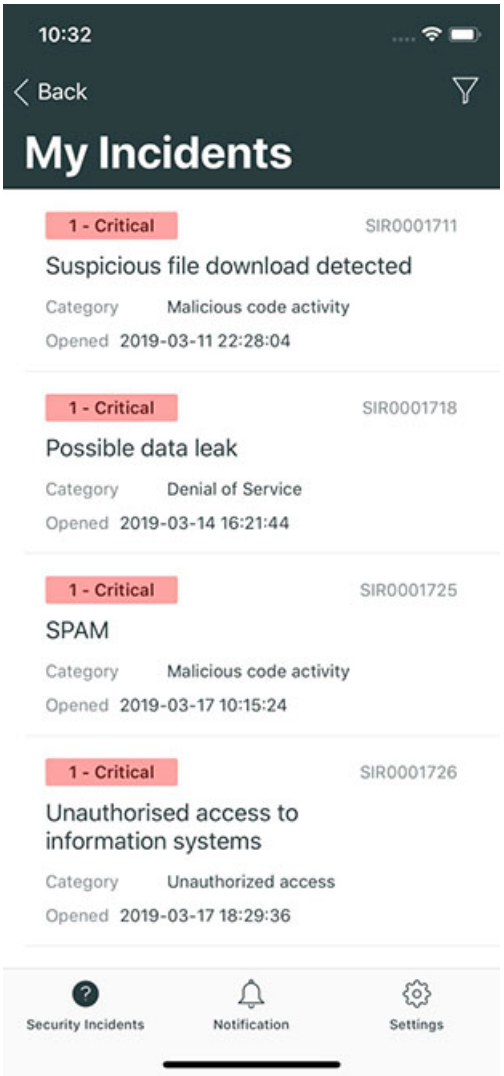
Procedure
1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **My Incidents**.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



   The My Incidents screen is displayed with a list of open security incident records that are assigned to you.

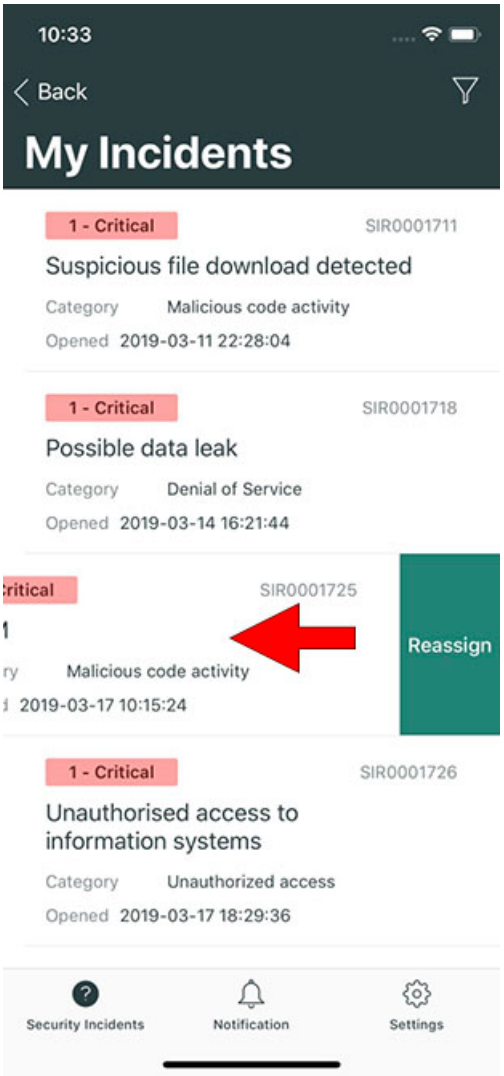
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.
4. To reassign an incident directly from the list, with the list of open security incident records displayed, swipe left on a record to open the menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

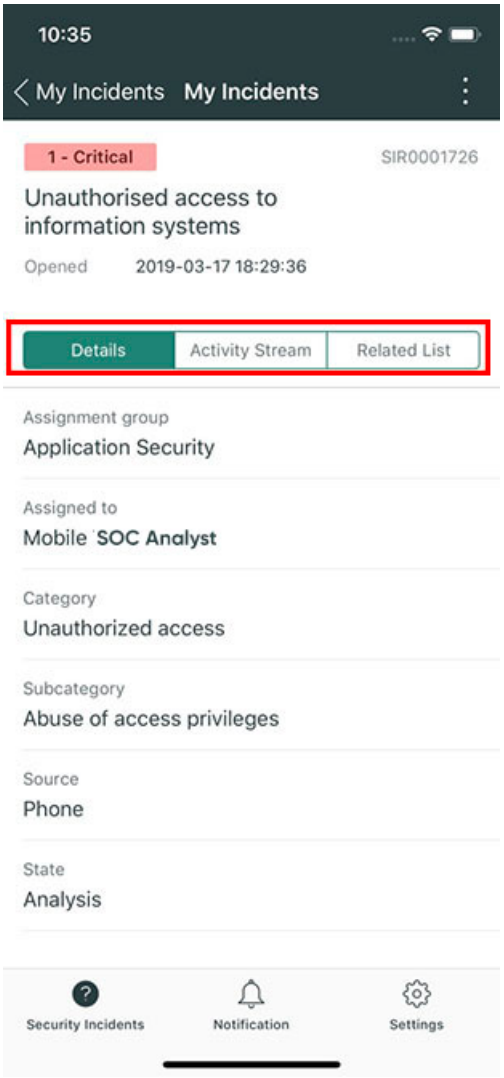


5. Edit the Assignment group or the Assigned to fields from the menu that is displayed.

Option	Description
Reassign	To reassign the assignment group: **a.** Tap **Assignment group**. **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. To assign or reassign the security incident to a member of the assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed, or enter text in the search field. Tap the send icon ( ) or **Submit** to save and submit your changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Alternatively, to view the details of the open security incident record, with the My Incidents screen displayed, tap a record on the list.
7. On the open record that is displayed, choose one option from the following table to continue.



Option	Description
Tap the menu icon ( ) on the upper right of the screen.	From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text. ○ To reassign the incident, tap **Reassign**. Fol low the instructions described in the previ ous table. After you complete your edits, tap the send icon ( ) or **Submit** to save your changes and update the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Activity Stream tab	With the Activity Stream tab selected, review the audit trail of work notes, activities, and ad ditional comments of the record. Tap the plus icon () to add a work note or attach a file.
Related List tab	With the Related List tab selected, view the items on any Related Lists that are populated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to con tinue to view the activity streams and related lists associated with the parent security inci dent.
Screen icons at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Security Incidents icon to return to the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Securi ty Incident Response Mobile app. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

View, edit and assign unassigned security incidents with the Security Incident Response Mobile app

From your mobile device, view, edit, and assign unassigned Security Incident Response (SIR) incidents. View related lists and the audit trail of work notes for more details about incidents.

Before you begin

Role required: sn_si.analyst

About this task

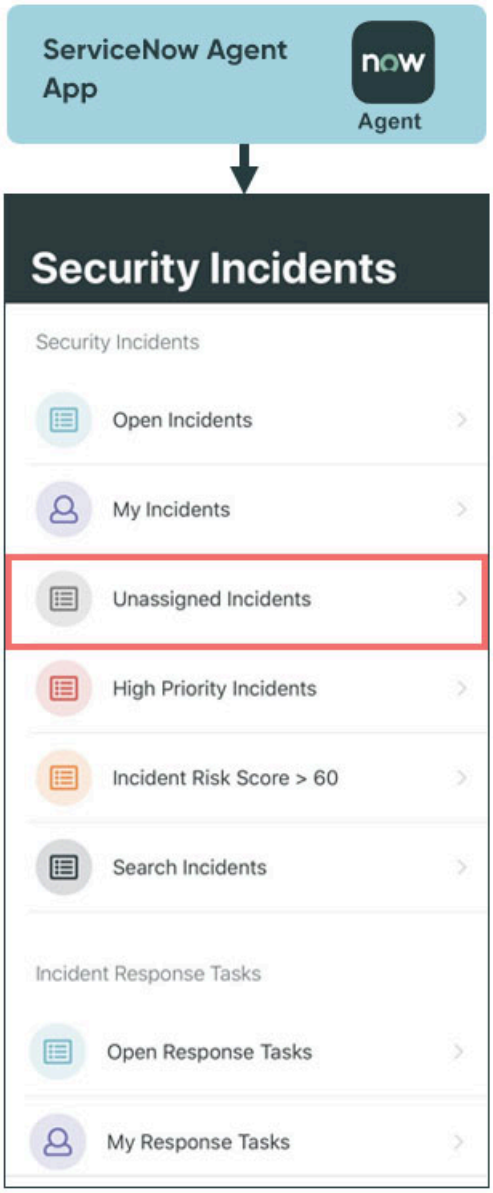
From the list of records, assign an open, unassigned security incident to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **Unassigned Incidents**.

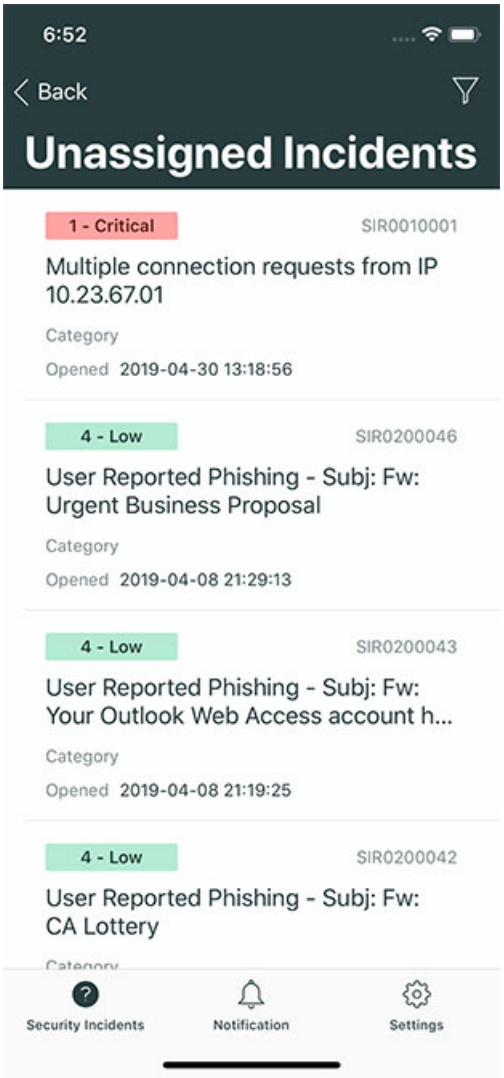
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



The Unassigned Incidents screen is displayed with a list of unassigned security incident records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

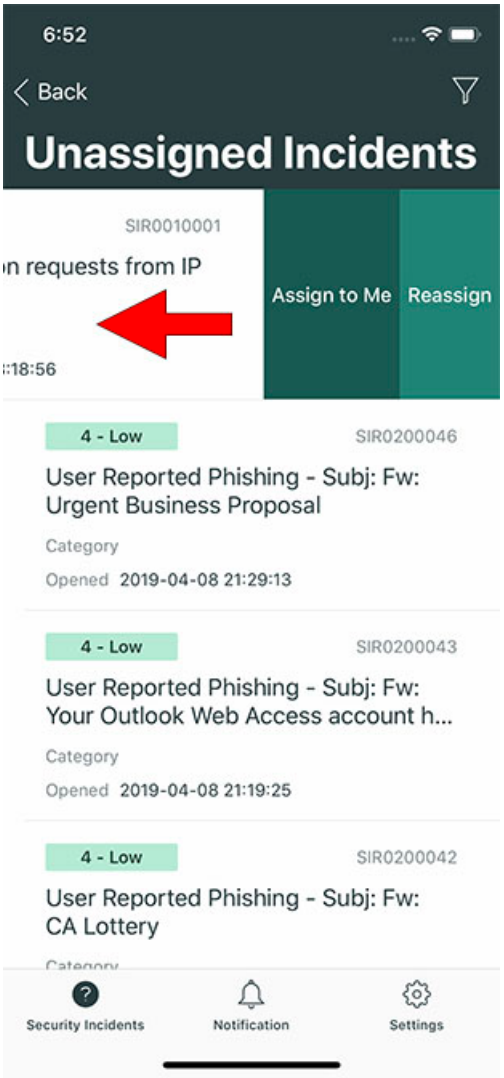


3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

4. To assign or reassign an open security incident record directly from the list, with the list of open unassigned security incident records displayed, swipe left on a record to open the menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



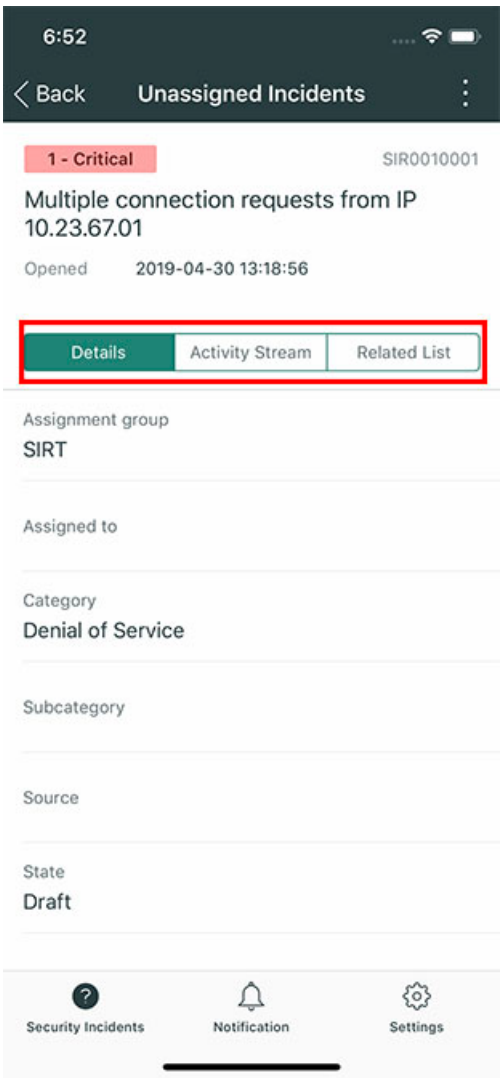
5. Choose one from the menu to continue.

Option	Description
Assign to Me	Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.
Reassign	To assign or reassign the assignment group: **a.** Tap **Assignment group**. **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. To assign or reassign the security incident to a member of the assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed, or enter text in the search field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Tap the send icon ( ) or **Submit** to save and submit your changes.

6. Alternatively, with the Unassigned Incidents screen displayed, tap a record on the list.
7. On the open record that is displayed, choose one option from the following table to continue.



Option	Description
Tap the menu icon ( ) on the upper right of the screen.	From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text. ○ To assign or reassign the incident, tap **Re assign** or **Assign to Me**. Follow the instruc tions described in the previous table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	After you complete your edits, tap the send icon () or **Submit** to save your changes and update the security incident.
Activity Stream tab	With the Activity Stream tab selected, review the audit trail of work notes, activities, and ad ditional comments of the record. Tap the plus icon () to add a work note or attach a file.
Related List tab	With the Related List tab selected, view the items on any of the Related Lists that are pop ulated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to con tinue to view the activity streams and related lists associated with the parent security inci dent.
Screen icons at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Security Incidents icon to return to the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Securi ty Incident Response Mobile app. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

View, edit, and assign high priority incidents with the Security Incident Response Mobile app

From your mobile device, view, edit, and assign high priority Security Incident Response (SIR) incidents. View related lists and the audit trail of work notes for more details about incidents.

Before you begin

Role required: sn_si.analyst

About this task

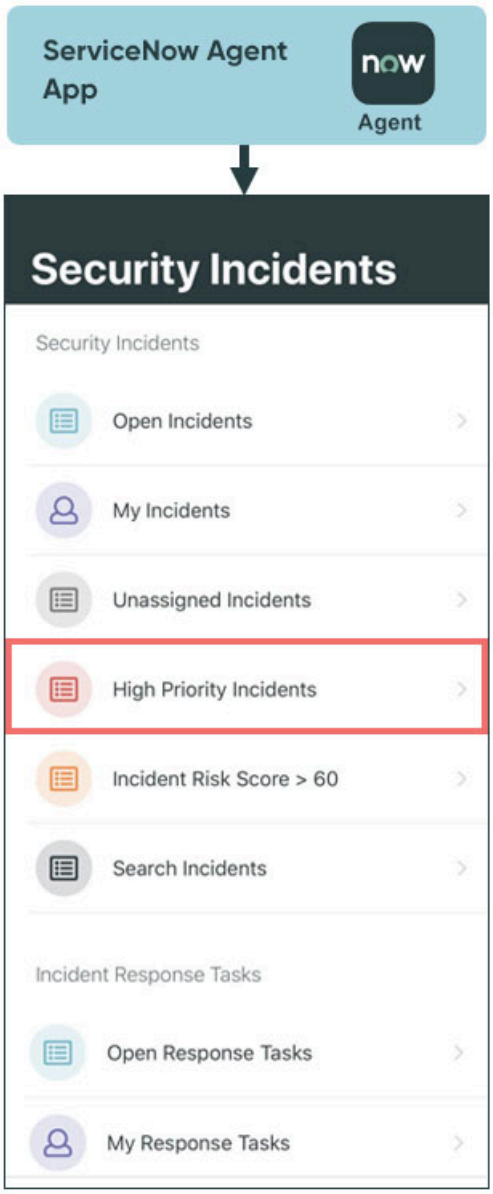
From the list of records, assign an open, critical security incident to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

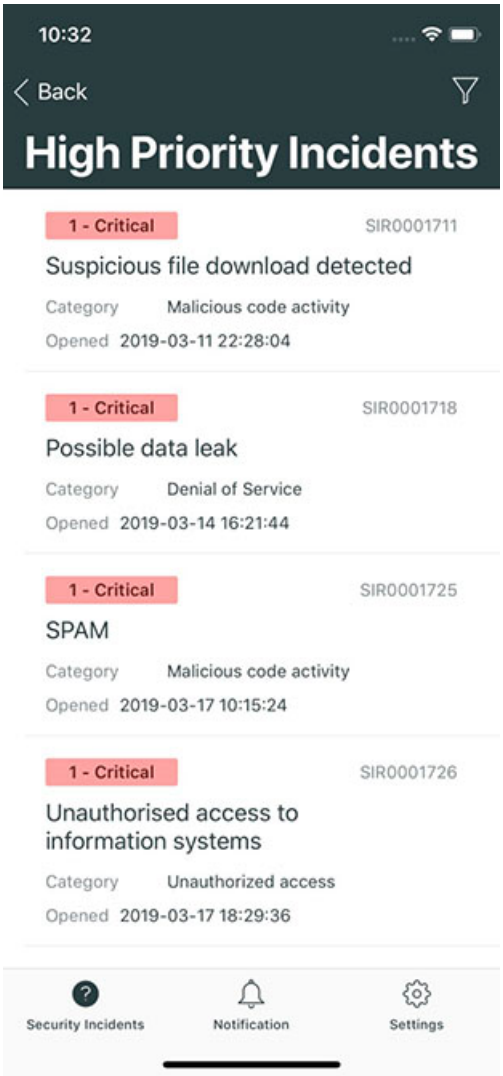
1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **High Priority Incidents**.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



The High Priority Incidents screen is displayed with a list of critical (high priority) security incidents.

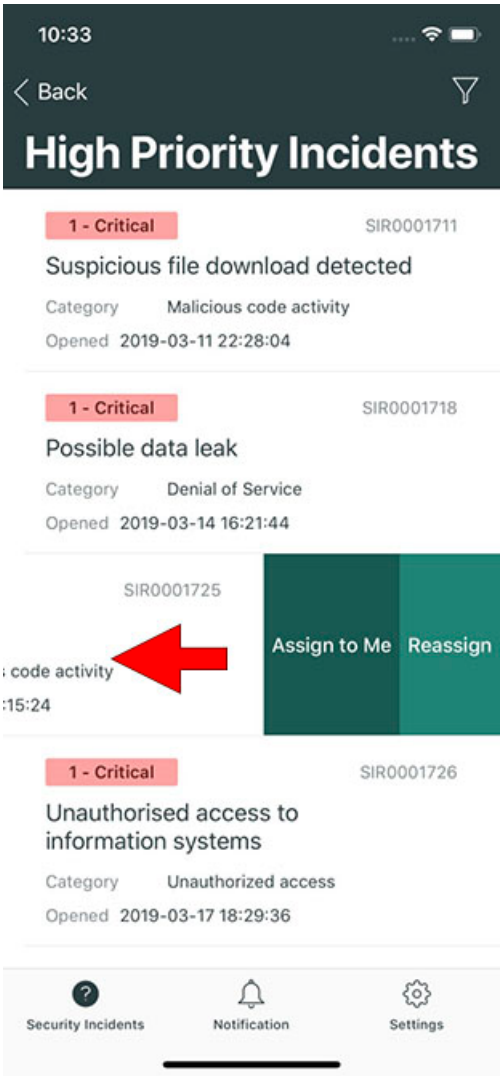
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.
4. With the list of open high priority security incident records displayed, swipe left on a record to open the menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



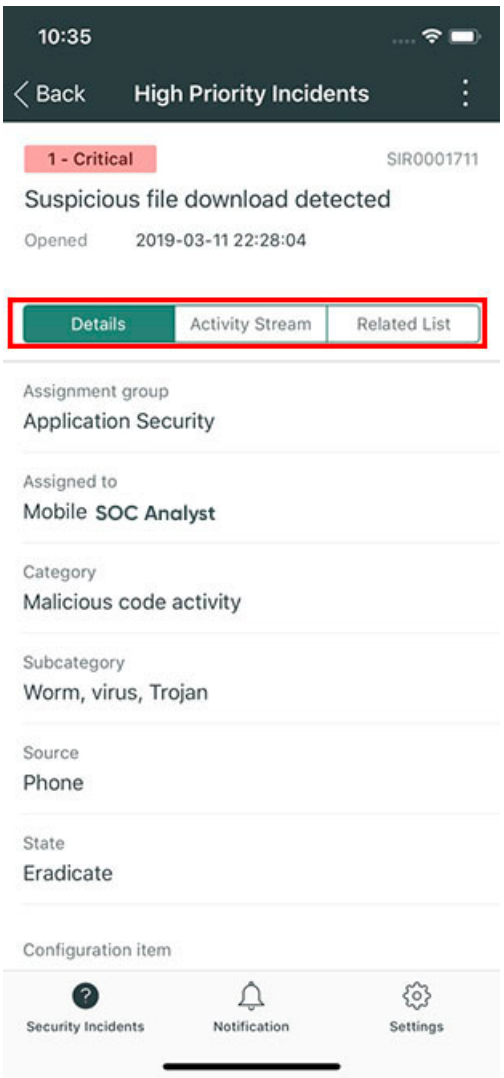
5. Choose one to continue.

Option	Description
Assign to Me	Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.
Reassign	To assign or reassign the assignment group: **a.** Tap **Assignment group** **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. To assign or reassign the security incident to a member of the assignment group: **a.** Tap **Assigned to**. **b.** Tap a name from the list that is displayed, or enter text in the search field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Tap the send icon ( ) or **Submit** to save and submit your changes.

6. To view the details of an open security incident record and to see more associated records and related lists, with the High Priority Incidents screen displayed, tap a record on the list.
7. On the open record that is displayed, choose one option from the following table to continue.



Option	Description
Tap the menu icon ( ) on the upper right of the screen.	From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	are displayed. Alternatively, tap the search icon and enter text. ○ To reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions de scribed in the previous table. After you complete your edits, tap the send icon ( ) or **Submit** to save your changes and update the security incident.
Activity Stream tab	With the Activity tab selected, review the au dit trail of work notes, activities, and addition al comments of the record. Tap the plus icon ( ) to add a work note or attach a file.
Related List tab	With the Related List tab selected, view the items on any of the Related Lists that are pop ulated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associat ed with the parent security incident.
Tap a screen icon at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Security Incidents icon to return to the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Securi ty Incident Response Mobile app. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

View, edit, and assign security incidents with a risk score greater than 60 with the Security Incident Response Mobile app

From your mobile device, view and edit Security Incident Response (SIR) incidents with a value in the risk score field that is greater than 60. View related lists and the audit trail of work notes for more details about incidents.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

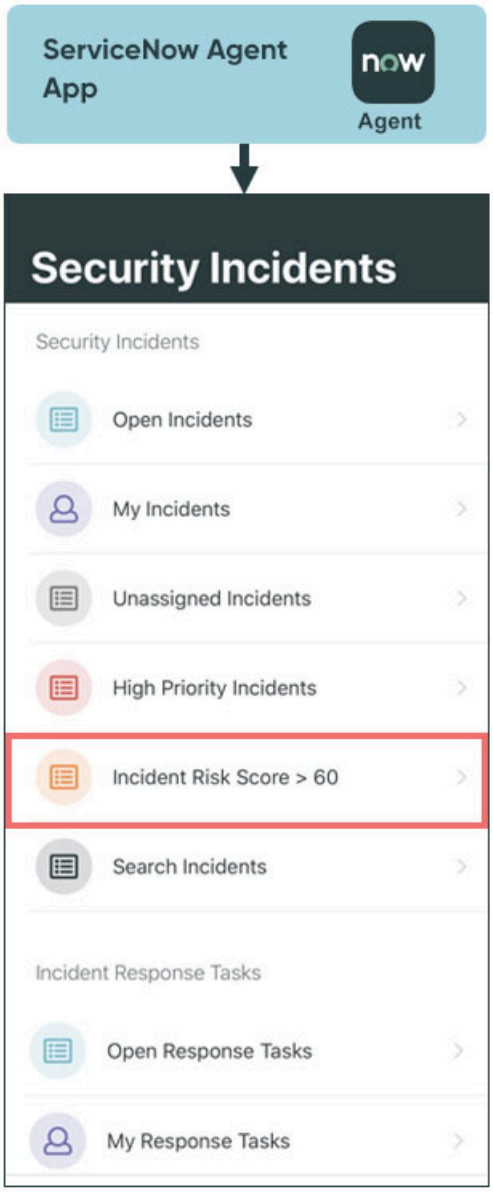
About this task

From the list of records, assign an open security incident that has a risk score that is greater that 60 to yourself or to another analyst in your group. Alternatively, view the details and related lists of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure

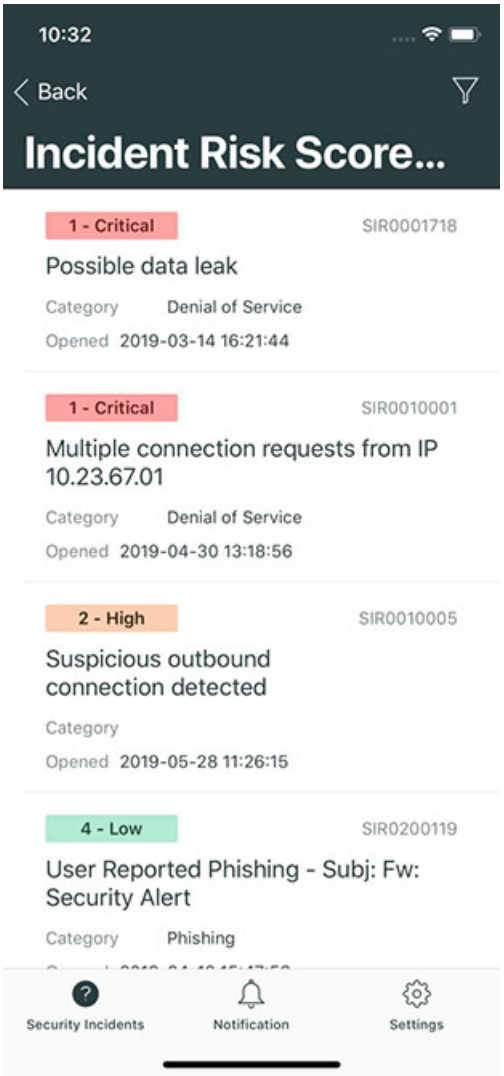
1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **Risk Score > 60**.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



The Incident Risk Score screen is displayed with a list of security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

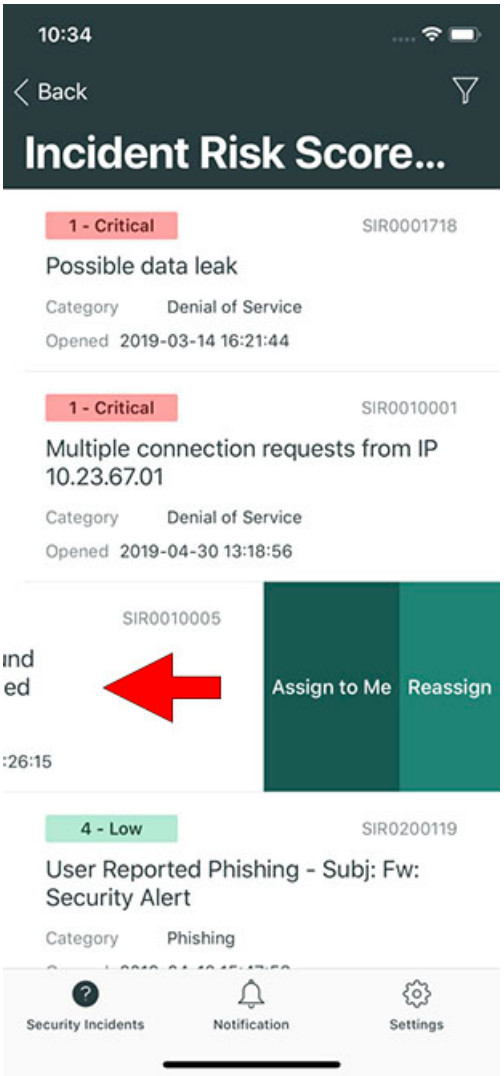


3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for security incidents that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

4. To assign a security incident to yourself or reassign it directly from the list of open security incident records displayed, swipe left on a record to open the menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



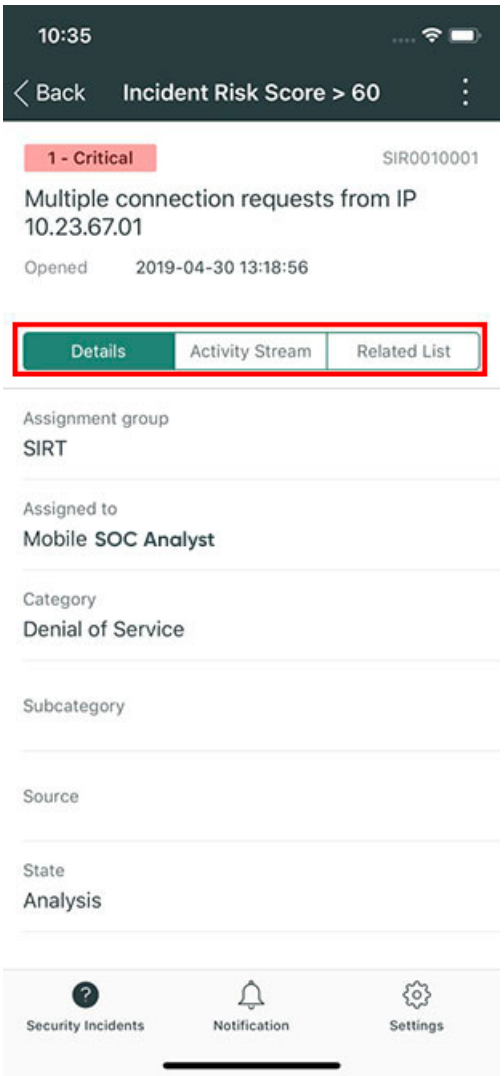
5. Choose one to continue.

Option	Description
Assign to Me	Assign the security incident to yourself. If the security incident is already assigned to you, this option is not displayed.
Reassign	To assign or reassign the assignment group: **a.** Tap **Assignment group**. **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group. To assign or reassign the security incident to a member of the assignment group: **a.** Tap **Assigned to** and **b.** Tap a name from the list that is displayed, or enter text in the search field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Tap the send icon ( ) or **Submit** to save and submit your changes.

6. Alternatively, to view the details of an open security incident record and to see more associated records and related lists, with the Incident Risk Score screen displayed, tap a record on the list.
7. On the open record that is displayed, choose one option from the following table to continue.



Option	Description
Tap the menu icon on the upper right of the screen.	From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Security Incident screen displayed, tap a field to expand it and choose one or more of the options that

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	are displayed. Alternatively, tap the search icon and enter text. ○ To reassign the incident, tap **Reassign** or **Assign to Me**. Follow the instructions de scribed in the previous table. After you complete your edits, tap the send icon () or **Submit** to save your changes and update the security incident.
Activity Stream tab	With the Activity Stream tab selected, review the audit trail of work notes, activities, and ad ditional comments of the record. Tap the plus icon () to add a work note or attach a file.
Related List tab	With the Related List tab selected, view the items on any of the Related Lists that are pop ulated on the security incident. Tap an item on the list that is displayed to view the details for a related list. From the lists of items that are displayed, tap an item to continue to view the activity streams and related lists associat ed with the parent security incident.
Screen icons at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ Tap the Security Incidents icon to return to the landing screen. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications from the ServiceNow AI Platform and the Securi ty Incident Response Mobile app. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance on your device. ▪ Log out of the current ServiceNow AI Plat form instance.

Search for security incidents with the Security Incident Response Mobile app

Search for Security Incident Response (SIR) security incidents on a ServiceNow AI Platform® instance. Only incidents that match the specific search criteria that you enter are displayed.

Before you begin

Role required: sn_si.analyst

About this task

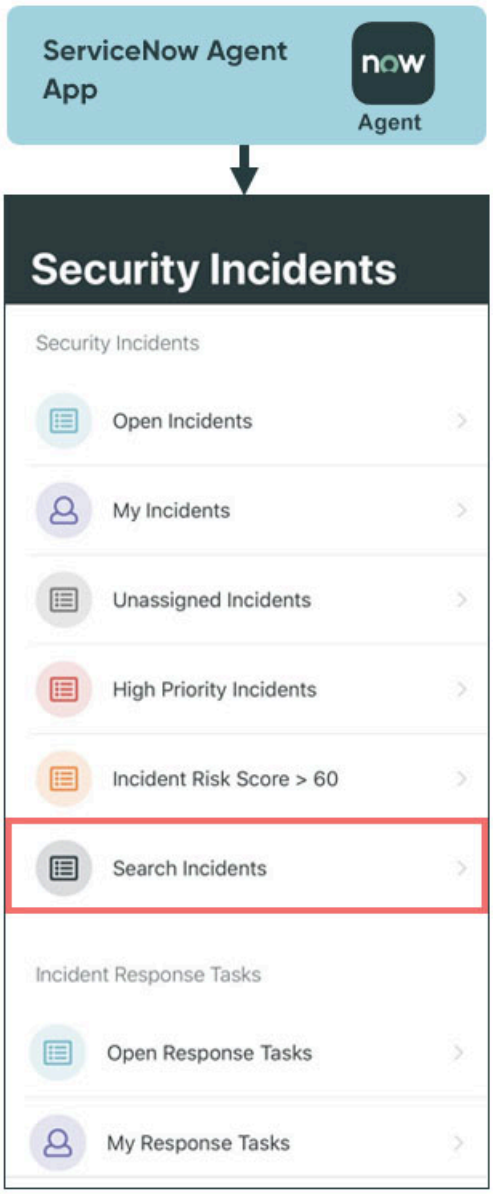
Time to complete this task: 5-10 minutes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **Search Incidents**.

   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent at any time to return to the last screen you had displayed.



3. To limit the number of search results that are returned, you may prefer to fill out as many fields on the form as you can.
   To add search criteria, refer to the following table. Follow the instructions after the table to edit existing search criteria, clear search criteria, or submit a search.

Tap this field	To add an entry on Android devices	To add and entry on iOS devices
Number	Enter an alpha-numeric value for a security incident, for	Enter an alpha-numeric value for a security incident, for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tap this field	To add an entry on Android devices	To add and entry on iOS devices
	example, SIR0010004. This number is displayed in the upper right of the security incident. The feature searches on numeric strings and partial numeric strings. For more refined searches, enter more digits. Wild cards (*) are not accepted. Tap a new field to enter more criteria or  to submit a search.	example, SIR0010004. This number is displayed in the upper right of the security incident. The feature searches on numeric strings and partial numeric strings. For more refined searches, enter more digits. Wild cards (*) are not accepted. Tap a new field to enter more criteria or **Search** to submit a search.
Short Description	Enter text in the field for example, `malware`. The feature searches on text strings and partial text strings from the Short Description field. For more refined searches, enter more text. Wild cards (*) are not accepted. Tap a new field to enter more criteria or  to submit a search.	Enter text in the field for example, `malware`. The feature searches on text strings and partial text strings from the Short Description field. For more refined searches, enter more text. Wild cards (*) are not accepted. Tap a new field to enter more criteria or **Search** to submit a search.
Priority	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search Incidents screen.
Category	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search Incidents screen.
State	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap the check mark icon to return to the Search Incidents screen.	To add an entry, tap one or more items or tap the search icon and type an entry in the search field. Tap **Done** to return to the Search Incidents screen.
Assigned to	Select one from the list or tap the search icon and type an entry in the search field.	Select one from the list or tap the search icon and type an entry in the search field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tap this field	To add an entry on Android devices	To add and entry on iOS devices
	To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.	To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.
Assignment group	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.	Select one from the list or tap the search icon and type an entry in the search field. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**.

For Android devices, with the Search Incidents screen displayed and all your criteria entered, choose one to continue.

Option	Description
Clear or modify search criteria prior to exe cuting a search	To clear all entered criteria, with the Search In cidents screen displayed, tap the back arrow to clear all the fields and return to the Securi ty Incidents landing screen. The search is not submitted and the search criteria are cleared. Alternatively, to edit a field: ○ With the Search Incidents screen dis played, tap a field with search criteria to ex pand it. ○ Tap an item to deselect it. Tap **All** to select all items. Tap **All** again to clear all items. To clear a value for the Assignment group and Assigned to fields, for no entry, select **None**. ○ Tap the check mark icon to save the changes and return to the Search Incidents screen.
Submit a search	With the Search Incidents screen displayed with your entered search criteria, tap the send icon ( ). The security incidents that match your search criteria are displayed. After the search is com pleted, the search criteria are not saved.

4. For iOS devices, with the Search Incidents screen displayed, choose one to continue.

Option	Description
Clear or modify search criteria prior to exe cuting a search	To clear all criteria and return to the landing screen, tap the close icon (X). Any entered

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	search criteria are not saved. Alternatively, to edit a field: ○ With the Search Incidents screen dis played, tap a field with search criteria to ex pand it. ○ Tap an item on the list to deselect it, or tap **Clear All**. To clear a value for the Assign ment group and Assigned to fields, for no entry, select **None**. ○ Tap **Done** to save the changes and return to the Search Incidents screen.
Submit a search	With the Search Incidents screen displayed with your entered search criteria, tap **Search**. The security incidents that match your search criteria are displayed. After the search is com pleted, the search criteria are not saved.

5. **Optional:** If your search returns multiple records, you can Filter records with the Security Incident Response Mobile app to refine the search results.

View, edit, and assign open response tasks with the Security Incident Response Mobile app

View, edit, and assign open response tasks. Your changes are saved on the Security Incident Response Task of the parent security incident.

Before you begin
Role required: sn_si.analyst

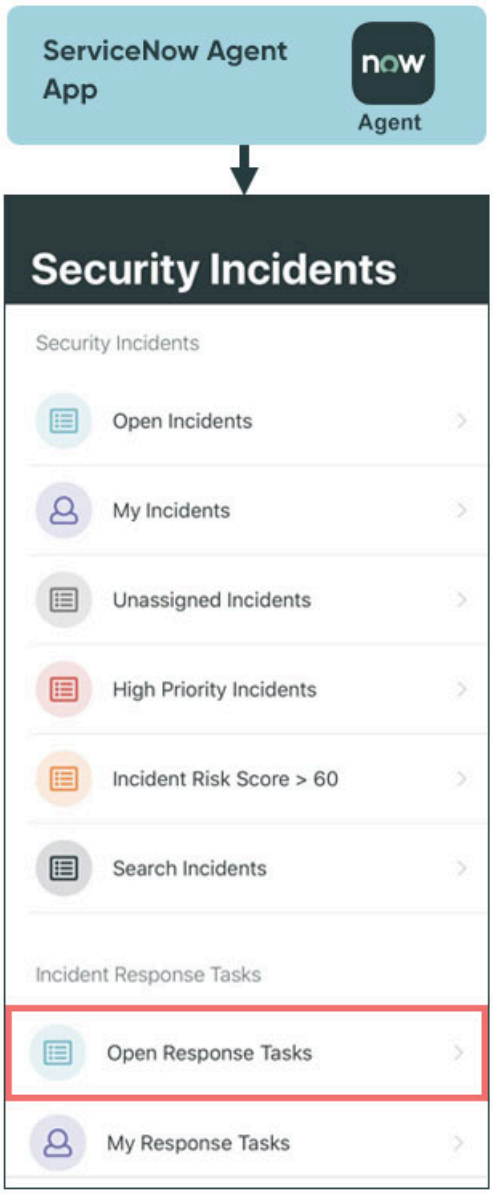
About this task
From the list of records, assign an open, unassigned response task to yourself or to another analyst in your group. Alternatively, view the details of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **Open Response Tasks**.

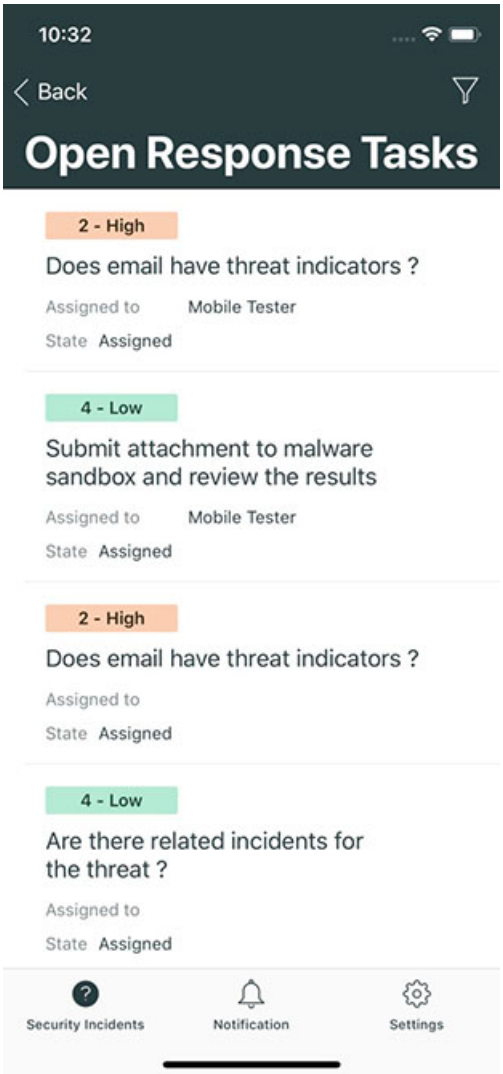
   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Open Response Tasks screen is displayed with a list of open tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for tasks that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

4. With the list of open response tasks displayed, to assign or reassign directly from the list, swipe left on a record to open the menu.

5. Choose one to continue.

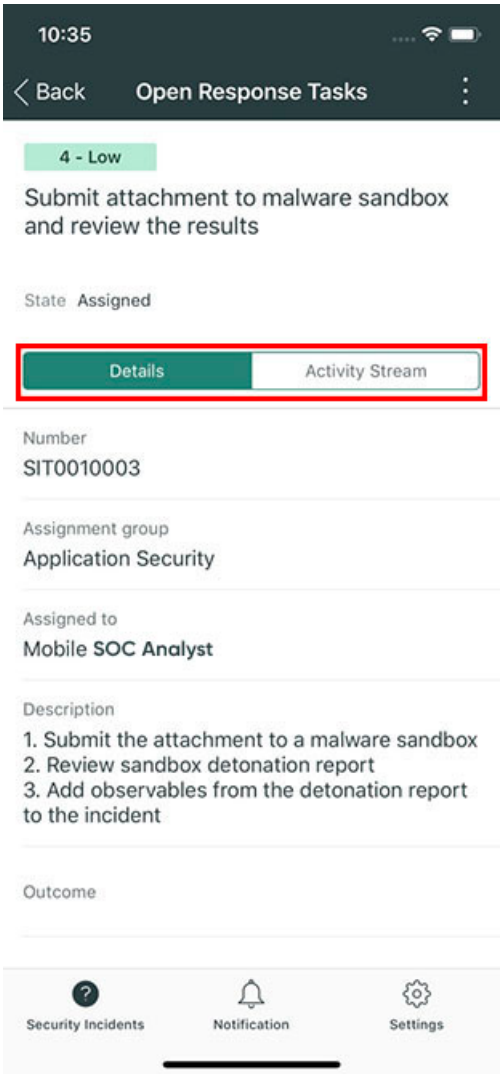
Option	Description
Assign to Me	Assign the response task to yourself. If the task is already assigned to you, this option is not displayed.
Reassign	To assign or reassign the assignment group: **a.** Tap **Assignment group** **b.** Tap a group from the list that is displayed, or enter text in the search field. The group must be a security-related assignment group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	To assign or reassign the task to a member of the assignment group: **a.** Tap **Assigned to** and **b.** Tap a name from the list that is displayed, or enter text in the search field. A message is displayed that confirms the record is updated. The task on the parent se curity incident is assigned to a new user and updated in your ServiceNow AI Platform in stance. Tap the send icon () or **Submit** to save and submit your changes.

6. Alternatively, to view the details of an open response task record, with the Open Response Tasks screen displayed, tap a record on the list.
7. With the tabs on the response task record displayed, choose one in the following table to continue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Option	Description
Details tab	With the Details tab selected, review the fields on the response task. To edit fields or assign the task, tap the menu icon ( ). From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Response Task screen displayed, tap a field to expand it and choose one or more of the options that are displayed. Alternatively, tap the search icon and enter text. ○ To reassign the task, tap **Reassign** or **As sign to Me**. After you complete your edits, tap the send icon ( ) or **Submit** to save your changes and update the record. The Security Incident Response Task on the parent security inci dent in your ServiceNow AI Platform instance is updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Activity Stream tab	With the Activity Stream tab selected, choose one to continue. ○ View the audit trail created by the Work notes on the record. To add a work note or attach a file, tap the plus icon (). ○ Tap the menu icon () to edit or reassign the task.
Screen icons at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ If displayed, tap an icon to open another ServiceNow® mobile app. ○ Tap **Notification** to view notifications for crit ical security incidents that are assigned to you or to your assignment group. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance. ▪ Log out of the current instance. To log out of a ServiceNow AI Platform instance on your device, with the details page dis played, tap **Logout**.

View, edit, and reassign your response tasks with the Security Incident Response Mobile app

View, edit, and reassign response tasks that are assigned to you. Your changes are saved on the Security Incident Response Task of the parent security incident.

Before you begin

Role required: sn_si.analyst

About this task

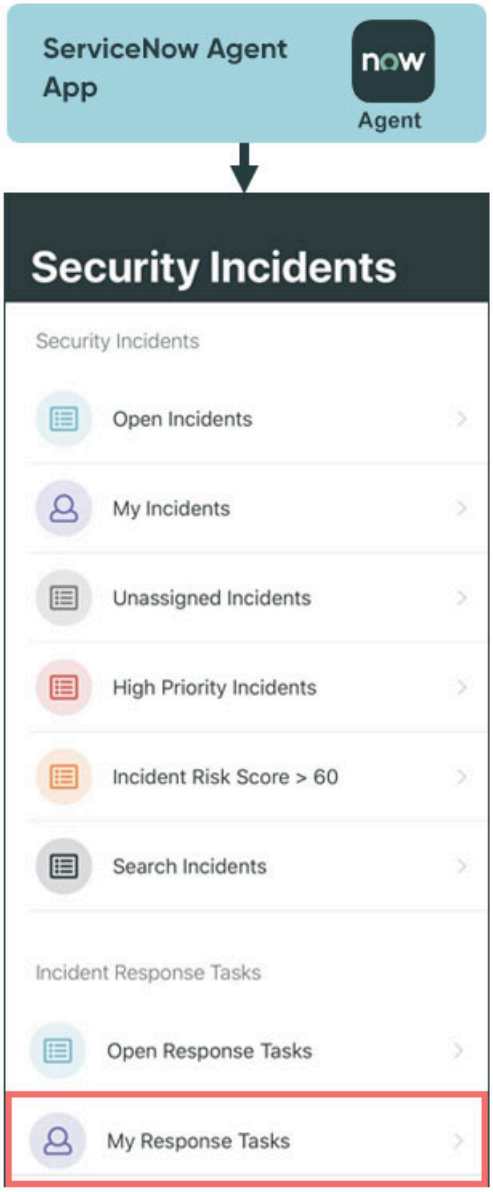
From the list of records, reassign an open response task that is assigned to you to another analyst in your group. Alternatively, view the details of the record or add a work note prior to reassignment. Time to complete this task: 5-10 minutes.

Procedure

1. If you are not logged in to your ServiceNow AI Platform instance on your mobile device, for more information see Log in to the Security Incident Response Mobile app.
2. With the Security Incidents landing screen displayed, tap **My Response Tasks**.

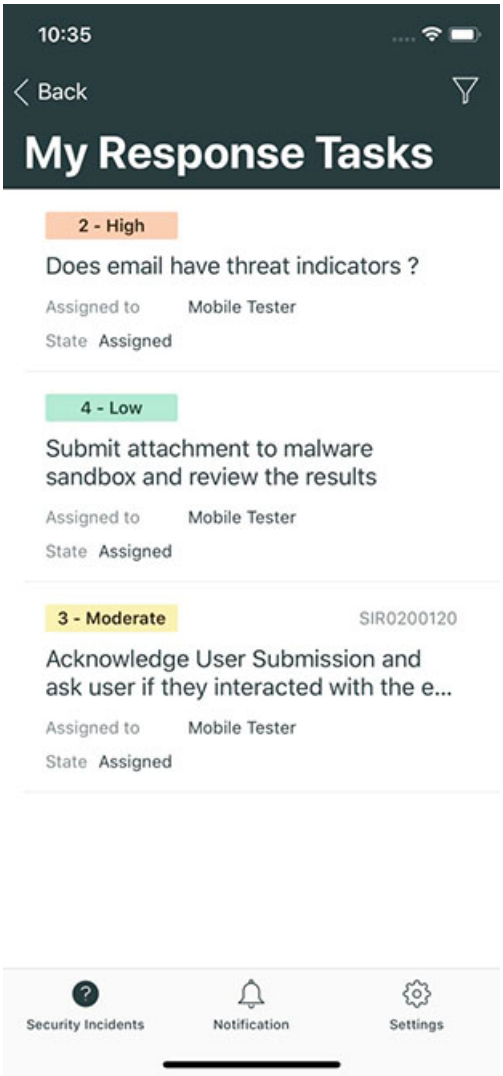
   If you navigate away from the Security Incident Response Mobile app after you have logged in, tap the Now Agent (Fulfiller) app at any time to return to the last screen you had displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The My Response Tasks screen is displayed with a list of the response tasks that are assigned to you.

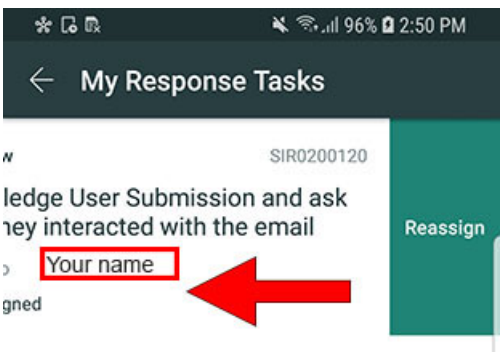
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. **Optional:** Refer to Search for security incidents with the Security Incident Response Mobile app to search for tasks that match specific criteria.

   Alternatively, with the filter icon ( ) displayed, Set filters to limit the number of records on the list. Filtering records on screens in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

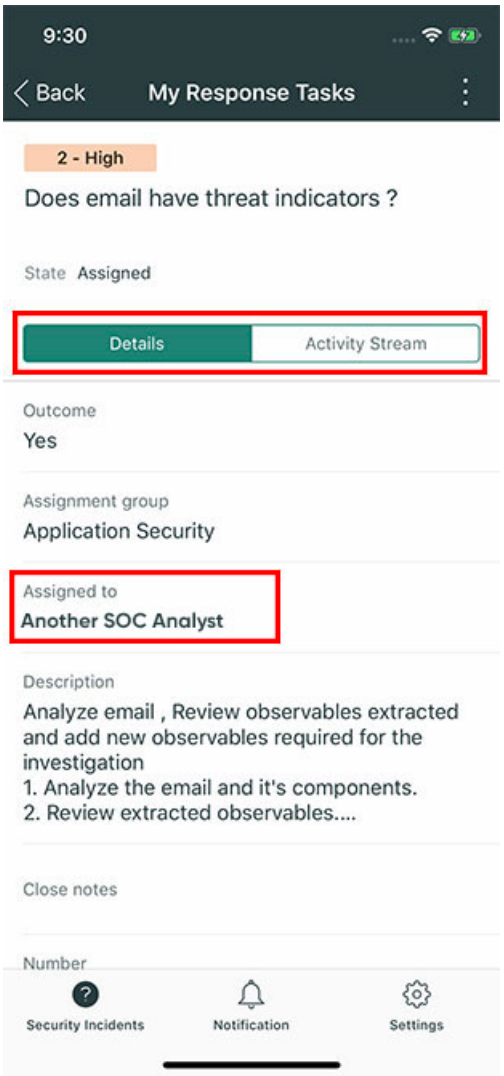
4. To reassign a task directly from the list of task records that are assigned to you, swipe left on a record to open the menu.



5. Tap **Reassign**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. On the Assign Response Task to Another screen that is displayed, tap a field to expand it and select another group or user for the task.
7. Tap the send icon ( ) or **Submit** to save your changes and update the response task.
   A message is displayed that confirms the record is updated. The task is assigned to a new user on the parent security incident and your ServiceNow AI Platform instance is updated.
8. To view the details of an open response task and to see the work notes, with the My Response Tasks screen displayed, tap a record on the list.
9. With the fields on the response task displayed, choose one in the following table to continue.



Option	Description
Details tab	With the Details tab selected, review the fields on the response task. To edit fields or reassign the task, tap the menu icon ( ). From the menu that is displayed, choose from the following options. ○ Tap **Edit**. With the Edit Response Task screen displayed, tap a field to expand it and choose one or more of the options that

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	is displayed. Alternatively, tap the search icon and enter text. ○ To reassign the task, tap **Assign to Another**. After you complete your edits, tap the send icon () or **Submit** to save your changes and update the record. The Security Incident Response Task on the parent security incident in your ServiceNow AI Platform instance is updated.
Activity Stream tab	With the Activity Stream tab selected, choose one to continue. ○ View the audit trail created by the Work notes on the task record. To add a work note or attach a file, tap (). ○ Tap () to edit or reassign the task.
Tap a screen icon at the bottom of the screen.	On the bottom of the screen, choose one to continue. ○ If displayed, tap another icon to open another ServiceNow® core application to open it. ○ Tap **Notification** to view notifications for critical security incidents that are assigned to you or to your assignment group. ○ Tap **Settings** and choose one to continue. ▪ View information about the ServiceNow AI Platform instance. ▪ Log out of the current instance. To log out of a ServiceNow AI Platform instance on your device, with the details page displayed, tap **Logout**.

Filter records with the Security Incident Response Mobile app

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the ServiceNow AI Platform.

Before you begin

Role required: sn_si.analyst

About this task

Time to complete this task: 5 minutes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon ().
2. With the Filters screen displayed, tap a field to expand it.
3. From the options that are displayed, tap the check box or tap an item for your filter.
   For many of the filters, you can select more than one option.
4. Tap the Back arrow () or **DONE** to save your changes to a field.
   The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap **RESET** to remove any filters and restore the default setting.
5. **Optional:** Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.
6. Tap the intersection icon  to create AND conditions.
   Alternatively, tap the intersection icon to create OR conditions.
7. After you have added all the criteria you want, with the Filters screen displayed, tap **DONE**.
   On the screen, only the records that match your filter criteria are displayed.

Security Incident Response Orchestration

Security Incident Response Orchestration activities allow users to interact with and retrieve data from Windows or UNIX-based systems and environments using workflow orchestration.

Set up Security Incident Response Orchestration

Prior to using Security Incident Response Orchestration, perform steps to set up various parts of the system, including populating the CMDB, configuring the mid-server, and configuring credentials.

Before you begin

Role required: admin

To use Security Incident Response, you need a fully populated CMDB with domain names. For more information, see Discovery.

About this task

Procedure

1. Activate Security Incident Response plugin.
2. Configuring MID Servers.
3. Configure Windows MID Server service credentials.

Understand Security Incident Response Orchestration workflows and workflow templates

The Security Incident Response base system includes a series of workflows and workflow templates designed to work with security incident records.

Before you begin

Role required: sn_si.basic

About this task

You can tailor all workflows and workflow templates to better suit your needs, assuming you have the appropriate role: sn_sec_cmn.admin. Workflows are used throughout the Security Operations system to perform a variety of tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Workflow templates, however, are triggered by selecting a value in the **Category** field in a security incident. When this occurs, the workflow template associated with the selection kicks off a workflow template that instructs the security analysts how to deal with a specific type of threat.

For example, if you select **Denial of Service** from the **Category** field in a security incident, the **Security Incident - Denial of Service - Template** is executed and the analyst is directed to determine whether the target of the DOS is business critical. If so, the next task causes the priority of the security incident to be set to **1 - Critical**, and then executes the next task. And so on.

So Security Incident Response workflows and workflow templates are essentially the same, except the templates are used for a specific set of functions within a security incident.

Procedure

1. Navigate to **All** > **Security Operations** > **Workflows** > **View Security Workflows**.
2. A list of the workflows and workflow templates shipped in the base system are displayed. Any new workflows that you have created in the Security Operations application suite are also included in the list.
3. Click the name of the workflow or workflow template you want to view.

Note: Workflows can be triggered in several different ways. Be aware that associating a workflow with a workflow trigger does not necessarily mean the workflow is active.

Security Incident Response Orchestration flows and actions

Several flows and actions are included with Security Incident Response Orchestration.

Create Lookup Request for IoC Changes Flow

The **Security Incident Response - Create Lookup Request for IoC Changes** flow is triggered by a business rule to run automatically when an IoC is added or changed. Malware scans are triggered only when new data is entered and only the new data is scanned.

Before you begin

Role required: sn_si.basic

About this task

If the IoC is empty, the flow does not run. Historical scans are retained and viewable in the **Security Scan Requests** tab and worknotes of the security incident. The existing security incidents are automatically updated.

Important:

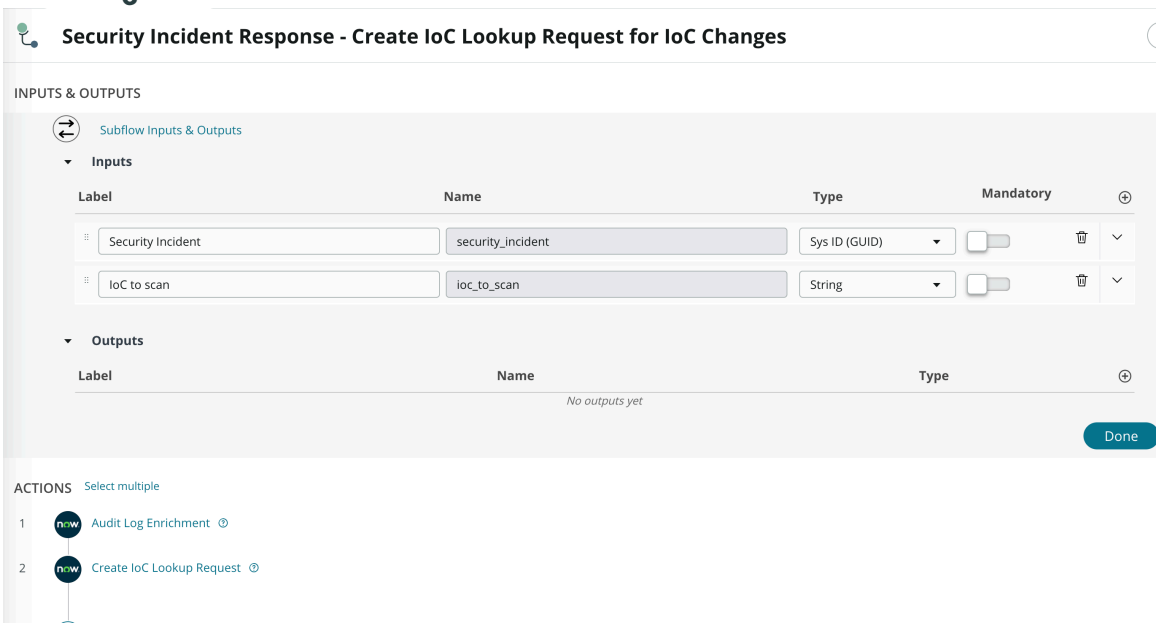
The **Security Incident Response - Create Lookup Request for IoC Changes** workflow is migrated to the Flow Designer. The flow gets triggered only when the sn_ti_scanner has at least one record.

The Flow Designer actions include:

- Audit Log Enrichment
- Create IoC Lookup Request Flow Action

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IoC Changes flow



Create IoC Lookup Request Flow Action

The **Create IoC Lookup Request** flow action can be used with any flow to create a malware lookup request for added or modified IoC fields.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Lookup request created.
Failure	Lookup request not created.

Input variables

Variable	Description
iocString	JSON formatted IoC information. IP, hash, url.
sild	Security incident system identifier

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
scnReqID	Lookup request identifier

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response- Get Network Statistics Flow

The **Security Incident Response** > **Get Network Statistics** flow retrieves the network statistics for an affected Windows-based resource when added to a security incident in the **Analysis** state.

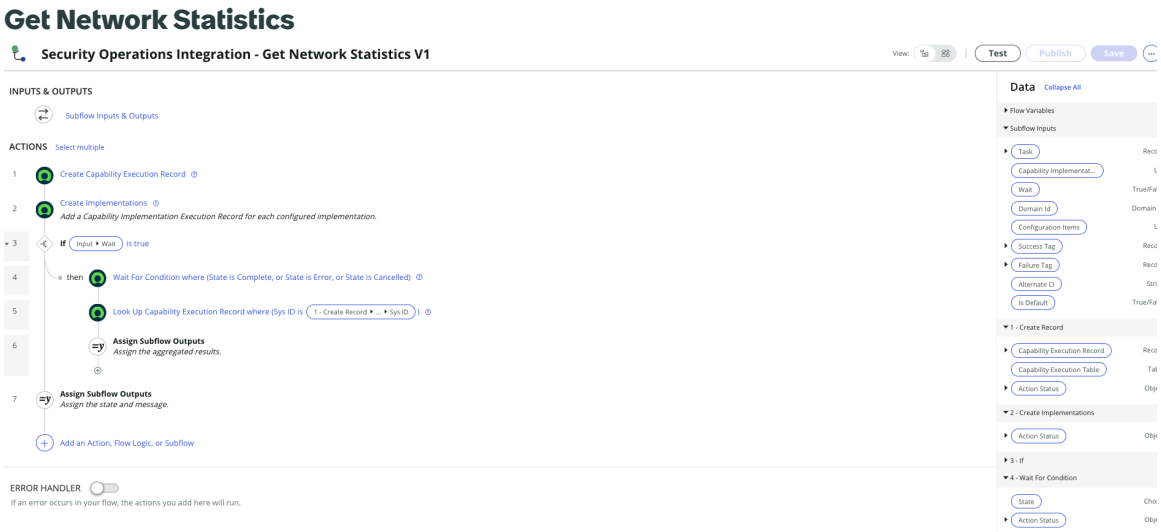
Before you begin

Role required: sn_si.analyst

About this task

For new security incidents that contain configuration items, the flow runs automatically when the state changes to **Analysis**.

Existing security incidents are automatically updated when you are in the **Analysis** state and you add a new configuration item.



The flow process actions include:

- Get Configuration Item FQDN Flow Action
- Determine Shell Script by OS
- If statement is executed by Powershell
- Execution Tracking - Begin Flow Action
- Get Network Statistics via netstat Flow Action
- Capability Execution Tracking- Failure Flow Action
- Create Enrichment Data records Flow Action
- Capability Execution Tracking- Failure Flow Action - Returns enrichment ID.

Procedure

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Response Orchestration provides network statistics information in the **Related Links** > **Security Incident Enrichments** tab. For more information see, Security Operations enrichment data mapping.

Actions specific to this flow are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

Security Incident Response - Get Running Services Flow

The **Security Incident Response - Get Running Services Flow** retrieves a list of running services from Windows-based, ServiceNow, configuration items (CIs). This flow is used for incident enrichment during investigations.

Before you begin

Role required: sn_si.analyst

About this task

The **Security Incident Response - Get Running Services Flow** runs automatically when you add a new configuration item to a Windows security incident after the state changes to **Analysis**. The information this flow obtains appears on the **Show Enrichment Data** tabs for the security incident.

Note: If the security incident remains in the **Draft** state, the **Security Incident Response - Get Running Services Flow** does not run.

The flow activities include:

Audit Log Enrichment Script flow action

Get Configuration Item FQDN Flow Action

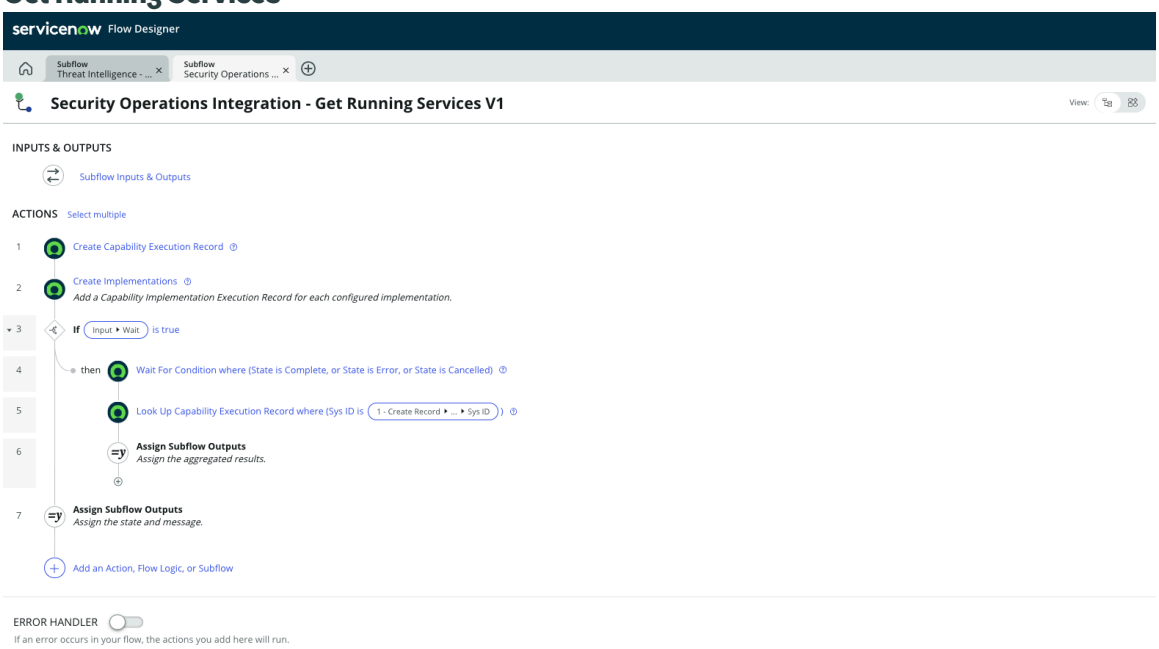
Determine Shell Script by OS Flow Action

Is Execution via PowerShell flow action

Get Running Services - WMI Enrichment activity

Create Enrichment Data records Flow Action

Get Running Services



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a Windows-based configuration item (server, laptop, or similar).
4. Click **Update**.
   Security Incident Response provides running services information in the **Related Links** > **Security Incident Enrichments**tab. For more information, see Security Operations enrichment data mapping.

Determine Shell Script by OS Flow Action

The Determine Shell Script by OS flow action determines which operating system to use in the flow.

The Determine Shell Script by OS flow action can be used with any flow to determine which shell script to run based on the operating system running on the system containing the configuration item.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Found operating system.
Failure	No operating system found. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
ciSysId	System identifier of the configuration item.
processType	Internal identifier that defines which script to pull from the table.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
processScript	ECC agent that gathers the running process.
executionTemplate	Determines whether the script is run through a probe or using PowerShell.
enrichmentMappingId	System identifier of the enrichment mapping used to transform the response data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get Running Services - WMI Enrichment

The **Security Incident Response - Get Running Services** flow gathers running services on a configuration item added to a security incident.

The **Get Running Services - WMI Enrichment** flow action is launched automatically to retrieve running services information for a Windows host.

Input variables

Input variables determine the initial behavior of the flow action.

Input variables

Variable	Description
target [string]	The fully qualified domain name (FQDN) of the target system.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response [string]	A JSON string representing the current running services on the target system. JSON data includes: **name** The name of the service **pid** The process identifier of the running service **service_type** (Optional) The type of running service. **start_name** The system name for the service **path** The file path of the running service executable **start_mode** The start mode of the running service. **display_name** The name of the running service as it appears to the user

Restrictions

The MID Server must support **PowerShell**.

SHA-256 hash requires PowerShell V4.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

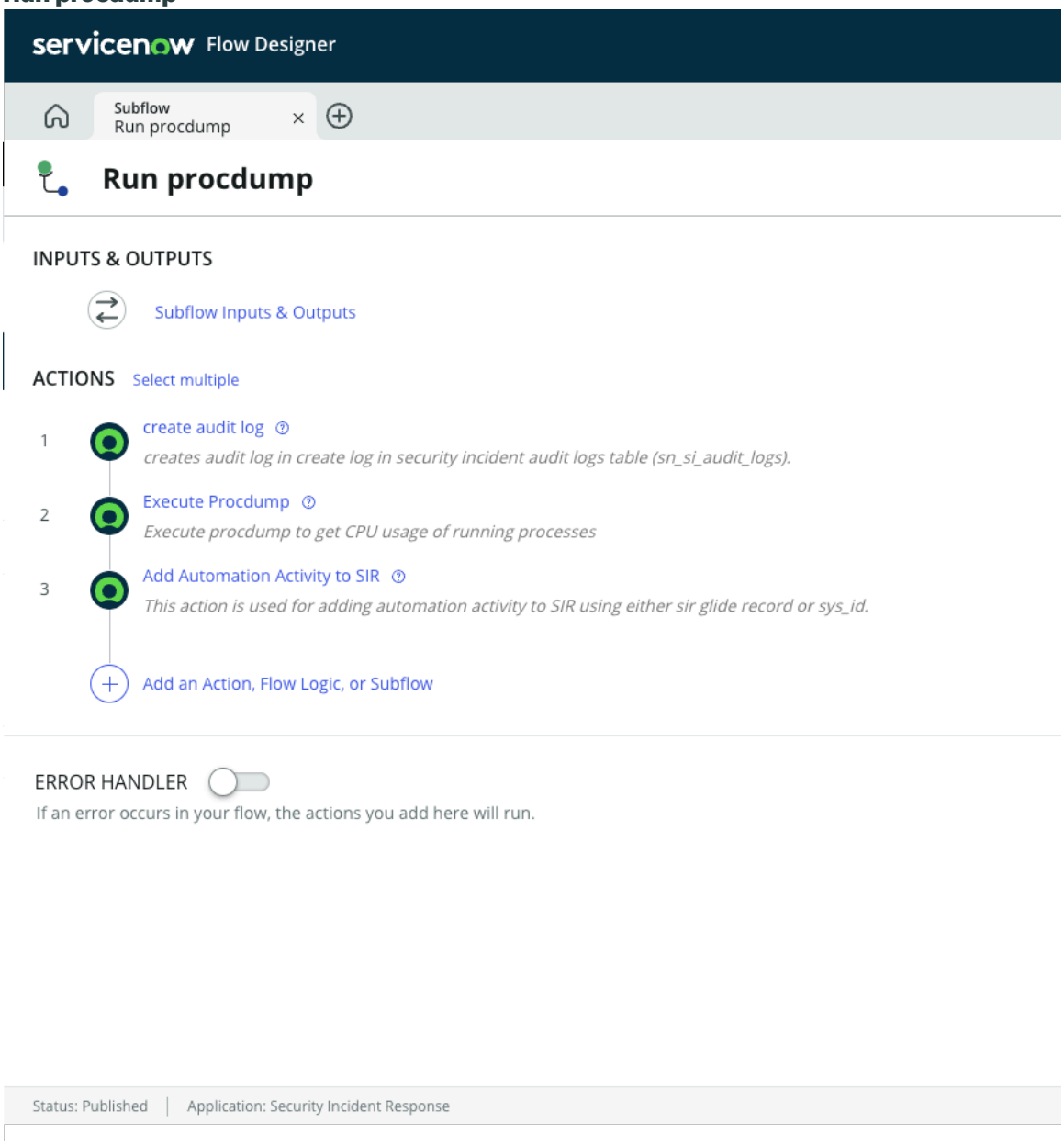
Run procdump flow

The **Run procdump** flow runs a process dump on a specified process and saves it to a file that can be targeted by security analysts.

Role required: sn_si.analyst

This flow is triggered when enriched processes are selected and a **Run procdump** UI action is executed.

Run procdump



Reasons the procdump can fail includes:

- Invalid dump path
- Invalid file share path
- Unable to fetch the fully-qualified domin name of the Windows machine the procdump is running on
- The process name is not specified

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The PROCDUMP environment variable not found
- A copy of the dump file fails to copy from the dump path to the file share path

Execute procdump action

Execute procdump is a powershell action that runs the procdump on the selected processes, dumps the data into a file, and posts it to a shared site on an internal network. An analyst can then view a deny listed process, highlighted in red in a security incident, and perform additional analysis on the file.

Results

Possible results for this action are:

Results

Result	Description
Success	The procdump executed successfully on the process_name, and the details are available in actionOutput.response.
Failure	The procdump failed to execute on the process_name, and the details are available in actionOutput.response.

Input variables

Input variables are used to create the requested outputs.

Input variables

Variable	Description
targetId	[Mandatory] The target ID to run the procdump on.
process_name	[Mandatory] The process name for the procdump.
dump_path	[Mandatory] The local file path to which the generated dump file will be saved.
dump_filename	[Mandatory] The filename of the file generated by the procdump. All special characters will be replaced with hyphens (-) from the dump file name when the file is generated.
file_share_path	[Mandatory] The file share path to which the dump file will be copied.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
share_path	The file share path to which the dump file was copied.
response	A JSON representation of the result of the procdump.
result	The result of the procdump.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident - Evaluate response task outcome workflow

Security Incident - Evaluate Response task outcome workflow determines the task to use, invokes a chosen workflow and evaluation script based on the outcome evaluator record provided as input to the chosen workflow.

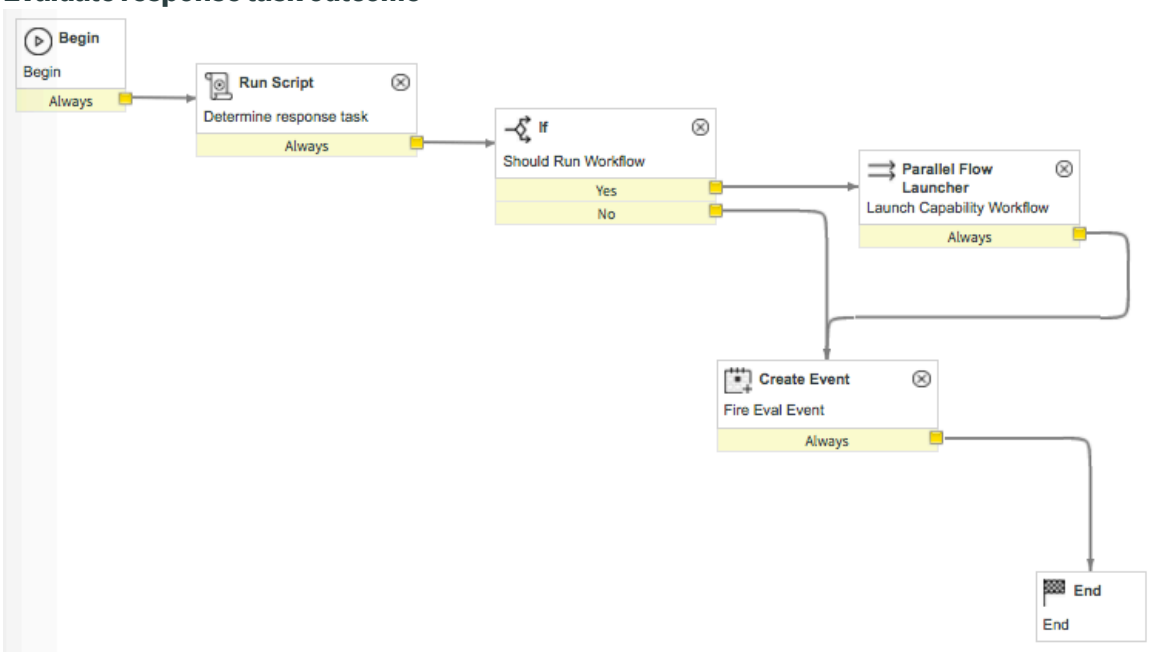
Before you begin
Role required: sn_si.write

About this task
This workflow is intended to run at the same time as the create task activity to be evaluated. The evaluation script queries the artifacts (such as sightings search records, or running processes) of the configured capability using context information from the response task (such as its parent security incident) to determine the appropriate outcome for the response task. The outcome could potentially be workflow activity dependent, but is generally **yes** or **no**. When creating an outcome evaluator record only capabilities that have a configured workflow, with the **Is task based capability** box checked, and a task input variable set are available to select.

Workflow process activities include:

- Run script to determine response task
- Should Run Workflow
- Parallel Flow Launcher Launch Capability Workflow
- Create Evaluation Event

Evaluate response task outcome



Threat Intelligence

The ServiceNow® Threat Intelligence application enables you to find indicators of compromise (IoC) and enrich security incidents with threat intelligence data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

Explore



Learn Threat Intelligence concepts and its key features.

Configure



Set up, learn the components installed, and user roles required to meet your business needs.

Administer



Set Threat Intelligence properties.

Integrate



Extend Threat Intelligence capabilities by integrating with ServiceNow and third-party applications.

Use



Manage Indicators of Compromise (IoC) and various artifacts.

MITRE ATT&CK Framework



Manage MITRE-ATT&CK framework quickly identify threats and coordinate cyberattack responses.

Security Case Management



Manage Security Case Management by gathering information on suspicious activities.

Learning resources

- Developer training
- Developer documentation
- Find components installed with an application

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Troubleshoot and get help

- Ask questions and explore other resources for Threat Intelligence in the ServiceNow Community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Understanding Threat Intelligence

The Threat Intelligence application allows you to access and provide a point of reference for your company's Structured Threat Information Expression (STIX™) data. Included in Threat Intelligence is the Security Case Management application, which provides a means for analyzing threats to your organization posed by targeted campaigns or state actors.

STIX is a language for describing cyber threat information in a standardized and structured manner. Using STIX data and Trusted Automated Exchange of Indicator Information (TAXII™) profiles, threat professionals can use shared cyber threat information to isolate threats that have been previously identified by your company and from other sources. TAXII makes widespread automated exchange of cyber threat information possible.

Threat Intelligence supports STIX versions 1.1, 2.0, and 2.1.

STIX™ and TAXII™ are trademarks of The MITRE Corporation.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Domain separation and Threat Intelligence

Domain separation is supported in the Threat Intelligence module that is available as part of Security Incident Response. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Includes **Basic** level support.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

Overview

In the Threat Intelligence module (as part of the Security Incident Response application), domain separation enables service providers (SPs) to create and manage the threat intelligence repository in the following ways:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Threat sources and Trusted Automated Exchange of Indicator Information (TAXII) profiles
- Observables
- Indicators of compromise
- Threat attack modes / methods and case management across the customer base they serve with lowered operational costs and a higher quality of service

Having separate customer work spaces for workflows, dashboards, reports, and so on, ensures that customer data is separated and never exposed to other clients.

Domain separation support in Threat Intelligence by version release

Domain separation for the Threat Intelligence module (as part of the Security Incident Response application) covers the following product functionality:

- Security incident observables are directed to the appropriate domain of the user whose ID/ Credential/ Scope generates the incident. The observables extracted from the incident are stored in the domain of the security incident.
- Setting up of TAXII service profiles to download one or more TAXII collections that offer cyber-threat information feeds. The configuration is stored in the domain under which the profile is being set up.
- Setting up the download of threat feeds into the IOC repository in the domain under which the configuration is being performed.
- Creation of attack mode/methods in the domain of the threat intelligence source that provides the information automatically or the domain under which a new attack mode/method is being added manually by the user
- Creation of cases for long-term investigation of incidents, observables, CIs, users, and indicators of compromise (IOC) associated with the case. The case is stored in the domain created by the user.

Note: In all the above cases, the overarching principles of visibility in separated domains in the ServiceNow AI Platform apply. As always, an incident in the parent domain can reference artifacts in the child domain, but not the other way around.

How domain separation works in Threat Intelligence (as part of Security Incident Response)

Threat Intelligence is part of Security Incident Response in the Professional and Enterprise Tiers, but not with the Standard Tier. Therefore a separate plugin is needed. The Threat Intelligence module (as part of the Security Incident Response application) creates and manages the threat intelligence information associated with security incidents in an organization. The following use cases are domain-separation aware:

- Creation of security incident observables at the time of incident creation
  - From email parsers (Platform-based, user-reported phishing, custom)
  - From applications in third-party Security Information and Event Management (SIEM) stores
  - Manually keyed in by the SOC analyst
- Collection of observables from threat feed sources - Threat intelligence sources from TAXII collections
- Manage security incident observables

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Associate observables with related indicators
  - Associate observables with security incidents
  - Associate observables with child observables
  - Associate observable to threat feed source
  - Add security annotations to observables
- Manage indicators of compromise
  - Associate indicators with related observables
  - Associate indicators with attack mode/method
  - Associate indicators with indicator types
  - Associate indicators to threat feed source
  - Add security annotations to indicators
- Manage cases
  - Create case (manually or from an incident)
  - Edit a new case to add details (choose case type and severity, add incidents, observables, configuration items, users, indicators)
  - Delete a case

Domain separation setup

Setting up domain separation for Threat Intelligence does not require any additional steps. All Threat Intelligence tables acquire the Domain column after the instance is domain separated.

Domain-separated data

Data can be domain separated, which means:

- Security incident observables in one domain cannot be viewed from the scope of other domains.
- Indicators of compromise in one domain cannot be viewed from the scope of other domains.
- Attack modes/methods associated with one domain cannot be viewed from the scope of other domains.
- TAXII service profiles associated with one domain cannot be viewed from the scope of other domains.
- Threat intelligence sources associated with one domain cannot be viewed from the scope of other domains.
- Cases associated with one domain cannot be viewed from the scope of other domains.

Threat Intelligence properties are set at the global level and are not, therefore, domain-separated. The settings include:

- The domain name to retrieve additional information for IP addresses/URLs
- The API key to be used for retrieval
- Lookup of local IoC tables before sending to remote scanner
- Number of days local observables are considered

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Marking an attack mode/method as inactive when not received from threat intel sources
- Marking an indicator as inactive when not received from any source for a specified number of days

Configuration

All aspects of the threat intelligence functionality configuration are self-contained in a domain-separated environment.

The following tasks can be configured per domain:

1. Creation of TAXII service profiles
   - Choose a Discovery service configuration
   - Choose a Collection service configuration - Assign roles to users and groups of users
2. Creation of threat intelligence sources
   - Configure the REST service that supplies the threat intel information
   - Schedule the download of threat intel information
   - Choose threat details information to assign to the source
3. Creation of attack mode/methods (manual)
   - Source, malware type, attack mechanism, threat actor type, description, handling, intended effect, first seen, last seen
   - Related indicators, child attack mode/method, associated security incidents

   Note: Attack modes/methods are auto-created from the threat feed sources as well.

4. Setting default lists for the following threat information categories:
   - Attack mechanisms
   - Discovery methods
   - Feeds
   - Indicator types
   - Intended effects
   - Notifications
   - Observable types
   - Rate limit definitions
   - Threat actor types
   - Attack motivations
   - Infrastructure types
   - Malware capabilities
   - Malware types
   - Report types
   - Threat actor roles
   - Tool types

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

How tenant domains manage their own application data

- Tenant domain owners can create their own TAXII service profiles.
- Tenant domain owners can create their own threat intelligence sources.
- Tenant domain owners can create their own attack mode/methods.
- Tenant domain owners can create their own default lists for threat information categories.

Note: Business logic and processes enable threat intelligence source download schedules to be domain separated by instance owner.

Related topics

Domain separation for service providers

Set up Threat Intelligence

Before you run Threat Intelligence in your instance, you must download it from the ServiceNow Store. You can also set up properties and define a threat source.

Install Threat Intelligence

Before you run Threat Intelligence in your instance, you must download it from the ServiceNow Store.

Before you begin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation and configuration.

Setup tasks	Description
Verify that you have the required ServiceNow roles for your instance.	The following roles are required for installation, configuration, and verification of expected results: • If not already assigned, the System Administrator [admin] installs the application and assigns the Threat Admin [sn_ti.admin] role. • The Threat Admin [sn_ti.admin] oversees configuration and verifies expected results.

Role required: admin

Procedure

Follow the instructions for downloading an application from the ServiceNow Store.

What to do next

Set Threat Intelligence properties.

Components installed with Threat Intelligence

Several types of components are installed with activation of the Threat Intelligence plugin, including tables and user roles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Roles installed

Role title [name]	Description	Contains roles
Threat Administrator [sn_ti.admin]	Has full control over all threat properties, SLAs, and notifications.	sn_ti.write
Threat Reader [sn_ti.read]	Has read access to threat information.	sn.sec_cmn.int_read
Threat Writer [sn_ti.write]	Has write access to threat information. Cannot delete attack modes, indicators nor observables. Only a Threat Administrator can delete them.	• sn_sec_cmn.int_write • sn_ti.read
MITRE Analyst [sn_ti.mitre_analyst]	This role enables read access to the MITRE-ATT&CK modules in Threat Intelligence and to the SIR module.	• sn_ti.read • sn_si.read

Tables installed

Table	Description
Attack mechanism [sn_ti_attack_mechanism]	Organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system.
Attack mode/method [sn_ti_attack_mode]	Attack modes and methods are representations of the behavior of cyber adversaries. They characterize what an adversary does and how they do it in increasing levels of detail.
Discovery method [sn_ti_discovery_method]	An expression of how an incident was discovered.
Feed [sn_ti_feed]	Used for configuring the Threat Feed (RSS) in the Threat Overview.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Indicator Attack mode/method [sn_ti_m2m_indicator_attack_mode]	Used to map attack modes/methods to indicators.
Indicator of Compromise [sn_ti_indicator]	Used to convey specific observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context.
Indicator of Compromise Metadata [sn_ti_indicator_metadata]	Used to populate TAXII records.
Indicator Source [sn_ti_m2m_indicator_source]	Used to collect all the sources reporting the specific indicator.
Indicator Type [sn_ti_indicator_type]	Characterizes a cyberthreat indicator made up of a pattern identifying certain observable conditions as well as contextual information about the patterns meaning, how and when it is acted on, and so on.
Associated Indicator Type [sn_ti_m2m_indicator_indicator_type]	Links indicators with their applicable types
Incident count [sn_ti_observable]	Number of security incidents associated with an observable.
Intended effect [sn_ti_intended_effect]	Used for expressing the intended effect of a threat actor.
IP Scan Result [sn_ti_ip_result]	Used to show the results of an IP lookup.
Malware Rate limit [sn_ti_rate_limit]	Defines a rate limit to be used on a lookup source.
Malware Scan [sn_ti_scan]	A lookup. Contains what to look up, with what look up source, and a summary of the lookup results.
Malware Scan Queue Entry [sn_ti_scan_q_entry]	A lookup record queued for lookup or processing. Facilitates the requests within stated rate limits.
Malware Scan Result [sn_ti_scan_result]	Displays the result of a lookup.
Malware Scanner	Defines third-party lookup sources to use in performing lookups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
[sn_ti_scanner]	
Malware Scanner Rate Limit [sn_ti_scanner_rate_limit]	Associates a lookup source with a rate limit.
Malware Type [sn_ti_malware_type]	Used for expressing the types of malware instances.
Observable [sn_ti_observable]	Observables in STIX represent stateful properties or measurable events pertinent to the operation of computers and networks.
Observable Context Type [sn_ti_observable_context_type]	Stores the context (source, destination of an IP address, and so forth) for an observable.
Observable Indicator [sn_ti_m2m_observable_indicator]	Used to relate observables to indicators.
Observable Source [sn_ti_observable_source]	Used to relate observables to threat sources.
Observable Type [sn_ti_observable_type]	Lists the various types of observables, such as IP addresses.
Observable Type Category [sn_ti_observable_type_category]	Stores the first categorization of observables (for example, IP addresses and URLs). It is used for more accurately determining observable types.
Related attack mode/method [sn_ti_m2m_attack_mode_attack_mode]	Used to relate attack modes to each other.
Related Observables [sn_ti_m2m_observables]	Used to relate observables to each other.
Scan type [sn_ti_scan_type]	The definition of a lookup type, with initial records for File, URL, and IP.
Security Case [sn_ti_case]	Stores security case records created using Case Management.
Security Case IoC [sn_ti_case_ioc]	Used to manage the relationship between observables and cases.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Security Case Related Task [sn_ti_m2m_case_task]	Used to manage the relationship between tasks (security incidents, change requests, and so forth) with security cases.
Security Case Relationship Exclusion [sn_ti_case_relationship_exclusion]	Provides the definition of inclusion and exclusion of related records in security cases.
Sighting [sn_ti_sighting]	The m2m link between the observable and the Sightings Search detail result used in the execution of a Sighting Search request.
Sighting Configuration Items [sn_ti_m2m_sighting_ci]	Maps configuration items to a Sightings Search.
Sighting Search Detail [sn_ti_sighting_search_detail]	Details of a Sighting Search for example the number of internal external items found.
Sighting Search Result [sn_ti_sighting_search]	The header for a Sightings Search execution.
Supported Observable Types [sn_ti_m2m_ind_type_obs_type]	Relates indicator types to valid observable types.
Supported Scan Type [sn_ti_supported_scan_type]	Maps the lookup type to a lookup source/ vendor-specific implementation. Indicates that a specific lookup source supports the type.
Task Attack mode/method [sn_ti_m2m_task_attack_mode]	Relates attack modes to tasks.
Task Indicator [sn_ti_m2m_task_indicator]	Relates indicators to tasks.
Task Observable [sn_ti_m2m_task_observable]	Relates observables to tasks.
Task Sighting [sn_ti_m2m_task_sighting]	Stores task records (security incidents and cases) related to a sighting record.
TAXII Collection [sn_ti_taxii_collection]	Defines a cyber-risk intelligence feed that can be imported by a TAXII server.
TAXII Profile [sn_ti_taxii_profile]	Defines a repository for sharing cyber-risk intelligence. Contains TAXII collections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Threat Actor type [sn_ti_threat_actor_type]	Provides characterizations of malicious actors (or adversaries) representing a cyber attack threat, including presumed intent and historically observed behavior.
Threat Intelligence Source [sn_ti_source]	Defines a source for importing threat data.
Associated Attack Motivation [sn_ti_stix2_m2m_object_attack_motivation]	Collects all attack motivations associated with a STIX Object.
Associated Infrastructure Type [sn_ti_stix2_m2m_infra_type]	Links infrastructure with their types.
Associated Kill Chain Phase [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Links kill chain phases to indicators.
Associated Kill Chain Phase [sn_ti_stix2_m2m_object_kill_chain_phase]	Links kill chain phases to STIX objects.
Associated Malware Capability [sn_ti_stix2_m2m_malware_capability]	Links malware with their capabilities.
Associated Malware Type [sn_ti_stix2_m2m_malware_malware_type]	Links malware with their types.
Associated Observable [sn_ti_stix2_m2m_malware_observable]	Collects all observables associated with a malware.
Associated Observable [sn_ti_stix2_m2m_observed_data_observable]	Collects all observables associated with an observed data.
Associated Report Type [sn_ti_stix2_m2m_report_report_type]	Links threat reports with their types.
Associated Threat Actor Role [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Links threat actors with their roles.
Associated Threat Actor Type [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Links threat actors with their types.
Associated Tool Type [sn_ti_stix2_m2m_tool_tool_type]	Links tools with their types.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Attack Motivation [sn_ti_stix2_attack_motivation]	Attack Motivation shapes the intensity and the persistence of an attack. Threat Actors and Intrusion Sets usually act in a manner that reflects their underlying emotion or situation, and this informs defenders of the manner of attack.
Attack Pattern [sn_ti_stix2_attack_pattern]	A TTP type that describes methods that adversaries use to attempt to compromise targets.
Campaign [sn_ti_stix2_campaign]	A grouping of adversarial behaviors that describe a set of malicious activities or attacks (sometimes named as waves) that occur over a period against a specific set of targets.
Course of Action [sn_ti_stix2_course_of_action]	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to intelligence.
External Reference [sn_ti_stix2_external_reference]	Pointers to information represented outside of STIX.
Identity Sighting [sn_ti_stix2_m2m_sighting_identity]	Collects all Identities associated with a Sighting.
Identity [sn_ti_stix2_identity]	Actual individuals, organizations, or groups (example ACME, Inc.) as well as classes of individuals, organizations, systems, or groups (example the finance sector).
Indicator External Reference [sn_ti_stix2_indicator_external_reference]	Represents external references associated with indicators.
Indicator Sighting [sn_ti_stix2_indicator_sighting]	Represents sightings of indicators.
Infrastructure Type [sn_ti_stix2_infrastructure_type]	Represents the various infrastructure types.
Infrastructure [sn_ti_stix2_infrastructure]	A TTP type that describes any systems, software services, and any associated physical or virtual resources, intended to support some purpose (example C2 servers used as part of an attack, device, or server that are part of defense, database servers targeted by an attack, and the like).
Installed software [sn_ti_stix2_m2m_malware_analysis_sw]	Collects all software (SCO software types) associated with a malware analysis.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Intrusion Set [sn_ti_stix2_intrusion_set]	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
Kill Chain Phase [sn_ti_stix2_kill_chain_phase]	Represents kill chain phases associated with a kill chain.
Kill Chain [sn_ti_stix2_kill_chain]	Represents various kill chains.
Location [sn_ti_stix2_location]	Represents a geographic location provided through STIX.
Malware Analysis [sn_ti_stix2_malware_analysis]	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
Malware Capability [sn_ti_stix2_malware_capability]	Represents common capabilities that a malware family or instance exhibits.
Malware Operating System [sn_ti_stix2_m2m_malware_operating_system]	Collects all Operating Systems (SCO software types) associated with malware.
Malware [sn_ti_stix2_malware]	A TTP type that represents malicious code.
Marking Definition [sn_ti_stix2_marking_definition]	Represents handling or sharing requirements for STIX Objects.
Object Sighting [sn_ti_stix2_object_sighting]	Represents sightings of STIX Objects.
Object-Indicator Relationship [sn_ti_stix2_m2m_object_indicator]	Collects all relationships between STIX objects and STIX indicators.
Object-Object Relationship [sn_ti_stix2_m2m_object]	Collects all relationships between STIX Objects and other STIX objects excluding the indicators.
Object-Observable Relationship [sn_ti_stix2_m2m_object_observable]	Collects all relationships between STIX observables and STIX objects.
Observed Data Sighting [sn_ti_stix2_m2m_sighting_observed_data]	Collects all the observed data objects associated to a sighting.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Observed Data [sn_ti_stix2_observed_data]	Conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-Observable Objects (SCOs).
Report Type [sn_ti_stix2_report_type]	Represents primary purpose or subject of Threat Reports.
Reported Observable [sn_ti_stix2_m2m_malware_analysis_observable]	Collects all observables associated to Malware Analysis.
STIX V2 Object [sn_ti_stix2_object]	Common parent table for STIX Object.
STIX V2 Sighting [sn_ti_stix2_sighting]	Common parent table for STIX sighting tables.
Threat Actor Role [sn_ti_stix2_threat_actor_role]	Represents roles that can be played by threat actors.
Threat Actor [sn_ti_stix2_threat_actor]	Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent.
Threat Grouping [sn_ti_stix2_threat_grouping]	Groups all the STIX Objects that share some common context.
Threat Note [sn_ti_stix2_threat_note]	Provides context and additional analysis not contained in the corresponding STIX Object.
Threat Opinion [sn_ti_stix2_threat_opinion]	Provides assessment of accuracy of information in a STIX object produced by a different entity.
Threat Report [sn_ti_stix2_threat_report]	Reports are collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details. They are used to group-related threat intelligence together to publish as a comprehensive cyber threat story.
Tool Type [sn_ti_stix2_tool_type]	The categories of tools that can be used to perform attacks.
Tool [sn_ti_stix2_tool]	Tools are legitimate software that is used by threat actors to perform attacks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Description
Vulnerability [sn_ti_stix2_vulnerability]	Represents weakness or defect in the requirements, designs, or implementations of the computational logic (example code) found in software and some hardware components (example firmware). They can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

Set Threat Intelligence properties

Threat Intelligence properties allow you to control how different aspects of the system function, including the setting of API keys.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Administration** > **Properties**.
2. Set the following properties, as needed.

Properties for Threat Intelligence

Property	Description
The domain name to retrieve additional information for IP addresses/URLs sn_ti.ip_lookup.web_site	The domain name to use for retrieving additional information into your IoC database. This property is used by the `ThreatAdditionalInfo` script include to populate additional information on the Observables form. Default value: http://api.ipinfodb.com/v3/ip-country/ **Note:** The pinfodb.com third-party API is available at no extra charge and used in many commercial software programs. If you replace it with a different domain name, you must also provide the API key in the next field.
The API key to be used for the domain, if any sn_ti.ip_lookup.api_key	The API key to use for retrieving additional information into your IoC database. This property is used (along with the sn_ti.ip_lookup.web_site property) by the `ThreatAdditionalInfo` script include to populate additional information on the Observables form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
Do not run automated threat lookup on an observable when the observable is associated with an IoC or found to be malicious. sn_ti.scan_ioc_before_sending **Note:** You need to define the duration in the next property (sn_ti.scan_ioc_num_days).	Option to stop running the automated threat lookup on an observable when the observable is found to be malicious or associated with an IoC for the configured duration (in days). If you still need to run the threat look up for the observable, you can do it manually. Default value: Yes
Duration (in days) sn_ti.scan_ioc_num_days	Option to define the duration until which the automated threat lookup of the observable is skipped. Default value (in days): 30
Do not run automated threat lookup on an observable if already run. sn_ti.enable_threat_lookup_bypass **Note:** You need to define the duration in the next property (sn_ti.threat_lookup_bypass_times).	If there is a threat lookup result for an observable already available, then you have an option to skip the rerun of the automated threat lookup for the same observable until the configured duration has passed. Default value: No **Note:** If you're enabling this property, make sure that you are adding an appropriate value.
Duration (in minutes) sn_ti.threat_lookup_bypass_time	Option to define the duration after which the automated threat lookup of the observable can be rerun. Default value (in minutes): 0
Set a validity duration for user overrides on observable finding. sn_ti.enable_observable_finding_system_override **Note:** You need to define the validity in the next property (sn_ti.observable_finding_override_expiry).	Option to set a validity duration for user overrides on the observable findings. Threat lookup finding of the observable will not be changed by the base system during this validity duration. Default value: No. **Note:** If you're enabling this property, make sure that you are adding an appropriate value.
Validity (in minutes) sn_ti.observable_finding_override_expiry	Option to define the validity period of the observable finding. Default value (in minutes): none

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
When an attack mode/method has not been received from any source for the specified number of days, mark it as inactive sn_ti.attack_mode_inactivate_days	Number of days from when an attack mode/method was last received for the record to be marked inactive. Default value: 360 **Note:** The **Active** check box is not visible on the **Attack mode/ method** form by default. However, you can add it. When attack modes/methods are inactive, they cannot be selected on other forms.
When an indicator has not been received from any source for the specified number of days, mark it as inactive sn_ti.indicator_inactivate_days	Number of days from when an indicator was last received for the record to be marked inactive. Default value: 180 **Note:** The **Active** check box is not visible on the **Indicator** form by default. However, you can add it. When indicators are inactive, they cannot be selected on other forms.
The maximum payload size (in MB) for a STIX attachment that can be parsed. sn_ti.stix.max_payload_size	Specifies the maximum payload size for the STIX attachment that you can parse. Default value: none Maximum allowed value: No limit.
Maximum time in seconds an outbound HTTP connection waits to fetch TAXII collection data sn_ti.taxii.http.max_timeout	Specifies the maximum amount of time an outbound HTTP connection waits before fetching the next packet of TAXII collection data. Default value: 300
Maximum number of objects retrieved in one REST call from a TAXII server (Applicable only for TAXII versions 2.0 and 2.1) sn_ti.taxii.max_page_size	Specifies the maximum number of objects retrieved in one REST call from the TAXII server for one page. Default value: 5000 Maximum allowed value: 50000
Maximum number of retries for a failed TAXII 2.X REST call sn_ti.taxii2.retry_count	Specifies the maximum number of retries for a failed TAXII REST call.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
	Default value: 3

3. Click **Save**.

Define a threat source

You can maintain a list of Threat Intelligence threat sources. Each source includes the ability to define how often a source is queried. You can also execute a threat source on demand to import the needed Structured Threat Information eXpression (STIX) data.

Before you begin

Role required: sn_ti.admin

About this task

Threat Intelligence employs two technologies for importing threat-related information: STIX and Trusted Automated Exchange of Indicator Information (TAXII).

STIX provides a standardized, structured language for representing an extensive set of cyberthreat information that includes indicators of compromise (IoC) activity (for example, IP addresses and file hashes), as well as contextual information regarding threats, such as attack modes/methods, that together more completely characterize the motivations, capabilities, and activities of a cyber adversary. As such, STIX data provides valuable information on how your organization can best to defend against cyberthreats.

Trusted Automated Exchange of Indicator Information (TAXII) is used to facilitate automated exchange of cyberthreat information. TAXII defines a set of services and message exchanges that enable sharing of actionable cyberthreat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyberthreats. TAXII profiles can be set up as repositories for sharing STIX-formatted information. Each profile contains one or more TAXII collections or feeds.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Sources** > **Threat Sources**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the threat source.
Application	The application that contains this record.
Active	Select this check box to activate the threat source.
Advanced	Select this check box to display the scripts in the **Integration factory script** and **Report processor** fields.
Description	A description of this threat source.

4. Fill in the fields in the **Schedule** section, as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Run	The frequency you want the integration to run, Daily, Weekly, Periodically, and so on. As noted, subsequent fields are displayed based on the setting of this field.
Day	The day you want the integration to run. ○ If you selected **Weekly** in the **Run** field, this field displays the days of the week. ○ If you selected **Monthly** in the **Run** field, this field displays the days of the month.
Time	The time you want the integration to start.
Repeat Interval	If you selected **Periodically** in the **Run** field, this field displays the number of days, and hours before the integration runs again.
Starting	If you selected **Periodically** in the **Run** field, this field displays the dates, and time to be used as the starting point for periodic updates.
Conditional	Select this field if you want to add conditional parameters.
Condition	If you selected the **Conditional** check box, enter the conditions here.

5. Fill in the fields in the **Threat Details** section, as appropriate.

Field	Description
Indicator	The indicator to use when the data doesn't explicitly provide one. For blocklists, if empty, a new indicator is created for each observable.
Indicator type	The indicator type to use for indicators that are created and the data doesn't explicitly provide an indicator type.
Attack Mode/ Method	The attack mode/method to use when the data doesn't explicitly provide one.
Observable Type	The observable type to use for observables that are created and the data doesn't explicitly provide an observable type.[SI1]
Weight	Enter a weight value for this source to be used in the confidence calculation.

Note: The usage of the **Indicator**, **Indicator Type**, **Attack Mode/Method**, and **Observable Type** fields are implementation-specific. The default processor, SimpleBlocklistProcessor, behaves as the tooltips describe. However, a TAXII threat source is fully data driven. Any custom threat source processor would be able to use its own strategy. These fields are basically items to expose to the integration/processor and the implementation decides how to use them.

6. Fill in the fields in the **Source Details** section, as appropriate.

Field	Description
Endpoint	Enter the web service endpoint URL where the threat source is accessed by Threat Intelligence. Click the lock icon to lock the URL.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Use REST Message	If you need a REST message to access the threat source, select this check box. The **REST message** and **REST method** fields become required.
REST message	Click the lookup icon, and select the REST message from the list or click **New** to define a new REST message.
REST method	Click the lookup icon, and select the REST method from the list or click **New** to define a new REST method.
Integration script	The default integration script is **SimpleRESTSecurityDataIntegration**. It runs a simple REST call, saves the response as an attachment, and then returns the attachment to the processor. This script meets the needs of most organizations. But if you want, you can click the lookup icon, and select a different integration script or define a new one.
Integration factory script	If the **Advanced** check box is selected, this field displays the actual script for constructing the integration script. You can edit the script as needed. This ability is useful for custom implementations. Integrations in the base system usually don't need any custom constructor logic.
Report processor	The default integration script is **SimpleBlocklistProcessor**. This script is a simple processor that accepts a simple blocklist (simple, meaning a single column document with observables such as URLs or IP addresses) and creates observables. It uses the various **Threat Details** fields to determine which fields to set when observables are created.
Processor factory script	If the **Advanced** check box is selected, this field displays the actual script for constructing the processor. You can edit the script as needed. This script is generally useful for custom implementations. The integrations in the base system usually don't need custom constructor logic.

7. Click **Submit**.

Note: For more information on how to configure the threat source's pagination, see KB1213825 article.

Create a TAXII profile

You can maintain TAXII profiles for sharing STIX-formatted information. Each profile contains one or more TAXII collections or feeds.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Sources** > **TAXII Profiles**.
2. Click **New**.
3. Complete the following fields as appropriate.

Field	Description
Name	The name of the TAXII profile

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Application	The application that contains this record.
Use REST messages as template	If you require a REST message to access the TAXII profile, select this check box.
TAXII Version	Specify the TAXII version. The supported STIX versions are 1.1, 2.0, and 2.1.
Description	A description of this TAXII profile.

4. Fill in the fields in the **Discovery Service Configuration** section, as appropriate.

Field	Description
Discovery Service endpoint	Discovery Endpoint authorizes clients to ob tain information about a TAXII Server and get a list of API Roots.
Use REST message	Select this option if you require a REST mes sage to access the TAXII profile. The **Dis covery Service REST message** and **Discov ery Service REST method** fields become re quired.
Discovery Service REST message	Click the lookup icon, and select the REST message from the list or click **New** to define a new REST message.
Discovery Service REST method	Click the lookup icon, and select the REST message from the list or click **New** to define a new REST method.

5. Fill in the fields in the **Collection Service Configuration** section, as appropriate.

Field	Description
Collection Info Service endpoint	A TAXII Collection is an interface to a logical repository of CTI objects provided by a TAXII Server and is used by TAXII Clients to send in formation to the TAXII Server or request infor mation from the TAXII Server. A TAXII Server can host multiple Collections per API Root, and Collections are used to ex change information in a request–response manner.
Use REST message	Select this option if you require a REST mes sage to access the TAXII profile. The **Collec tion Info Service REST message** and **Col lection Info Service REST method** fields be come required.
Collection Info Service REST message	Click the lookup icon, and select the REST message from the list or click **New** to define a new REST message.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Collection Info Service REST method	Click the lookup icon, and select the REST message from the list or click **New** to define a new REST method.

6. Click **Submit**.

IoC Repository

IoC repository contains STIX objects, each of these objects contain a specific piece of information.

When you combine STIX objects together through relationships, you allow for easy or complex representations of Cyber Threat Intelligence (CTI).

Threat Intelligence supports STIX versions 1.1, 2.0, and 2.1.

Attack modes and methods

Attack modes and methods, sometimes referred to as Tactics, Techniques, and Procedures (TTPs), are representations of how cyber adversaries behave. They characterize what these adversaries do and how they do it, in increasing levels of detail. Attack modes and methods apply for STIX 1.1.

For example, an attack mode/method might be to use malware to steal credit card credentials. Or another, related tactic (at a lower level of detail) might be to send targeted emails with attachments that contain malicious code, which executes upon opening, captures credit card information from keystrokes, and uses http to communicate with a command and control server to transfer information.

Attack modes and methods apply for STIX 1.1.

Define an attack mode/method

Attack modes and methods are imported with STIX data, but you can add new modes/methods, as needed.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Attack Mode/Method**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Select classification tag	If you set up and activated classification tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the attack mode/method. If you did not set up or activate classification tags, this drop-down list is not displayed.
Title	Enter a descriptive name for this attack mode/method.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Malware Type	Select the malware type for this attack mode/method. The available malware types are retrieved from the vendor server as STIX data.
Source	Select the threat data source for this attack mode/method. Some data sources are included with the base system. You can create new data sources as needed.
Attack mechanism	Select the attack mechanism for this attack mode/method. Attack mechanisms represent the different techniques used to attack a system. The available attack mechanisms are retrieved from the vendor server as STIX data.
First Seen	This date is retrieved from the vendor server as STIX data.
Last Seen	This date is retrieved from the vendor server as STIX data.
Threat Actor Type	Select the threat actor type for this attack mode/method. Threat actor types characterize malicious actors (or adversaries) representing a cyber attack threat, including presumed intent and historically observed behavior. The available threat actor types are retrieved from the vendor server as STIX data.
Description	Enter a description of the attack mode/method.
Handling	Enter instruction for how to handle this attack mode/method.
Intended effect	Enter the intended effect of this type of attack.

4. Right-click in the form header and click **Save**.
   You can view any of the following related lists to view additional information.

Related List	Description
Related Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source.
Child Attack mode/method	Lists attack modes/methods that are children of the parent attack mode/method.
Associated Tasks	Lists changes associated with the parent attack mode/method.

Add an IoC to an attack mode/method

In addition to importing indicators as STIX data, you can add IoCs to an attack mode/method manually.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Attack Mode/Method**.
2. Click the attack mode to which you want to add an IoC.
3. Click the **Related Indicators** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the IoC you want to add.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Using the slushbucket, add the IoC to the **Related Indicators** list.
7. Click **Save**.

Add a related attack mode method

In addition to importing attack modes/methods as STIX data, you can add related attack modes/methods manually.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Attack Mode/Method**.
2. Click the attack mode to which you want to add a related attack mode/method.
3. Click the **Child Attack mode/method** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the attack mode/method you want to relate to the current one.
6. Using the slushbucket, add the attack mode/method to the **Child Attack mode/method** list.
7. Click **Save**.

Add associated task to an attack mode/method

In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an attack mode/method manually.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Attack Mode/Method**.
2. Click the attack mode to which you want to add an associated task.
3. Click the **Associated Tasks** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the tasks you want to associate with the attack mode/method.
6. Using the slushbucket, add the task to the **Associated Tasks** list.
7. Click **Save**.

Indicators of compromise

Indicators of Compromise (IoC) are artifacts observed on a network or operating system that are likely to indicate an intrusion. Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs, or domain names. IoC applies for STIX 1.1 and 2.x.

An IoC can be a single observable or a collection of observables (for example, a single known bad URL or the presence of a specific file and a couple of specific registry key values).

After IoCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IoC applies for STIX 1.1 and 2.x.

View an IoC

IoCs, sometimes referred to as indicators, are most typically retrieved from a threat data source as STIX data. If needed, you can also create IoCs.

Before you begin

Role required: sn_ti.write

Procedure

1. After the scheduled job has retrieved IoC data from the defined data source, navigate to **Threat Intelligence** > **IoC Repository** > **Indicators**.
   The retrieved IoCs are listed.
2. Click the IoC you want to view.
3. The following information displays.

Field	Description
Select classification tag	If you set up and activated security tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the IoC. If you did not set up or activate security tags, this drop-down list is not displayed.
Title	A descriptive name for this indicator.
First Seen	The first date this indicator was observed in the system.
Last Seen	The most recent date this indicator was observed in the system.
Encountered count	The number to times the indicator has been encountered.
Sourced count	The number to times the indicator was imported from defined threat sources.
Notes	Any additional notes about the indicator. This field can also contain JSON key/value pairs.

4. You can click any of the following related lists to view additional information.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Related Observables	Lists observables that are linked to the current indicator.
Related Attack mode/method	Lists related attack modes/methods that have been identified as related to this indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Associated Type	Lists other indicator types that are associated with this IoC.
Indicator Sources	Lists the sources of this indicator, along with the confidence level of the source.
Associated Tasks	Lists all tasks, changes, and incidents associated with the IoC.
Indicator Metadata	If the **Notes** field contains valid JSON key/value pairs, they are parsed and displayed. If no JSON key/value pairs are present, or if the JSON is invalid, this related list is not displayed.
Security Annotations	
Indicator External References	
Associated Kill Chain Phases	Lists kill chain phases associated with this object.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.

Add a related observable to an IoC

In addition to importing observables as STIX data, you can add related observables to an IoC manually.

Before you begin

Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicators**.
2. Click the indicator to which you want to add a related observable.
3. Click the **Related Observables** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the observable you want to relate with the IoC.
6. Using the slushbucket, add the observable to the **Related Observables** list.
7. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add a related attack mode/method to an IoC

In addition to importing related attack modes/methods as STIX data, you can add related attack modes/methods to an IoC manually.

Before you begin
Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicators**.
2. Click the indicator to which you want to add a related attack mode/method.
3. Click the **Related Attack mode/method** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the attack mode/method you want to relate with the IoC.
6. Using the slushbucket, add the attack mode/method to the **Related Attack mode/method** list.
7. Click **Save**.

Identify associated indicator types

If an IoC has no associated indicator types defined, it tracks all types of observables. However, if you associate one or more types of indicators to an IoC, it limits the types of observables that can be associated with the IoC.

Before you begin
Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicators**.
2. Click the indicator to which you want to associate an indicator type.
3. Click the **Associated Type** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the indicator type you want to associate with the IoC.
6. Using the slushbucket, add the indicator type to the **Associated Type** list.
7. Click **Save**.

Identify indicator sources

Indicator sources are normally tracked automatically as part of the threat import process, but more sources can be manually added.

Before you begin
Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicators**.
2. Click the indicator to which you want to add indicator sources.
3. Click the **Indicator Sources** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the indicator source you want to associate with the IoC.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Using the slushbucket, add the indicator source to the **Indicator Sources** list.
7. Click **Save**.

Add associated tasks to an IoC

In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an IoC manually.

Before you begin
Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicators**.
2. Click the IoC to which you want to add an associated task.
3. Click the **Associated Tasks** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the tasks you want to associate with the IoC.
6. Using the slushbucket, add the task to the **Associated Tasks** list.
7. Click **Save**.

Observables

Observables represent stateful properties (such as the MD5 hash of a file or the value of a registry key) or measurable events (such as the creation of a registry key or the deletion of a file) that are pertinent to the operation of computers and networks. Observables apply for STIX 1.1 and 2.x.

Sets of cyber observables are useful for identifying indicators of compromise when they are combined with contextual information that represents the behaviors of cyber threats.

Observables apply for STIX 1.1 and 2.x.

Define an observable

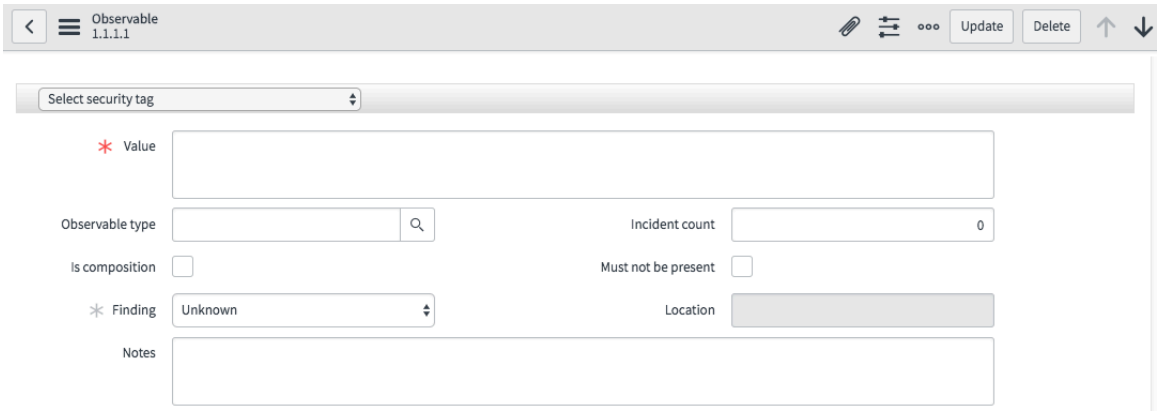
Observables are retrieved from the vendor server as STIX data. However, you can create observables, as needed.

Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Fill in the fields on the form, as appropriate.

Field	Description
Select classification tag	If you set up and activated security tags to add metadata to the record, you can select one or more tags to specify the degree of sensitivity of the observable. If you did not set up or activate security tags, this drop-down list is not displayed.
Value	The value (for example, IP address or hash) associated with the observable. **Note:** If a threat scan on an IP address or hash, returned malware or some other failure, the IP address or hash value is automatically added to the Observable [sn_ti_observable] table. As such, it can be searched for from the Observables form.
Observable type	Select the observable classification, such as an IP address or file hash. These observable types are defined in the **Observable Types** module.
Incident count	The number of times the observable value has been encountered.
Is composition	This field displays only after the observable record has been saved. If the **Observable Type** is set to anything other that **Observable Composition**, and this new observable is a composition, select this check box. If the **Observable Type** is already set to **Observable Composition**, the check box is selected and read-only. An observable composition is an observable that contains child observables.
Finding	Select one of the following: ○ **Malicious**: Indicates that the observable is harmful to the organization. ○ **Suspicious**: Indicates that the observable might be harmful to the organization. ○ **Clean**: Indicates that the observable is not harmful to the organization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Unknown**: Indicates that we are yet to determine the observable's finding. ○ Default value: Unknown. For more information, see Threat Lookup Finding Calculators. **Note:** After an upgrade, existing observables are marked Malicious.
Operator	This field appears only when the **Is composition** check box is selected. Depending on your setting in this field, the observables and their children are considered when deciding whether an associated indicator is present. Set this field to **AND** if all the child observables must be present for an associated indicator to be considered present. Set it to **OR** if any of the child observables are present for an associated indicator to be considered present.
Must not be present	This field displays only after the observable record has been saved. If selected, this field signifies that the absence of the observable is the potential issue (for example, a missing registry key).
Location	Using the settings in two properties and a script include definition, you can load Load more IoC data in this field.
Notes	Enter any additional notes about the observable.

4. Right-click in the form header and click **Save**.
You can now click any of the following related lists to view additional information.

Related List	Description
Related Indicators	Lists indicators that have been identified by the threat source.
Associated Tasks	Lists changes associated with the observable.
Child Observables	Lists related observables that have been identified by the threat source.
Matching Resources for IP	If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address.
Observable Sources	Lists the sources of this observable, along with the confidence level of the source.
Security Annotations	Lists security annotations added to this observable.

Add a related IoC to an observable

In addition to importing observables as STIX data, you can add related observables to an IoC manually.

Before you begin

Role required: sn_ti.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click the observable to which you want to add a related IoC.
3. Click the **Related Indicators** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the indicator you want to relate with the observable.
6. Using the slushbucket, add the indicator to the **Related Indicators** list.
7. Click **Save**.

Add associated tasks to an observable

In addition to importing associated tasks (such as changes and incidents) as STIX data, you can add them to an observable manually.

Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click the observable to which you want to add an associated task.
3. Click the **Associated Tasks** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the tasks you want to associate with the observable.
6. Using the slushbucket, add the task to the **Associated Tasks** list.
7. Click **Save**.

Add a related observable

In addition to importing observables as STIX data, you can add related observables manually.

Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click the observable to which you want to add a related observable.
3. Click the **Child Observables** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the observable you want to relate to the current one.
6. Using the slushbucket, add the observable to the **Child Observables** list.
7. Click **Save**.

Load more IoC data

Depending on settings in two properties and a script include definition, you can load geolocation information for IP addresses and websites in the Observables form. With further customization, you can also add other information, such as country codes, city names.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

The following two properties must be set:

- **The domain name to retrieve additional information for IP addresses/URLs** [sn_ti.ip_lookup.web_site]
- **The API key to be used for the above domain, if any** [sn_ti.ip_lookup.api_key]

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click the IP address or URL of the observable to which you want to view more IoC data. The **Location** field shows the geolocation of the IoC.
3. Click the **Enrich data** button to load the additional IoC data.
4. You can also configure the Observable form to add other location-related fields, such as the country code and city code.

> **Note:** To load more location-related information, edit the **ThreatAdditionalInfo** script include and provide the appropriate API key from the website that provides the additional information.

Identify observable sources

If an observable has no sources defined, it uses all types of sources. However, if you add one or more threat sources to an observable, it limits the sources used.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Click the observable to which you want to add observable sources.
3. Click the **Observable Sources** related list.
4. Click **Edit**.
5. As needed, use the filters to locate the source you want to associate with the observable.
6. Using the slushbucket, add the observable source to the **Observable Sources** list.
7. Click **Save**.

Perform lookups on observables

You can perform threat intelligence lookups on one or more observables to determine whether they're associated with known security threats. The scanning implementations that run depend on the ones you've activated.

Before you begin

Before you can perform lookups, you must activate the Threat Intelligence plugin. You must also install the plugin for one or more of the scanning implementations:

- CrowdStrike Falcon Intelligence integration
- OPSWAT Metadefender

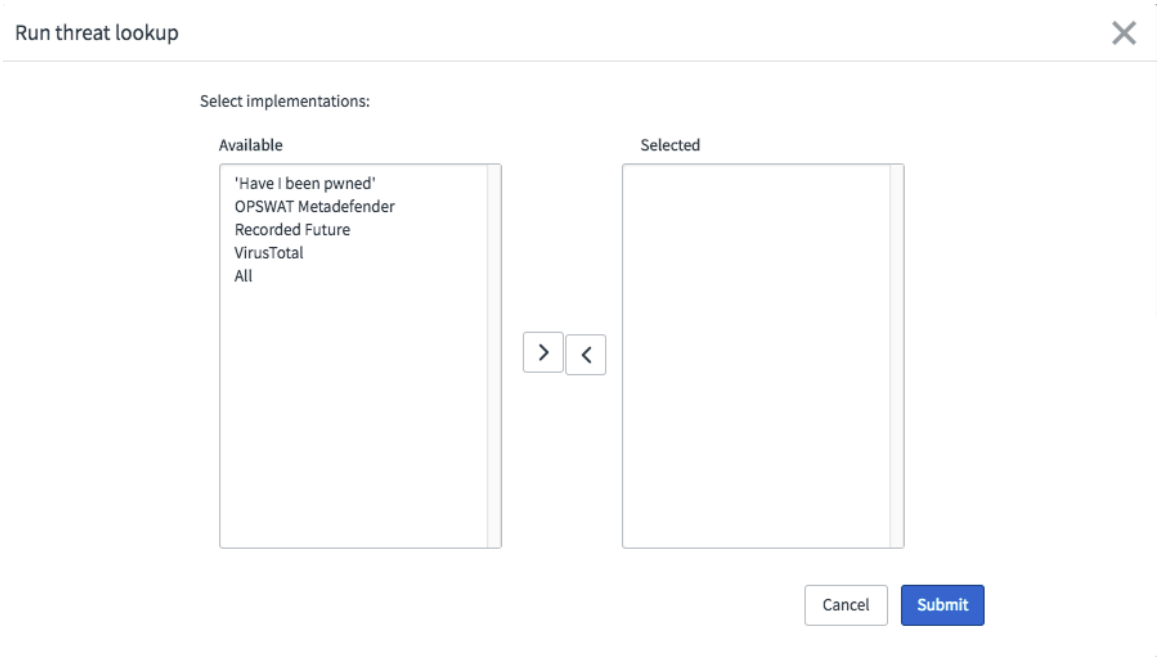
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Operations Have I been pwned?
- VirusTotal

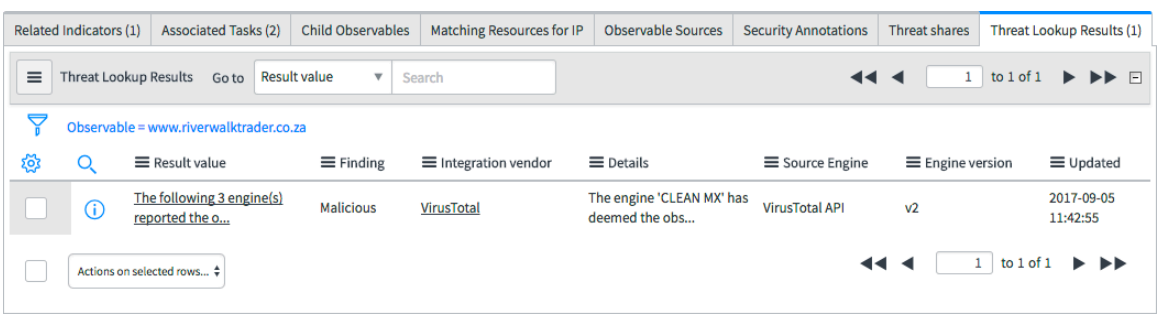
Role required: sn_ti.write

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Do one of the following steps:
   - To perform a lookup on more than one observable, select the observables, click **Actions on selected rows**, and select **Run threat lookup**.
   - To perform a lookup on a single observable, open the observable record, and click the **Run threat lookup** related link.



3. Select the threat lookup implementations you want to use, or select **All** to perform lookups using all of the active implementations, then click **Submit**.
   A message indicates that the threat lookups have begun. The Security Operations Integration - Threat Lookup workflow runs and also executes the implementation workflows for the threat lookup implementations you selected. The lookups are performed and the results are generated.
4. When the lookups are completed, you can click the **Threat Lookup Results** tab to view the results.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recent Threat Lookup Result: You can also see the latest or recent threat lookup results from each integration vendor when you click the **Recent Threat Lookup Result** tab.

Note: The **Recent Threat Lookup Result** tab is not a part of the base system.

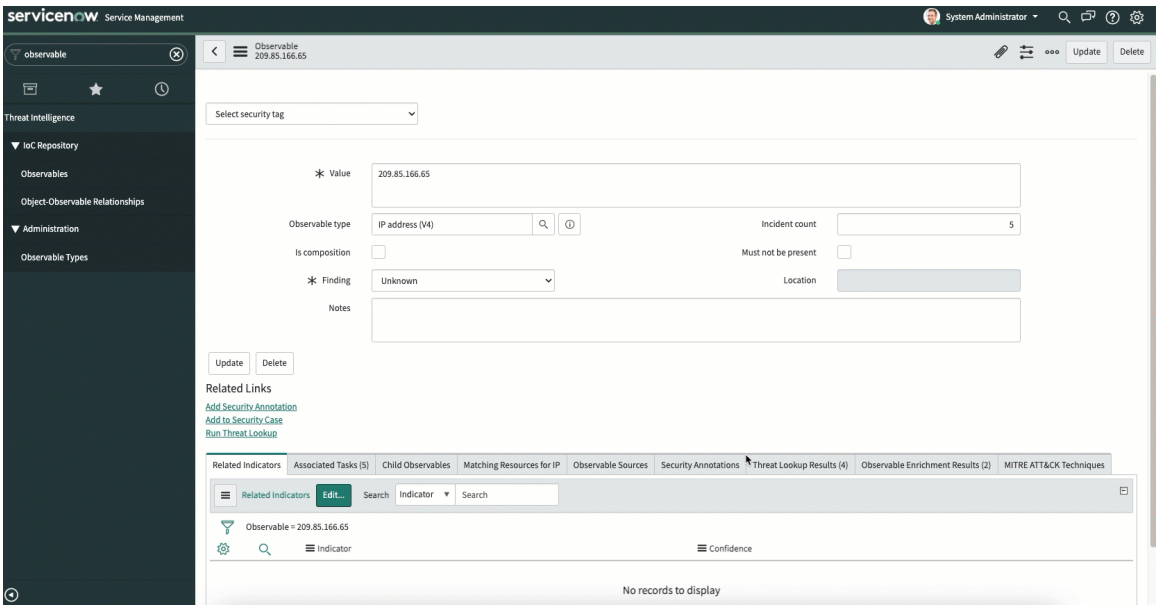
To enable this tab, perform the following:

a. Right-click on the form header.

b. Navigate to **Configure** > **Related Lists**.

c. Locate **Recent Threat Lookup Results** on the Available list and move it to the Selected list.

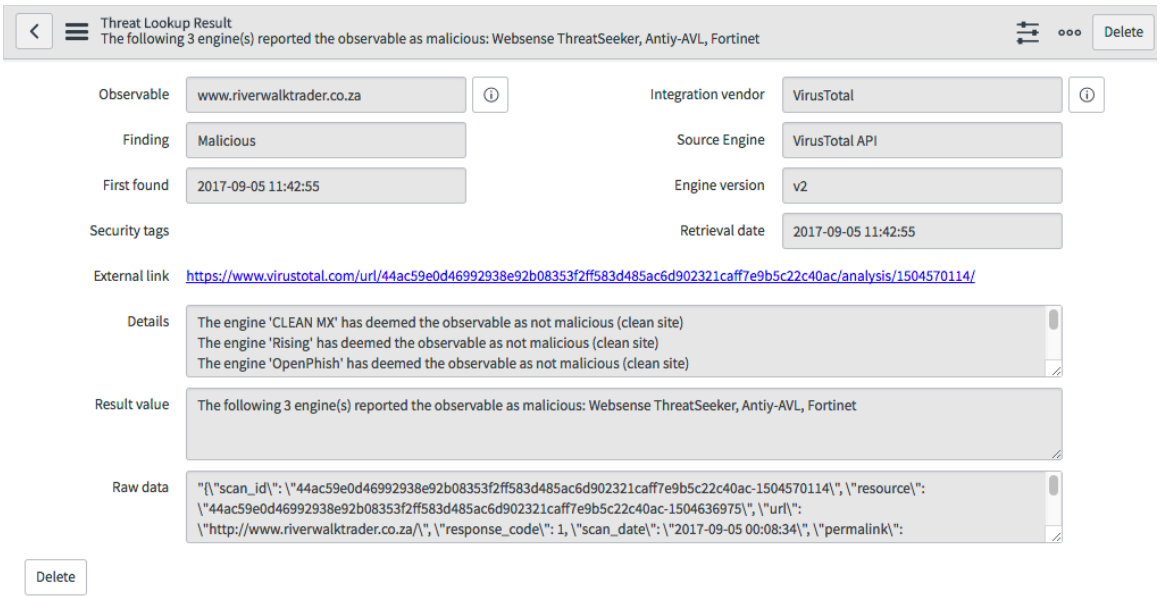
d. Click **Save**.
You can now view the recent threat lookup results from each integration vendor in the **Recent Threat Lookup Result** tab.



5. To see additional details, including raw results for a specific lookup, click the **Result value**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When the VirusTotal or OPSWAT Metadefender implementations are used, the details are consolidated, as shown below.



Perform threat enrichment on observables

You can perform threat intelligence enrichment on one or more observables to determine whether they're associated with known security threats. The implementations that run depend on the ones you've activated.

Before you begin

Before you can perform enrichment, you must activate the Threat Intelligence plugin. You must also install the plugin for one or more of the enrichment implementations:

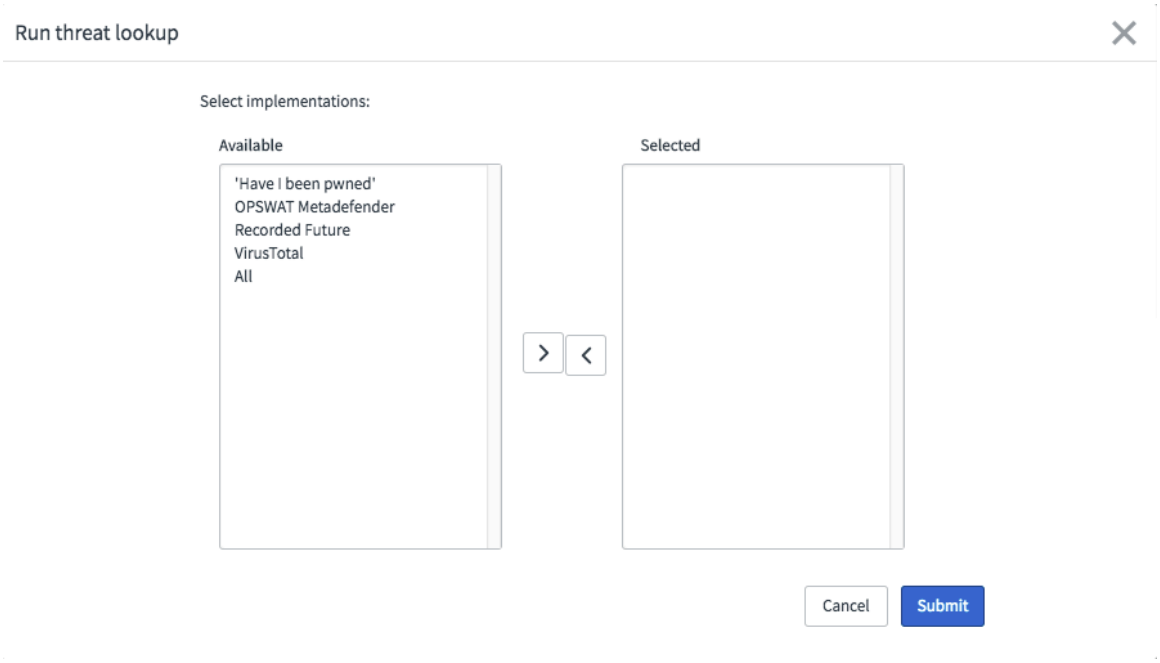
- CrowdStrike Falcon Intelligence integration
- OPSWAT Metadefender
- Security Operations Have I been pwned?
- VirusTotal
- WhoIs?

Role required: sn_ti.admin

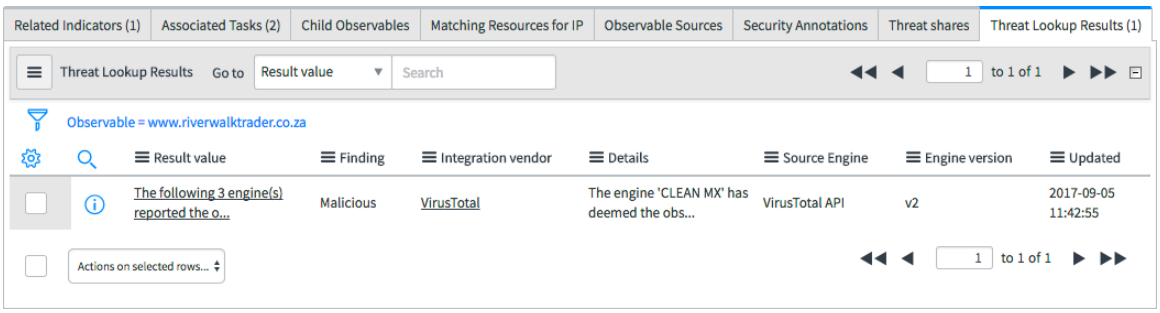
Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observables**.
2. Do one of the following steps:
   - To perform a lookup on more than one observable, select the observables, click **Actions on selected rows**, and select **Run threat lookup**.
   - To perform a lookup on a single observable, open the observable record, and click the **Run threat lookup** related link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



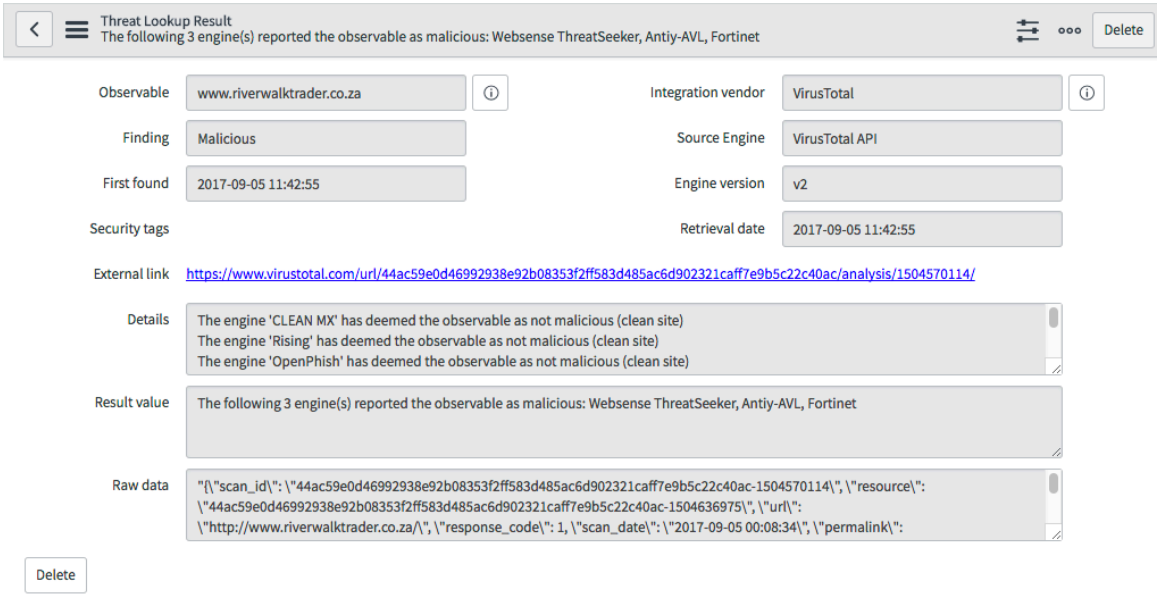
3. Select the threat lookup implementations you want to use, or select **All** to perform lookups using all of the active implementations, then click **Submit**.
   A message indicates that the threat lookups have begun. The Security Operations Integration - Threat Lookup workflow runs and also executes the implementation workflows for the threat lookup implementations you selected. The lookups are performed and the results are generated.
4. When the lookups are completed, you can click the **Threat Lookup Results** tab to view the results.



5. To see additional details, including raw results for a specific lookup, click the **Result value**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: When the VirusTotal or OPSWAT Metadefender implementations are used, the details are consolidated, as shown below.



Attack patterns

Attack patterns are a type of Tactics, Techniques, and Procedures (TTPs) that describe the methods that adversaries attempt to compromise targets. Attack Patterns apply for STIX 2.x.

Attack patterns are used to help categorize attacks. They generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.

For example, spear phishing is a common type of attack where an attacker sends a carefully crafted email message to a party with the intent of getting them to click a link or open an attachment to deliver malware. Attack Patterns are more specific, such as spear phishing by a particular threat actor (example - that the target won a contest) can also be an Attack pattern.

Define an attack pattern

Define an attack pattern to help categorize attacks.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Attack Patterns**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name for this attack pat tern.
Spec Version	The version of the STIX specification used to represent this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The value of this property must be 2.1 for STIX Objects defined according to this specifica tion.
Source	Specifies the threat source from which this record is created.
Description	Enter a description of the attack pattern.
Aliases	Alternative names to identify this attack pat tern.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

You can now click any of the following related lists to view additional information about objects associated with the attack pattern.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Kill Chain Phases	Lists kill chain phases associated with this object.
Campaigns	Lists campaigns associated with this object.
Course of Actions	Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Campaigns

A Campaign is a grouping of adversarial behaviors. These behaviors describe a set of malicious activities or attacks that occur over time against a specific set of targets. Campaigns apply for STIX 2.x.

Campaigns usually have well-defined objectives and may be part of an Intrusion Set.

Campaigns are often attributed to an intrusion set and threat actors. The threat actors may reuse known infrastructure from the intrusion set or may set up new infrastructure specific for conducting that campaign.

Campaigns have a common objective in the incidents they cause, to people, or to the resources they target, and the resources they use.

For example, a crime syndicate attacks the executives of ACME Bank. They attack by using a specific variant of malware, and new servers to gain secret information about an upcoming merger with another bank.

Define a campaign

Define a campaign to group adversarial behaviors.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Campaigns**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name for this campaign.
Spec Version	The version of the STIX specification used to represent this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The value of this property must be 2.1 for STIX Objects defined according to this specifica tion.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the campaign. This includes its purpose and its key characteristics.
Aliases	Alternative names to identify this campaign.
Objective	The campaign's primary goal, objective, de sired outcome, or intended effect. What the threat actor or intrusion set hopes to accom plish with this campaign.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

You can now click any of the following related lists to view additional information about objects associated with the campaign.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Course of actions

A course of action is an action taken either to prevent an attack or to respond to an attack that is in progress. Course of actions apply for STIX 2.x.

Course of actions describes technical or automated responses (applying patches, reconfiguring firewalls). It can also describe higher-level actions like employee training or policy changes.

For example, a course of action to mitigate a vulnerability could describe applying the patch that fixes it.

Define a course of action

Define a course of action to prevent an attack or to respond to an attack that is in progress.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Course of Actions**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name for this course of ac tion.
Action	To capture structured or automated courses of action.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the course of action, potentially

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	including its purpose and its key characteris tics.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the course of action.

Related Links	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Malware	Lists malicious code associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Identities

Identities represent actual individuals, organizations, or groups (ACME, Inc.) and classes of individuals, systems, or groups (the finance sector). Identities apply for STIX 2.x.

The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity represents targets of attacks, information sources, object creators, and threat actor identities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define identities

Define identities who represent actual individuals, organizations, or groups.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Identities**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name for this identity. When referring to a specific entity (an individual or organization), this property must contain the canonical name of the specific entity.
Identity Class	The type of entity that this identity describes. For example, individual or organization.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the identity, potentially including its purpose and its key characteristics.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated the identity.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Infrastructure

The Infrastructure SDO represents a type of Tactics, Techniques, and Procedures (TTPs). They describe any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack. Infrastructure applies for STIX 2.x.

The elements of an attack are represented by other SDOs or SCOs. However, the Infrastructure SDO represents a named group of data that constitutes the infrastructure.

Examples of infrastructure include, C2 servers used in an attack, a device, or a server that is part of a defense, or database servers targeted by an attack.

Define infrastructure

Define an Infrastructure that is any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Infrastructure**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the infra structure.
First Seen	The time that this infrastructure was first seen performing malicious activities.
Last Seen	The time that this infrastructure was last seen performing malicious activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the Infrastructure, potentially in cluding its purpose, how it is being used, how it relates to other intelligence activities cap tured in related objects, and its key character istics.
Aliases	Alternative names to identify this infrastruc ture.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

You can now click any of the following related lists to view additional information. You can also associate other objects with the infrastructure.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Types	Lists indicator types associated with this object.
Associated Kill Chain Phases	Lists kill chain phases associated with this object.
Associated Observables	Lists observables associated with this object.
Associated Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Observed Data	Lists observed data associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Intrusion set

An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties. An Intrusion Set usually involves a single organization. Intrusion set applies for STIX 2.x.

An Intrusion Set may capture multiple Campaigns or other activities. These activities share attributes indicating a commonly known or unknown Threat Actor.

New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.

An Intrusion Set is the entire attack package and may be used over a long period in multiple Campaigns to achieve potentially multiple purposes.

Define an intrusion set

Define an intrusion set that is a grouped set of adversarial behaviors and resources with common properties.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Intrustion Set**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the intru sion set.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
First Seen	The time that this intrusion set was first seen performing malicious activities.
Last Seen	The time that this intrusion set was last seen performing malicious activities.
Primary Motivation	The primary reason, motivation, or purpose behind this intrusion set. The motivation is why the Intrusion Set wants to achieve the goal (what they are trying to achieve). For example, an intrusion set with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capital ism.
Resource Level	This property specifies the organizational lev el at which this intrusion set typically works, which in turn determines the resources avail able for use in an attack.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteris tics.
Aliases	Alternative names to identify this intrusion set.
Goals	The high-level goals of this intrusion set, namely, what are they trying to do. For example, they may be motivated by per sonal gain, but their goal is to steal credit card numbers. To do this, they may execute specif ic campaigns that have detailed objectives like compromising point of sale systems at a large retailer.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the intrusion set.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Attack Motivations	Lists any secondary motivations why this intrusion set wants to achieve.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Locations

A Location represents a geographic location. Locations are primarily used to give context to other SDOs. Locations apply for STIX 2.x.

The location may contain, some or all of the following: region (North America), civic address (New York, US), latitude, and longitude.

The Location SDO may relate to an Identity or Intrusion Set to indicate that the identity or intrusion set is in that location. It can also relate to a malware or attack pattern to indicate that the target victim is in a particular location.

For example, a Location could be used in a relationship to describe that the Bourgeois Swallow intrusion set originates from Eastern Europe.

At least one of the following properties or sets of properties must be provided:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- region
- country
- latitude and longitude

Define Location

Define a geographic location to provide more context to other SDOs.

Before you begin
Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Locations**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the loca tion.
Street Address	The street address that this location de scribes. This property includes all aspects or parts of the street address.
City	The city that this location is in.
Postal Code	The postal code that this location is in.
Region	The region that this location is in.
Country	The country that this location is in.
Latitude	The latitude of the Location in decimal de grees. Positive numbers describe latitudes north of the equator, and negative numbers describe latitudes south of the equator. The value of this property must be from -90.0 through 90.0 respectively.
Longitude	The longitude of the location in decimal de grees. Positive numbers describe longitudes east of the prime meridian and negative num bers describe longitudes west of the prime meridian. The value of this property must be from -180.0 through 180.0, inclusive.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the intrusion set, potentially

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	including its purpose and its key characteris tics.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the location.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Identities	List of identities associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Malware

Malware is a type of TTP that represents malicious code. It refers to a program that is covertly inserted into a system. Malware applies for STIX 2.x.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The intent of a malware is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS).

The Malware SDO characterizes, identifies, and categorizes malware instances and families from data that is derived from analysis. This SDO captures detailed information about how the malware works and what it does.

Define a Malware

Define a malware that represents malicious code.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Malware**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a name to identify the malware instance or family, as specified by the producer of the SDO. For a malware family, the name must be defined.
First Seen	The time that this malware instance or family was first seen performing malicious activities.
Last Seen	The time that this malware instance or family was last seen performing malicious activities.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the malware instance or family, potentially including its purpose and its key characteristics.
Aliases	Alternative names to identify this malware in stance or family.
Source ID	Unique identifier for this object in the threat source.
Is Family	Specifies if the object represents a malware family or a malware instance.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the malware.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Types	Lists indicator types associated with this object.
Associated Capabilities	Lists the capabilities identified and associated with this object.
Associated Kill Chain Phases	Lists kill chain phases associated with this object.
Associated Observables	Lists observables associated with this object.
Associated Malware	Lists the associated malware identified with this object.
Associated Operating Systems	The operating systems that the object is executable on. This applies to virtualized operating systems as well as those running on bare metal.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Course of Actions	Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware Analysis	Lists malware analysis records associated with this object.
Reported Observables	Lists observables reported as part of this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Malware analysis

Malware Analysis captures the metadata and results of a malware. Malware analysis applies for STIX 2.x.

Malware Analysis includes static or dynamic analysis performed on a malware instance or family.

Define malware analysis

Define malware analysis that captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Malware Analysis**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the intru sion set.
Analysis Engine Version	The version of the analysis engine or product (including AV engines) that was used to per form the analysis.
Analysis Definition Version	The version of the analysis definitions used by the analysis tool (including AV tools).
Analysis Started	The date and time that the malware analysis was initiated.
Analysis Ended	The date and time that the malware analysis was ended.
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Result	The classification result as determined by the scanner or tool analysis process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Result Name	The classification result or name assigned to the malware instance by the scanner tool.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information on the objects associated with malware analysis.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Malware	Lists the associated malware identified with this object.
Reported Observables	Lists observables reported as part of this object.
Installed Software	Lists any non-standard software installed on the operating system used for the dynamic analysis of the malware instance or family.

Observed data

Observed Data conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs). Observed data applies for STIX 2.x.

Observed Data captures both a single observation of a single entity (file, network connection) as well as the aggregation of multiple observations of an entity.

You can use Observed Data by itself (without relationships) to convey raw data collected from any source. Sources include analyst reports, sandboxes, and network and host-based detection tools.

For example, Observed Data can capture information about an IP address, a network connection, a file, or a registry key. Observed Data is not an intelligence assertion, it is simply the raw information without any context for what it means.

Define observed data

Define observed data that conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Observed Data**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
First Observed	The initial time when the data was seen.
Last Observed	The last time when the data was seen.
Observed Count	The number of times that each Cyber-observable object was seen. The value must be an integer from 1 through 999,999,999.
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next
Click any of the following related lists to view additional information about objects associated with the observed data.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Observables	Lists observables associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat actors

Threat Actors are individuals, groups, or organizations who act with malicious intent. Threat actors applies for STIX 2.x.

A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.

Threat Actors use their resources, and the resources of an Intrusion Set, to conduct attacks, and run Campaigns against targets.

You can identify Threat Actors by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

Define threat actors

Define threat actors who are individuals, groups, or organizations who act with malicious intent.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Threat Actors**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a name to identify the malware instance or family, as specified by the producer of the SDO. For a malware family, the name must be defined.
First Seen	The time that this malware instance or family was first seen performing malicious activities.
Last Seen	The time that this malware instance or family was last seen performing malicious activities.
Primary Motivation	The primary reason, motivation, or purpose behind this threat actor. The motivation is why the threat actor wants to achieve the goal (what they are trying to achieve). For example, a threat actor with a goal to dis rupt the finance sector in a country might be motivated by ideological hatred of capitalism.
Resource Level	The organizational level at which this threat actor typically works, which in turn deter mines the resources available to this Threat Actor for use in an attack.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the threat actor, potentially in cluding its purpose and its key characteris tics.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Aliases	A list of other names to identify this threat ac tor.
Goals	The high-level goals of this threat actor, name ly, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat actor.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Associated Types	Lists indicator types associated with this object.
Associated Roles	Lists the associated roles with the threat actor.
Associated Attack Motivations	Lists the associated attack motivations with the threat actor.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Threat groupings

A Threat Groupings object explicitly asserts that the referenced STIX Objects have a shared context. Threat groupings applies for STIX 2.x.

A Threat Groupings object represents a set of data that, given sufficient analysis, matures to convey an incident or threat report as a STIX Report object. For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident.

A Threat Groupings object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process. For example, a threat analyst may collaborate with others in their trust community to examine a series of Campaigns and Indicators.

The Threat Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.

Define threat groupings

Define threat groupings as objects that have a shared context.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Threat Groupings**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a name to identify the threat grouping.
Context	A description of the particular context shared by the content referenced by the grouping.
Source	Specifies the threat source from which this record is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	A short description that provides details and context about the grouping. This includes its purpose and its key characteristics.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat grouping.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Grouped Objects	Lists objects grouped as part of the threat grouping.
Grouped Indicators	Lists indicators grouped as part of the threat grouping.
Grouped Observables	Lists observables grouped as part of the threat grouping.

Marking definitions

The marking definitions object represents a specific marking.

Data markings represent restrictions, permissions, and other guidance for how data can be used and shared.

For example, data may be shared with the restriction that it must not be reshared, or that it must be encrypted at rest.

In STIX, data markings are specified using the marking definition object. These definitions are applied to STIX Objects using object markings and to individual properties of STIX Objects via granular markings.

Define marking definitions

Define marking definitions that represent a specific data marking.

Before you begin

Role required: sn_ti.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Marking Definitions**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Definition	Specify the marking object (example, TLP) or some other marking definition that has been defined.
Definition Type	Identifies the type of marking definition - state ment or TLP (Traffic Light Protocol).
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the marking definition.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Marked Objects	Lists of objects marked with the marking definition.
Marked Indicators	Lists of indicators marked with the marking definition.

Threat notes

A Threat Note conveys informative text to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to. Threat notes applies for STIX 2.x.

For example, an analyst may add a Note to a Campaign object created by another organization. The note may indicate that they've seen posts related to that Campaign on a hacker forum.

Notes are usually created by human analysts and are composed of human-oriented text, they contain an extra property to capture the author that created the Note.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define threat notes

Define threat notes that convey information to provide further context or analysis that is not available in existing objects.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Threat Notes**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Abstract	Specify a brief summary of the note content.
Content	Specifies the content of the note.
Authors	Specifies the name of the author (example, an analyst).
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat notes.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Associated Objects	Lists of objects that the threat notes apply to.
Associated Indicators	Lists of indicators that the threat notes apply to.
Associated Observables	Lists observables associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat opinions

An Opinion is an assessment of the accuracy of the information in a STIX Object produced by a different entity. Threat opinions apply for STIX 2.x.

The opinion property captures the level of agreement or disagreement using a fixed scale. The fixed scale also supports a numeric mapping to enable consistent statistical operations across opinions.

For example, an analyst from a consuming organization might say that they "strongly disagree" with a Campaign object and provide an explanation about why.

Opinions are subjective, and the specification does not address how best to interpret them.

Human analysts create Opinions and are composed of human-oriented text, they contain an extra property to capture the author that created the Opinion.

Define threat opinions

Define threat opinions as an assessment of the accuracy of the information in a STIX object.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Threat Opinions**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Opinion	The producer's opinion about the STIX object.
Explanation	The producer's explanation about the opin ion.
Authors	Specifies the name of the author (example, an analyst).
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat opinion.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Associated Objects	List of objects the threat opinion applies to.
Associated Indicators	List of indicators the threat opinion applies to.
Associated Observables	Lists observables associated with this object.

Threat reports

Threat Reports are collections of threat intelligence focused on one or more topics. Threat reports apply for STIX 2.x.

Threat reports include description of a threat actor, malware, attack technique, including context and related details. They are used to group-related threat intelligence together so that it can be published as a comprehensive cyber threat story.

The Threat Report SDO contains a list of references to STIX Objects along with a textual description and the name of the report.

Define threat reports

Define threat reports that describe a threat actor, malware, attack technique, including context and related details.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Threat Reports**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Specify a name to identify the threat report.
Published	The date that this report has been officially published by the report author.
Description	A description that provides additional insight and context about the report.
Source	Specifies the threat source from which this record is created.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat reports.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
Associated Types	Lists indicator types associated with this object.
Reported Objects	List of objects reported in the threat report.
Reported Indicators	Lists of indicators reported in the threat report.
Reported Observables	Lists of observables reported in the threat report.

Sightings

Sightings denote that an indicator or object was seen. Objects may be a malware, tool, threat actor, and so on.

Sightings track who and what is the target, how attacks are carried out, and to track trends in attack behavior.

The Sighting relationship object contains extra properties not present in the generic relationship objects. These extra properties represent data specific to sighting relationships.

For example, a count, or representing how many times something was seen.

Sighting is captured as a relationship because you cannot have a sighting unless you have something that has been sighted.

- What was sighted, such as the malware, campaign, or other SDO
- Who sighted it and/or where it was sighted, represented as an identity
- What was seen on systems and networks, represented as observed data

Define indicator sightings

Define sightings that denote that an indicator was seen.

Before you begin

Role required: sn_ti.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Indicator Sightings**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Indicator	Identifies the indicator. Search and select the indicator.
Count	The number of times the object was seen.
First Seen	The time that this object first seen performing malicious activities.
Last Seen	The time that this object was last seen per forming malicious activities.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the indicator sighting, potential ly including its purpose and its key character istics.
Source ID	Unique identifier for this object in the threat source.
Is Summary	
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the indicator sighting.

Related Lists	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Identities	List of identities associated with this object.
Observed Data	Lists observed data associated with this object.

Define object sightings

Define object sighting that describes that an object (malware, tool, threat actor, and so on) was seen.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Object Sightings**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Object	Identifies the object. Search and select the object.
Count	The number of times the object was seen.
First Seen	The time that this object first seen performing malicious activities.
Last Seen	The time that this object was last seen per forming malicious activities.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the object sighting, potentially including its purpose and its key characteris tics.
Source ID	Unique identifier for this object in the threat source.
Is Summary	
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next
Click any of the following related lists to view additional information about objects associated with the object sighting.

Related Lists	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Identities	List of identities associated with this object.
Observed Data	Lists observed data associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tools

Tools are legitimate software that are used by threat actors to perform attacks. Tools apply for STIX 2.x.

Tools enable you to know how and when threat actors use them for executing campaigns. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, administrators, network administrators, or even normal users.

For example, remote access tools (RDP) and network scanning tools (Nmap) are tools that a threat actor uses during an attack.

Define tools

Define tools as legitimate software that is used to perform attacks.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Tools**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the tool.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the tool, potentially including its purpose and its key characteristics.
Aliases	Alternative names to identify this tool.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the tool object.

Related Links and Related Lists	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Associated Kill Chain Phases	Lists kill chain phases associated with this object.
Associated Types	Lists indicator types associated with this object.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Course of Actions	Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.

Vulnerabilities

A Vulnerability is a weakness or defect in a software or hardware component that attackers exploit. Vulnerabilities apply for STIX 2.x.

The weakness or defect is in the requirements, designs, or implementations of the code found in a software or hardware component. This weakness is directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

CVE is a list of information security vulnerabilities and exposures that provides common names for publicly known problems [CVE].

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, if a piece of malware exploits CVE-2015-12345, a Malware object could be linked to a Vulnerability object that references CVE-2015-12345.

Define vulnerabilities

Define vulnerability as a weakness or defect in a software or hardware component that attackers exploit.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Vulnerabilities**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Name	Enter a descriptive name to identify the vul nerability.
Source	Specifies the threat source from which this record is created.
Description	A description that provides more details and context about the vulnerability, potentially in cluding its purpose and its key characteris tics.
Aliases	Alternative names to identify this tool.
Source ID	Unique identifier for this object in the threat source.
Created Time in Source	Specifies the time the object is created in the source.
Modified Time in Source	Specifies the time the object is modified in the source.

4. Click **Submit**.

What to do next

Click any of the following related lists to view additional information about objects associated with the vulnerability object.

Related Links and Related Lists	Description
Show Relationships	Opens the STIX Visualizer where you can view the relationship of the STIX object. Show Relationships appears only when the object has an associated object.
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Links and Related Lists	Description
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists campaigns associated with this object.
Course of Actions	Lists the associated course of actions with this object that are technical or automated responses (applying patches, reconfiguring firewalls) to prevent an attack.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Relationships

Use the relationship objects to link together two SDOs or STIX Cyber-observable Objects (SCOs) to describe how they relate to each other.

STIX Relationship Objects (SROs) represent types of relationships between various STIX objects. The following relationship objects are available:

- **Object-Object Relationship**: This object defines relationships between SDOs, except the indicator object. An example of an object-object defined relationship is that an attack pattern delivers a malware.
- **Object-Indicator Relationship**: This object defines relationships between the indicator object and other SDOs. An example of an object-indicator defined relationship is that an indicator detects evidence of a campaign.
- **Object-Observable Relationship**: This object defines relationships between SDOs and the observable object (SCO). An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.

STIX Object Relationships

Relationship Object	Example Source	Example Target	Example Description
Object-Object Relationships	Attack-pattern	Malware	This relationship describes that this Attack Pattern is used to deliver this malware instance (or family).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

STIX Object Relationships (continued)

Relationship Object	Example Source	Example Target	Example Description
Object-Indicator Relationships	Indicator	Attack-Pattern, Campaign, Infrastructure, Intrusion-set, Malware, Threat-actor, Tool	This relationship describes that the indicator can detect evidence of the related attack pattern, campaign, infrastructure, intrusion set, malware, threat actor, or tool. The evidence may not be direct. For example, the indicator may detect secondary evidence of the campaign such as malware that is commonly used by that particular campaign.
Object-Observable Relationships	Infrastructure	Observed data	This relationship describes that the indicator is created based on information from an observed data object. An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.

Define object-object relationships

Define relationships between SDOs, except the indicator object.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Object-Object-Relationships**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source Object	Select and define the source object.
Source Object Type	Defines the type of source object.
Target Object	Select and define the target object.
Target Object Type	Defines the type of target object.
Relationship Type	A description that provides more details and context about the relationship type.
Source	Specifies the threat source from which this record is created.
Source ID	Uniquely identifies the source object.

4. Click **Submit**.

Define object-indicator relationships

Define relationships between the indicator object and other SDOs.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Object-Indicator-Relationships**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Object	Select and define the object.
Type	Specifies the object type based on the object you selected.
Indicator	Select the indicators of compromise.
Relationship Direction	Define the relationship direction whether it is direct or inverse.
Relationship Type	A description that provides more details and context about the relationship type.
Source	Specifies the threat source from which this record is created.
Source ID	Uniquely identifies the source object.

4. Click **Submit**.

Define object-observable relationships

Define relationships between SDOs and the observable object (SCO).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_ti.admin

Procedure
1. Navigate to **All** > **Threat Intelligence** > **IoC Repository** > **Object-Observable-Relationships**.
2. Click **New**.
3. Complete the fields in the form as appropriate.

Field	Description
Object	Select and define the source object.
Type	Enter a descriptive name to identify the ob ject type.
Observable	Select and define the observable.
Relationship Type	A description that provides more details and context about the relationship type.
Source	Specifies the threat source from which this record is created.
Source ID	Uniquely identifies the source object.

4. Click **Submit**.

STIX Visualizer
The STIX Visualizer visually represents the structure of the STIX object and its relationship.

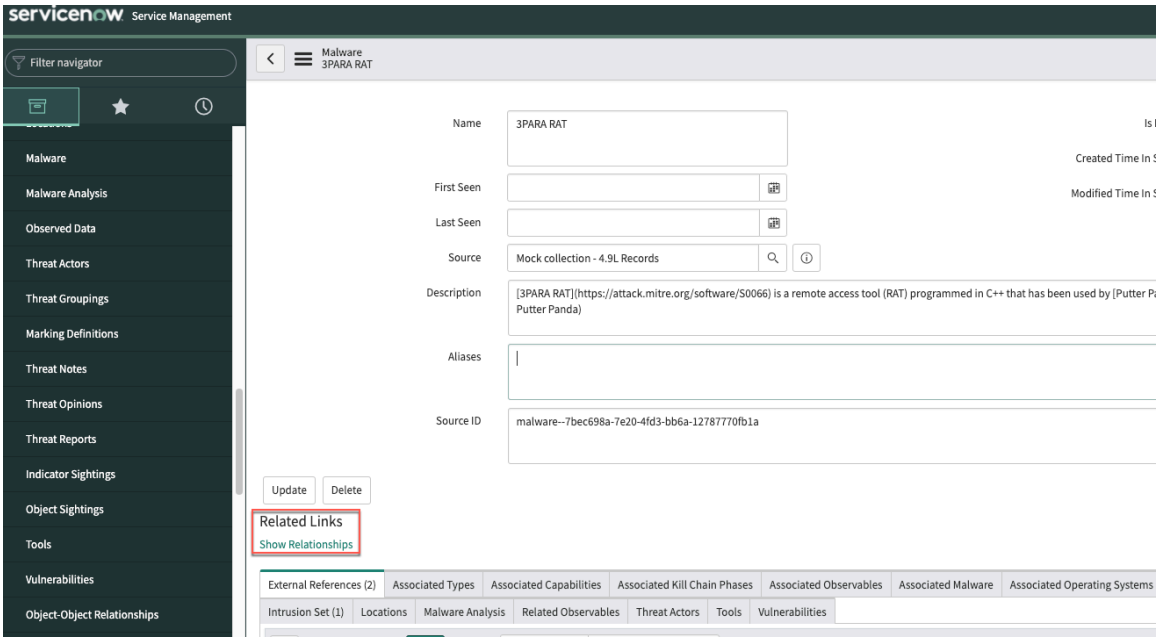
You can learn more information about the selected object or relationship from the details pane.

The relationship graph shows the relationships for an object and provides context for you to investigate. You can click any node in the graph to see more details.

Note: The STIX Visualizer is available for all SDOs except the Report and Observed Data objects.

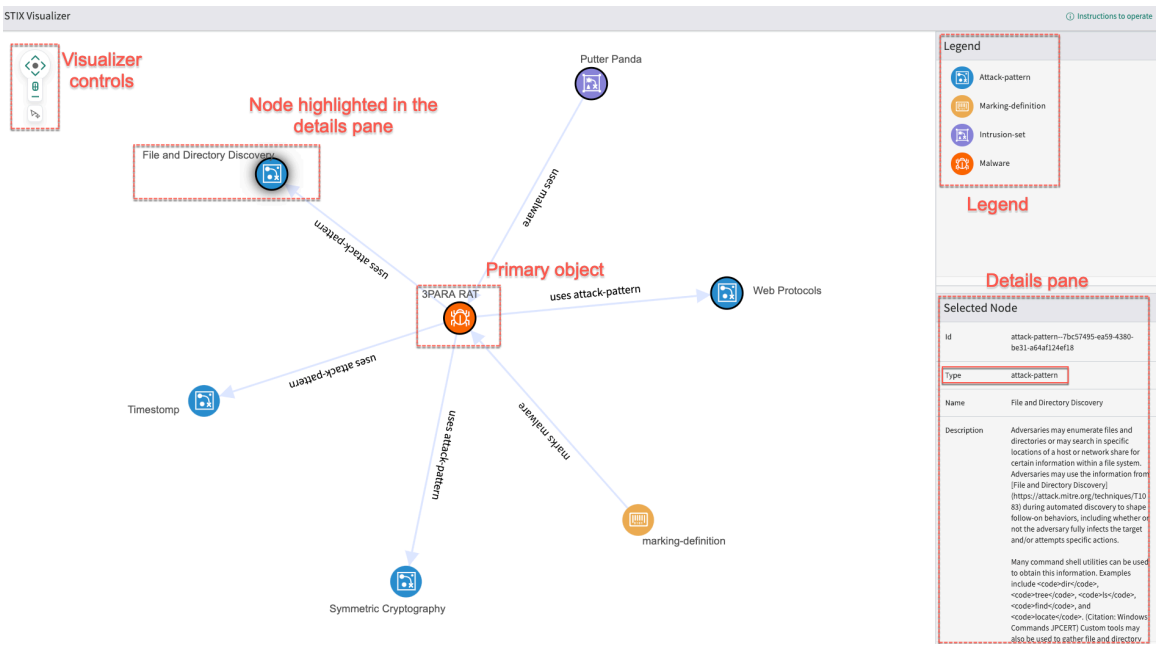
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Access STIX Visualizer



Click Show Relationships in the Related Links section for any of the SDOs to view the STIX Visualizer.

View details in STIX Visualizer



In the Visualizer, you can view the object and its relationship which provides context for you to further investigate. The Visualizer uses colors and icons to illustrate various information about the objects.

You can zoom in to an object, drag the nodes, or pin them to focus on a particular relationship.

Click any object to open the details pane. On the details pane, you can learn more information that is associated with the object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MITRE-ATT&CK™ framework overview

The MITRE-ATT&CK framework is a knowledge base of common tactics, techniques, and procedures (TTP) that your organization can access to develop specific threat models and methodologies against cyberattacks.

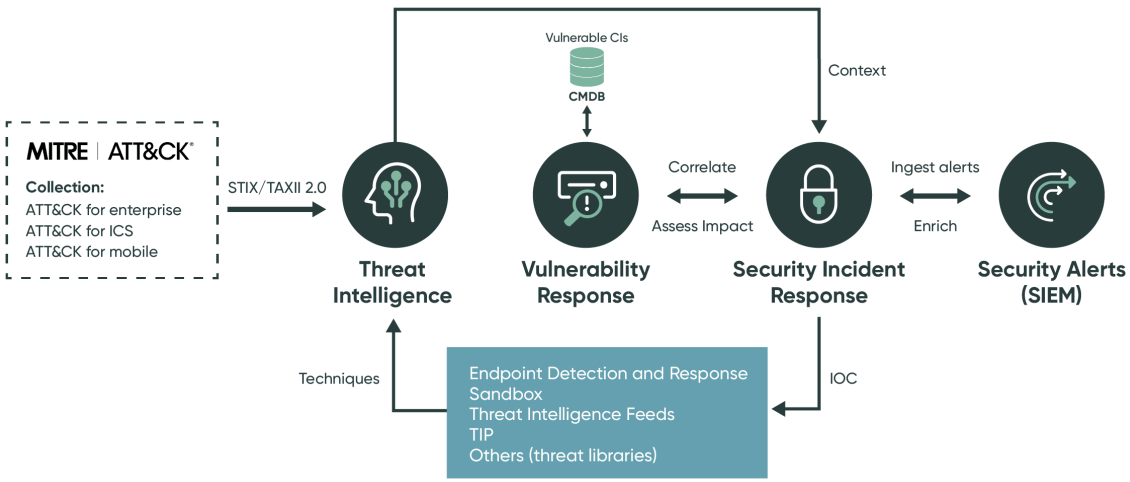
Overview

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework documents and tracks various adversarial techniques that are used during different stages of a cyberattack.

By using the MITRE-ATT&CK framework's knowledge base, the cyberthreat intelligence community can quickly identify threats and coordinate cyberattack responses.

MITRE-ATT&CK and Security Operations

See the following diagram to learn how the MITRE-ATT&CK information flows with Security Operations applications.



- The pre-loaded TAXII client connects to the TAXII server to ingest the data collections to Threat Intelligence.
- Existing Security Information and Event Manager (SIEM) integrations ingest their threat data (alerts and events), with relevant TTPs and are associated with security incidents.
- When an IoC is associated to a security incident, Threat Intelligence automatically searches threat feeds for relevant information and sends IoCs to third-party sources such as EDR, Sandbox, or TIP for additional analysis.
- If any third-party source contains the MITRE-ATT&CK information, then Threat Intelligence extracts the technique information and enriches the data in the Threat Intelligence repository for correlation and analysis.
- MITRE-ATT&CK also shares CVE context information for each technique. Your security team can review the exploited techniques in Vulnerability Response to determine if your business-critical assets are threatened.

MITRE-ATT&CK matrices, tactics, and techniques

The core of the MITRE-ATT&CK framework is a matrix of adversary tactics and techniques. The sequence of the tactics represents what an adversary is trying to accomplish at the stage of an incident. When your security team understands this sequence, you have an opportunity to

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

anticipate an adversary's next move and break the kill chain. ATT&CK consists of the following matrices:

- Enterprise ATT&CK: Describes the behaviors and actions that an adversary takes to compromise and operate in an enterprise network and cloud.

  Note: The Pre ATT&CK matrix has been deprecated by MITRE and is merged with the Enterprise matrix.

- ICS ATT&CK: Describes the actions that an adversary takes while operating within an Industrial Control Systems (ICS) network.
- Mobile ATT&CK: Describes the adversary behaviors and actions that focus on mobile devices.

Tactics represent the why of an ATT&CK technique. It is the adversary's tactical objective for performing an action.

Techniques represent how an adversary achieves a tactical objective by performing an action.

Techniques may be associated with more than one tactic. For example, Access Token Manipulation is used by an adversary to achieve either the tactic of Privilege Escalation or Defense Evasion.

Using an intent-based approach for incident responses

An intent-based response uses a dynamic and contextual kill chain framework that can help your organization to correlate security incidents and to identify a large scope of attacks. Your security team can use an intent-based response to understand how the organization is being attacked and what the attacker might do next. This type of response enables you to predict an attacker's behavior so that you can focus your resources effectively.

Using Security Incident Response, your security team can manage the life cycle of each security incident from analysis to containment by focusing on indicators of compromise (IOCs) like IP addresses, file hashes, and domains.

By integrating Security Incident Response with the MITRE-ATT&CK framework, security incidents are handled as links in a larger enterprise-wide attack.

How your organization can benefit from MITRE-ATT&CK in Security Operations



Using the MITRE-ATT&CK framework can help your organization do the following:

- Equip security analysts with MITRE-ATT&CK tactics, techniques, and procedures (TTPs) to better analyze and respond to security incidents.
- Automate the incident workflows using the playbook for detecting and containing threats in the context of the MITRE-ATT&CK framework.
- Prioritize indicators of compromise and threat hunting with MITRE-ATT&CK information.
- Understand the high-level security posture of your organization in the context of the MITRE-ATT&CK framework.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MITRE-ATT&CK administration

You can set up, map data sources, map overall technique detection coverage, and maintain the MITRE-ATT&CK repository in the ServiceNow AI Platform.

Get started with MITRE-ATT&CK framework

Review the following information before you start setting up your MITRE-ATT&CK framework.

Checklist

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform, Threat Intelligence, and Security Incident Response roles.	The following roles are used across the MITRE-ATT&CK features: • The administrator (admin) installs the applications from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) and threat intelligence administrator (sn_ti.admin) roles. • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst - The MITRE analyst role has been introduced to allow cross-navigation for the MITRE features between Security Incident Response and Threat Intelligence Support Common. With this role, you can view both the Threat Intelligence MITRE module and the Security Incident Response module in read-only mode. • sn_si.read For more information, see Setup Threat Intelligence.
Verify that the ServiceNow core applications that are required to support the MITRE-ATT&CK module are installed and activated.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. • Threat Intelligence Support Common UI Components (sn_ti_seismic) - Version 1.0 or higher • Threat Intelligence Support Common - Version 12.0 or higher • Threat Intelligence - Version 12.0 or higher • Security Incident Response - Version 12.0 or higher

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	For more information on setting up your ServiceNow AI Platform instance for the integration, see get entitlement for a Security Operations product or application and activate a ServiceNow Store application.
Domain separation	Verify the domain separation section if you intend to separate data, processes, and administrative tasks.

Understand the MITRE to STIX data model

Review the terminology used by MITRE and STIX to efficiently use and understand the MITRE-ATT&CK™ framework in the ServiceNow AI Platform.

MITRE objects to STIX mapping

STIX is a language for describing cyber threat information in a standardized and structured manner. The parent data model in the Threat Intelligence module are the STIX objects. While the MITRE objects are a subset to the parent STIX data model. In the MITRE-ATT&CK framework, MITRE provides similar STIX information with certain labels and objects.

MITRE to STIX object mapping

MITRE terminology	STIX terminology
Technique	Attack Pattern
Mitigation	Course of Action
Groups	Intrusion Sets
Malware	Malware
Tool	Tool

Extending data in the Threat Intelligence module

You can maintain a list of Threat Intelligence threat sources and import the needed STIX data that includes an extensive set of cyber threat information. You can also use the TAXII profiles to facilitate automated exchange of cyber threat information.

Note: For more information, see define a threat source and create a TAXII profile.

Extending data in the MITRE-ATT&CK module

You can extend the Malware, Group, Mitigation, and Tool objects to a technique in the MITRE-ATT&CK repository.

You can create an object and establish a relationship between a technique and the new object in the MITRE ATT&CK Repository module, but you can't define the relationship type in this module. To define a relationship type, navigate to the **Threat Intelligence** > **IoC Repository** > **Object-Object Relationships** module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you map the relationship type between an existing technique and an existing object, then you must define the technique as the target object and the object as the source object. To do so, navigate to the **IoC Repository** > **Object-Object Relationships** module.

You can create a group and associate it with an attack pattern, but in the MITRE ATT&CK Repository, you can only establish the relationship between the group and the attack pattern. To define the object-to-object relationship type, you must do so in the IoC Repository.

Note: For more information, see extend MITRE-ATT&CK data and IoC repository.

Domain separation and MITRE-ATT&CK

This domain separation overview pertains to MITRE-ATT&CK. Domain separation allows you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with MITRE-ATT&CK

Follow these steps to achieve domain separation:

- Create a user with the required sn_ti.admin roles in the respective domain.
- Replicate the following for every domain:
  - TAXII Collections

    Note:
    - Do not activate the collections in the global domain. Activate only the collections that are replicated and available in your domain.
    - Change the **Run as** field in the collections to the user with the sn_ti.admin role in the respective domain.

  - Technique Coverage Definition
  - Technique Extraction Rule
  - Detection Rules – MITRE ATT&CK Mappings
  - Mitigation Coverage
    - Copy all the mitigation coverage definition records.
    - Copy the mitigate coverage calculator or create a new calculator for the respective domain.
  - Threat Group - Technique Heatmap Definitions

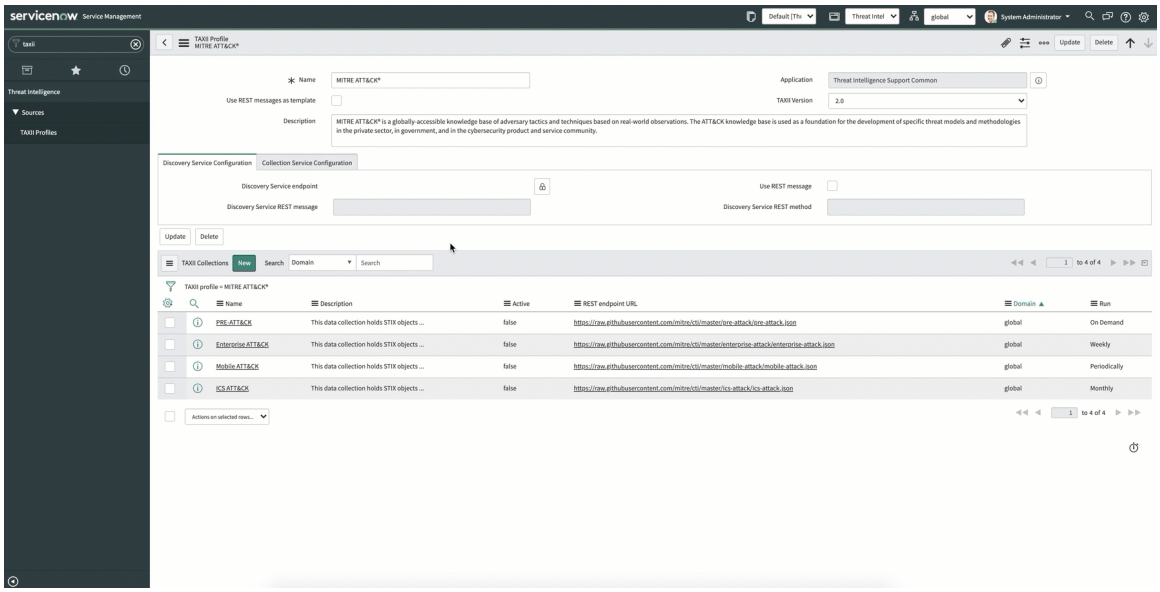
Replicate TAXII Collection

1. Navigate to **Threat Intelligence** > **Sources** > **TAXII Profiles**.
2. In the header bar, use the domain picker to select your domain.
3. Select the TAXII collection that is relevant to your organization (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Right-click in the header bar and select **Insert and Stay**. The duplicate TAXII collection is created under the selected domain
5. Navigate back to the MITRE ATT&CK TAXII Profile to view the duplicate TAXII collection.

The following illustration shows how to select the domain TOP/Initech, replicate the TAXII collection in the domain, and verify the replicated TAXII collection.



Set up the MITRE-ATT&CK™ framework

Activate the MITRE-ATT&CK profile, and set up a scheduled job so that you can set up MITRE-ATT&CK collections for threat detection in your organization.

Before you begin

Role required: sn_ti.admin

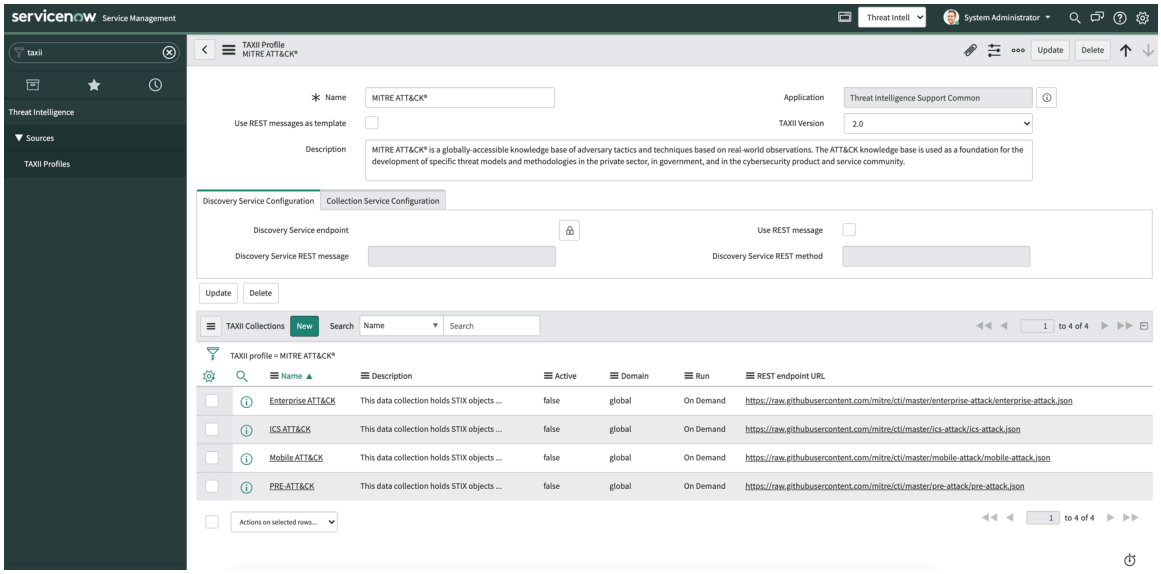
About this task

Structured Threat Information Expression (STIX™) is a language for describing cyberthreat information in a standardized and structured manner. Using STIX data and Trusted Automated Exchange of Indicator Information (TAXII™) profiles, security teams can use shared cyberthreat information to isolate threats that have been previously identified by your company and from other sources.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Sources** > **TAXII Profiles**.
   You see the available TAXII profiles.
2. Click the **MITRE ATT&CK** profile that is provided with the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. To activate the TAXII collection, set the **Active** option to true for the TAXII collection that is relevant to your organization (Enterprise ATT&CK, Mobile ATT&CK, or ICS ATT&CK).

TAXII collection	Description
Enterprise ATT&CK	Describes the behaviors and actions that an adversary takes to compromise and operate in an enterprise network and cloud. **Note:** The Pre ATT&CK matrix has been deprecated by MITRE and is merged with the Enterprise matrix.
Mobile ATT&CK	Describes the adversary behaviors and actions that focus on mobile devices.
ICS ATT&CK	Describes the actions that an adversary takes while operating within an Industrial Control Systems (ICS) network.

4. To periodically refresh the collection, set the **Run** option as appropriate for your organization.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By default this option is set to On Demand.

Note:

a. Collections are packaged as part of Threat Intelligence Core plugin. Installing or updating the Threat Intelligence Support Common - Version 12.0 or higher, and Threat Intelligence - Version 12.0 or higher ensures that your collections data is auto-populated.

b. Activate the TAXII collection only for the collection that you intend to use in your organization and disable the other collections. For example, if you intend to use Enterprise ATT&CK matrix, then activate Enterprise ATT&CK at the TAXII collection level and at the Matrices level. Disable the other Mobile ATT&CK and ICS ATT&CK matrices at the TAXII collection and at the Matrices level.

c. In the TAXII Collections related lists, if you select the Run option as Daily, then an error occurs and the option defaults to On Demand. This error occurs as scheduling the MITRE-ATT&CK data refresh daily is restricted to optimize the load on the MITRE servers. Also, MITRE updates the ATT&CK data only twice a year.

d. The TAXII collections are not refreshed unless you activate the TAXII collection.

e. Updates to existing collections can be retrieved from the MITRE server by scheduling the 'run' frequency in each collection.

f. The customizations that you make to the MITRE-ATT&CK repository data (Malware, Group, Mitigation, and Tool objects to a technique) are saved during scheduled updates.

g. MITRE updates the MITRE-ATT&CK knowledge base where some objects are identified as revoked or deprecated, new objects are added, or existing objects are modified. If MITRE revokes any tactic or technique, then these objects are marked as revoked in the ServiceNow AI Platform. The revoked objects are kept in the repository but are not available for use in the ServiceNow AI Platform.

What to do next

After the TAXII profile setup is complete, the MITRE-ATT&CK repository data is imported at regular intervals to the ServiceNow AI Platform®. You can see this data by navigating to **MITRE ATT&CK Repository** > **Matrices** and **MITRE ATT&CK Repository** > **Techniques**.

Manage matrices

Manage the matrices that have been imported from the MITRE TAXII collections. Matrices are a collection of tactics and techniques. You can view the matrices to review if your collections are available in the MITRE-ATT&CK repository.

Before you begin

Note: Review and verify that only the matrix you intend to use in your organization is set to active and disable the other matrices. For example, if you intend to use the Enterprise ATT&CK matrix, then the Enterprise ATT&CK matrix is activated at the TAXII collection level and in the Matrices level. Disable the other Mobile ATT&CK and ICS ATT&CK matrices at the TAXII collection and at the Matrices level.

Role required:

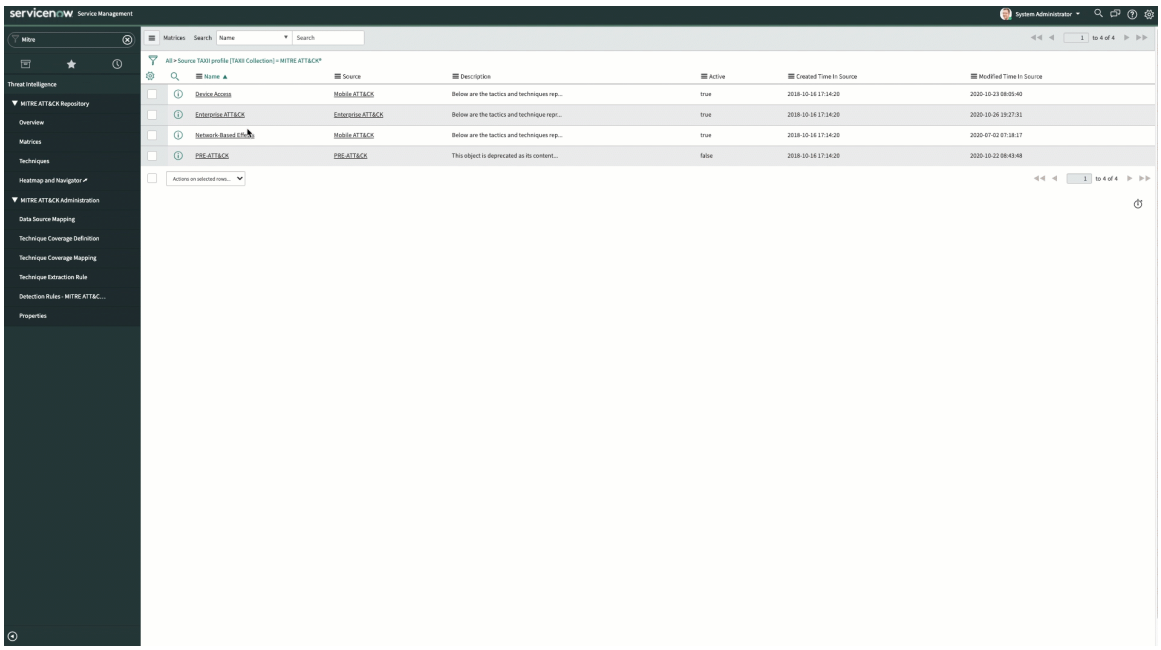
- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Matrices**.
   All matrices are disabled by default.
2. To activate a matrix, point to **Active**, double-click, and select **true**.
3. To view all the associated information, click a matrix.
4. To view all the tactics that are associated with this collection, click the **MITRE Tactics** tab.
5. To view additional details and the techniques that are associated with a selected tactic, click a tactic.
6. Under the **MITRE ATT&CK Techniques** tab, select a technique.
7. Under the related lists, view the associations that are available for the technique that you selected.

   In the following illustration, you can see the navigational path from the Enterprise ATT&CK matrix, to the Initial Access (TA0001) tactic, and then to the Phishing (T1566) technique. On the Attack Pattern - Phishing technique page, you can view the related list - Tactic, Sub Technique, Group, Mitigation, External References, Malware, and Tools.



What to do next

You can extend the information in some of these related list objects based on the technique that you selected. For example, you can add new information for Group, Mitigation, External References, Malware, and Tools.

Manage techniques

Manage the techniques that have been imported from the MITRE TAXII collections. The techniques contain various ways attackers have developed to employ a given tactic. You can review and deactivate techniques that are not relevant to your organization. In STIX, techniques are known as attack patterns.

Before you begin

Role required:

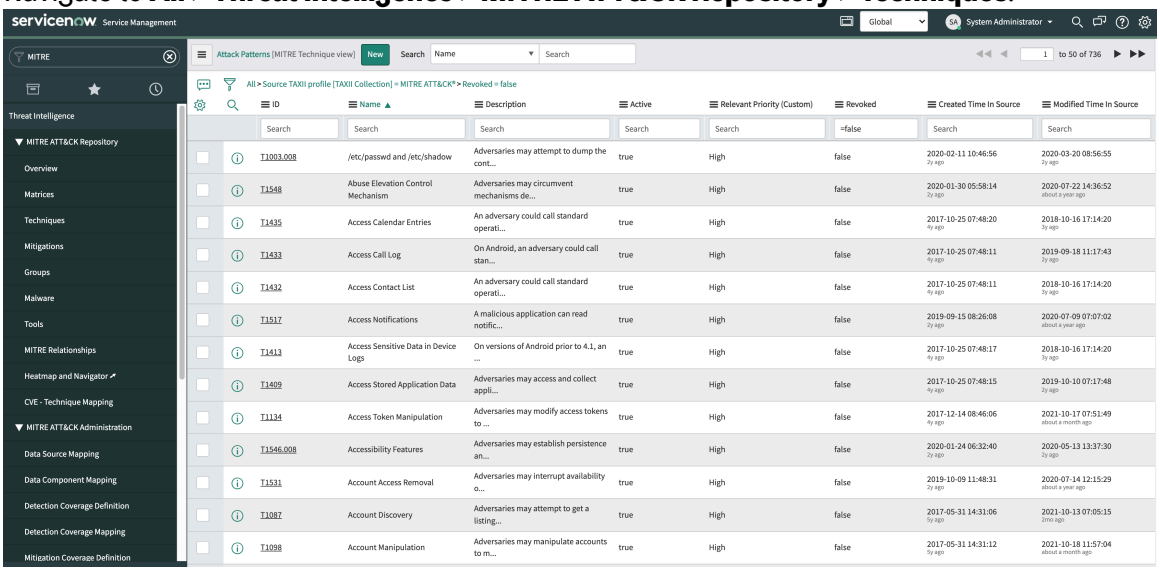
- sn_ti.admin: delete access
- sn_si.admin: create, write, delete access

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_ti.read: read access
- sn_ti.write: create, write access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Techniques**.



   The list of techniques and subtechniques are now listed.

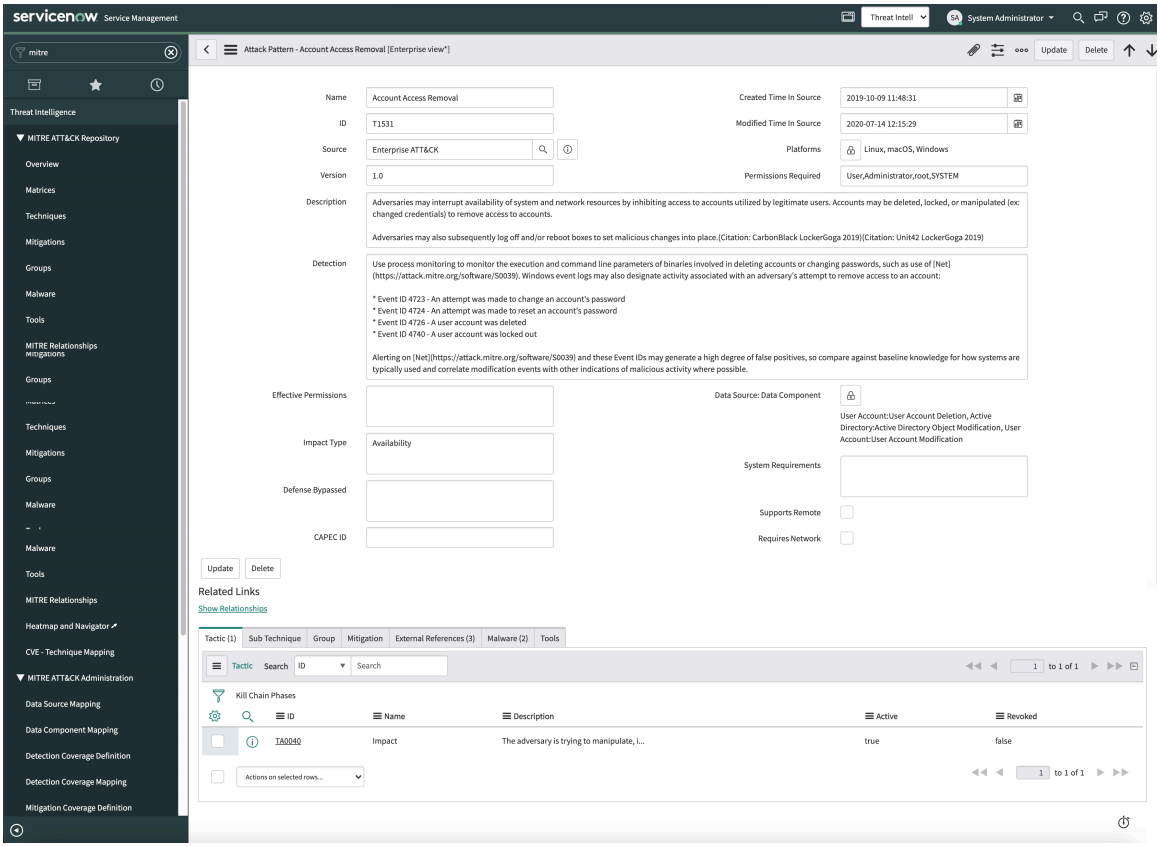
2. To review and deactivate techniques that are not relevant to your organization, go to the list view for the selected technique, and under the Active column, update the setting to **false**, and save the setting.
   Deactivate the techniques that aren't used by the other objects in the MITRE-ATT&CK repository.

3. To prioritize a technique, assign a priority in the **Relevant Priority (Custom)** field.
   The base system relevant priority is set to none. The **Relevant Priority (Custom)** field is not imported from the MITRE-ATT&CK TAXII collections but a custom field introduced in the ServiceNow AI Platform. You can use the relevant priority information to filter and prioritize techniques in the dashboards, during the data source mapping, or when analyzing the heat map.

4. Click a technique to view all the associated information with this technique.

   In the following illustration, you can view the details for each Account Access Removal technique, its ID, source, and other related information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: The Data Source: Data Component element introduced by MITRE replaces the previous Data Source field. Data component provides an extra sublayer of context to the data sources. If your MITRE-ATT&CK repository contains the old TAXII collections, then you can view the Data Source field. Otherwise, you can view the data sources with the additional context of data components in the Data Source: Data Component field. You can view the new data component field only when the source is Enterprise ATT&CK. For more information, see data component mapping.

5. To view how these objects are related, click **Show Relationships**.

What to do next

You can extend the information in some of these related list objects. For example, you can add new information for Group, Mitigation, and External References.

Manage mitigations

Manage the mitigations that have been imported from the MITRE TAXII collections. Mitigations enable you to prevent an adversary from successfully executing techniques or sub-techniques against your organization. In STIX, mitigations are known as course of actions.

Before you begin

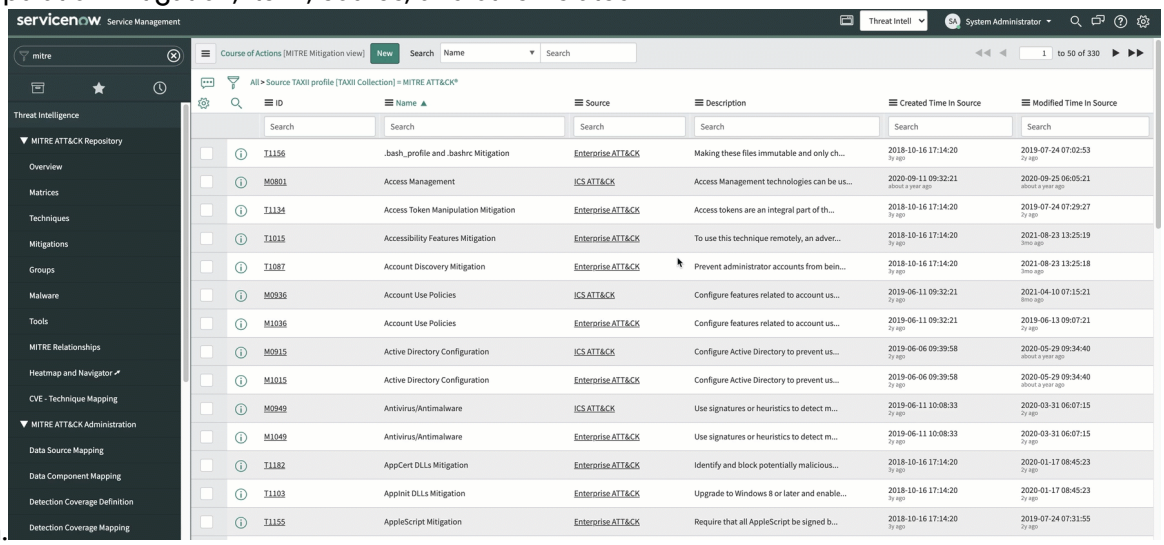
Role required:

- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Mitigations**.
   The mitigations are now listed.
2. Click a mitigation to view all the associated information.
   In the following illustration, you can view the details for Access Token Manipulation mitigation, its ID, source, and other related information.



3. To view how these objects are related, click **Show Relationships**.

What to do next

Use the techniques module to add or modify the mitigations data.

Manage groups

Manage the groups that have been imported from the MITRE TAXII collections. Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. In STIX, groups are known as intrusion sets.

Before you begin

Role required:

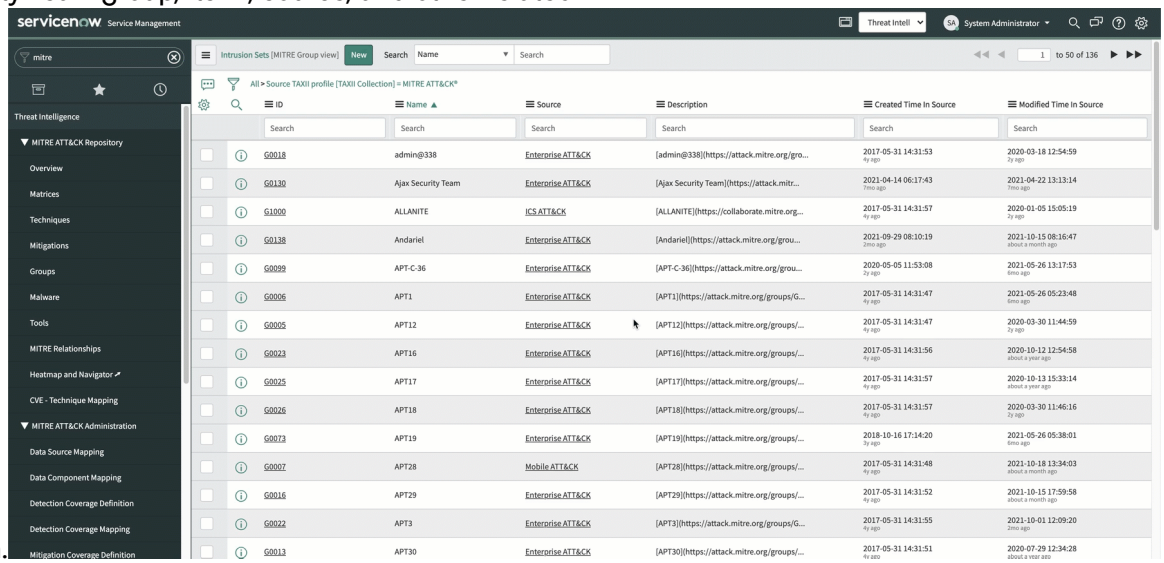
- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Groups**.
   You can view the listed groups.
2. Click a group to view all the associated information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can view the details for the Ajax Security Team group, its ID, source, and other related information.



3. To view how these objects are related, click **Show Relationships**.

Note: To associate the threat groups to a security case for deeper investigation, click **Add to Security Case**.

What to do next

Use the techniques module to add or modify the groups data.

Manage malware

Manage the malware information that you imported from the MITRE TAXII collections. Malware is a type of TTP that represents malicious code. It refers to a program that is covertly inserted into a system. The intent of a malware is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS).

Before you begin

Role required:

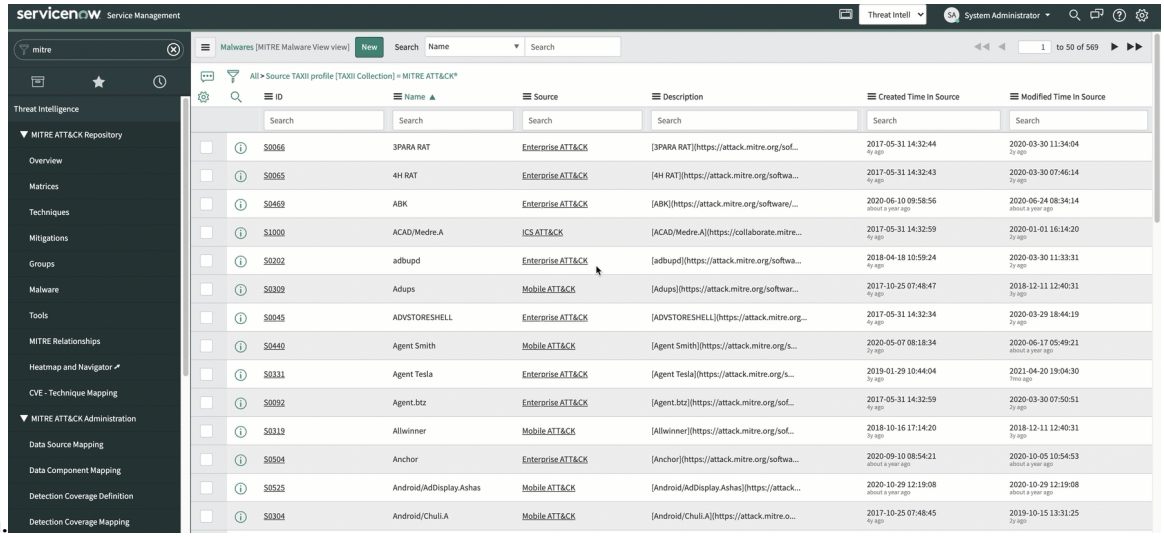
- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Malware**.
   You can view the listed malware.
2. Click a malware to view all the associated information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can view the details for the 3PARA RAT malware, its ID, source, and other related information.



3. To view how these objects are related, click **Show Relationships**.

What to do next

Use the techniques module to add or modify the malware data.

Manage tools

Manage the tools information that you imported from the MITRE TAXII collections. Tools are legitimate software that are used by threat actors to perform attacks.

Before you begin

Role required:

- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

About this task

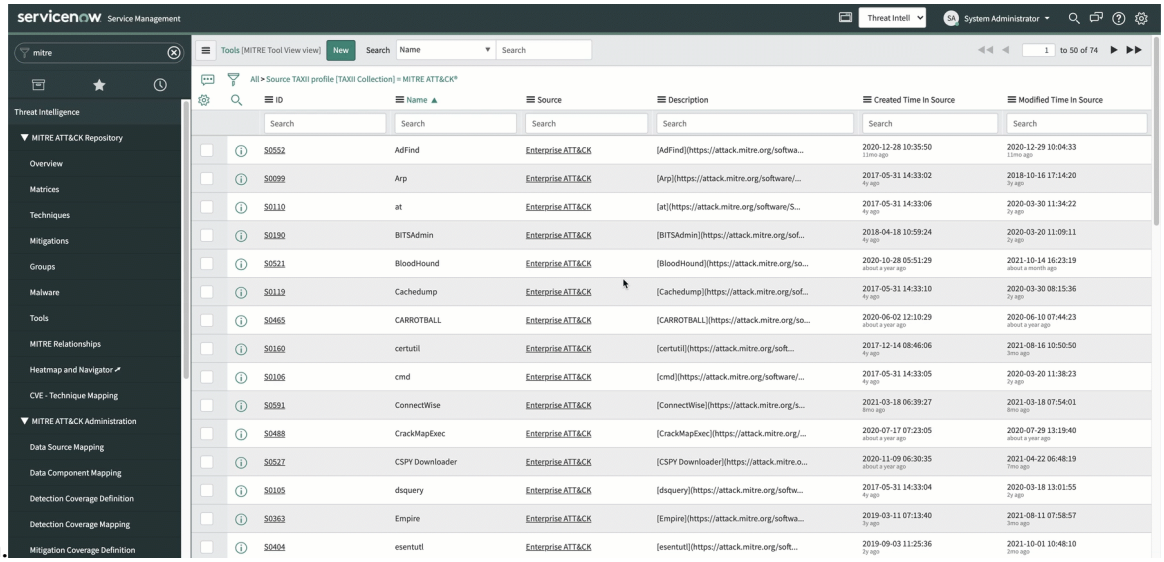
Tools enable you to know how and when threat actors use them for executing campaigns. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, administrators, network administrators, or even normal users.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Tools**.
   You can view the listed tools.
2. Click a tool to view all the associated information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can view the details for the CARROTBALL tool, its ID, source, and other related information.



3. To view how these objects are related, click **Show Relationships**.

What to do next

Use the techniques module to add or modify the tools data.

Manage MITRE relationships

Manage the MITRE relationships information that you imported from the MITRE TAXII collections.

Before you begin

Role required:

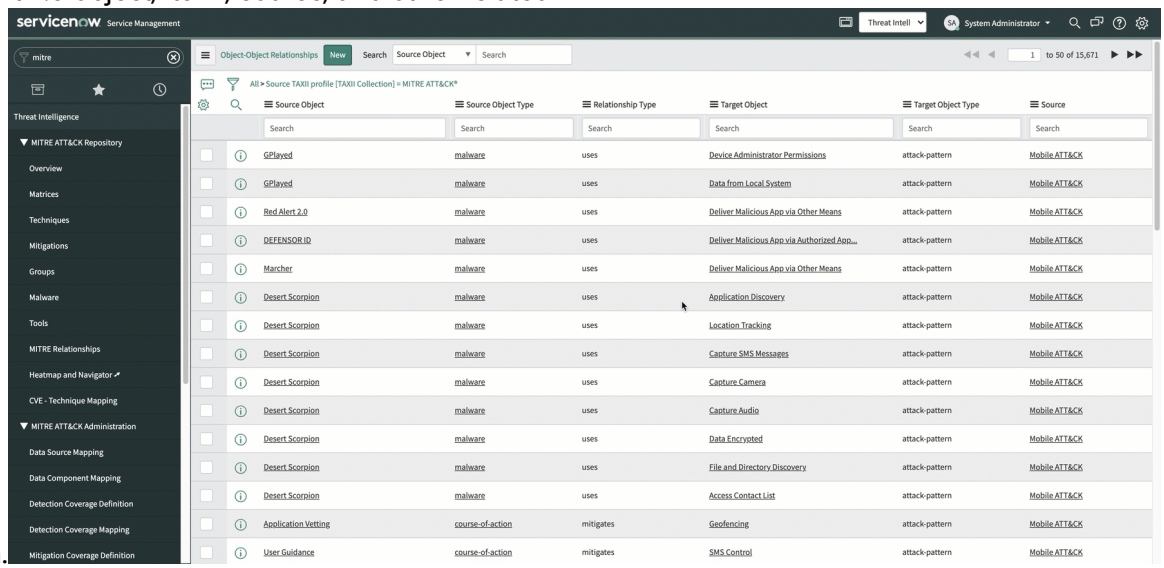
- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **MITRE Relationships**. You can view the listed tools.
2. Click a source object to view all the associated information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can view the details for the Red Alert 2.0 object, its ID, source, and other related information.



3. To view how these objects are related, click **Show Relationships**.

What to do next

Use the techniques module to add or modify the MITRE relationships data.

Manage CVE and technique mapping

Manage the CVE and technique information that is mapped after you import the MITRE TAXII collections.

Before you begin

Role required:

- sn_ti.admin: delete access
- sn_si.admin: create, write, delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

Note: The **CVE-Technique Mapping** module is available only when the Vulnerability Response product is installed in your environment.

About this task

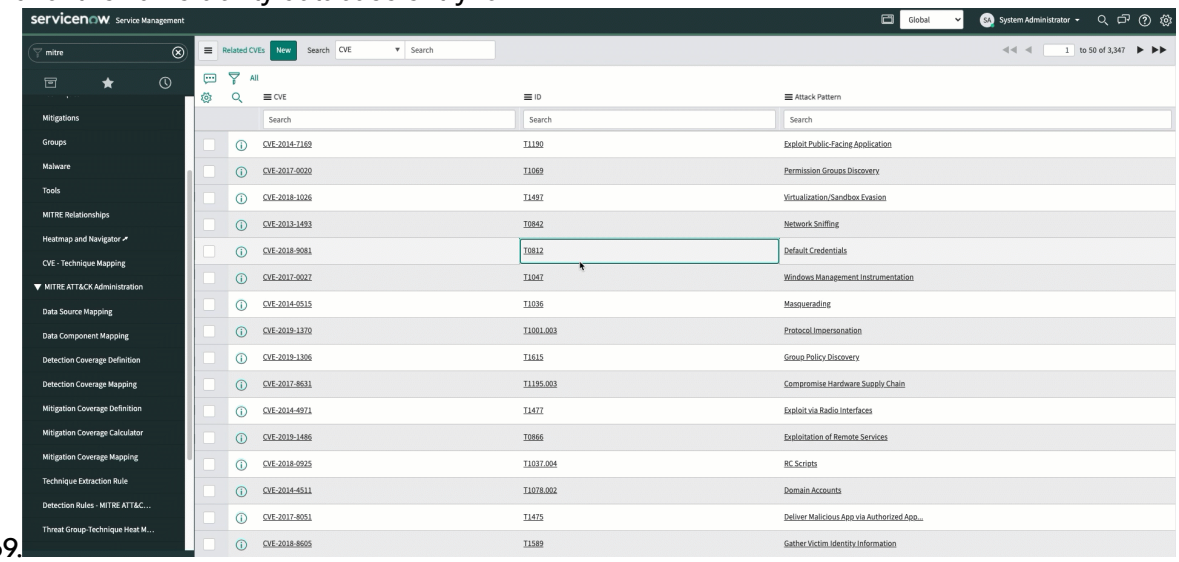
Once you import the MITRE TAXII collections you can view the CVEs in your environment and their relationship with the associated MITRE-ATT&CK techniques. You can also create associations with CVEs and the attack patterns.

Procedure

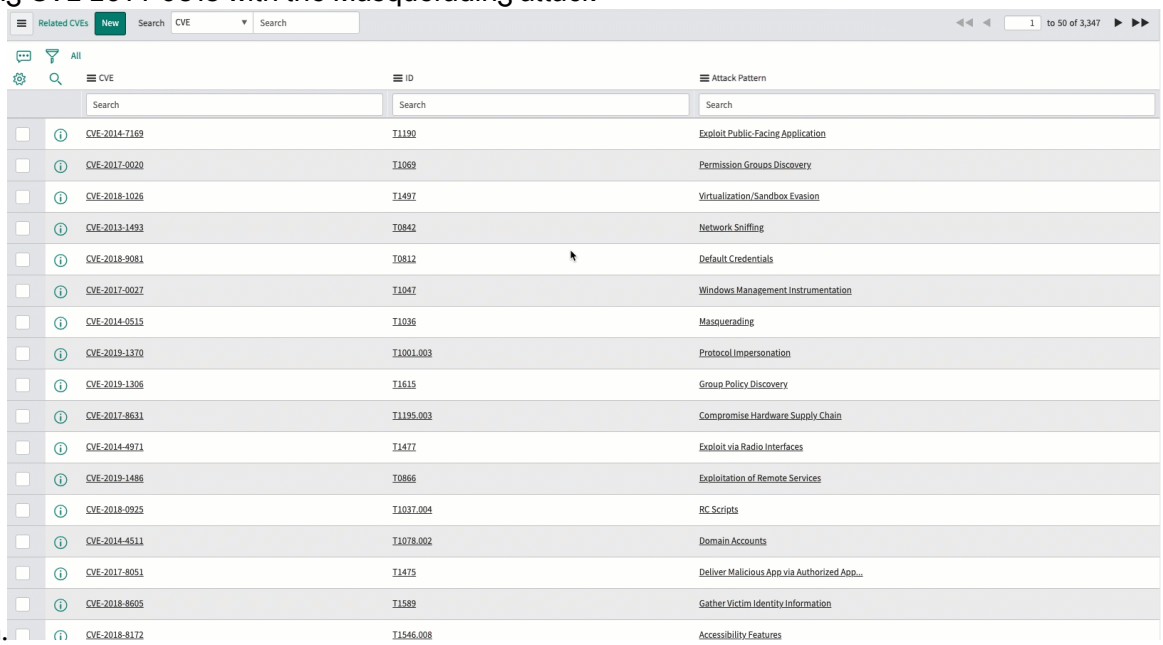
1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **CVE - Technique Mapping**.
   You can view the listed CVEs and techniques.
2. Click a CVE to view the vulnerability database entry.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can view the details for the CVE list and for the vulnerability database entry for CVE-2014-7169.



3. To add an entry, click **New**, map the CVE to an Attack Pattern, and click **Submit**.
   In the following illustration, a new entry is created by mapping CVE-2014-0515 with the Masquerading attack pattern.



Extend the MITRE-ATT&CK data

Extend the MITRE-ATT&CK repository data in the ServiceNow AI Platform by enriching it.

Before you begin

Role required:

- sn_ti.admin: delete access
- sn_ti.read: read access
- sn_ti.write: create, write access

About this task

You can extend the Malware, Group, Mitigation, and Tool objects to a technique in the MITRE-ATT&CK repository.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can create a new object and establish a relationship between a technique and the new object in the MITRE ATT&CK Repository module, but you can't define the relationship type in this module. For more information about defining relationship types, see object to object relationships. To define a relationship type, navigate to the **Threat Intelligence** > **IoC Repository** > **Object-Object Relationships** module.

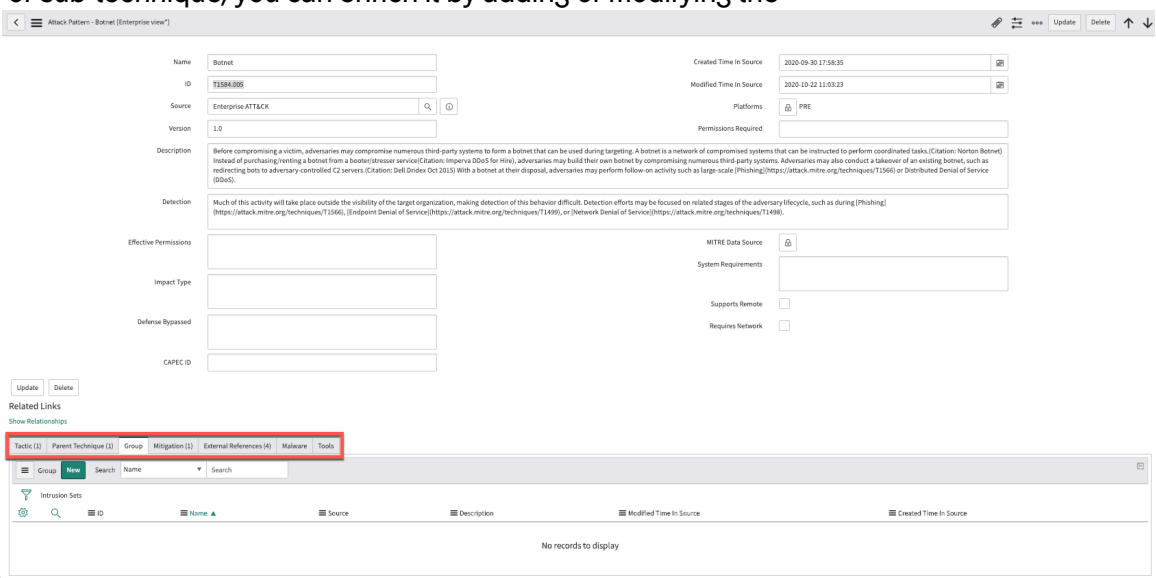
If you map the relationship type between an existing technique and an existing object, then you must define the technique as the target object and the object as the source object. To do so, navigate to the **IoC Repository** > **Object-Object Relationships** module.

You can create a group and associate it with an attack pattern, but in the MITRE ATT&CK Repository, you can only establish the relationship between the group and the attack pattern. To define the object-to-object relationship type, you must do so in the IoC Repository.

Note: Any customizations that you make to the objects are saved during scheduled updates.

Procedure

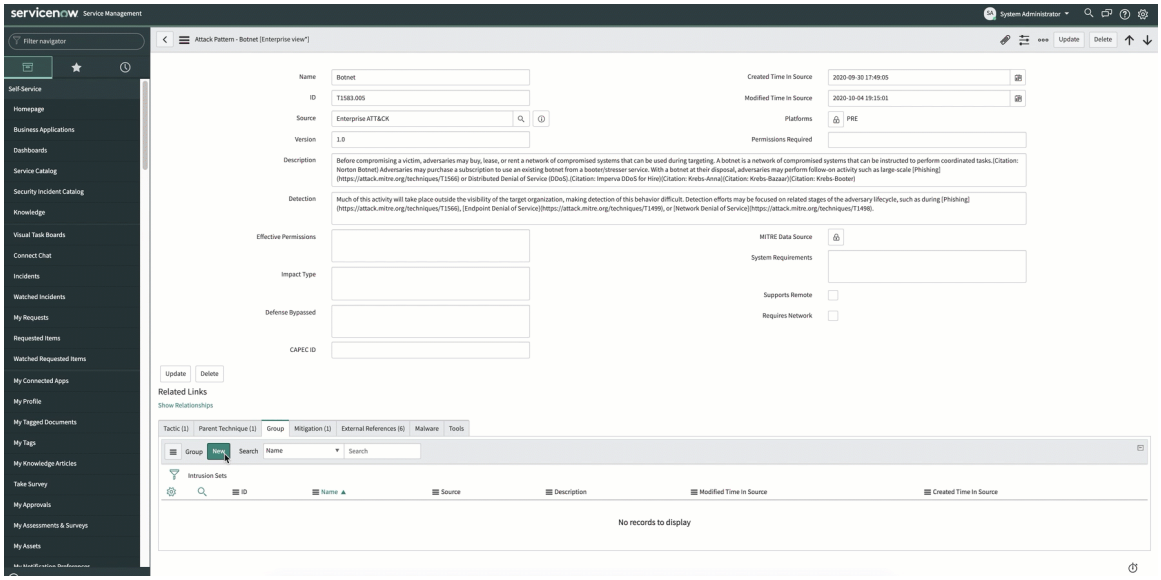
1. Navigate to **Threat Intelligence** > **MITRE ATT&CK Repository** > **Techniques**.
2. Click a techniques or sub-technique to view all the associated information with this technique. In the following illustration, you can see that the Botnet (T1584.005) technique is not associated with any group. If you have additional information about a technique or sub-technique, you can enrich it by adding or modifying the information.



3. Click a related list to enrich its data to associate it with a new group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, a group, Custom1, has been associated with the Botnet sub-technique.



Define the data source and detection tool mapping

Define the data source and detection tool mapping for MITRE-ATT&CK tactics and techniques. The data source mapping provides you with insight into the relevance and availability of the data sources and the detection tools for monitoring the data sources in your environment.

Before you begin

Role required:

- sn_ti.admin, sn_si.admin: write, delete access
- sn_ti.read: read access

About this task

You can identify the data sources and the detection tools that your organization needs to detect the techniques effectively.

For example, if your organization focuses on 5 techniques, you may need 10 data sources and 10 detection tools to monitor those sources. Let's say that you identify that your organization does not have two data sources and five detection tools. This exercise gives you visibility into the data sources, their relevance to your organization, and to identify gaps in the coverage. You can also focus on enhancing your environment with the right data sources and detection tools.

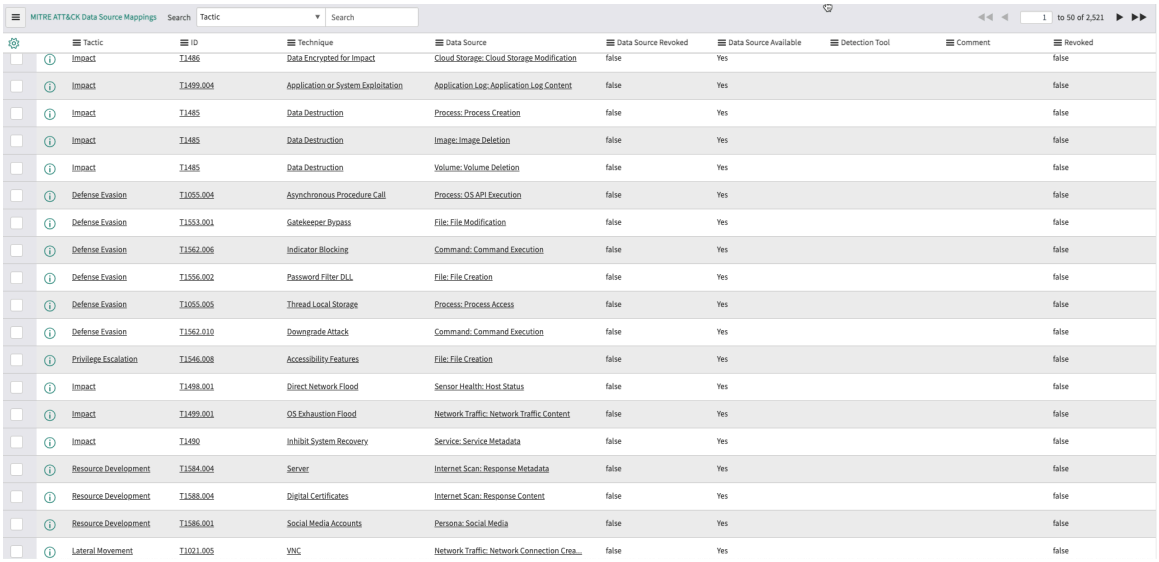
All the active tactics, techniques, ID, and data sources are automatically populated based on your TAXII profile

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Data Source Mapping**.

   The following illustration shows the list of tactics, techniques, and their IDs that have been populated based on your collection updates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

Field	Description
Tactic	Adversary's objective or the reason for performing an action.
ID	Technique's unique identity.
Technique	How an adversary achieves a tactical objective by performing an action.
Data Source	Data source that is associated with the technique.
Data Source Revoked	Data source is revoked if set to true, however the data source mapping is still retained. If the data source value is not found in MITRE, then the Data Source Revoked value is automatically marked as true. The data source mapping for a record is revoked if the technique and data source relationships are missing from the updated MITRE data. Default: false
Data Source Available	Availability of the data source.
Detection Tool	Tool that supplements the data source by detecting the techniques that are used. The detection tool is mapped with the alert sensor in SIR.
Revoked	The data source mapping for a record is revoked if the technique and data source relationships are missing from the updated MITRE data. Default: false

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Review the listed data sources and modify the value in the **Data Source Available** field based on your environment.

3. **Note:** You cannot edit this entry from the list view.

   In the **Detection Tool** field, do the following steps:

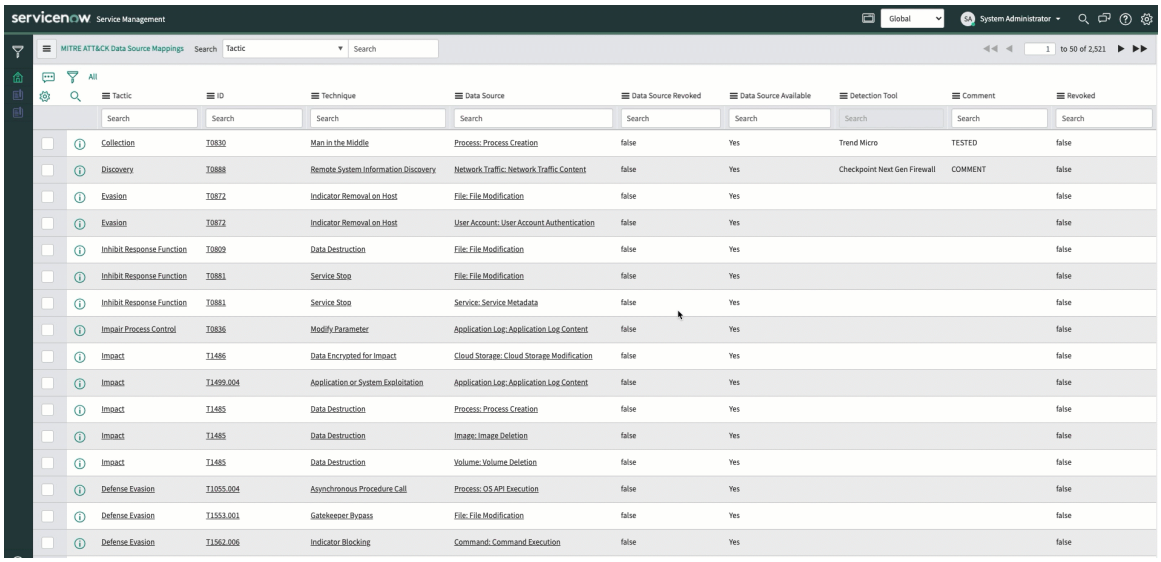
   a. Click the information icon, and click **Open Record**.

   b. Unlock **Detection Tool** entry.

   c. Use the lookup list to select a detection tool. You can multi-select detection tools.

   d. Click **Update**.

   In the following illustration, multiple detection tools are added to monitor the data source.



Define the data source and data component mapping

Use the Data Component Mapping if you are using the latest TAXII collections, and you want to maintain a relationship between the data sources, data components, and the various techniques. Map the data sources with the additional context of data components that provides an extra sublayer of context to data sources that enable you to understand adversary behaviors in MITRE-ATT&CK better.

Before you begin

Role required:

- sn_ti.admin, sn_si.admin: write, delete access
- sn_ti.read: read access

About this task

Mapping the data sources and data components provides visibility into the data sources or components and the techniques that are relevant for your organization.

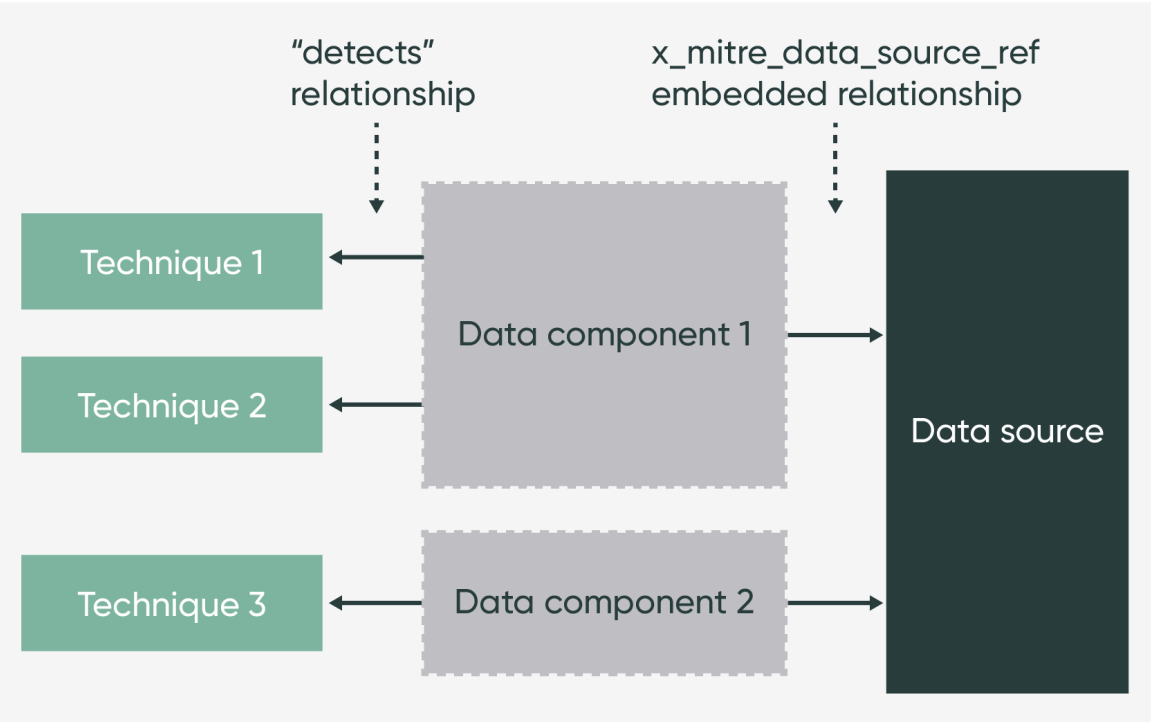
For example, if your organization focuses on 7 techniques, you may need 5 data sources and 10 data components to monitor these sources. Your evaluation of internal tools reveals that your organization doesn't have two data sources and four data components. This mapping exercise provides visibility into the data sources, components, & techniques, their relevance to your organization, and to identify the gaps in coverage. You can thus focus your investment on the right data sources and alert sensors to detect and mitigate adversary threats.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The MITRE-ATT&CK framework contains an updated structure for the data sources - Data Source: Data Component. This new form of data source provides an extra context to the data sources. The data source object features the name of the data source as well as key details about the collected data (file, process, network traffic, and so on) and specific values or properties required to detect adversary behaviors.

The following illustration shows the MITRE-ATT&CK STIX™ structure representation for data sources and data components. You can see both the data sources and data components captured as custom STIX™ objects. The illustration shows that each data source contains one or more data components, and each data component detects one or more techniques.

General structure of data sources and data components

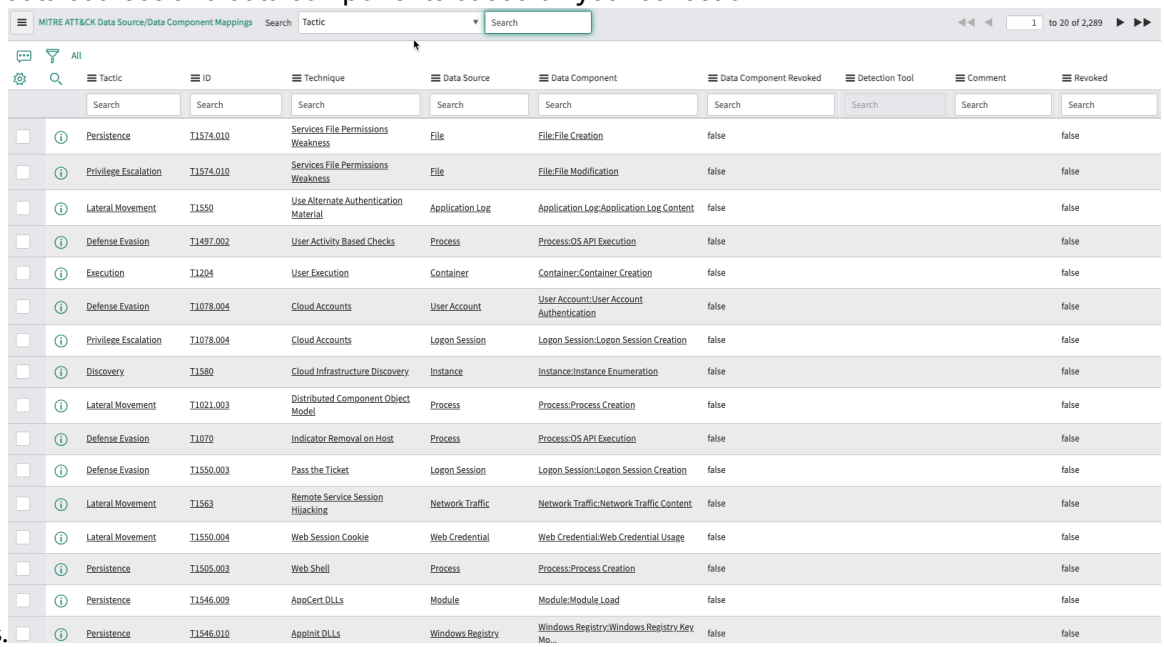


You can continue using the Data Source Mapping if your MITRE-ATT&CK repository contains the old TAXII collections, and you've mapped your data sources to various techniques. However, use the Data Component Mapping if you're using the latest TAXII collections, and you want to maintain a relationship between the data sources, data components, and the various techniques.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Data Component Mapping**.
   The following illustration shows the list of tactics, IDs, techniques along with the data sources and data components based on your collection updates.

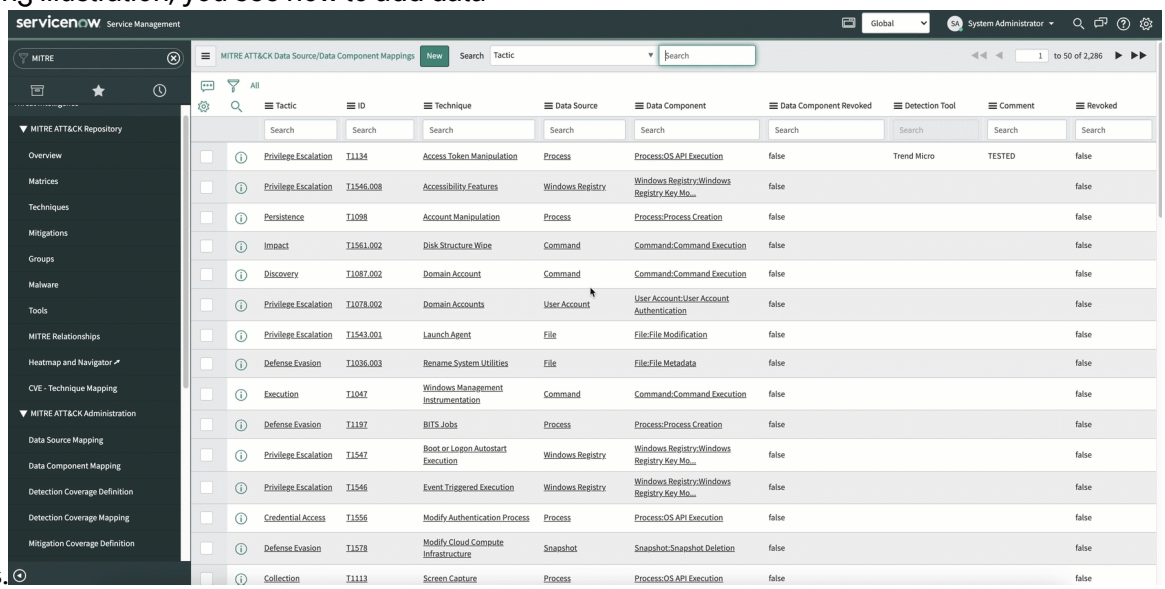


Field	Description
Tactic	Adversary's objective or the reason for performing an action.
ID	Technique's unique identity.
Technique	How an adversary achieves a tactical objective by performing an action.
Data Source	Data source that is associated with the technique.
Data Component	Data component that is associated with the data source. A data component can only have one parent data source.
Data Component Revoked	Identifies if the data component has been revoked in the MITRE-ATT&CK knowledge base.
Detection Tool	Tool that supplements the data source by detecting the techniques that are used. The detection tool is mapped with the alert sensor in SIR.
Comment	Description about the data source and data component mapping.
Revoked	Identifies if the data component to technique mapping is revoked by MITRE-ATT&CK.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Review the listed data sources and data components and modify the values based on your environment.
3. Follow these steps to add a data component.
   a. Navigate to **Threat Intelligence** > **MITRE ATT&CK Administration** > **Techniques**.
   b. Click a technique that you want to modify the data source: data component information.
   c. Unlock Data Source: Data Component.
   d. Use the lookup list to select MITRE-ATT&CK data components.
   e. Lock Data Source: Data Component.
   f. Click **Update**.

In the following illustration, you see how to add data components.



Define the technique detection coverage

Define the technique detection coverage that your organization must measure and detect specific adversary techniques.

Before you begin

- Role required: sn_ti.admin, sn_si.admin: write access
- Role required: sn_ti.read: read access

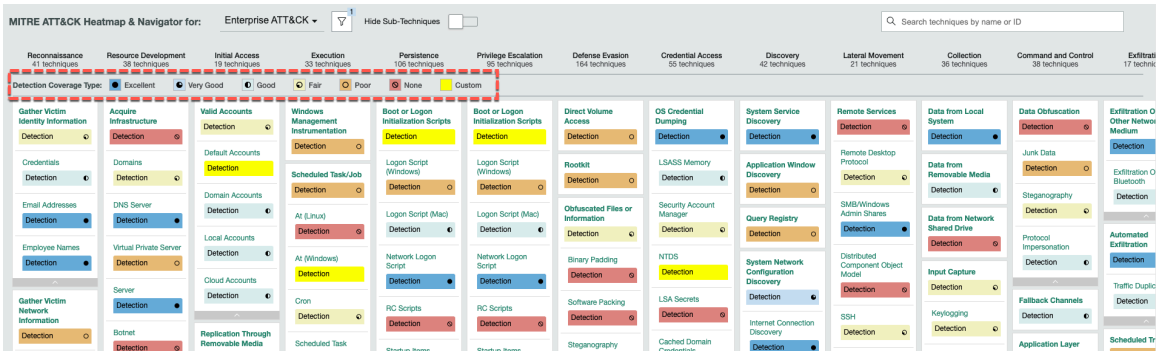
About this task

The technique coverage definitions are used in the overall technique detection mapping. You can use the base system technique coverage. The base system technique coverage consists of coverage types None, Poor, Fair, Good, Very Good, and Excellent. The base system technique coverage is also associated with pre-defined colors. You can customize the coverage type entries and colors, or create your own entries. For example, you can modify the base system coverage types to Not Applicable, Partial Coverage, and Complete Coverage. Alternatively, you can also create numerical measures for the coverage types such as 0-25 percent, 25–50 percent, and 50–100 percent. The type of modifications done to the base system coverage are not limited to the examples shared.

The customizations that you make to the coverage type and color are used in the overall technique detection mapping and also in the heat map.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you modify the base system coverage definition, the Coverage Type icons do not display with the techniques in the heat map. The heat map works as expected when you modify the same fields as the base system's-defined technique detection coverage and coverage colors. However, if you delete existing fields from the overall technique detection coverage, the heat map does not display the coverage type icons.



Procedure

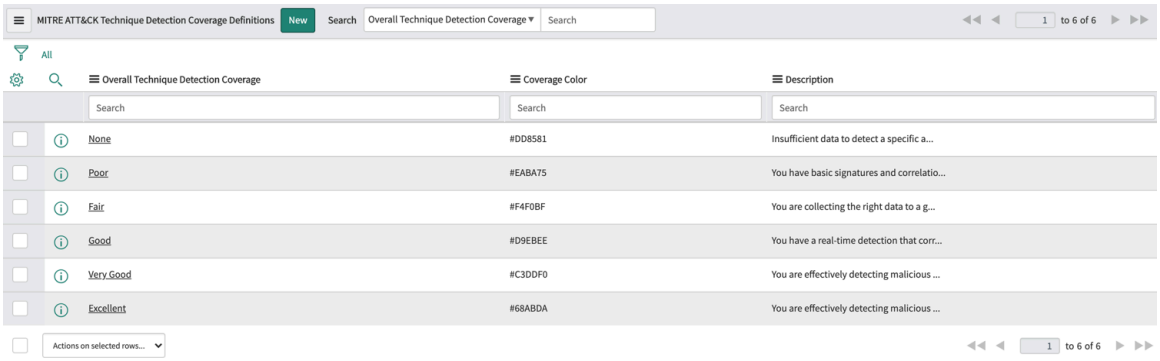
1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Detection Coverage Definition**.
2. Review the overall technique detection entries and customize the entries for your environment.

Detection Coverage Definition

Field	Description
Overall Technique Detection Coverage	Name of the overall technique detection coverage. The base system technique coverage consists of None, Poor, Fair, Good, Very Good, or Excellent.
Coverage Color	Color that is assigned to the detection coverage score. The color that you define is used for the technique detection coverage in the heat map. You can customize the colors using HEX codes and RGB(A) values.
Description	Overall technique detection coverage. See the base system definition in the Scoring Definition.

The following illustration shows the Detection Coverage Definition list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. To add an entry, click **New**, complete the entries, and click **Submit**.

MITRE-ATT&CK Scoring definition

Define your organization's MITRE-ATT&CK scoring system so that you can measure how effectively your organization can detect specific adversary techniques.

Scoring definition

Score	Score mapping	Description
None	0	Insufficient data to detect a specific adversary technique.
Poor	1	Basic signatures and correlation rules are in place to detect specific adversary techniques. Threat detection is not in real time and covers only a minimal number of aspects of a technique. For example, hunting occurs only on one endpoint at a time. Your organization might still have thousands or hundreds of events that hunters must review and correlate with other events to find outliers. The number of false positives is high.
Fair	2	Collecting the right data to a great extent and the data quality is fair. For example, your organization might be starting to add Sysmon Logs, ETW, PowerShell logs, and the like. However, the threat detection is still not in real time. Your organization may not have all the right tools to effectively aggregate and analyze the data. Hunters must manually run queries and correlate to accurately analyze the data. The number of false positives is high.
Good	3	Real-time detection that correlates and integrates multiple data across your endpoints. Threat detection covers many aspects of a technique's procedures. Your adversaries could possibly bypass detection with evasion and obfuscation. Your organization can easily identify false positives and filter them out. Your organization uses basic data science techniques to analyze the data in the central repository.
Very Good	4	Effectively detect malicious techniques in real time and cover most aspects of a technique's procedures.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scoring definition (continued)

Score	Score mapping	Description
		The possibility of your adversaries bypassing detection with evasion and obfuscation methods is harder than at the Good level. Your organization can easily identify false positives and filter them out. Your organization uses advanced data science techniques to detect the adversary techniques.
Excellent	5	Effectively detect malicious techniques in real time and cover all aspects of a technique's procedures. Your organization has a good understanding of your environment with the right automation and quality of data. The possibility of your adversaries bypassing detection with evasion and obfuscation methods is not possible at this level. The number of false negatives is low.

Map your technique detection coverage to a technique

Map your overall technique detection coverage with the technique that enables your organization to detect specific adversary techniques.

Before you begin

- Role required: sn_ti.admin, sn_si.admin: write access
- Role required: sn_ti.read: read access

About this task

You can use the technique detection coverage to get an overview into your organization's overall technique detection coverage. For example, if an adversary is attacking your organization, you see the kind of coverage that you have to detect the attacker's techniques.

The technique and ID are automatically populated for all the collections and techniques that you have activated. The coverage type and scoring definition that you have defined are available for as an option that you can select in the overall technique detection coverage.

You can map the overall technique detection coverage with the technique to complete the mapping. You can associate a technique with only one overall technique detection coverage.

The technique detection coverage mapping that you define is used in the coverage visualization in the heatmap.

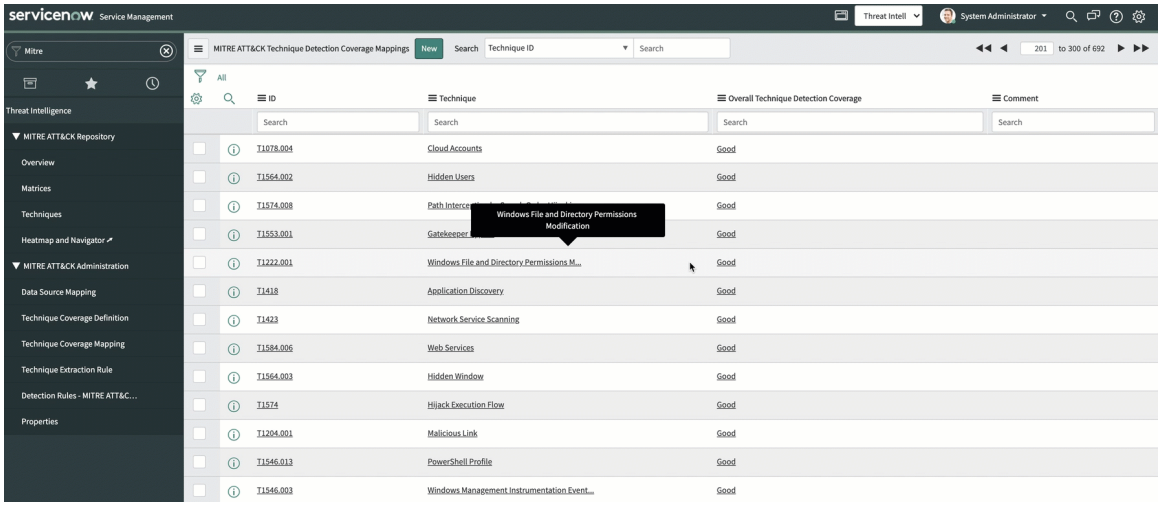
Note: You can arrive at the overall technique detection coverage using your organization-specific calculations. You may use any Breach & Attack Simulation (BAS) products, the Cyber Analytics Repository (CAR), or any other methods as necessary to define the scoring definition, and use it in this procedure for the overall technique detection coverage mapping.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Detection Coverage Mapping**.

   In this illustration, you see that the Cloud Accounts (T1078.004) sub-technique has excellent coverage in the organization and that the Overall Technique Detection Coverage is mapped to **Excellent**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. Review each technique and map your overall technique detection coverage based on your detection coverage definition and your organization's coverage availability.

Define the mitigation coverage

Define the mitigation coverage for each mitigation that is associated with a technique so that you gain visibility into how well your organization can prevent the attacks that happen due to a particular technique.

Before you begin

- Role required: sn_ti.admin, sn_si.admin: create, write, delete access
- Role required: sn_ti.read: read access

About this task

The mitigation coverage definitions are used in the overall mitigation and technique coverage mapping. You can use the base system mitigation coverage. The base system mitigation coverage consists of coverage types None, Poor, Fair, Good, Very Good, and Excellent. The base system mitigation coverage is also associated with pre-defined colors, and coverage percentages. You can customize the coverage types (add or remove coverage types), coverage percentages for lower limits and higher limits, and colors, or create your custom mitigation coverage.

The customizations that you make to the coverage types, colors, or percentages are used in the mitigation coverage mapping and also in the heat map.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Mitigation Coverage Definition**.
2. Review the mitigation detection entries and customize the entries for your environment.

Technique Mitigation Coverage Definition

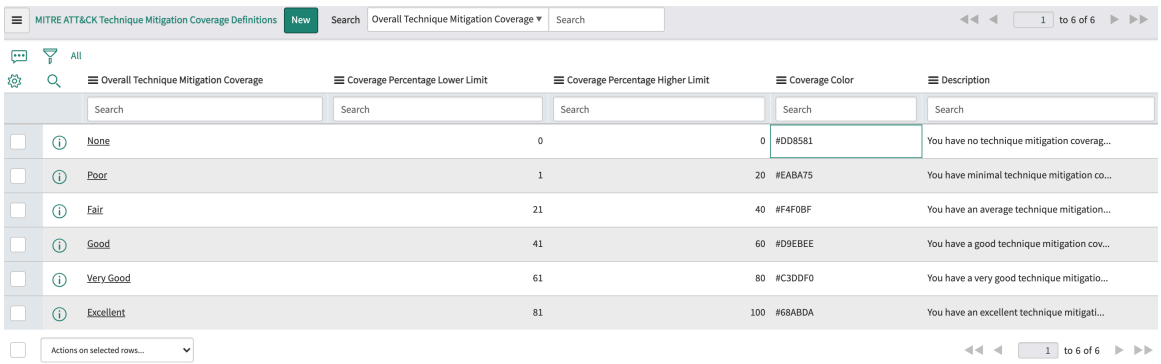
Field	Description
Overall Technique Mitigation Coverage	Name of the technique mitigation coverage. The base system mitigation coverage consists of None, Poor, Fair, Good, Very Good, or Excellent.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Coverage Percentage Lower Limit	The lower percentage limit of the mitigation coverage. Define the numerical values between 0 through 100.
Coverage Percentage Higher Limit	The higher percentage limit of the mitigation coverage. Define the numerical values between 0 through 100.
Coverage Color	Color that is assigned to the detection coverage score. The color that you define is used for the technique mitigation coverage in the heat map. You can customize the colors using HEX codes and RGB(A) values.
Description	Overall mitigation detection coverage. See the base system definition in the technique mitigation coverage definition.

Note: Ensure that you do not overlap the coverage percentage ranges if you customize the percentage limits (lower or higher). For example, if a coverage record has the ranges 0 to 20, then the next consecutive record must have lower limit range of 21 or higher to avoid overlapping the coverage percentage range.

The following illustration shows the mitigation coverage definition list.



3. To add an entry, click **New**, complete the entries, and click **Submit**.

Technique mitigation coverage definitions

Define your organization's mitigation coverage so that you can effectively measure and detect specific adversary techniques.

MITRE ATT&CK Technique Mitigation Coverage Definitions

Overall Technique Mitigation Coverage	Coverage Percentage Lower Limit	Coverage Percentage Higher Limit	Coverage Color	Description
None	0	0	#DD8581	You have no technique mitigation coverage, and your defence controls have no

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MITRE ATT&CK Technique Mitigation Coverage Definitions (continued)

Overall Technique Mitigation Coverage	Coverage Percentage Lower Limit	Coverage Percentage Higher Limit	Coverage Color	Description
				ability to prevent an attack in any scenario.
Poor	1	20	#EABA75	You have minimal technique mitigation coverage. The chances of an attack are very high, and your defence controls can prevent an attack in 0 to 20 percent of the scenarios.
Fair	21	40	#F4F0BF	You have an average technique mitigation coverage. The chances of an attack are high, and your defence controls can prevent an attack in 21 to 40 percent of the scenarios.
Good	41	60	#D9EBEE	You have a good technique mitigation coverage. However, the chances of an attack are relatively high, and your defence controls can prevent an attack in 41 to 60 percent of the scenarios.
Very Good	61	80	#C3DDF0	You have a very good technique mitigation coverage. The chances of an attack are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MITRE ATT&CK Technique Mitigation Coverage Definitions (continued)

Overall Technique Mitigation Coverage	Coverage Percentage Lower Limit	Coverage Percentage Higher Limit	Coverage Color	Description
				low, and your defence controls can prevent an attack in 61 to 80 percent of the scenarios.
Excellent	81	100	#68ABDA	You have an excellent technique mitigation coverage and the chances of an attack using this technique is very low and your defence controls can prevent an attack in 81 to 100 percent of the scenarios.

Map your mitigation coverage to a technique

Map your mitigation coverage with the technique that enables you to detect your organization's overall mitigation strategy.

Before you begin

- Role required: sn_ti.admin, sn_si.admin: write, delete access
- Role required: sn_ti.read: read access

About this task

Mitigations enable you to prevent an adversary from successfully executing techniques or sub-techniques against your organization. Each MITRE-ATT&CK technique contains mitigations that you can deploy in your organization to reduce the chance of being attacked. You can use the mitigation coverage to get an overview of your organization's overall mitigation strategy. For example, if an adversary is attacking your organization, you see the kind of coverage that you have to mitigate the attacker's techniques.

The technique, and mitigation information are automatically populated for all the collections and techniques that you have activated. The mitigation coverage definition that you have defined are available for you to select in the technique mitigation coverage.

You can identify mitigations that are relevant to your organization. If a mitigation is relevant, then you can define if the mitigation strategies have been deployed. You can specify if the strategies are applied as part of your organization's SOC Policy. You can also identify if your organization has preventive tools in place to mitigate an attacker's techniques and you can map any security controls that your organization has deployed to minimize security risks. Populate the mitigation coverage (percentage) for each of the records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After mapping the information for each of the techniques, the mitigation coverage calculator auto populates the Calculated Technique Mitigation Coverage. To calculate the overall mitigation coverage for any technique, the technique mitigation mapping records must be active and relevant to the organization. The records which are inactive and not relevant are not considered for calculating the overall technique mitigation coverage. Based on the values in the Calculated Technique Mitigation Coverage and the mitigation coverage definition, your Overall Technique Mitigation Coverage (Calculated) is populated.

The customizations that you make to the coverage types, colors, or percentages are used in the mitigation coverage mapping and also in the heat map.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Mitigation Coverage Mapping**.
2. Review each technique to mitigation mapping and update the **Mitigation Coverage (Percentage)** to calculate your organization's coverage availability.

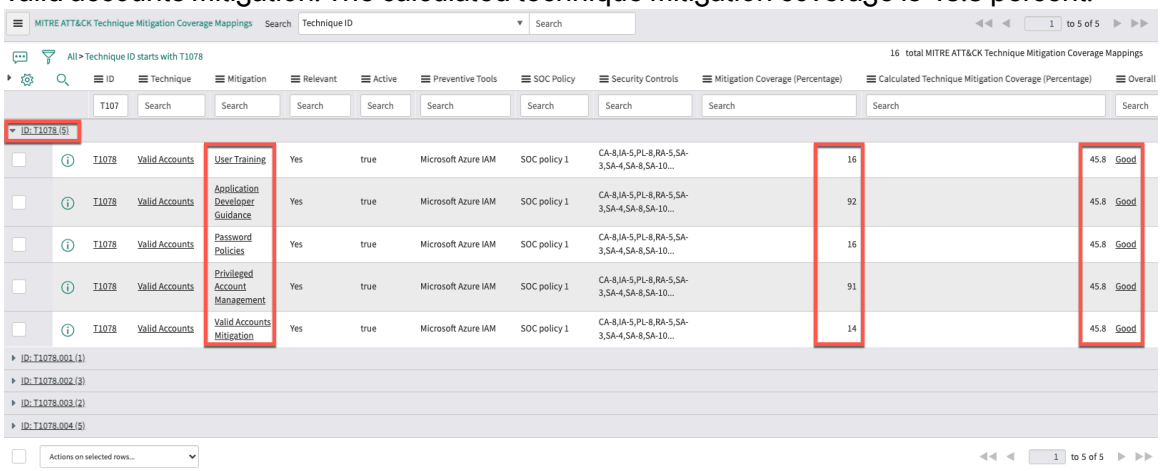
Technique Mitigation Coverage Mappings

Field	Description
ID	Technique's unique identity. The IDs are automatically populated for all the collections and techniques that you have activated.
Technique	How an adversary achieves a tactical objective by performing an action. The technique information is automatically populated for all the collections and techniques that you have activated.
Mitigation	Mitigations that enable you to prevent an adversary from successfully executing techniques or sub-techniques against your organization. The mitigation information is automatically populated for all the collections and techniques that you have activated.
Relevant	Option to specify if the mitigation is relevant to your organization.
Active	Option to specify if the mitigation strategies are deployed in your organization. This is a required option required to calculate the technique mitigation coverage.
Preventive Tools	Option to specify if your organization has preventive tools in place to mitigate an attacker's techniques.
SOC Policy	The SOC policies that define the mitigation strategies in your organization.
Security Controls	Your organization's security controls contain the mitigation strategies to minimize security risks.
Mitigation Coverage (Percentage)	A scoring system to calculate the technique mitigation coverage. Define numerical values between 0 through 100. This is a required

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	option required to calculate the technique mitigation coverage.
Calculated Technique Mitigation Coverage (Percentage)	The calculated technique mitigation coverage in percentage. This value is determined based on the formula defined in the mitigation coverage calculator.
Overall Technique Mitigation Coverage (Calculated)	The overall technique mitigation coverage. This value is determined based on the mitigation coverage that is defined for your organization.
Comment	Description about the technique and mitigation coverage mapping.
Revoked	The technique to mitigation coverage mapping is revoked.

In this illustration, you see that the technique Valid Accounts has five mitigations associated, each with a mitigation coverage of 16 for user training, 92 for application developer guidance, and 16 for password policies, 91 for privileged account management, and 14 for valid accounts mitigation. The calculated technique mitigation coverage is 45.8 percent.



Overall technique mitigation coverage calculator

The overall technique mitigation coverage is determined based on the formula defined in the mitigation coverage calculator.

Before you begin

- Role required: sn_ti.admin, sn_si.admin: create, write, delete access
- Role required: sn_ti.read: read access

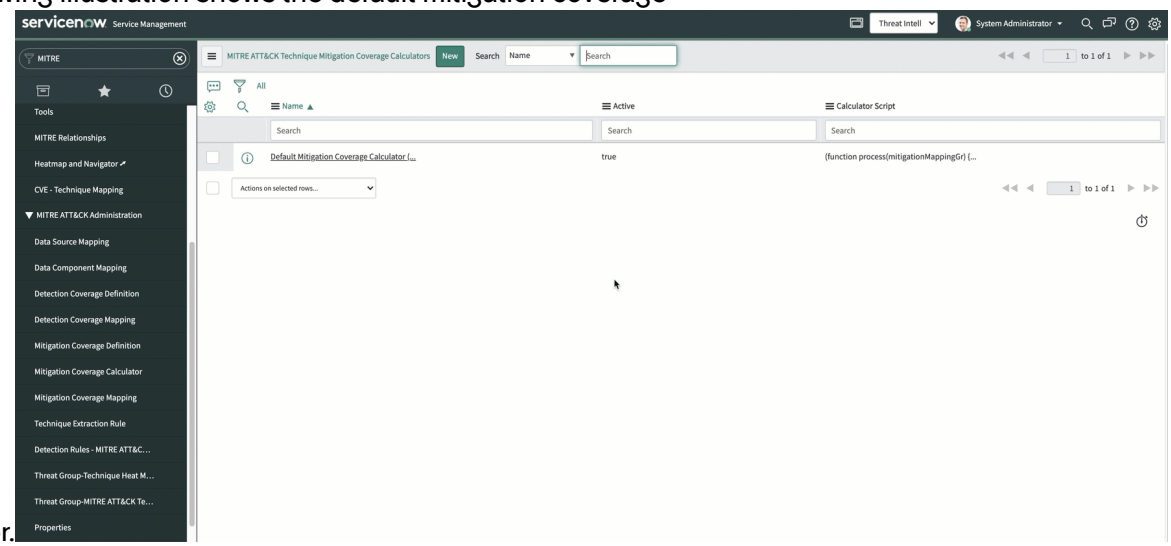
About this task

- You can set to active only one mitigation coverage calculator per domain.
- The base system mitigation coverage calculator is an average calculator.
- Any customizations to the calculator script should ensure that the final output is a numeric value between 0 through 100.
- The mitigation coverage definition is applied based on the range of the final output.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Mitigation Coverage Calculator**.
The following illustration shows the default mitigation coverage calculator.



Create and map detection rules

Create detection rules and map them against the tactics and techniques. With this mapping, you can see the coverage for the detection rules in your organization.

Before you begin

Role required:

- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

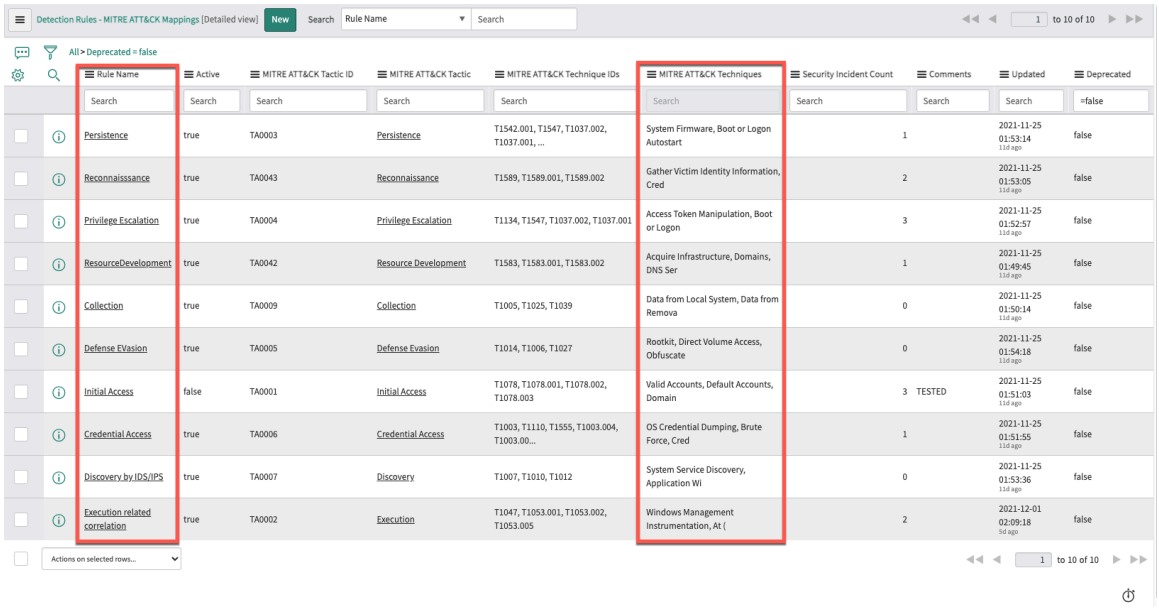
About this task

Detection rule mapping enables your organization to see which detection rules are available to identify specific techniques.

The primary purpose of the mapping is to provide visibility if your organization has the necessary detection rules to identify when an alert or event is triggered as a result of an attack by an adversary using a specific technique.

For example, view the following illustration that shows a list of the detection rules mapped to various techniques. You can also view this information in the MITRE-ATT&CK navigator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



If you do not intend to use the base system SIEM auto-extraction rules, then enable the automatic rollup of MITRE-ATT&CK TTPs based on the detection rule mapping. You can populate the alert or event rule that triggers the security incident in the Alert Rule name field. You can also populate the Alert Rule name field by using SIEM integration, email parsing, manual creation, etc. For more information, see Rollup MITRE-ATT&CK information from detection rules.

Note:

The detection rules feature has been updated to include mapping a single tactic to multiple techniques. Previously, you could map a single tactic with a single technique. If you are upgrading the Threat Intelligence plugin from version 12.0.4 to a higher version, then review the following points before using the detection rules in MITRE-ATT&CK module.

- You find multiple records merged into a single record if the fields - rule name, alert sensor, source, category, subcategory, and MITRE-ATT&CK tactic are common.
- The old records are marked as true in the deprecated column and false in the active column.
- The new merged records are available for use and are marked as false in the deprecated column and true in the active column.
- After you verify the upgrade, and view that all your detection rules are successfully migrated, you can delete the old records that are marked as true in the deprecated column.

Procedure

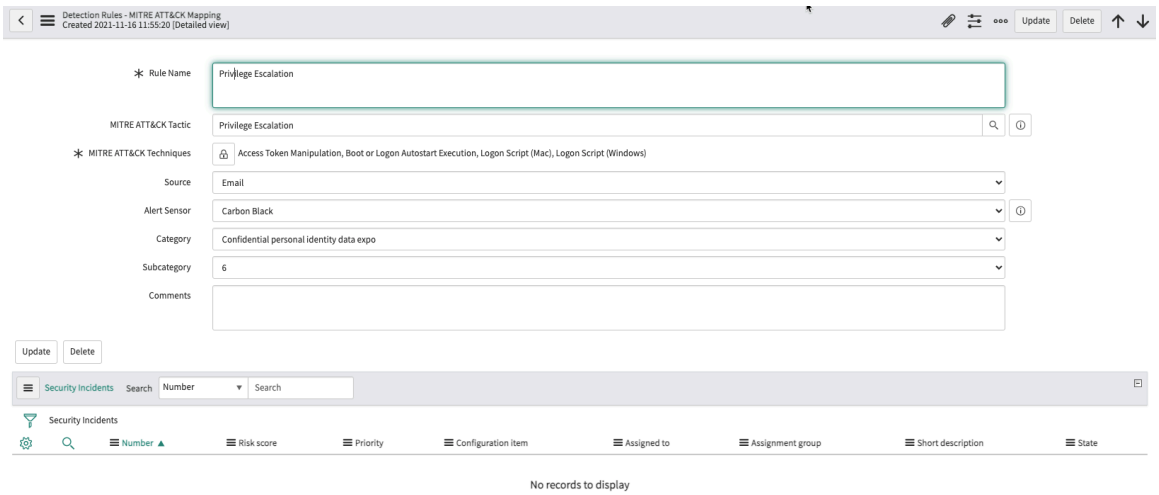
1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Detection Rules - MITRE ATT&CK Mappings**.
2. Use one of the following methods to create your detection rule:
   Method 1: Manually create detection rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Click **New** and on the form, fill in the fields.

Detection Rules - MITRE-ATT&CK Mapping

Field	Description
Rule Name	Detection rule's name.
MITRE-ATT&CK Tactic	Relevant MITRE-ATT&CK tactic.
MITRE-ATT&CK Techniques	Relevant MITRE-ATT&CK technique. You can select multiple techniques for a single tactic.
Source	Source of the security incident, such as email, firewall, network monitoring, and so on.
Alert Sensor	Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee, and so on.
Subcategory	Subcategory that further defines the issue.
Category	Category that identifies the type of security issue.
MITRE-ATT&CK Technique	Relevant MITRE-ATT&CK technique. You can select multiple techniques for a single tactic.
Security Incident Count	The number of security incidents that the techniques are appended to. This count appears when you have enabled the roll up of MITRE-ATT&CK information automatically from alert rules to security incidents.
Deprecated	The detection rule mapping is deprecated.
Active	Option to specify if the detection rule is active and deployed in your environment.



b. Click **Submit**.

Method 2: Import and create detection rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

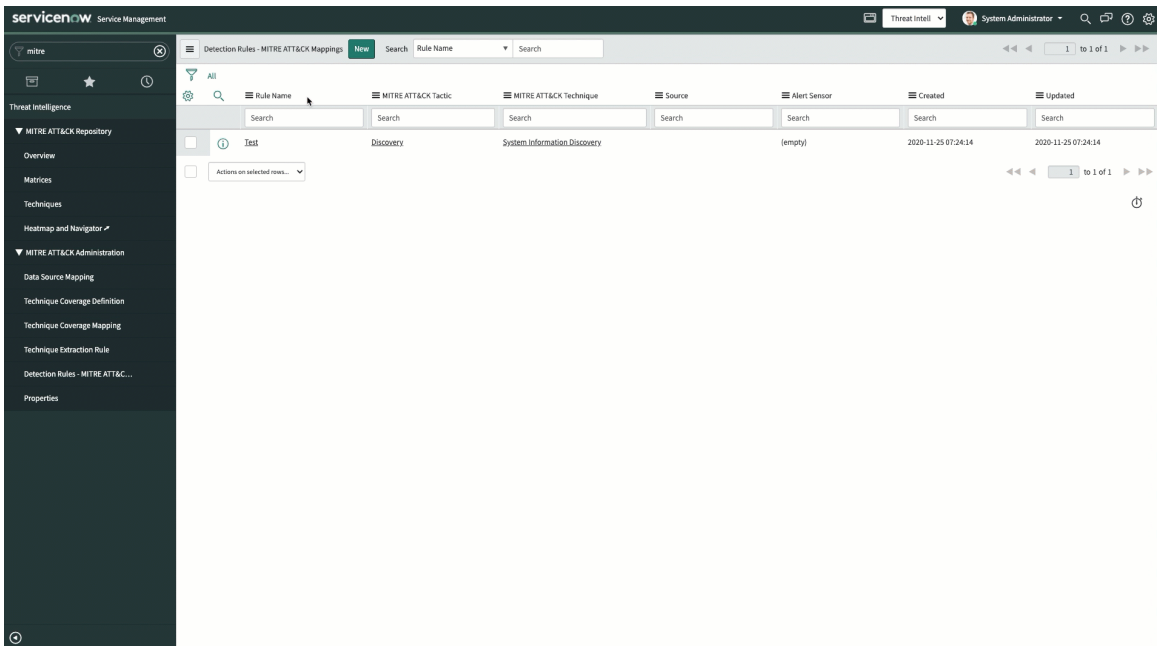
a. Right-click the Rule Name column header.

b. From the list, click **Import**.

c. Click **Create Excel template**.

d. Click **Download** after the export completes. An excel template with the filename sn_ti_alert_rules_mitre_attack_technique_mapping is downloaded to your computer.

In the following illustration, you see how to export the excel template, fill the details in the spreadsheet, upload the file, preview the fields, and import it back to the ServiceNow AI Platform.



e. Open the spreadsheet, select the second sheet tab, and review what you entered. On the form, fill in the fields and then, save your file.

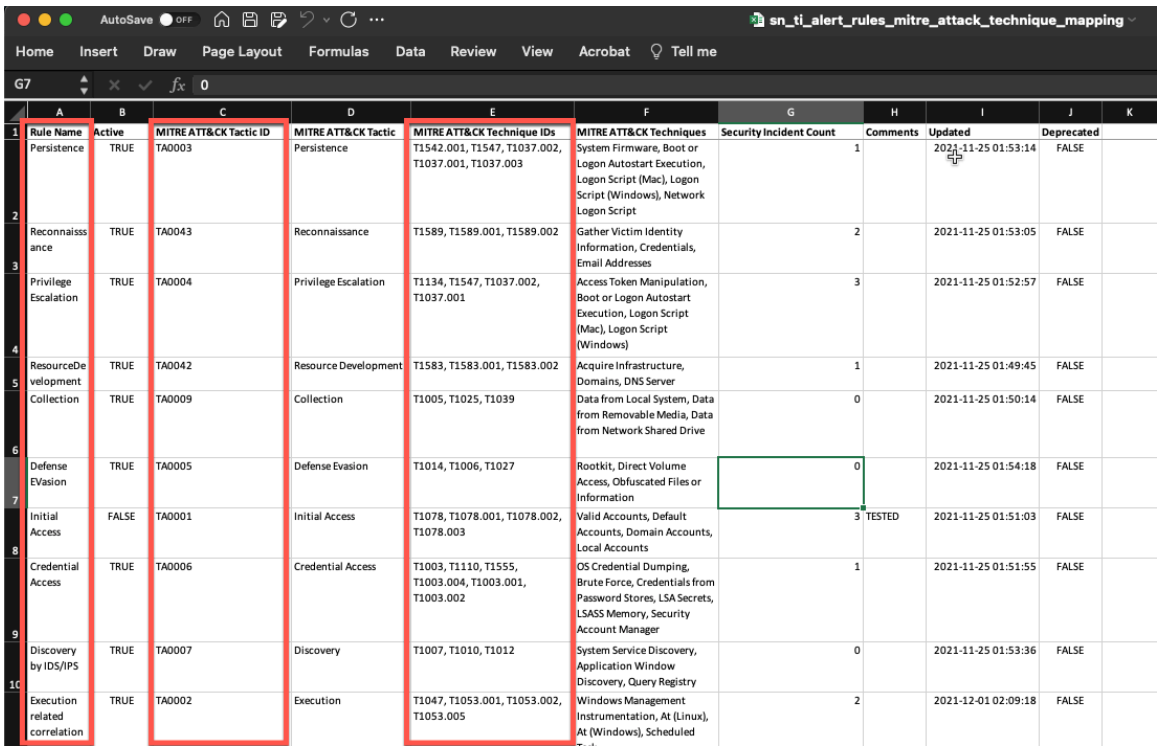
Import template

Field	Description
Rule Name	Detection rule name.
Active	Option to specify if the detection rule is active and deployed in your environment.
Alert Sensor	Security integration through which you ingest the alert or event data such as CarbonBlack, CrowdStrike, McAfee, and so on.
Category	Category that identifies the type of security issue.
Comments	Description about the detection rule.
Deprecated	The detection rule mapping is deprecated.
MITRE-ATT&CK Technique IDs	MITRE-ATT&CK technique ID, such as T1546.008, for Accessibility Features.
MITRE-ATT&CK Tactic ID	MITRE-ATT&CK tactic ID, such as TA0003, for Persistence.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Security Incident Count	The number of security incidents that the techniques are appended to. This count appears when you have enabled the roll up of MITRE-ATT&CK information automatically from alert rules to security incidents and the detection rule is active.
Source	Source of the security incident, such as email, firewall, network monitoring, and so on.
Subcategory	Subcategory that further defines the issue.
MITRE-ATT&CK Tactic	Relevant MITRE-ATT&CK tactic.
MITRE-ATT&CK Technique	Relevant MITRE-ATT&CK technique.

The following illustration shows the spreadsheet template. The required fields are highlighted in red - Rule Name, MITRE-ATT&CK Tactic ID, and MITRE-ATT&CK Technique ID.



	A	B	C	D	E	F	G	H	I	J	K
1	Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated	
2	Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE	
3	Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE	
4	Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE	
5	ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE	
6	Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE	
7	Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE	
8	Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE	
9	Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE	
10	Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE	
	Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE	

f. Click **Choose file** and select the spreadsheet on your computer.

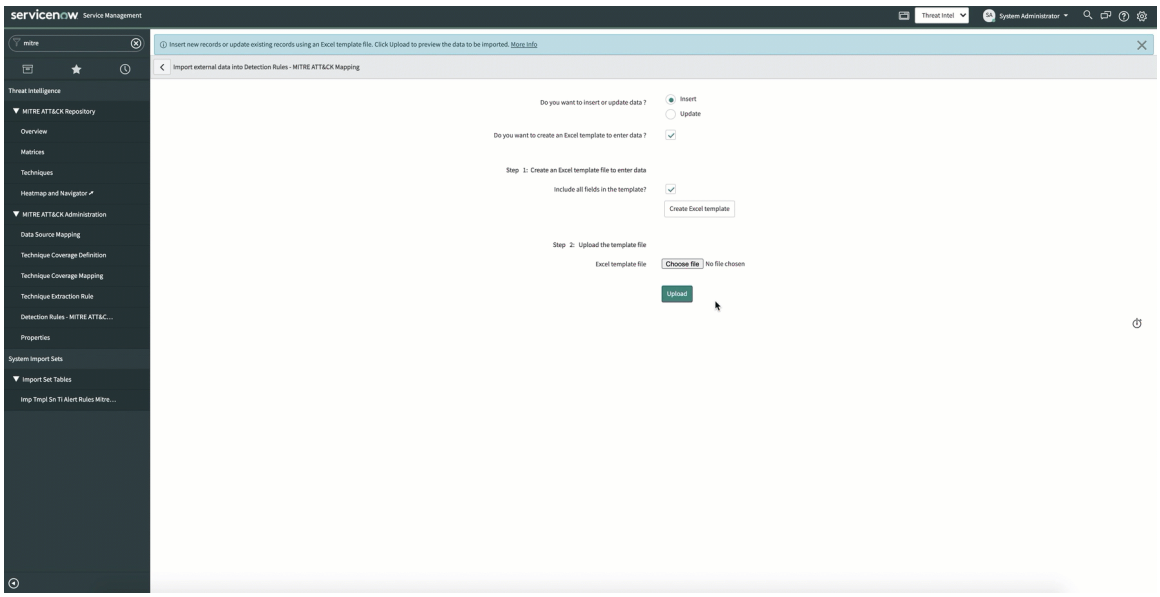
g. Click **Upload**.

h. Click **Preview Imported Data**.

i. Preview the mappings and click **Complete Import**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows how to upload the spreadsheet, preview the data, review any errors, and complete the detection rule mapping import process.



Auto-extract technique rules for importing MITRE-ATT&CK information

Use the base system auto-extraction rules to import the MITRE-ATT&CK information from any existing third-party integrations.

Use threat-lookup auto-extraction rules

Use the threat lookup auto-extraction rules to import the MITRE-ATT&CK information from any existing Threat Intelligence third-party integrations.

Before you begin

Role required:

- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

About this task

When any Threat Intelligence integration, such as Sandbox or a TIP, supports the MITRE-ATT&CK framework and if the MITRE-ATT&CK information is parsed at each integration level, then the information is displayed in each threat lookup result record. However, not all Threat Intelligence integrations parse the MITRE-ATT&CK information. The threat lookup global auto-extraction rule can extract MITRE-ATT&CK information from all Threat Intelligence integrations.

You can choose to roll up the MITRE-ATT&CK information automatically from the threat lookup results to a security incident. For automatic rollup of threat lookup results to security incidents, enable the system property. Alternatively, you can rollup the information manually for each individual threat lookup.

The base system Threat Intelligence automatically extracts the MITRE-ATT&CK information from the third-party integrations raw payload to the threat lookup result record, if the Threat Intelligence integration provides you with MITRE-ATT&CK information like the technique or tactic.

If the MITRE-ATT&CK information is not available in the raw payload field of the threat lookup record, then you must define your own rule for auto-extraction from the third-party integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Technique Extraction Rule**.
2. Click **New**.
3. On the form, fill in the fields.

Technique Extraction Rule form

Field	Description
Name	Auto-extraction rule name.
Rule Type	Auto-extraction rule type. Select **Threat Lookup**.
Ignore Auto-Extraction	Setting that by default, is cleared. This setting enables automatic extraction of MITRE-ATT&CK techniques.
Source Engine	Source engine.
Global	Source engine setting. When you set the source engine to **Global**, the extraction runs on all threat lookup integration results.
Description	Description of the auto-extraction rule.
Process Method	Regex or a script method that you specify to link the technique information from the raw payload.
Regex Extraction	Option that you specify for the **Target Field** when using the regex extraction method. Regex is the default.
Script Extraction	Process that you select when running a script. The script reviews the following: ○ threatLookupResultSysId:sys_id of the threat lookup result record ○ sourceName: Name of the threat lookup source.
Tactic Extraction	Option that you specify to extract tactic related information from the raw payload. If a payload contains specific tactic and technique related information, you can extract and append the information to the security incident.

4. Click **Submit**.

Use SIEM auto-extraction rules

Use the SIEM auto-extraction rules to import the MITRE-ATT&CK information from any existing Security Operations SIEM third-party integrations.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

About this task

The technique extraction rule is available for all base system Security Operations SIEM integrations such as Splunk, IBM QRadar, and ArcSight integrations. When the ServiceNow AI Platform ingests alert or event data from these SIEM integrations and they contain MITRE-ATT&CK information, the ServiceNow AI Platform processes the raw payload and auto-extracts the MITRE-ATT&CK information.

If your ServiceNow AI Platform contains base system SIEM integrations, that means that the technique extraction rules are already created in the MITRE-ATT&CK module. You should review and modify the rules as needed.

Enable either the SIEM auto-extraction rule or the alert rule at a time.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Technique Extraction Rule**.
2. Click **New**.
3. On the form, fill in the fields.

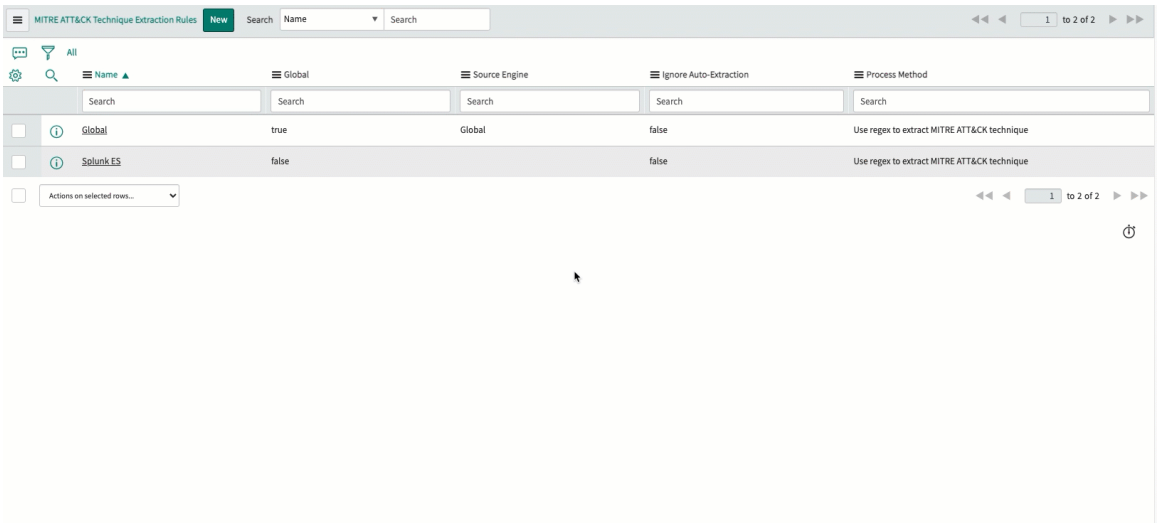
Technique Extraction Rule form

Field	Description
Name	Auto-extraction rule name.
Rule Type	Auto-extraction rule type. Select **SIEM**.
Ignore Auto-Extraction	Setting that by default is cleared. This setting enables automatic extraction of MITRE-ATT&CK techniques.
Import Table	Import table that is automatically mapped for base system SIEM integrations. Review this field for other SIEM integrations for the MITRE-ATT&CK information and map accordingly.
Import Field	Import field that is automatically mapped for base system SIEM integrations. Review this field for other SIEM integrations for the MITRE-ATT&CK information and map accordingly.
Description	Auto-extraction rule.
Process Method	Regex or a script method that you specify to link the technique information from the raw payload.
Regex Extraction	Option that you specify for the **Target Field** when using the regex method. Regex extraction is the default process method.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Script Extraction	Script process method that you use if you want to customize how the MITRE-ATT&CK information is extracted.
Tactic Extraction	Option that you specify to extract tactic related information from the raw payload. If a payload contains specific tactic and technique related information, you can extract and append the information to the security incident.

In the following illustration, you see an example of the Splunk Enterprise SIEM technique extraction rule in the form view. This rule is similar to all the other SIEM technique extraction rules.



4. Click **Submit**.

Review threat group and MITRE-ATT&CK techniques mapping

Review the threat group and techniques object to object relationship mapping information that is imported from the MITRE TAXII collections. This mapping enables you to view the technique group and the corresponding technique mapping.

Before you begin

Role required:

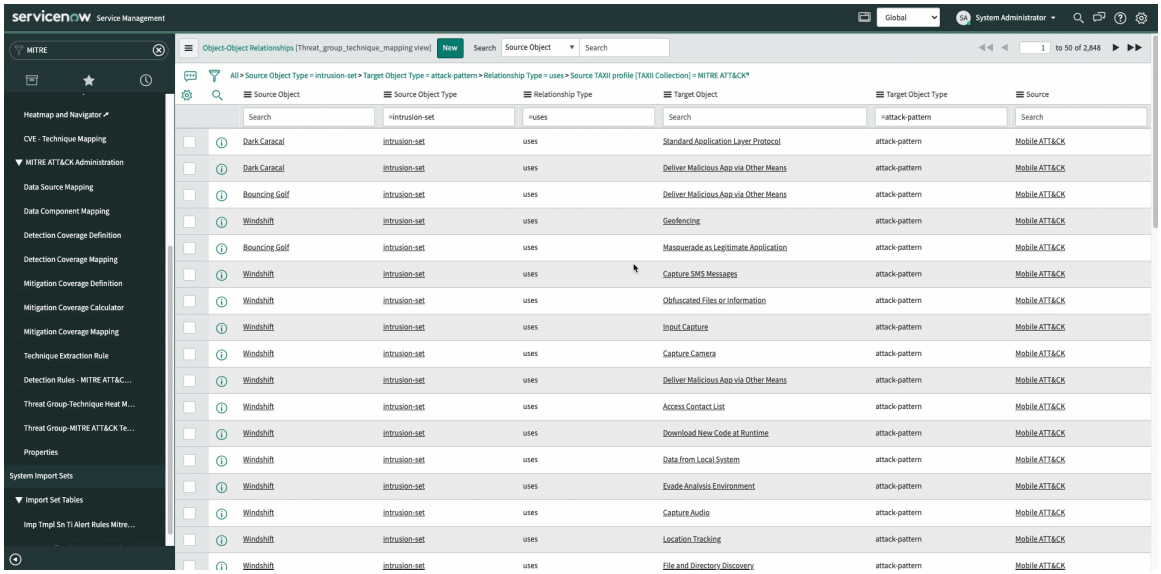
- sn_ti.admin, sn_si.admin: create, write, delete access
- sn_ti.read: read access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Threat Group-MITRE ATT&CK Techniques**.
2. Right click the **Source Object** and select **Group By Source Object** to view all the attack patterns associated with a threat group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows the threat group admin@338 and the various attack patterns adopted by this threat group which are part of the enterprise attack source.



Threat group to technique heatmap definition

Define the threat group to technique heatmap definition so that on the heatmap you can measure and detect the attack patterns that threat groups are using to attack your organization. The probability of an attack using a particular technique increases when you have a high number of attackers.

Before you begin

Role required:

- sn_ti.admin, sn_si.admin: write access
- sn_ti.read: read access

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Threat Group-Technique Heat Map Definition**.
2. Review the threat group to technique heatmap definition and customize the entries for your environment.

Threat Group-Technique Heat Map Definitions

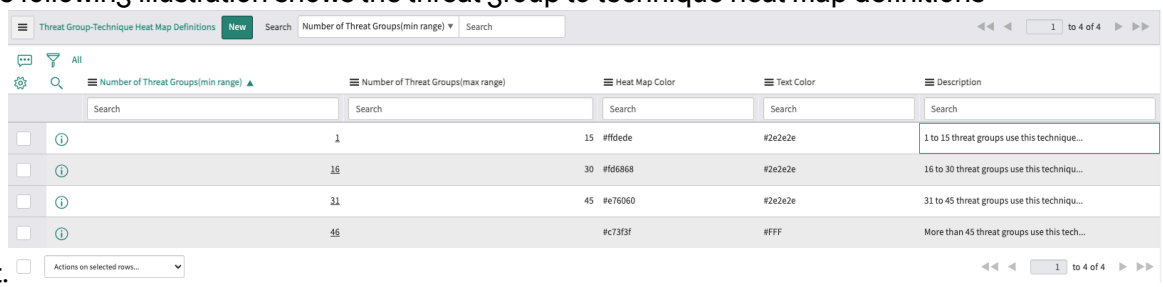
Field	Description
Number of Threat Groups (min range)	The minimum number of threat groups using a particular technique.
Number of Threat Groups (max range)	The maximum number of threat groups using a particular technique. The probability of an attack using a particular technique increases when you have a high number of attackers.
Heat Map Color	Color that is assigned to the threat group category. The color that you define is used to highlight the threat group category in the heat map.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	You can customize the colors using HEX codes and RGB(A) values.
Text Color	Color that is assigned to the threat group text. The color that you define is used to highlight the threat groups in the heat map. You can customize the colors using HEX codes and RGB(A) values.
Description	Description about the threat group range and definition.

Note: Ensure that you do not overlap the threat group count ranges if you customize the threat group range (min or max).

The following illustration shows the threat group to technique heat map definitions list.



3. To add an entry, click **New**, complete the entries, and click **Submit**.

Review the MITRE-ATT&CK system properties

Review the MITRE-ATT&CK system property values.

Before you begin

Role required: sn_ti.admin, sn_si.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Administration** > **Properties**.
2. On the form, fill in the fields.

MITRE-ATT&CK Properties form

Field	Description
Roll up MITRE ATT&CK information automatically from Observables to security incident [sn_ti.rollup_mitre_att&ck_technique_observable_si]	Rollup of MITRE-ATT&CK information from observables to the security incident. For more information, see Associate MITRE ATT&CK information with observables. Default value: Yes
Roll up MITRE ATT&CK information automatically from Threat Lookup results to security incident	Rollup of MITRE-ATT&CK information from threat lookup results to the security incident. For more information, see Threat lookup auto-extraction.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
[sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Default value: Yes
Roll up MITRE ATT&CK information automatically from alert rules to security incidents [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Rollup of MITRE-ATT&CK TTP information automatically from alert rules to security incidents. For more information, see map detection rules. Default value: No
Roll up MITRE ATT&CK information automatically from child security incidents to parent security incident [sn_ti.rollup_mitre_att&ck_technique_child_si_s]	Roll up MITRE-ATT&CK information automatically from child security incidents to parent security incident. Default value: Yes
Enabling this property allows mapping of Security Incident Fields like category and sub category with Detection Rules in "Detection Rules - MITRE ATT&CK mapping" table [sn_ti.enable_category_mapping_with_alert_rule]	Category and sub-category in the Detection Rules - MITRE ATT&CK mapping page. Default value: No
Time(in hours) to calculate "CVE - VUL Count" [sn_ti.time_to_calculate_cve_vits_count]	The scheduled time in hours to calculate the CVE and VUL information. Default value: 24
[sn_ti.include_cve_vit_indirect_relation]	Includes the number of VITs that are indirectly associated to a CVE through TPEs. This property identifies all the TPEs associated to a CVE and then identify all the CVEs that are associated to those TPEs. The total count of VITs include the following: ○ The VITs directly associated to that particular CVE. ○ The VITs that are associated indirectly to the CVEs through TPEs.

3. Click **Save**.

Using MITRE-ATT&CK to detect and analyze threats

Use the MITRE-ATT&CK framework across the Threat Intelligence and the SIR module to detect and analyze threats to your organization.

Associate MITRE-ATT&CK™ information with security incidents

Associate the MITRE-ATT&CK tactics and techniques to the security incident for better security incident and threat analysis.

Before you begin

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Add the MITRE-ATT&CK tactics and techniques information to the security incident so that you can correlate your security incident and threat information for better analysis. For example, your organization may be receiving tactics, techniques, and procedures (TTP)-related information from your third-party sources, such as Threat Intelligence reports or other sources outside of the Security Incident Response. You then add this information back to SIR for better correlation and threat analysis.

You can choose to roll up the MITRE-ATT&CK information automatically from the threat lookup auto-extraction results, from observables, or from a child security incident to a security incident. For automatic roll up to security incidents, enable the system property. Alternatively, you can roll up the information manually for each individual threat lookup or observable.

Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.
3. Click the **Associate MITRE ATT&CK Technique** related link.
   The Associate MITRE ATT&CK Technique pane appears.

   This illustration shows how to navigate to the related list and look for Associate MITRE-ATT&CK Technique, review the source Enterprise ATT&CK, add a tactic Impact, and add a technique System Shutdown/Reboot.

4. Select **Source**.

   Note: Only the collections and matrices that have been activated appear in the source list.

   The tactics and techniques that are associated with the source are available for selection. You can also associate multiple sources.
5. Select the **Tactic** and **Techniques**.
6. **Optional:** Review the information based on the relevance with the security incident and do the following:
   - To completely remove the association, click the bin icon. Clicking this icon deletes the source and its associated tactics and techniques.
   - To remove a tactic, click the minus icon next to the tactic.
   - To remove a technique, click the x icon next to the technique.
7. Click **Save**.

Result

The MITRE-ATT&CK information is associated with the security incident. You can now view the associated information in the **MITRE ATT&CK Card**.

Associate MITRE-ATT&CK information with closed security incidents

You can now associate MITRE-ATT&CK tactics and techniques to the closed security incidents for better security incident and threat analysis.

Using the MITRE-ATT&CK Card to see related information in a security incident

You can use the MITRE-ATT&CK card to see the MITRE-ATT&CK related information in a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the information is rolled up from a threat lookup, an observable, or a SIEM integration, it is added to the security incident. Then, the aggregated information is presented in the MITRE-ATT&CK Card. The **MITRE ATT&CK Card** provides two views:

- Navigator view: This view, which is similar to the MITRE-ATT&CK navigator, shows all the techniques that have been manually added or rolled up from the observable or threat lookup tables. **Show origin of techniques** displays the source of the technique if it has been manually rolled up or through a Source. **Show ID** displays the technique ID.

  The following illustration shows how to navigate to the **MITRE ATT&CK Card** navigator view. By clicking any of the available links, the information opens in the Threat Intelligence module.

- List view: This view shows the data in a list or table format. You can see all the data that is spread across different tables and groups in this view.

  The following illustration shows how to navigate to the MITRE ATT&CK Card list view. By clicking any of the available links, the information opens in the Threat Intelligence module.

Associate MITRE-ATT&CK information with observables

Associate MITRE-ATT&CK tactics and techniques to an observable for better security incident and threat analysis at a granular level.

Before you begin

Role required: sn_si.analyst

About this task

Some SIEMs may provide MITRE-ATT&CK information with events, alerts, or observables. To associate the MITRE-ATT&CK information at a granular level, you can add the information with an observable.

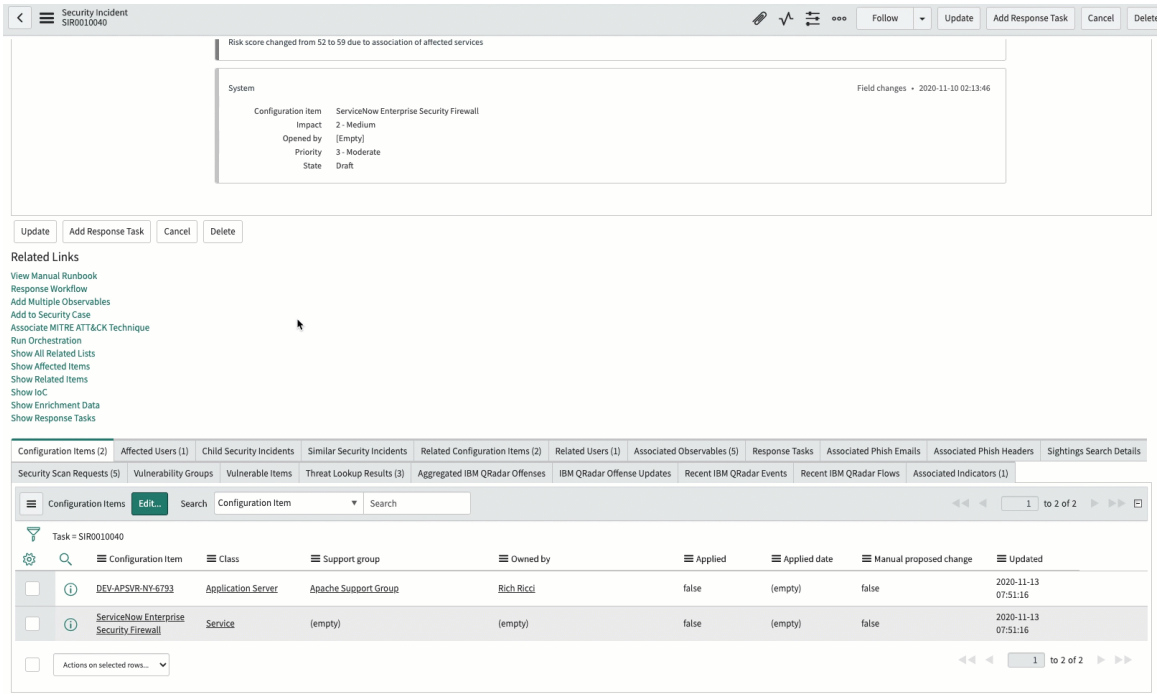
You can choose to roll up the MITRE-ATT&CK information automatically from the observables to a security incident. For automatic rollup of observables to security incidents, enable the system property. Alternatively, you can roll up the information manually for each observable.

Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.
3. Click **Show All Related Lists** and the **Associated Observables** tab.
4. Point to the observable that you want to associate, right-click, and select **Associate MITRE ATT&CK Technique**.

   In the following illustration, you can see how to navigate from the related list to **Associate MITRE ATT&CK Technique**, review the source, and add a tactic and technique.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



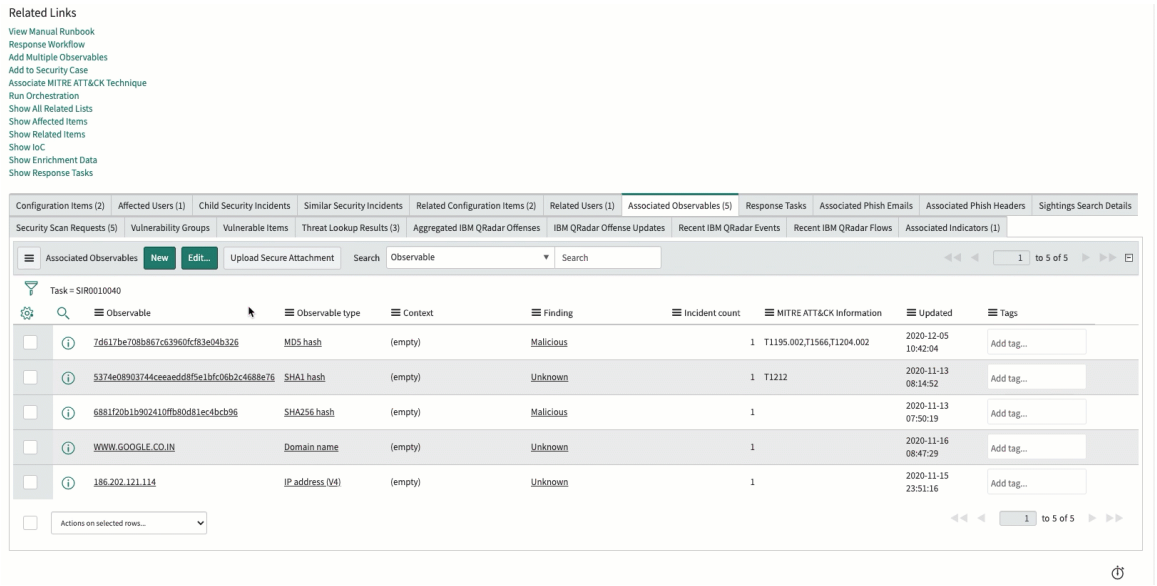
5. In the source lists, review the **Source**.

   Note: Only the collections and matrices that have been activated appear in the source list.

6. Review the **Tactic** and **Techniques**, and add or remove them based on the relevance with the observable.
7. Click **Save**.
   The tactics and techniques that you have added appear in the MITRE-ATT&CK Information column in the observables related list.
8. Select the observable and then from the Actions menu, click **Roll up MITRE ATT&CK Information to SI**.
   If you have enabled automatic roll up of MITRE-ATT&CK information from observables to security incident, then the information is automatically rolled up. If you have not enabled automatic rollup,you need to do this manually.

   The following illustration shows how to select an observable and roll up the MITRE-ATT&CK information to a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. To see an aggregated view of the techniques that are associated with the observables, select two or more observables from the list and then from the **Actions** menu on the selected rows list, click the **Show MITRE ATT&CK Information**.

Result

An aggregated view of the MITRE ATT&CK information for the selected observables is displayed.

Associate MITRE-ATT&CK information with security case

Associate MITRE-ATT&CK tactics and techniques to a security case for better security case management and threat analysis at a granular level.

Before you begin

Role required: sn_si.analyst

Procedure

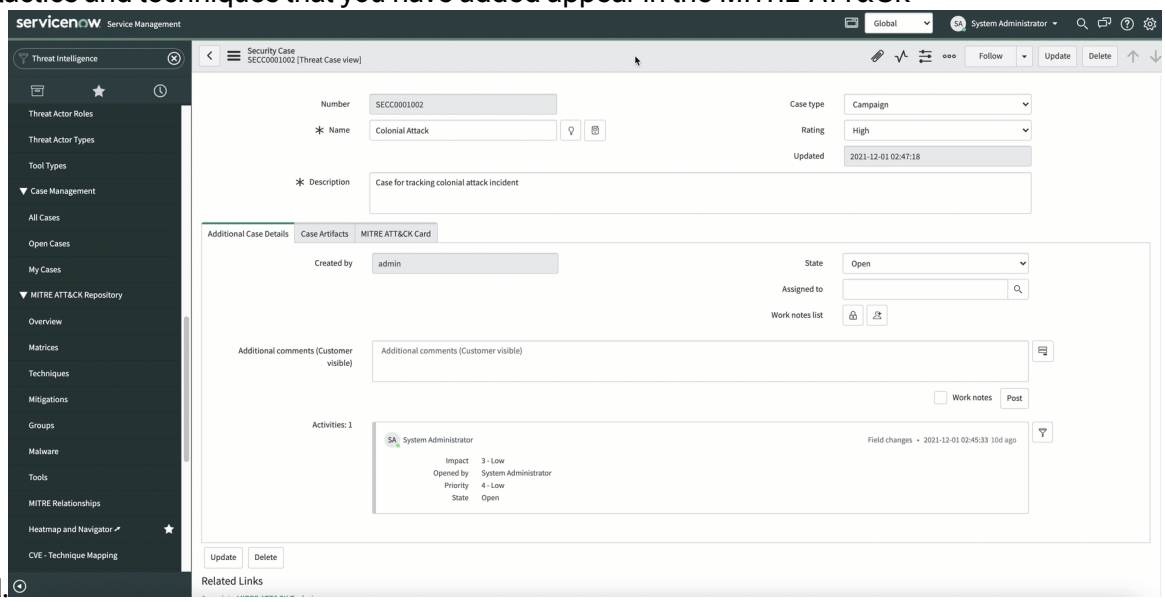
1. Navigate to **All** > **Threat Intelligence** > **Case Management** > **All Cases**.
2. Select the security case that you want to enrich with the MITRE-ATT&CK information.
3. From the related list, click **Associate MITRE ATT&CK Technique**.

   In the following illustration, you can see how to navigate from the related list to **Associate MITRE ATT&CK Technique**, review the source, and add a tactic and technique.

4. In the source lists, review the **Source**.
5. Review the **Tactic** and **Techniques**, and add or remove them based on the relevance with the case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Save**.
   The tactics and techniques that you have added appear in the MITRE-ATT&CK Card.



Rollup MITRE-ATT&CK information using Threat Lookup results

If you have not enabled automatic rollup of MITRE-ATT&CK information, you can do this manually.

Before you begin

Role required: sn_si.analyst

About this task

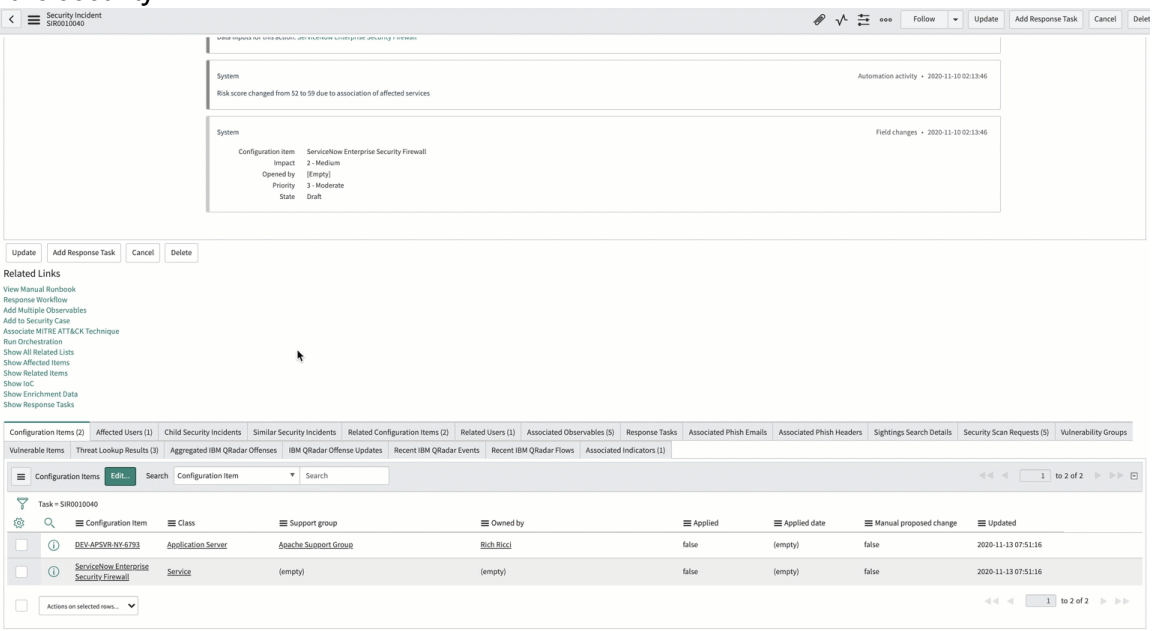
If you have enabled automatic roll up of MITRE-ATT&CK information from Threat Lookup results to security incident, then the information is automatically rolled up. If you have not enabled automatic rollup, you can do this manually.

Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.
3. Click **Show All Related Lists** and the **Threat Lookup Results** tab.
4. Select the observable and then from the Actions menu, click **Roll up MITRE ATT&CK Information to SI**.
   You can select multiple observables and rollup the information.
5. Click **Reload** to confirm the changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows how to select an observable and roll up the Threat Lookup results to the security



incident.
You can view the MITRE-ATT&CK Card to confirm that the Threat Lookup results have been rolledup to the security incident.

Rollup MITRE-ATT&CK information from detection rules

Enable rollup of MITRE-ATT&CK information from the detection rules to the security incidents for better security incident and threat analysis.

Before you begin

Role required: none.

Ensure that you have performed the following:

- Enable the Rollup MITRE ATT&ACK information automatically from alert rules to security incidents property in the Properties module. By default, this option is disabled. For more information, see Review the MITRE-ATT&CK system properties.
- Perform mapping of detection rules to MITRE-ATT&CK TTPs in Detection Rules - MITRE ATT&CK TTP Mapping module. The detection rule name must match the alert rule name that triggers the security incident. For more information, see Create and map detection rules.

About this task

If you do not intend to use the base system SIEM auto-extraction rules, then enable the automatic rollup of MITRE-ATT&CK TTPs based on the detection rule mapping. You can populate the alert or event rule that triggers the security incident in the Alert Rule name field. You can also populate the Alert Rule name field by using SIEM integration, email parsing, manual creation, and so on.

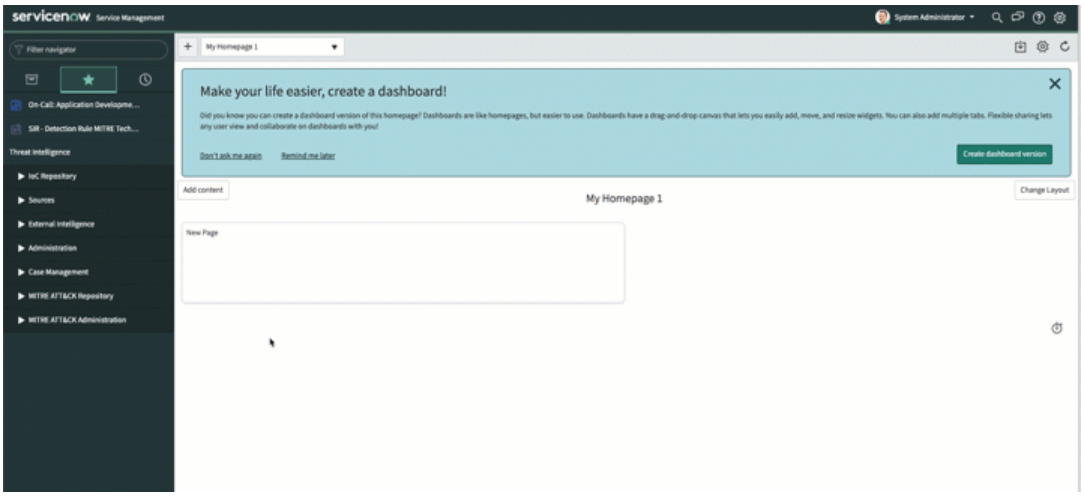
Procedure

1. Navigate to **MITRE ATT&CK Administration** > **Properties**.
2. Enable the Rollup MITRE ATT&ACK information automatically from alert rules to security incidents property, and click **Save**.
   By default, this option is disabled.
3. You need to populate the **Alert Rule** name field of the security incident with the required alert rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Ensure that you add the exact Alert Rule name. To add multiple rules, you need to add the rules using a comma separator.

4. Right-click the form, and click **Save**.
   If the alert rule name value in the security incident matches a record in the Detection rule - MITRE ATT&CK TTP Mapping module, the corresponding techniques and tactics associated to the alert rule are linked to the security incident automatically.



5. Open the security incident, select the **MITRE ATT&CK Card** and validate whether the techniques are rolled up.
6. Enable **Show origin of techniques** option to view the origin of the techniques.
   The origin of techniques should be Detection Rule.

Rollup MITRE-ATT&CK information from child security incidents

If you have not enabled automatic rollup of MITRE-ATT&CK information, you can do this manually.

Before you begin

Role required: sn_si.analyst

About this task

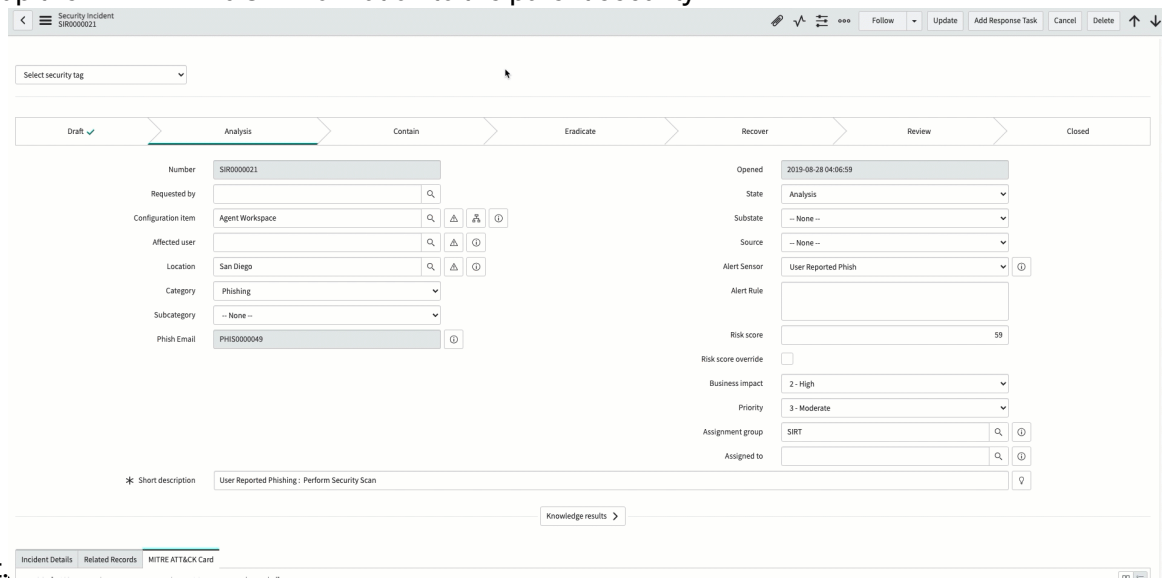
If you have enabled automatic roll up of MITRE-ATT&CK information from child security incidents, then the information is automatically rolled up. If you have not enabled automatic rollup, you can do this manually.

Procedure

1. Navigate to **All** > **Incidents** > **Show All Incidents**.
2. Select the parent security incident that you want to enrich with the child MITRE-ATT&CK information.
3. Click **Show All Related Lists** and the **Child Security Incidents** tab.
4. Select the child security incident and then from the Actions menu, click **Roll up MITRE ATT&CK Information to SI**.
   You can click **Show MITRE ATT&CK information** to view the child security incident's MITRE information before you roll up the MITRE ATT&CK information.
5. Click **Reload** to confirm the changes.
6. Click the **MITRE ATT&CK Card** to view the origin of techniques.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows how to select child security incident and roll up the MITRE-ATT&CK information to the parent security incident.



You can view the MITRE-ATT&CK Card to confirm that the child security incident MITRE-ATT&CK information has been rolled up to the parent security incident.

Perform link analysis and threat hunting using MITRE-ATT&CK specific filters

Correlate and perform link analysis of observables, security incidents, and MITRE-ATT&CK related information so that your organization can start hunting for threats.

Before you begin

Role required: sn_ti.mitre_analyst, sn_si.read

About this task

After you associate the security incidents with MITRE-ATT&CK information, you can use the MITRE-ATT&CK specific filters for threat hunting. Use the MITRE-ATT&CK filters with the existing Security Incident Response filters to correlate and perform link analysis.

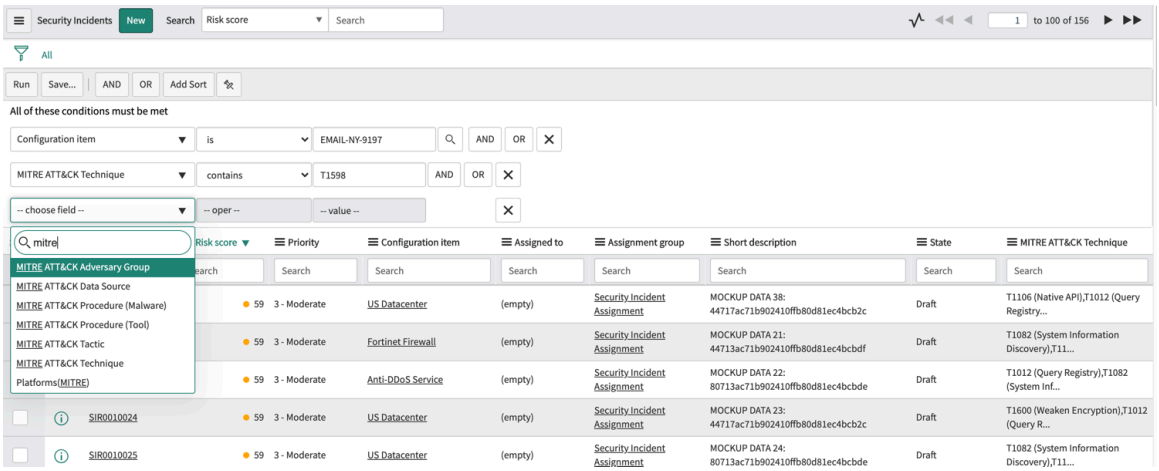
Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Click **Update Personalized List** to add the MITRE columns.
3. Select a filter condition so that you can view MITRE related information and associations with security incidents or observables:
   - MITRE-ATT&CK Adversary Group
   - MITRE-ATT&CK Data Source
   - MITRE-ATT&CK Procedure (Malware)
   - MITRE-ATT&CK Procedure (Tools)
   - MITRE-ATT&CK Tactic
   - MITRE-ATT&CK Technique
4. Create a filter condition that is based on the above criteria and click **Run** to perform a link analysis or correlation between security incidents, observables, and MITRE-ATT&CK related information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The MITRE-ATT&CK data is stored as a string and you can only use **contains** as the operator for filter conditions.

For example, if you want to review that a configuration item (CI) is compromised, you select a CI. You then correlate the CI with techniques that are present by adding a MITRE-ATT&CK Technique ID. You can then continue to build your filter criteria to correlate the information and for threat hunting.



MITRE-ATT&CK heat map and navigator

You can use the MITRE-ATT&CK heat map and navigator for basic navigation and to visualize your overall technique detection coverage.

Overview of the MITRE-ATT&CK heat map and navigator

You can use the navigator with the primary filters for basic navigation and observation of ATT&CK matrices. The heat map highlights the spectrum of the detection coverage including the blind spots where your organization does not have any coverage. This is available after you map the technique detection coverage.

With the heat map and navigator, you can:

- Quickly and efficiently identify your organization's detection capabilities and highlight gaps in the technique detection coverage.
- Hunt for threats and perform correlation of threats using associated features.

Access the MITRE-ATT&CK heat map and navigator

Access the MITRE-ATT&CK heat map and navigator so that you can visualize the matrix that enables you to use ATT&CK.

Before you begin

Role required: sn_ti.read, sn_ti.mitre_analyst

About this task

You can review the heat map, use the filters to correlate, and perform link analysis of MITRE-ATT&CK information, the observables, and the security incidents in your organization.

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Heatmap and Navigator**. The heat map and navigator open in a new tab.
2. Select the source to populate the heat map.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Only the collections and matrices that have been activated appear in the source list.

In the following illustration, you see how to navigate to the heat map and navigator, and how to select the source, which is Enterprise ATT&CK in this example.

3. Use the search box to quickly find a particular tactic or technique by using its name or ID.

   The following illustration shows how to search for a tactic, technique, or any information that is contained in them.

4. Click **Filters** and select a filter from the Primary or Advanced filters.
5. Click **Apply** and control the filters as follows:
   - To save your filters, create a custom view. You can create and save three custom views.
   - To remove the selected filters, click **Restore Default Filters** to load your default saved view.
   - To clear all filters and your existing view, click **Clear all filters**.

   Note: The views that you save are specific for a user.

6. Click **Hide Sub-Techniques** to remove all sub-techniques from the heatmap view.
   If a technique has sub-techniques, you can click the expand icon to view the sub-techniques.

Using the custom views

Custom views in the MITRE-ATT&CK heat map and navigator help you to save and view your favorite filters the next time that you land on the heat map.

Note: You can create and save three custom views for every MITRE-ATT&CK collection per user.

Create a view

Once you select the required filters from the Primary or Advanced filters, click the ellipsis (...) button on the Filters header and select **Create a new view**. Enter the custom view name and **Save View**.

Default views

Click **Save this as a default view** to directly load the view the next time that you land on the heat map. You can set a default view for each of the collections.

Note: If you are upgrading the Threat Intelligence plugin from an older version, then your existing default view from the old version appears as a custom view.

Update a view

You can make updates to an existing custom view by modifying the required Primary or Advanced filters. Select a custom view, update the filters as required, and then click the ellipsis (...) button on the Filters header and select **Update view** to save the filters.

Manage custom views

Use the checkboxes next to each custom view to apply the selected custom view filter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Click the ellipsis (...) button next to each custom view name to control the custom views as follows:

- Set a default view.
- Remove a custom view as the default view. This doesn't delete the custom view.
- Rename the custom view.
- Delete the custom view.

Export a saved view

To export the saved custom views to JSON files, click ellipsis (...) on the Filters header and select **Export saved views**. Click the download icon for the custom view you wish to download to your local computer.

Import a view

You can import only JSON files. To import the custom views, click the ellipsis (...) button on the Filters header and select **Import view(json)**.

Review the following conditions when importing views:

- You can only import JSON file format.
- You can import only one view or file at a time.
- You cannot import if you already have three custom views in your filters. Delete a custom view and import a view.
- You cannot import a view with an existing custom view name. Rename a view before you import.

Navigator with primary filters

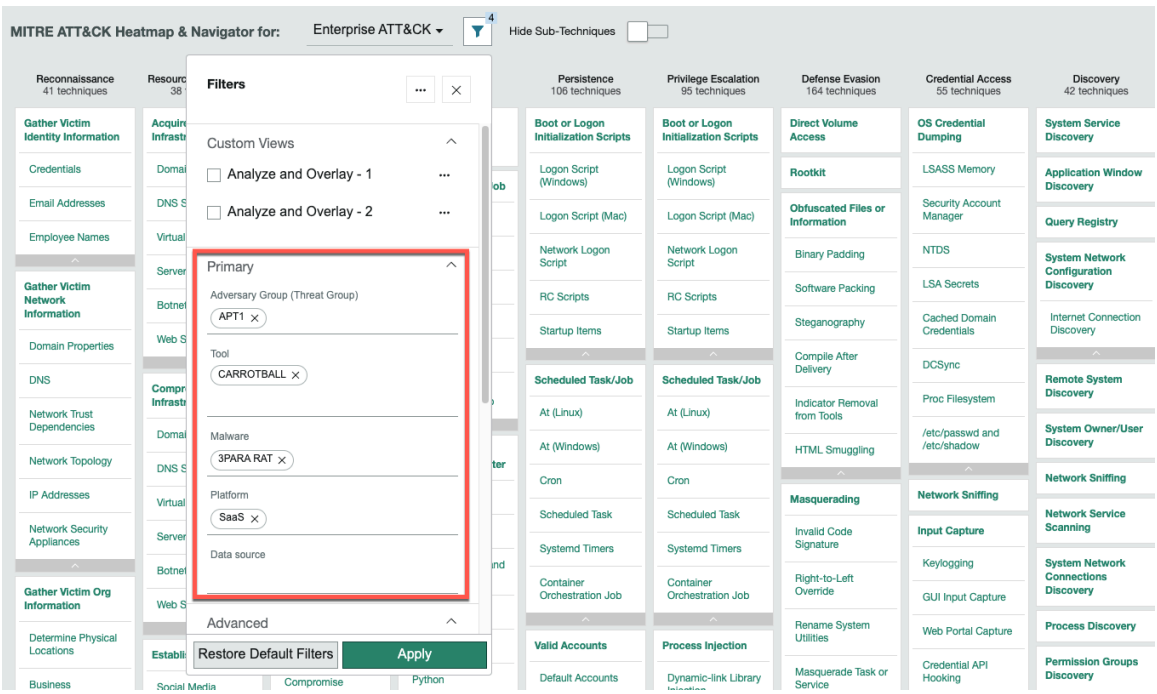
Use the primary filters to filter techniques in the MITRE-ATT&CK navigator. The information in the MITRE-ATT&CK repository is available for selection.

Filter	Description
Adversary Group (Threat Group)	Sets of related intrusion activity that are tracked by a common name in the security community. Groups can mean various threat groups, activity groups, threat actors, intrusion sets, and campaigns. You can add multiple groups to the **Adversary Group (Threat Group)** filter. For example, you add APT1 and AT12 as both are threat groups that are attributed to China. While both groups might target different sources, they could use similar techniques.
Tool	Legitimate software that is used by threat actors to perform attacks. You can understand how threat actors execute campaigns if you know how and what tools are used by threat actors. Tools includes both software that is not

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Filter	Description
	found on an enterprise system and software that is available as part of an operating system that is already present in an environment such as Microsoft Windows utilities. For example, gsecdump is a publicly available credential dumper that the APTI1 adversary group uses to obtain password hashes and LSA secrets (Local Security Authority) from Microsoft Windows operating systems.
Malware	Commercial, custom closed source, or open-source software that is intended to be used for malicious purposes by adversaries. Examples are PlugX, CHOPSTICK, and so on
Platform	Tactics and techniques that represent MITRE-ATT&CK in a particular platform. For example, MITRE-ATT&CK supports these platforms in the Enterprise ATT&CK matrix: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network.
Data source	Data sources that you are collecting in your environment and using to detect MITRE-ATT&CK techniques. Examples are DLL monitoring, and browser extensions.

The following illustration shows all the primary filters available in the MITRE-ATT&CK navigator.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using a heat map with primary and advanced features

You can use a heat map with advanced filters to perform an analysis by correlating security incidents with MITRE-ATT&CK information.

View technique IDs

You can view the MITRE-ATT&CK technique IDs with the technique names when you select the **Display technique IDs** filter.

View relevant techniques by priority

To filter the techniques based on their relevant priority in the navigator, select **Filter by technique relevant priority** filter and select the **Relevant Priority** from the menu. You can assign multiple priorities for filtering. You can also point to the techniques in the heat map to know the priority of the technique.

The relevant priority information is based on the prioritization you have set in the Techniques relevant priority field.

View technique detection coverage

To view the overall technique detection coverage in the heat map, select the **Display technique detection coverage** filter. The heat map highlights the visual spectrum of the detection coverage including the blind spots where you do not have any coverage. The base system scoring definition and the colors have been defined in the technique detection coverage. The information has been auto-extracted from the overall technique detection coverage.

For example, areas of the heat map that are marked in red indicate a lack of detection. Areas that are marked in blue indicate the presence of full detection capabilities. Areas that are marked in orange, yellow, and light blue reflect partial detection capabilities.

- The color visualization is based on the technique definition and color coding that you define.
- The coverage visualization is based on the technique detection coverage mapping that you define.
- If you modify the base system coverage definition, the Coverage Type icons do not display with the techniques in the heat map.

> **Note:** The heat map works as expected when you modify the same fields as the base system's-defined technique detection coverage and coverage colors.

In this illustration, you see the technique detection coverage for all the techniques and sub-techniques and the coverage type with their colors and icons.

View technique mitigation coverage

To view the overall technique mitigation coverage in the heat map, select the Display technique mitigation coverage filter. The heat map highlights the visual spectrum of the mitigation coverage including areas that you do not have any coverage. The mitigation coverage, colors, and percentage ranges have been defined in the Mitigation Coverage Definition. The information is extracted from the Overall Technique Mitigation Coverage.

For example, techniques highlighted in red indicate no mitigation coverage, orange indicates poor mitigate coverage, and blue indicate excellent mitigation coverage.

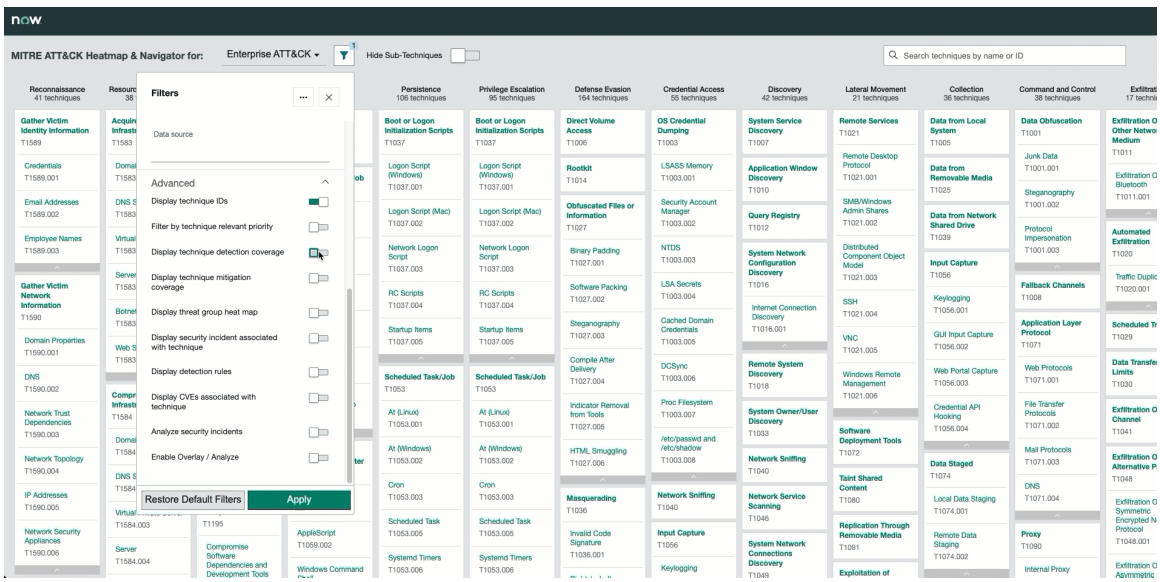
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The color visualization is based on the technique mitigation definition and color coding that you define.
- The coverage visualization is based on the technique mitigation coverage mapping that you define.
- If you modify the base system mitigation coverage definition, the Mitigation Coverage Type icons do not display with the techniques in the heat map.

Note: The heat map works as expected when you modify the same fields as the base system's-defined technique mitigation coverage and coverage colors.

View detection and mitigation coverage

You can use the technique detection and technique mitigation coverage filters together to gain an insight into the relevance of the technique detection and mitigate coverage for your organization.



View threat group

To view the threat group to technique information on the heat map, select **Display threat group heat map**. You can measure the number of threat groups that are using a particular technique. The probability of an attack using a particular technique increases when you have a high number of attackers. The threat group ranges, and heat map colors have been defined in the Threat Group-Technique Heat Map Definition.

- The color visualization for the heat map and text is based on the threat group to technique heatmap definition.
- The threat group range visualization is based on the threat group to technique mapping.
- You cannot use the **Display threat group heat map** filter when the technique detection coverage or technique mitigation coverage are enabled.

View Security incidents associated with technique

To view the techniques that are frequently exploited in your organization and that have resulted in security incidents, click **Display security incident associated with technique**. You can view

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

more information about each of the associated security incidents when you click the link that open in a new window for analysis.

- Priority: Select **Security Incident Priority** to filter by the security incident priority.
- Date range: Select the **Security Incident Date Range** to filter security issues by the date range.
- False positives: Select **Filter false positives security incident** to remove false positive issues. Selecting this filter reduces the number of security incidents you see in the heat map.

When you use this filter with the **Display technique detection coverage** filter, it provides you with an insight into the relevance of the technique detection coverage for your organization until the selected date.

For example, when you turn on both filters, you can see that under the Defense Evasion tactic, the Masquerading technique has no coverage. When you look further, the Masquerading technique is related to the Masquerade Task or Service, which also has a security incident that is associated with it. This shows that there is a gap in the technique detection coverage for the Masquerading technique and you may want to revise the overall technique detection coverage.

View detection rules

To view if you have the detection rules defined for a particular technique, click **Display detection rules**. You can also see each associated detection rule with their definition.

This information is based on the detection rules mapping that you have defined.

View CVEs associated with technique

To view the Common Vulnerabilities and Exposures (CVE) information that is associated with each of the techniques, click **Display CVEs associated with technique**. The CVE to technique information is based on the information available in the CVE - Technique Mapping module. This provides you insight into known vulnerabilities and lets you know if adversaries can potentially exploit your organization.

Important: The heat map is enhanced to display only the relevant CVEs that is associated with the VITs

To view VITs associated with CVEs and techniques, select **Display VITs associated with CVE and techniques**. Additionally, to further filter techniques without VITs, select **Hide techniques without VITs**. The CVE and VIT information you view is fetched from the Vulnerability Response product in your environment. You can view the filtered list of CVEs and VITs in the heat map and navigate to each CVE or VIT for every technique from the heat map.

Note:

- The **Display CVEs associated with technique** is available only when the Vulnerability Response product is installed in your environment.
- The VIT and CVE information is calculated based on the scheduled job you set in the MITRE-ATT&CK properties. The base system schedule job is set for 24 hours.

When you use this filter with the **Display security incident associated with technique** filter, you can learn if the known vulnerabilities have caused security incidents in your organization.

You can view more information about each CVE to analyze if the CVE is relevant to your organization. To do so, view the vulnerability items. If vulnerability items are created, you can view more information about any associated CI information in the Vulnerability Response module. You can also review the severity and priority to make informed decisions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Analyze Security Incidents

To analyze security incidents and review the techniques that are used by an adversary for an attack, click **Analyze Security Incidents**. You can add multiple security incidents for analysis by using comma-separated strings.

This filter helps you to analyze a security incident. You can learn why the incident occurred, what techniques were exploited, if any known threat actors were involved, if the threat actors used a particular sequence for an attack, and so on. Because you can analyze multiple security incidents at the same time, you can correlate the information to see if they are related or if they are an isolated incident. If the security incidents are related and you observe a pattern, you can review their progress on the kill chain to stop the attack or to form a defense strategy for your organization.

When you use the **Analyze Security Incidents** filter with primary filters, such as an **Adversary Group**, you can correlate if known adversaries are involved. For example, when multiple security incidents are being analyzed, the techniques that are associated with the security incidents are present in the form of a kill chain. As you overlap the information with the adversary, you will notice an overlap between the techniques that are associated with the security incident and the techniques that are associated with the adversary. Only the overlapped technique information is shown if both filters are enabled.

Using overlay to analyze security incidents and adversary groups

Use the **Enable Overlay / Analyze** filter to view the adversary behaviour and analyze one or more of the security incidents and correlate the information to see if an attack is an isolated incident or a coordinated attack by a known adversary.

For example, you can now view the security incidents and the threat adversary kill chain behaviour in the same view. This view provides overlap information which informs you of the attack and the known adversary behaviour. This enables you to analyze if this is an isolated attack or a coordinated attack by a known adversary.

Enabling the overlay analyze filter ignores all the primary filters except the **Adversary group** filter, and ignores the advanced filter **Filter by technique relevant priority** while generating a view.

Once you enable the overlay analyze filter, use the color palette to assign colors for the following:

- Analyze Security Incident
- Adversary Group
- Overlay

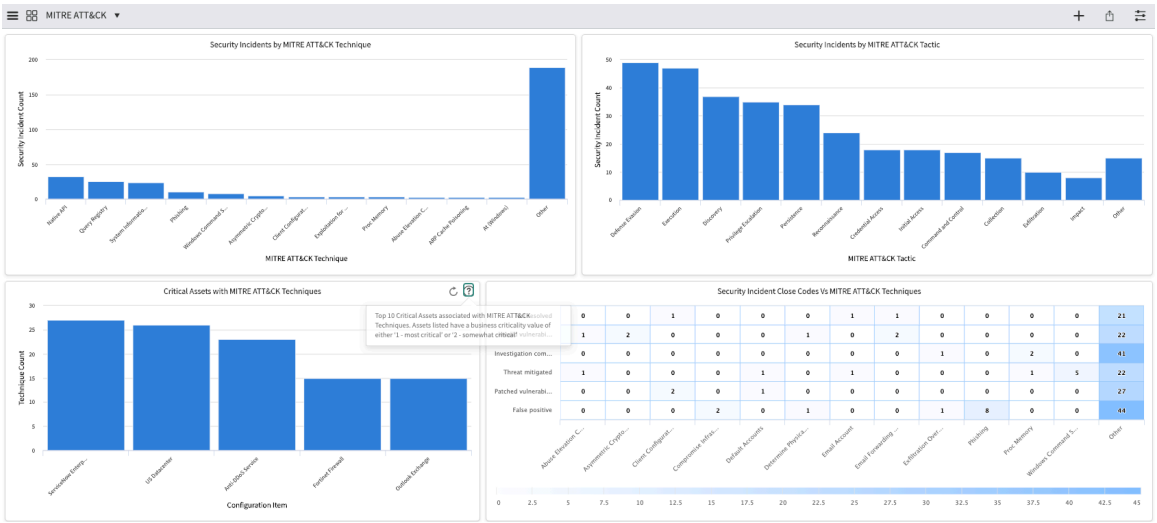
The following illustration shows that the adversary group APT18 is spread across multiple techniques and tactics in the kill chain. The analysis also shows that there are three techniques which overlay the adversary group and security incidents that you are tracking.

Using the MITRE-ATT&CK dashboard

The MITRE-ATT&CK dashboard provides an executive view of the data source coverage, tactics, and techniques that are used in your organization.

The MITRE-ATT&CK Overview module displays MITRE-ATT&CK information about security incidents including trends and reports. You can click any part of a widget (bar, data point, table, and so on) to view data that is specific to that part.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Use the MITRE-ATT&CK dashboard to see your security-related data

Use the MITRE-ATT&CK dashboard to get an overview of the data source coverage, tactics, and techniques that are used in your organization.

Before you begin

Role required: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Procedure

1. Navigate to **All** > **Threat Intelligence** > **MITRE ATT&CK Repository** > **Overview**.
2. Click any of the following widgets to see additional details:
   - Security Incidents by MITRE-ATT&CK Technique
   - Security Incidents by MITRE-ATT&CK Tactic
   - Critical Assets with MITRE-ATT&CK Techniques
   - Security Incident Close Codes Vs MITRE-ATT&CK Techniques
   - MITRE-ATT&CK Techniques by Detection Coverage
   - MITRE-ATT&CK Techniques by Mitigation Coverage
   - Threat Groups by MITRE-ATT&CK Technique
   - CVEs by MITRE-ATT&CK Technique

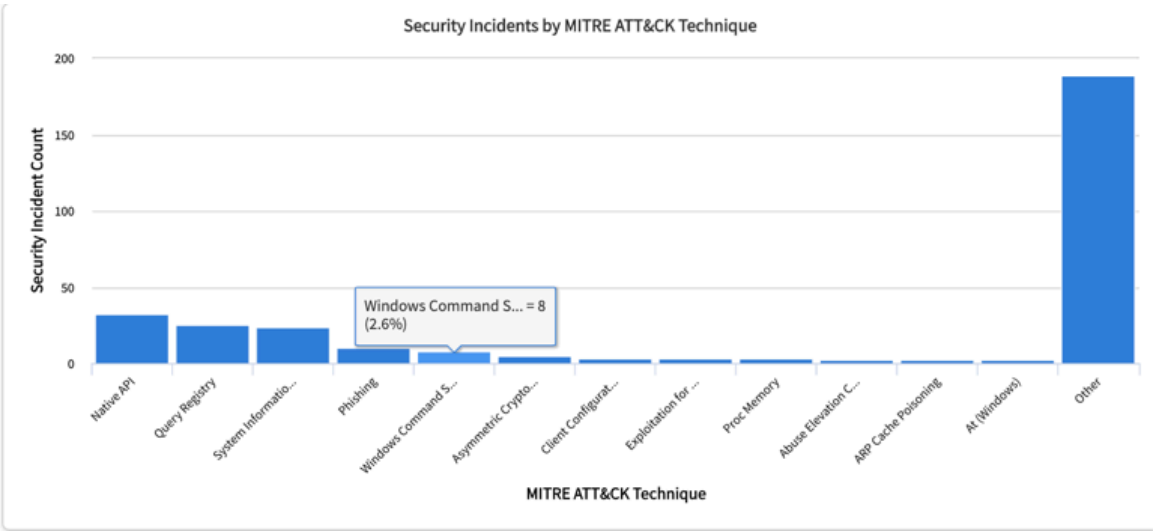
MITRE-ATT&CK widgets

The MITRE-ATT&CK Overview module consists of widgets that enable you to correlate the MITRE-ATT&CK information with the security incident information in your environment.

Example of Security Incidents by MITRE-ATT&CK Technique

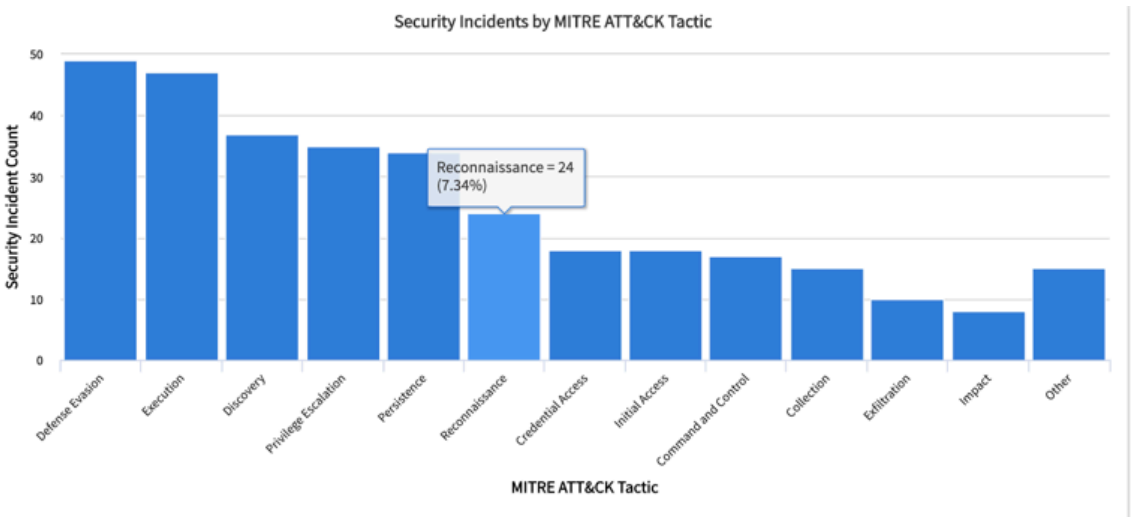
In this example, the **Security Incidents by MITRE ATT&CK Technique** widget displays the techniques by security incident in an organization's environment in the last 90 days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Example of Security Incidents by MITRE-ATT&CK Tactic

In this example, the **Security Incidents by MITRE ATT&CK Tactic** widget displays the top tactics by security incident in an organization's environment in the last 90 days.

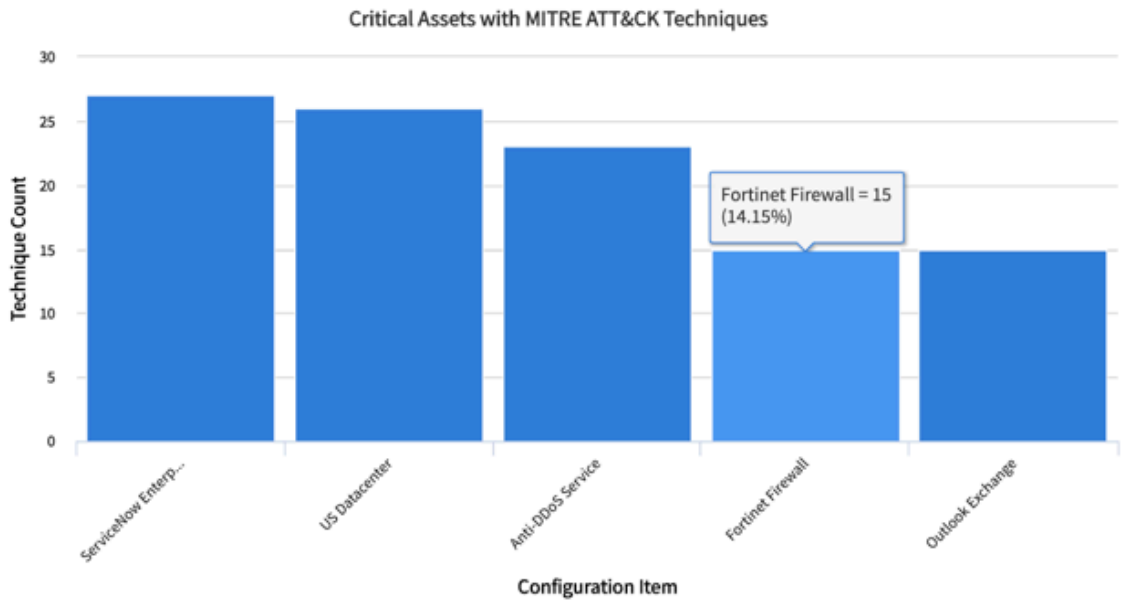


Example of Critical Assets with MITRE-ATT&CK Techniques

In this example, the **Critical Assets with MITRE ATT&CK Techniques** widget displays the top 10 critical assets that are associated with the MITRE-ATT&CK techniques. The assets have a business criticality of either 1 (most critical) or 2 (somewhat critical).

This report enables an organization to see the types and number of techniques that are used in carrying attacks against the critical assets.

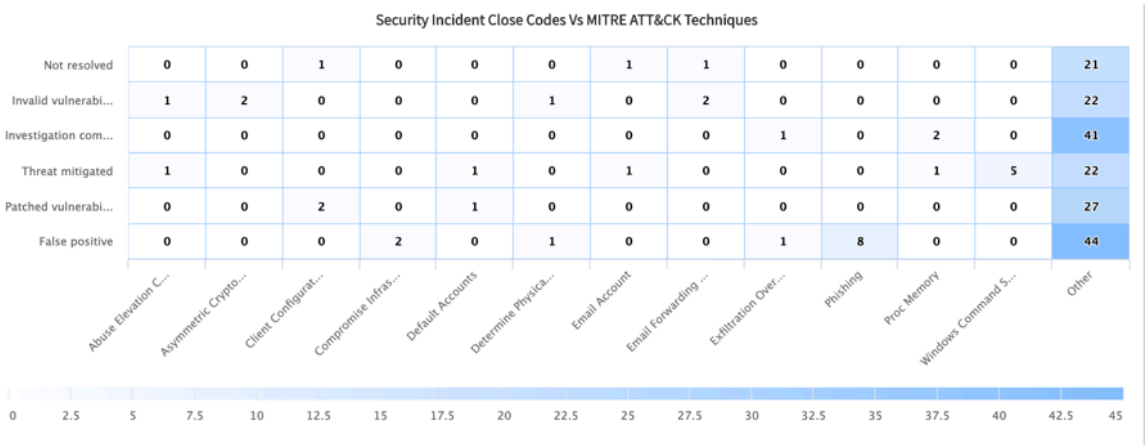
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Example of Security Incident Close Codes Vs MITRE-ATT&CK Techniques

In this example, the **Security Incident Close Codes Vs** *MITRE-ATT&CK* **Techniques** widget displays the security incident close codes that were mapped against the identified top techniques in an organization's environment.

The x-axis displays the top techniques that were used to carry attacks against the enterprise, and the y-axis displays the closed codes.

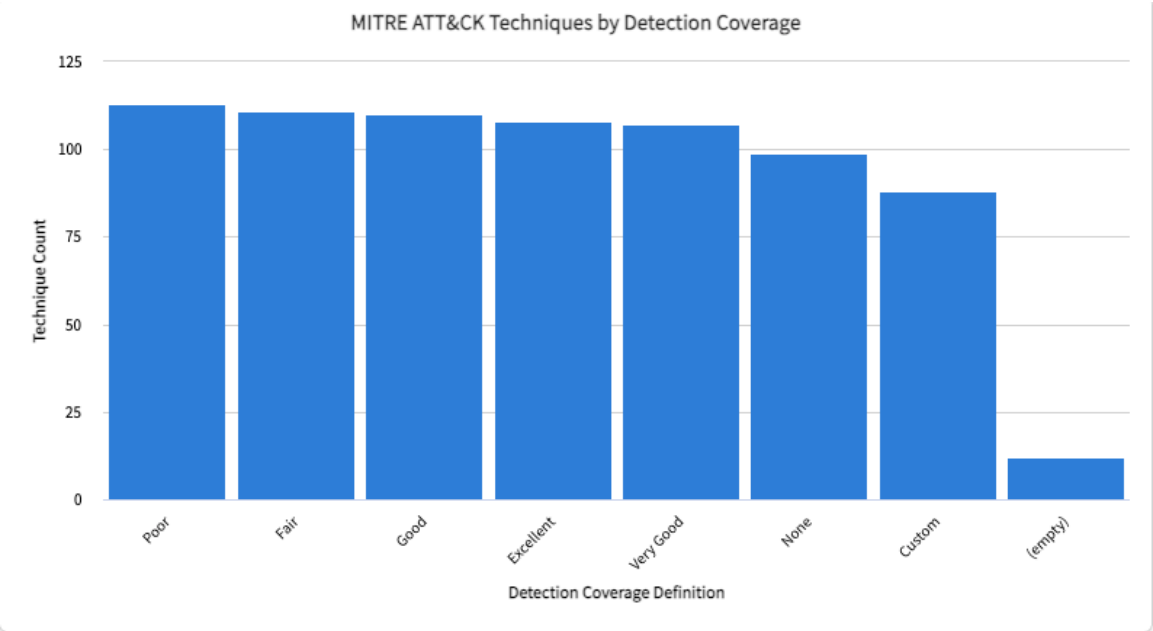


Example of detection coverage by MITRE-ATT&CK techniques

In this example, the **MITRE-ATT&CK Techniques by Detection Coverage** widget displays the technique count by the detection coverage in your environment.

The x-axis displays the technique count, and the y-axis displays the detection coverage types.

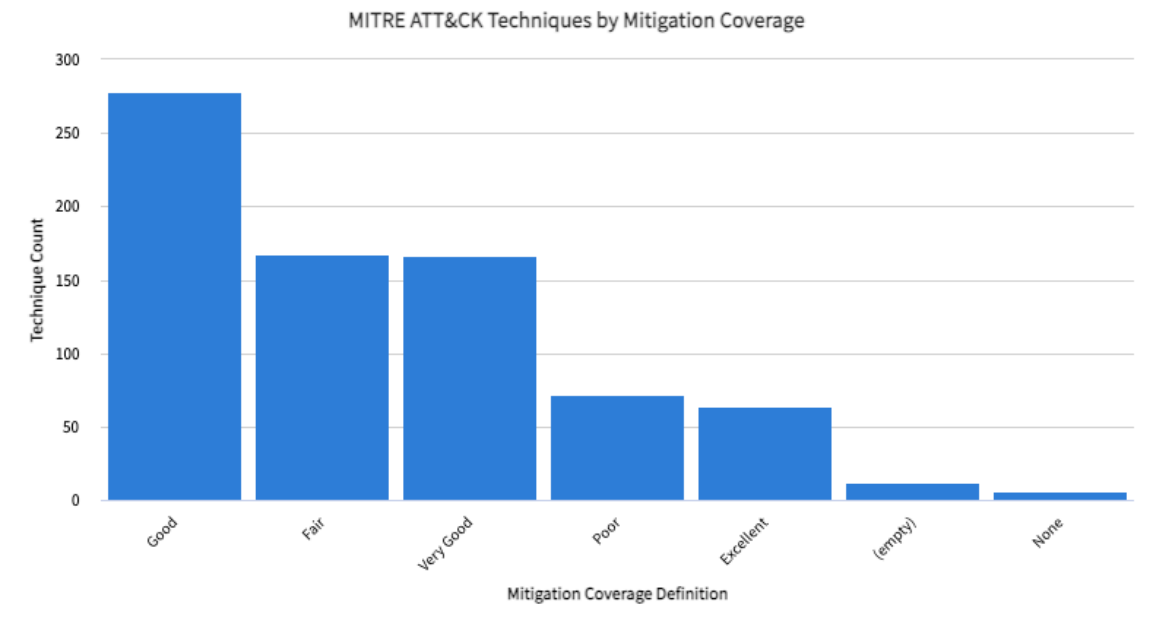
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Example of mitigation coverage by MITRE-ATT&CK techniques

In this example, the **MITRE-ATT&CK Techniques by Mitigation Coverage** widget displays the technique count by the mitigation coverage in your environment.

The x-axis displays the technique count, and the y-axis displays the mitigation coverage types.

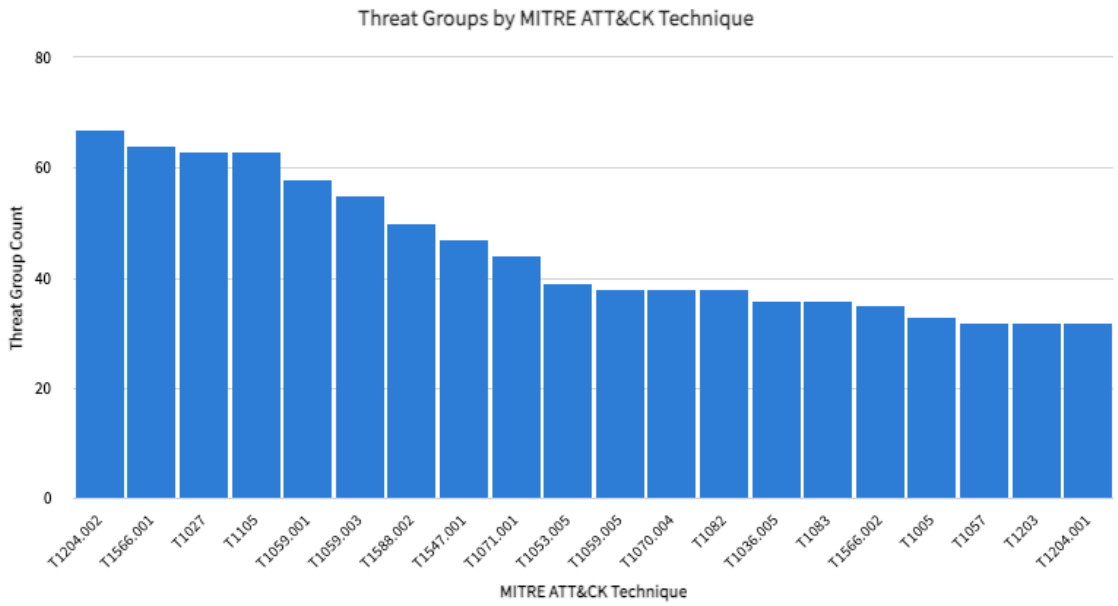


Example of threat groups by MITRE-ATT&CK techniques

In this example, the **Threat Groups by MITRE-ATT&CK Technique** widget displays the techniques by the threat group count. This widget displays 20 techniques with the highest threat group count.

The x-axis displays the threat group count, and the y-axis displays the MITRE-ATT&CK techniques.

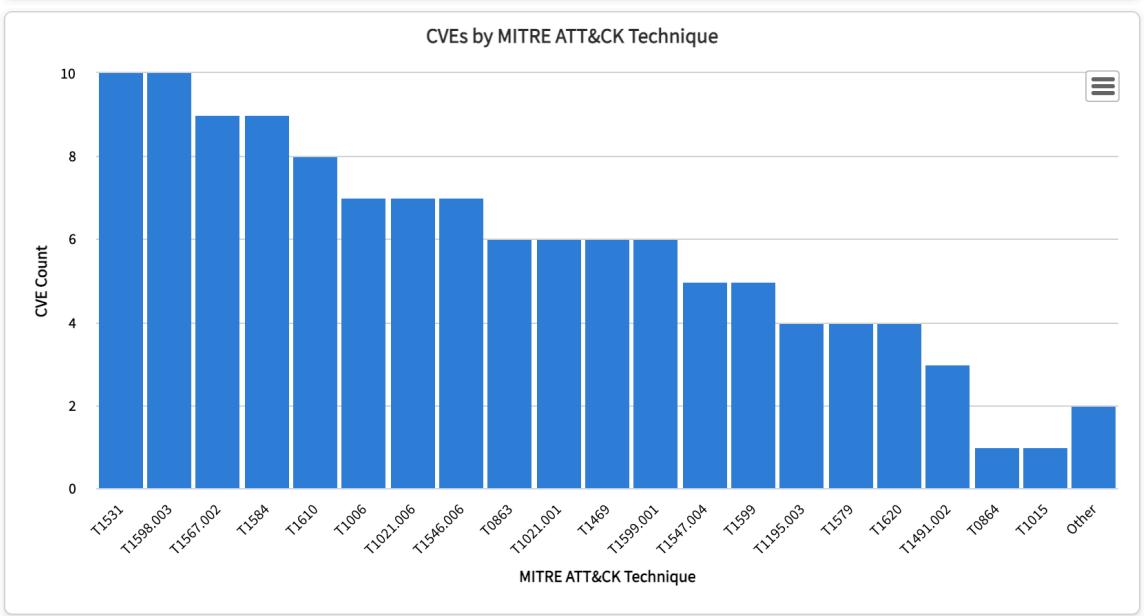
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Example of CVEs by MITRE-ATT&CK techniques

In this example, the **CVEs by MITRE-ATT&CK Technique** widget displays the techniques with the relevant CVE count in your environment.

The x-axis displays the relevant CVE count, and the y-axis displays the MITRE-ATT&CK techniques.



MITRE DEFEND Framework

MITRE D3FEND is a knowledge graph of cybersecurity countermeasure techniques that complements the MITRE-ATT&CK framework by providing defensive techniques.

MITRE defend framework overview

DEFEND (Detection, Denial, and Disruption Framework Empowering Network Defense) is a knowledge graph developed by MITRE that catalogs defensive cybersecurity countermeasure

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

techniques. It provides a standardized taxonomy of over 200 defensive techniques organized into seven tactical categories.

While MITRE ATT&CK describes "how adversaries attack," D3FEND describes "how defenders respond." The two frameworks are complementary and bidirectionally mapped, enabling security teams to identify appropriate defensive countermeasures for specific attack techniques.

Key concepts

Defensive Techniques

Over 200 standardized defensive techniques organized hierarchically with parent techniques and sub-techniques. Each technique includes a definition, digital artifacts it operates on, and mappings to ATT&CK offensive techniques.

DEFEND Tactics

Seven high-level tactical categories that organize defensive techniques:

- **Model:** Understand the system and its behavior
- **Harden:** Reduce attack surface and vulnerabilities
- **Detect:** Identify malicious activity
- **Isolate:** Contain threats and limit damage
- **Deceive:** Entice, and allow potential attackers access to an observed/ controlled environment
- **Evict:** Remove threats from the environment
- **Restore:** Return the system to a better state

Digital Artifacts

Over 800 asset types that defensive techniques operate on or protect, including processes, files, network traffic, user accounts, system calls, and more.

ATT&CK Mappings

Bidirectional mappings between D3FEND defensive techniques and ATT&CK offensive techniques, showing which defensive techniques can counter specific attack methods.

Integration with Threat Intelligence

The ServiceNow Threat Intelligence application integrates DEFEND to provide:

- Automatic ingestion of DEFEND techniques, tactics, and artifacts via API.
- Bidirectional mapping between DEFEND defensive and ATT&CK offensive techniques.
- Coverage analysis showing defensive posture against ATT&CK techniques.
- Task tracking for implementing defensive countermeasures.

Ingest MITRE DEFEND data

Ingest MITRE D3FEND data (tactics, techniques, and artifacts) from the MITRE website to integrate with SIR.

Before you begin

Role required: sn_ti.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. Select **MITRE DEFEND ingestion** from the list of scheduled jobs.
3. Select **Execute Now** to start the data ingestion.

Related topics

MITRE attack and defend technique graph

MITRE DEFEND tables

The section describes all the tables used in the MITRE Defend integration.

Defend Tactics

Defend Tactics table

Field	Description
Tactic ID	The ID of the defend tactic.
Tactic Name	The name of the defend tactic
Definition	The description or the use of the defend tactic.

Defend Techniques

Defend Techniques table

Field	Description
Name	The name of the defend technique.
Defend Tactic	The tactic to which the defend technique belong to.
Technique ID	The ID of the technique.
Definition	The description or the use of the defend technique.
KB Article	A link to the KB article or more information about this technique.
Parent Defend Technique	The parent technique of this defend technique.
Synonyms	The synonym of the defend technique.

Defend Artifacts

Defend Artifacts table

Field	Description
Artifact ID	The ID of the defend artifact.
Artifact Name	The name of the defend artifact.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Defend Artifacts table (continued)

Field	Description
Definition	The description or the use of the defend technique.
Revoked	The revoked status of this defend artifact.
Domain	The domain of the defend artifact.

Defend Techniques Artifacts

Defend Techniques Artifacts table

Field	Description
Defend Artifact	The name of the defend artifact.
Defend Technique	The defend technique to which the artifact belongs to.
Relationship Label	The action that the defend technique take on the defend artifact.
Revoked	The revoked status of this defend artifact.
Domain	The domain of the defend artifact.

Related Defend Techniques

Related Defend Techniques table

Field	Description
Automatically added	The defend technique is automatically added or not.
Defend Technique	The name of the defend technique.
Inheritance count	How many times this technique is inherited.
Domain	The domain of the defend technique.
Task	The related security incident.

Defend ATTACK Techniques

Defend ATTACK Techniques table

Field	Description
ATTACK Technique	The attack technique.
Defend Technique	The defend techniques correspond to the attack technique.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence administration

The Threat Intelligence base system is ready to use on activation. You can add records to certain modules in the Administration application menu, but most are already populated with industry-standard information.

The following applications are available under the **Administration** module of the Threat Intelligence navigation bar:

Threat Intelligence administration applications

Application	Description
Properties	Threat Intelligence properties allow you to control how different aspects of the system function, including the setting of API keys.
Attack Mechanisms	This module organizes attack patterns hierarchically, based on mechanisms that are frequently employed when exploiting a vulnerability.
Attack Motivations	This module lists the possible attack motivations that shape intensity of an attack by a threat actor or intrusion set.
Discovery Methods	This module describes how security incidents are discovered.
Feeds	This feature has been deprecated.
Indicator Types	This module is used to characterize cyber threat indicators made up of patterns that identify certain observable conditions, as well as contextual information about the meaning of the patterns, and how and when they are acted on.
Infrastructure Types	This module lists the possible classifications of infrastructure.
Intended Effects	This application is used for expressing the intended effect of a threat actor.
Malware Capabilities	This module lists the possible capabilities of malware.
Malware Types	This module lists the possible classifications of malware.
Notifications	This module is used for creating email notifications. This involves specifying when they are sent, who receives them, and what they contain.
Observable Types	This module lists the possible classifications of an observable, such as an IP address or file hash.
Report Types	This module lists the possible classifications of threat reports.
Threat Actor Roles	This module lists the roles the threat actors play.
Threat Actor Types	This module characterizes malicious actors (or adversaries) representing a cyber attack threat, including presumed intent and historically observed behavior.
Threat Lookup Finding Calculators	This module calculates the findings based on the responses received. For third-party integrations that provide the computed results, the threat lookup finding calculator maps the results to supported findings in the system. For more information, see Threat Lookup Finding Calculators.
Tool Types	This module lists the possible classification of tools.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Lookup Finding Calculators

Threat Lookup Finding Calculator helps you calculate the observable findings based on the responses received.

You can create a Threat Lookup Finding Calculator for your integration and use a script to determine how you want to identify the various observable findings. The Threat Lookup Finding Calculator includes a sample script that comes with the base system, which you can use to identify the observable findings or you can modify this script according to your requirements.

For third-party integrations that provide the computed results, the Threat Lookup Finding Calculator maps the results to supported findings in the base system.

Rollup Threat Lookup Results

When you have multiple threat lookup results for an observable from the various integration vendors, then the recent threat lookup results from all the vendors are considered, and the overall observable findings are marked as follows:

Rollup Threat Lookup Findings

Latest Observable Finding	Overall Observable Finding
Malicious	If one of the integration vendors reports the observable as Malicious, then the overall observable finding is marked as Malicious.
Suspicious	If none of the integration vendors report the observable as Malicious, one of them reports it as Suspicious, and then the overall observable finding is marked as Suspicious.
Clean	If all the integration vendors report the observable as Clean, then the overall observable finding is marked as Clean.
Unknown	If none of the integration vendors report the observable as Malicious or Suspicious and one of them report it as Unknown, then the overall observable finding is marked as Unknown.

Using Threat Lookup Finding Calculators

Use the Threat Lookup Finding Calculator to calculate the observable findings for your integration.

Before you begin

Role required: sn_ti.admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Administration** > **Threat Lookup Finding Calculators**.
2. Click **New**.
3. On the form, fill the fields.

Field	Description
Threat Lookup vendor	Name of the threat look-up vendor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Observable Type	Specify the classification of the observable type to which the script applies. For example, IP address or file hash, and so on. The script applies to all observables if you do not select any observable type.
Finding Script	Script editor to determine how you want to identify the various observable findings. The Threat Lookup Finding Calculator contains a sample script with the base system. You can use this script to determine the observable findings, or you can modify this script accord ing to your requirements.

4. Click **Update**.

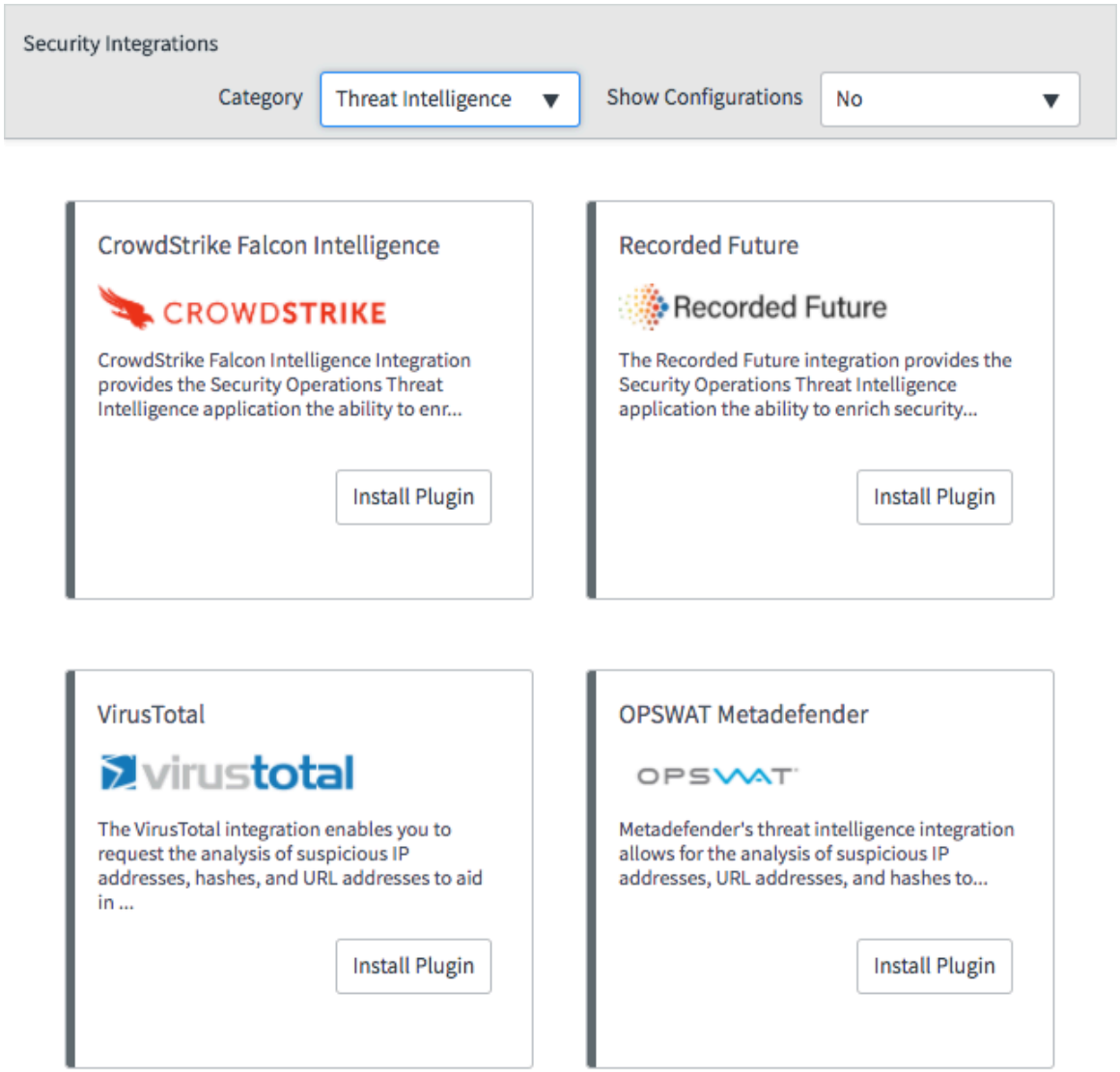
Threat Intelligence integrations

The Threat Intelligence base system includes integrations to third-party malware-detection software packages. This section provides instructions for activating the plugins and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.

Integration Configurations

The base system includes a series of "cards" for each of the integration implementations you can activate and use. Also, cards are displayed for any integrations posted on the ServiceNow Store that have dependencies on Security Operations plugins. The integration cards can be viewed by selecting **Security Operations** > **Integration Configurations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can filter the visible integrations using the **Category** drop-down menu. The **Show Configurations** drop-down menu lets you see multiple instances of implementations that allow their creation.

Buttons on integration cards

Integration cards display different buttons depending on the current state of the integration and the source of the card.

Button	Description
Install Plugin	Click this button to install the applicable plugin to activate the integration. After the plugin is installed, the button changes to **Configure**.
Configure	Click this button to enter information for configuring the integration. For some integrations, you may need to enter API keys or URLs acquired from the website of the third-party integration.
New	Certain integrations, such as Carbon Black and IBM QRadar, allow you to define multiple implementations of the same integration. For those integrations, click **New** after the plugin is activated. The cards allow you to install plugins (where applicable) and configure the implementations for use.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Button	Description
Open Page	In the base system, your instance performs a query to the ServiceNow Store for any applications that have dependencies on Security Operations plugins. When those applications are found, and the associated application plugins are activated, integration cards for them are displayed with the other security integration cards. Click **Open Page** to access the website of the third-party application to configure the integration. After you have completed the configuration, the **Open Page** button changes to **Configure**.

CrowdStrike Falcon Intelligence integration

CrowdStrike Falcon Intelligence enriches Threat Intelligence with data for security incidents and associated observables.

Explore

- CrowdStrike Falcon Intelligence integration overview
- Security Incident Response integrations

Set up

Activate and configure the CrowdStrike Falcon Intelligence integration

---

Use

- Perform lookups on observables
- Threat Lookup - CrowdStrike Falcon Intelligence flows

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

CrowdStrike Falcon Intelligence integration overview

CrowdStrike Falcon Intelligence provides cyber security intelligence that easily integrating with Security Operations.

Note: The Threat Intelligence plugin is required to implement the CrowdStrike Falcon Intelligence integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

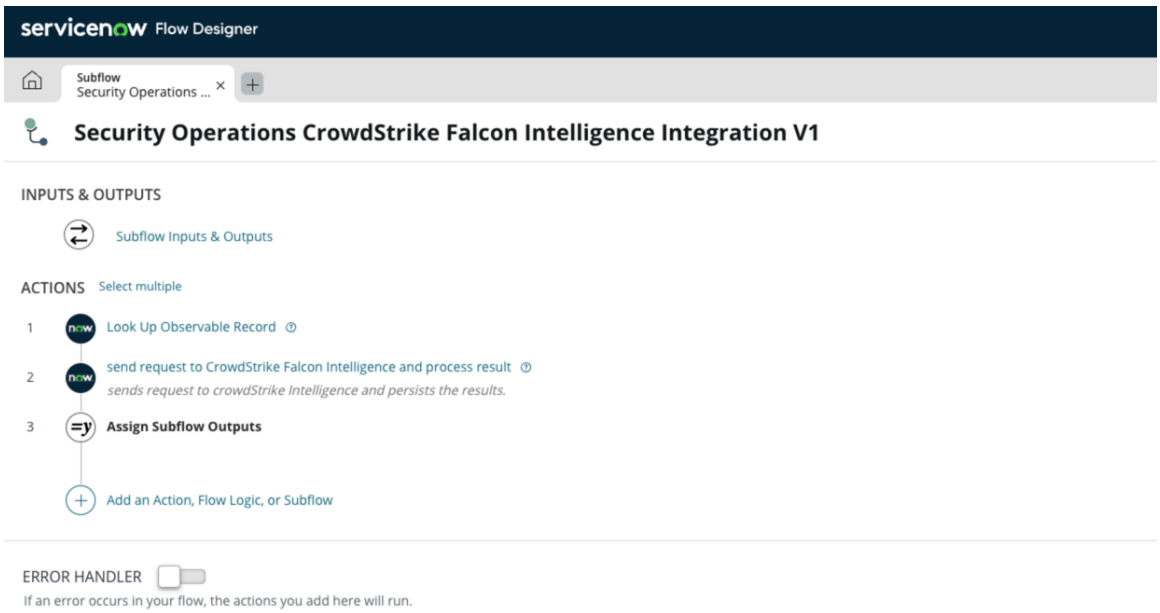
Submit an IoC Lookup request from the Security Incident Catalog

Threat Lookup - CrowdStrike Falcon Intelligence flows

The Threat Lookup - CrowdStrike Falcon Intelligence flow designer performs a lookup on selected observables. If the observables are of a type recognized by CrowdStrike Falcon Intelligence, the observables are scanned for malware, and the results are returned.

This flow is triggered by the Security Operations Integration - Threat Lookup capability when you publish one or more observables to a watchlist, and the CrowdStrike Falcon Intelligence implementation is selected. After they are published, the watchlists can be viewed in the CrowdStrike Falcon Host software.

Role required: admin



For information on the activities used by this flow designer, see Common Security Operations integration flows and orchestration Flow Actions.

Activate and configure the CrowdStrike Falcon Intelligence integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the CrowdStrike Falcon Intelligence integration. Before you can use the CrowdStrike Falcon Intelligence, you must download it from the ServiceNow Store and add the appropriate API key and ID.

Before you begin

Role required: admin

- The Threat Intelligence plugin must be installed and activated before you can use the CrowdStrike Falcon Intelligence integration.
- Obtain the API Client ID and API Client Secret under your CrowdStrike Falcon Intelligence profile.
- If you are upgrading CrowdStrike Falcon Intelligence integration from a previous version, then you must delete the existing configuration and set up a new configuration. The integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

supports OAUTH2 authentication. This update requires you to enter the **API Client ID** and the **API Client Secret** to authenticate and complete the configuration.

- In the CrowdStrike Falcon Intelligence portal **API Scopes**, enable the **Read** setting for **Indicators (Falcon X)** or **IOCs (Indicators of Compromise)**.

Procedure

1. Download the integration from the ServiceNow Store.
2. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configurations**. The available security integrations appear as a series of cards.
3. In the CrowdStrike Falcon Intelligence card, click **Configure**.
4. On the form, fill in the fields to complete the configuration:

CrowdStrike Falcon Intelligence Configuration

Field	Description
Name	Name of the integration, for example, `demo-1`.
API Client ID	The client ID that you obtain from the settings section of your account profile in CrowdStrike Falcon Intelligence portal.
API Client Secret	The client secret key that you obtain from the settings section of your account profile in CrowdStrike Falcon Intelligence portal.

5. Click **Submit**.

Result

After it is configured, CrowdStrike Falcon Intelligence can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related topics

Perform lookups on observables

Have I been pwned? integration

The Security Operations Have I been pwned? integration enables you to submit lookups on domain names and email addresses to determine whether user personal data has been compromised by data breaches.

Explore

Security Incident Response integrations

Set up

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

(continued)

- Security Operations Have I been pwned? integration setup
- Activate the Security Operations Have I been pwned? integration

Use	Develop
Perform lookups on observables Threat Lookup - Have I been pwned? flow	• ServiceNow Security Operations integration development guidelines • Tips for writing integrations • Developer training • Developer documentation • Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Security Operations Have I been pwned? integration setup

Have I been pwned? is a free resource used to assess if someone may have been put at risk due to their online account being compromised or "pwned" in a data breach. It easily integrates with Security Operations.

Before you can use the Have I been pwned? integration, you must activate the plugin. If necessary, you can also update your X509 SSL certification.

The Security Incident Response, Threat Intelligence, and Security Operations Have I been pwned? plugins are required to implement the Security Operations Have I been pwned? integration.

Threat Lookup - Have I been pwned? flow

The Threat Lookup - Have I been pwned? flow performs a lookup on selected observables. If the observables are of a type recognized by Have I been pwned?, the observables are scanned for malware, and the results are returned.

Role required: sn_si_admin

This flow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the Have I been pwned? implementation is selected. For more information, see Perform lookups on observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Have I been pwned flow



For information on the activities used by this flow, see Common Security Operations integration flows and orchestration Flow Actions.

Activate the Security Operations Have I been pwned? integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Have I been pwned? integration. Before you can use the Have I been pwned? integration, you must download it from the ServiceNow Store.

Before you begin

- The Threat Intelligence plugin must be installed and activated before you can use the Security Operations Have I been pwned? Integration.

Role required: sn_si_admin

Procedure

Download the integration from the ServiceNow Store.
This integration supports an open API and does not require further configuration. Have I been pwned? can now be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related topics

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Acquire the SSL certificate from the third-party vendor.
   For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.

   a. Enter the endpoint URL into the browser address bar.
      For example: `https://<3rdparty>/`.

   b. Click the lock icon in the address line.

   c. Click **More Information** and click the **Security** tab.

   d. Click **View Certificate** and click the **Detail** tab.

   e. Click **Export** to save the PEM into your local file system.

   f. Open the saved file in any text editor tool and copy the content to the clipboard.
      It must begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

2. Navigate to **System Definition** > **Certificates**.
3. Click **New** and create a new record for the integration.
4. In **PEM Certificate**, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Add the certificate to the Identity Provider record.
   a. Navigate to **Multi-Provider SSO** > **Identity Providers**.
   b. Select the active default identity provider for which you created the new certificate.
   c. Scroll down to **X.509 certificates** related list, and click **Edit**.
   d. Move the newly created certificate to the **Selected** column.
6. Click **Save**.
   The other fields in the record are generated automatically.

   Note: If you have a certificate that has expired, you need to remove it. For information on how to remove the expired certificate, refer to KB0691439 Replacing an expiring SAML certificate.

MISP integration for Security Operations

With MISP integration for Security Operations, you can investigate security incidents with sighting searches, observable enrichment, and create or update events in MISP. Using MISP, you can investigate targeted attacks faster, improve the detection ratio, and reduce the number of false positives in your environment.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

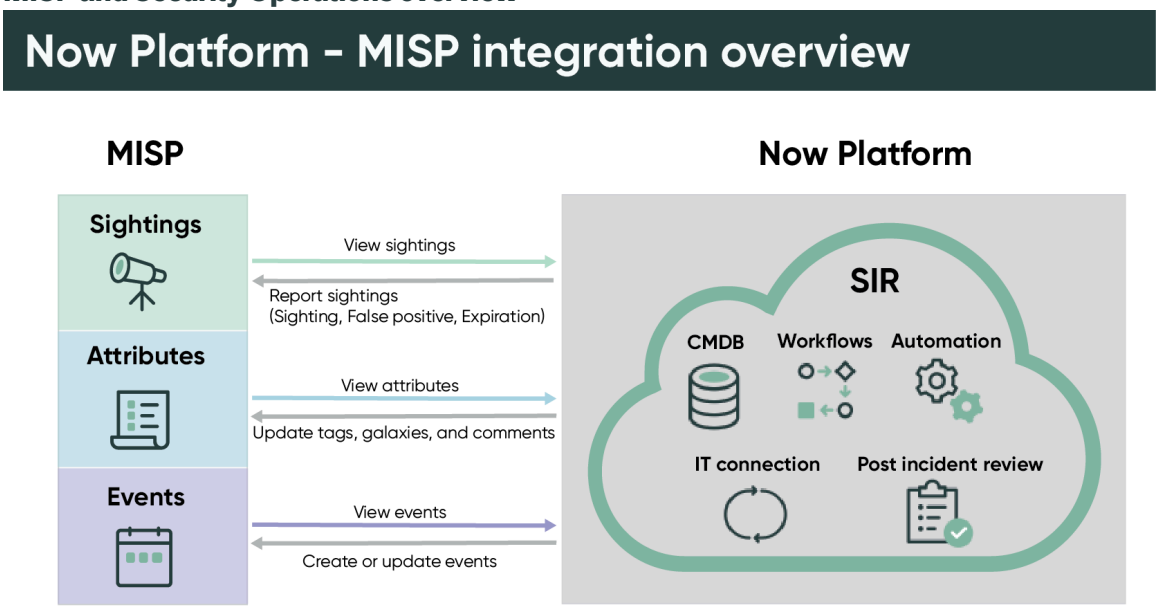
MISP Overview

MISP, which stands for Malware Information Sharing Platform, lets you exchange and share threat intelligence and Indicators of Compromise (IoCs) about the targeted malware and attacks within your community of trusted members. You can also share MISP information with private or open communities. By exchanging MISP information, you can investigate targeted attacks faster, improve the detection ratio, and reduce the number of false positives in your environment.

MISP and Security Operations

See the following example to learn how the MISP information flows with Security Operations applications.

MISP and Security Operations overview



Key features

This integration includes the things that you can do with the MISP key features:

- Connect to private and public MISP instances.
- Support manual and automatic sighting search of observables.
- Run sighting search from case management.
- Report or update sightings to an attribute:
  - Report an observable as a sighting (global)
  - Report an observable as a false positive (global)
  - Report an observable as expired
- Support manual and automatic observable enrichment. Results include the MISP attribute and event information that is associated with the observables.
- Attribute enrichment in MISP which includes adding or updating tags, galaxies, or comments.
- Event creation in MISP from SIR: Supports manual and the automatic creation of events in MISP from SIR.
- Update a MISP event from SIR which includes adding or updating tags, galaxies, or attributes.
- Add security incident associated observables as attributes to a MISP event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Auto-extract MITRE-ATT&CK™ information from MISP attributes and associate the information to SIR security incidents.
- Automatically add SIR MITRE-ATT&CK™ information as galaxies to a MISP event.

Key concepts

This integration includes the following key concepts that you must know:

- MISP is a Threat intelligence platform (TIP). You use TIPs to collect, correlate, categorize, share, and integrate security threat data in real time to support the prioritization of actions and aid in attack prevention, detection, and response.
- MISP is a Threat Intelligence Management (TIM). You use TIMs to turn threat data into threat intelligence through context and to automatically prioritize threats by user-defined scoring and relevance.
- MISP Data layer
  - Events are encapsulations for contextually linked information.
  - Attributes are individual data points, which can be indicators or supporting data.
  - Objects are custom template attribute compositions.
  - Object references are the relationships between the other building blocks.
  - Sightings are time-specific occurrences of a detected data-point.
- MISP Context layer
  - Tags are labels that are attached to events or attributes and may come from taxonomies.
  - Galaxy-clusters are knowledge base items that you can use to label events or attributes that come from galaxies.
  - Cluster relationships denote pre-defined relationships between clusters.
- Indicators contain a pattern that you can use to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (IP address), system indicators (a string in memory), or even bank account details. The attributes in MISP are known as observables in other SIEMs or formats such as STIX.
  - A type describes the attribute. For example, MD5 or a URL.
  - The attribute category describes an attribute. For example, a payload delivery.
  - An IDS tag determines if an attribute can be automatically used for detection.

Note: For more information about MISP concepts, see the MISP Documentation website

How your organization can benefit from MISP integration for Security Operations

Security analysts must gain and maintain situational awareness of the threat landscape, which means that they must manually consolidate and integrate an overwhelming amount of threat data. Gathering, consolidating, and integrating this data takes valuable time, which slows the detection and analysis of threats. MISP integration for Security Operations enables analysts to detect more threats and respond quicker by integrating the MISP security intelligence into an existing ServiceNow AI Platform instance.

By using the MISP integration for Security Operations, your organization can do the following actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Enable your security analysts to respond quickly and with the right context.
- Improve your security team's efficiency by automating the incident flows for detecting and containing threats.
- Reduce manual research time and enable security analysts to operationalize and curate indicators from within the ServiceNow AI Platform.

Learn about this integration

Document identifier	Document title
MISP documentation website	MISP Documentation website
ServiceNow product documentation website	ServiceNow Product Documentation website

MISP administration

You can set up MISP integration in the ServiceNow AI Platform to perform a sighting search, observable enrichment, and to create and update events in MISP.

Getting started with MISP integration for Security Operations

Review the following information before you set up your MISP integration for Security Operations.

Checklist

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform, Threat Intelligence, and Security Incident Response roles.	The following roles are used across the MISP features on the ServiceNow AI Platform: • The administrator (admin) installs the applications from the ServiceNow Store and assigns the security incident administrator (sn_si.admin) and threat intelligence administrator (sn_ti.admin) roles. • sn_si.admin and sn_ti.admin can configure the integration and set up the automatic MISP event creation profiles. • sn_sec_misp.write - The MISP analyst role has read and write permissions for MISP data that includes the event and attribute data. For more information, see Setup Threat Intelligence.
Assign the required MISP user roles.	Review the MISP user roles and the permissions required to use the MISP integration for Security Operations. **Note:** For more information about the user roles in MISP, see the Roles section in the MISP documentation website.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
Verify that you are using MISP version 2.4.137 or later.	The MISP integration for Security Operations is tested with a minimum MISP version 2.4.137.
Verify that the ServiceNow core applications that are required to support the MISP module are installed and activated.	Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation. • Security Incident Response • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) For more information on setting up your ServiceNow AI Platform instance for the integration, see get entitlement for a Security Operations product or application and activate a ServiceNow Store application.
Domain separation	Verify the domain separation section if you intend to separate data, processes, and administrative tasks.

MISP user roles and permissions

Review the user roles that are required in the MISP integration for Security Operations integration.

Observable Enrichment and Sighting Search Permissions

Note:

- **All ServiceNow MISP integration capabilities need the basic permissions to Manage Organization Events and Auth key access. Ensure that you have these basic permissions before you proceed.**
- **To add local galaxies, the user that configures the integration should belong to the host organization of the corresponding MISP server.**

MISP capability	Tagger	Tag editor
Observable Enrichment (Read-only)	#	#
Sighting Search (Read-only)	#	#

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Report Sighting Permissions

MISP capability	Sighting creator
Report Sighting	#

Attribute and Event Permissions

MISP capability	Tagger	Tag editor
Edit Event/Attribute Tags	#	#
Edit Event/Attribute Galaxies	#	#
Edit Attribute Comments	#	#
Add New Attribute to event	#	#
Create Event in MISP	#	#

Install and configure the MISP integration for Security Operations

Install and configure the MISP integration for Security Operations from the ServiceNow Store on your ServiceNow AI Platform instance so that you can start investigating security incidents using the MISP data.

Before you begin

Ensure that you've installed the valid SSL certificates on the MISP server.

Role required: sn_si.admin

Procedure

1. Download the MISP integration for Security Operations from the ServiceNow Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the MISP -SIR/TI Integration tile and click **Configure**.
4. On the form, fill in the fields.

MISP - SIR/TI Integration Configuration form

Field	Description
Name	Name for the MISP instance configuration.
MISP Server URL	URL for the MISP server that serves as the REST endpoint for the MISP server.
API Key	API key that is configured for your user account on the MISP server. The API key corresponds to the **Authkey** in the MISP server.
On Premises Deployment	Option that you can select if your MISP server is deployed in an on-premise instance. When you select the **On Premises Deployment** option, you must use the MID Server to connect to the MISP server.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
MID Application	String field that identifies the MID Application name that is used to communicate with MISP. This field is required when you select the **On Premises Deployment** option. For information on how to configure the MID server for your application, see Configure a MID Server for each application

5. Click **Submit**.

Result
After you successfully validate and submit the configuration, the MISP - SIR/TI Integration is saved on the Security Integrations page as a tile.

Review the MISP integration settings

Review the MISP integration for Security Operations settings and modify the default system properties to suit your environment.

Before you begin
Role required: sn_si.admin, sn_ti.admin

Procedure
1. Navigate to **All** > **MISP Integration** > **Integration Settings**.
2. Modify the following settings as required.

MISP Integration settings

Property name		Description
Observable Enrichment	Time (in hours) before fetching new data	Time in hours before you can fetch new data. Type: integer Default value: 24
Sighting Search	Run Sighting Search automatically when new observables are associated with the security incident	Sighting search that runs whenever a new observable is associated with a security incident. Default value: Yes
	Search Interval (in days) for sighting search in MISP	Number of days that the sighting search data is searched in MISP. Use this option only for the automatic sighting search feature. Default value: 90

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property name		Description
Data synchronization	Interval period (in minutes) for tags to be fetched and synchronized with MISP	MISP tags that are fetched at the time of the integration configuration. After the data is in the ServiceNow AI Platform, this property defines the frequency at which the data with the MISP server is synchronized. The value is defined in minutes. Default value: 1440 (minutes or 24 hours)
	Interval period (in minutes) to refresh MISP galaxies from configured sources	MISP galaxies that are fetched at the time of the integration configuration. After the data is in the ServiceNow AI Platform, this property defines the frequency at which the data with the MISP server is synchronized. The value is defined in minutes. Default value: 1440 (minutes or 24 hours)
	Interval period (in minutes) for organizations to be fetched and synchronized with MISP	MISP organizations that are fetched at the time of the integration configuration. After the data is in the ServiceNow AI Platform, this property defines the frequency at which the data with the MISP server is synchronized. The value is defined in minutes. Default value: 1440 (minutes or 24 hours)
MITRE™ Technique Extraction	Rollup MITRE-ATT&CK techniques automatically from MISP Observable Enrichment Results (Tags) to security incident	Rollup of MITRE-ATT&CK information from MISP observable enrichment results (tags) to the security incident. Default value: Yes
	Rollup MITRE-ATT&CK techniques automatically from MISP Observable Enrichment Results (Galaxies) to security incident	Rollup of MITRE-ATT&CK information from the MISP observable enrichment results (galaxies) to the security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property name		Description
		Default value: Yes

Note:

- To use the MITRE™ technique extraction features in MISP, you must enable the MITRE-ATT&CK feature in the Threat Intelligence module.
- The MISP integration for Security Operations introduces two base system MITRE-ATT&CK technique extraction rules for MISP - MISP galaxies and MISP tags. For more information on auto-extraction rules in MITRE-ATT&CK, see auto-extract technique rules for importing MITRE-ATT&CK information.

3. Click **Save**.

Result
Your modified integration settings are saved and applied.

Configure MISP sighting searches

Configure the ServiceNow AI Platform to do sighting searches for observables in the MISP instance. With this information, you can determine how often threats occur.

Before you begin

- Review the MISP user role and permissions that are required for using the MISP bi-directional features.
- Role required: sn_si.admin, sn_ti.admin

About this task
The Security Operations Integration - Sightings Search workflow executes the sighting searches. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries that are based on the sighting search configurations, and executes the searches that are based on the configured workflow.

The MISP integration for Security Operations provides a base system sighting search profile that enables you to configure automatic sighting searches. With this profile, you can access the related observable sighting information of an organization and also see the external sightings from other organizations.

Procedure

1. Navigate to **All** > **MISP Integration** > **Sighting Search Configuration**.
2. Click **New**.
3. On the form, fill in the fields.

Sightings Search Configuration form

Field	Description
Name	Name for the capability profile.
Is saved search	Search configuration that is saved when you select this option. The saved search configuration queries are example queries. You can substitute them with the parameters

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	for your environment and create additional saved search configurations as required.
Sightings search source	Source for the sightings search. Select the MISP log store as the source.
Active	Option that enables the saved search configuration. Only active search configurations can perform a sightings search.
Observable type	Observable type such as the IP address, hash value, URL, and domain name.
Maximum observable per search	Maximum number of observables that you can view from a search query.
Search	Default search string that is `$(observable)`. However, you define your own search query by specifying the MISP log store supported parameters.

4. Click **Submit**.

Result
You created a MISP sightings search configuration profile.

Configure how an automatic event is created

Configure the ServiceNow AI Platform to automatically create events in MISP.

Before you begin

- Review the MISP user role and permissions that are required for using the MISP bi-directional features.
- Role required: sn_si.admin, sn_ti.admin

Procedure

1. Navigate to **All** > **MISP Integration** > **Automatic Event Creation Profiles**.
2. Click **New**.
3. On the form, fill in the fields.

Name form

Field	Description
Name	Name of the automatic event creation profile.
Description	Brief description about the profile. A more detailed description is shared through the attributes in the next stage of the event's creation.
Order	Order of the profile when triggering conditions are met. The default is 100. Leave this setting at the default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If you create multiple profiles, this value provides a run-time execution priority when two or more profiles share triggering conditions. The profile with the lowest number has the highest priority.
Source	MISP source for the event creation.
Active	Option that indicates if the profile is active or inactive. The option is cleared by default to indicate that the profile is turned off. This profile is not active until you complete all the profile configuration steps and click **Finish**.

4. Click **Continue**.

Configure event trigger conditions

Configure the event trigger conditions in the ServiceNow AI Platform so that you can automatically trigger an event in MISP when the conditions are met.

Before you begin

Role required: sn_sec_misp.write

Procedure

1. On the Trigger Conditions form, fill in the details that can trigger an event.
   You can build a compound logic by providing the trigger conditions that are based on security incident fields or observable fields. You can also create events in MISP if observables don't have a corresponding event in MISP. You can choose to build a compound logic by using a combination of the three trigger conditions - Trigger based on security incident fields, Trigger based on observable fields, and Create MISP event, if an observable doesn't have corresponding events in MISP. If you select multiple triggers, you can join them by using the AND condition. Consider creating a profile with new conditions if you must use the OR condition.

Event Trigger Conditions form

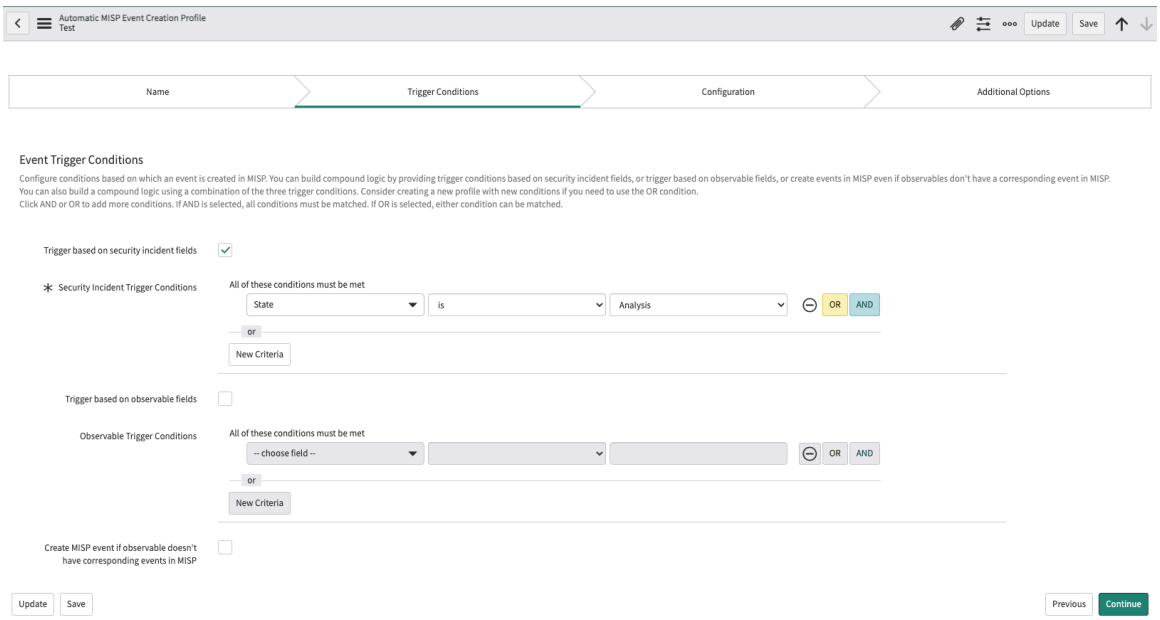
Field	Description
Trigger based on security incident fields	MISP event that you can create if all the security incident trigger conditions are met.
Security Incident Trigger Conditions	Filters in the first row that you can set by using the lists and fields of the conditions builder. To add more conditions, click AND or OR. If AND is selected, all conditions must be matched. If OR is selected, either condition can be matched. To set a second filter condition, click **New Criteria**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Trigger based on observable fields	MISP event that you can create if all the observable trigger conditions are met.
Observable Trigger Conditions	Filters in the first row that you can set by using the lists and fields of the conditions builder. To add more conditions, click AND or OR. If AND is selected, all conditions must be matched. If OR is selected, either condition can be matched. To set a second filter condition, click **New Criteria**.
Create MISP event if observable doesn't have corresponding events in MISP	MISP event that you can create if an observable doesn't have corresponding events in MISP.

Event trigger conditions

The following example shows the event trigger conditions as you set up the MISP event creation profile.



2. Click **Continue**.

Map the MISP event fields

Map the MISP event fields in the ServiceNow AI Platform so that security incident information is available when MISP events are created.

Before you begin
Role required: sn_sec_misp.write

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. On the form, fill in the fields.

Default MISP Event field mapping form

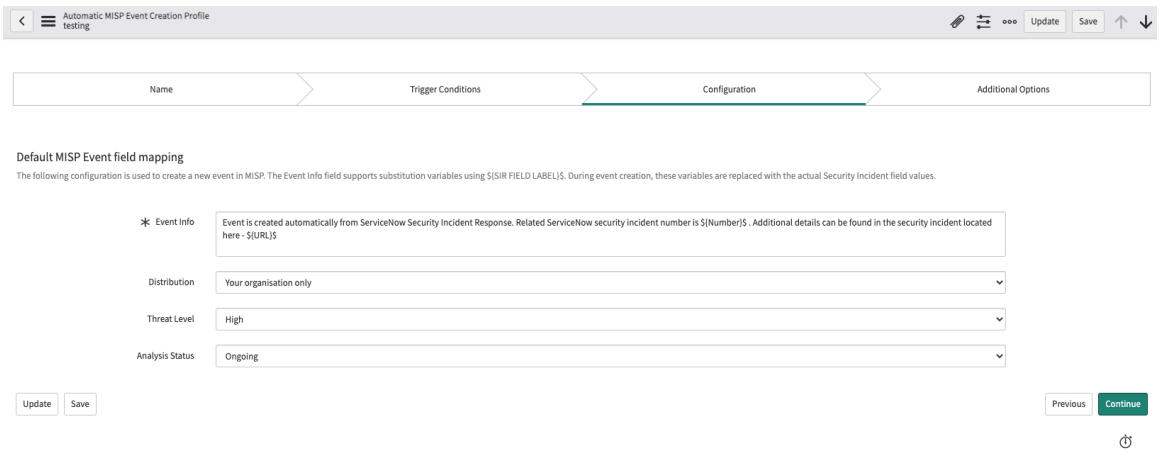
Field	Description
Event Info	Event information that is automatically created from the ServiceNow AI Platform Security Incident Response. The **Event Info** field supports substitution variables by using ${SIR FIELD LABEL}$. During an event creation, these variables are replaced with the actual security incident field values. The ${URL}$ substitution variable is replaced with the URL of the security incident.
Distribution	Option that controls who can view this event after the event is published. This option also controls whether the event is synchronized to other servers. The distribution is inherited by the attributes, and the most restrictive setting wins. The distribution options are as follows: ○ Your organization only: Enables only members of your organization to view this event. The event can be pulled to another instance by one of your organization members where only your organization can have the access to view it. Events with this setting are not synchronized. ○ This community only: Enables users that are part of your MISP community to view the event, including your own organization, organizations on this MISP server, and organizations that run MISP servers that synchronize with this server. Any other organizations that connect to your linked servers are restricted from viewing the event. ○ Connected communities: Enables users that are part of your MISP community to view the event including all organizations on this MISP server, all organizations on the MISP servers that synchronize with this server, and the hosting organizations of servers that connect to any server that is two hops away. Any other organizations that are connected to the linked servers that are two hops away are restricted from viewing the event. ○ All communities: Shares the event with all MISP communities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Threat Level	Field that indicates the risk level of the event. You can categorize incidents into three different threat categories (low, medium, high). This field can also be left as undefined. The following are the options: ○ Low: General mass malware ○ Medium: Advanced Persistent Threats (APT) ○ High: Sophisticated APTs and 0-day attacks
Analysis Status	Current stage of the analysis for the event, with the following possible options: ○ Initial: The analysis is just beginning ○ Ongoing: The analysis is in progress ○ Completed: The analysis is complete

The following example shows the form that you can use to create an event in MISP.

Default MISP Event field mapping



2. Click **Continue**.

Map or associate SIR observables as attributes to MISP events

Map the Security Incident Response observable types to the MISP attribute types because the MISP attribute types and the SIR observables may be different.

Before you begin

Role required: sn_sec_misp.write

About this task

The MISP integration for Security Operations provides a base system mapping that you use when you add SIR observables as attributes to a MISP event.

You can choose to modify the base system mapping to suit your environment. For example, you can map multiple SIR observables to only one MISP attribute type. If any observable types are not mapped, the **other** MISP attribute type is selected by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. On the Additional Options form, map the SIR observable and MISP attribute types.
2. Map the Security Incident Response observable types to the MISP attribute types as described in the following table.

SIR observable and MISP attribute type mapping

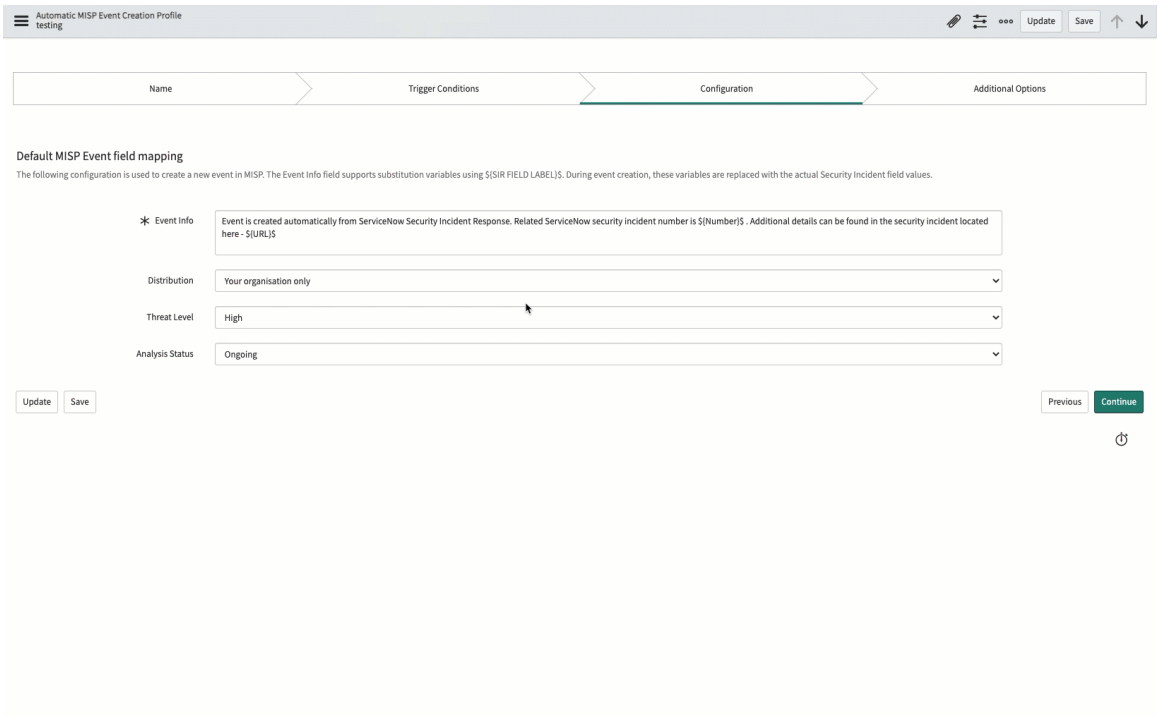
Field	Description
Add all associated observables as attributes	Option that you enable to add available observables in a security incident to a MISP event as attributes. This option enables the mapping in the Observable Type to Attribute Type Mapping section.
Observable Type To Attribute Type Mapping	Option to map the SIR observable types to the MISP attribute types. For example, you can map the CVE Number in SIR to the vulnerability attribute in MISP. You can add a SIR observable type to only one MISP attribute type. The base system provides a mapping of the SIR observable types to the MISP attribute types. If any SIR observable types are not mapped to a MISP attribute type, then the observable is mapped to the **other** attribute type in MISP. To add a new mapping, click **Add Observable Type**, search for the SIR observable type, and then map to the corresponding MISP attribute type. Click the Remove Mapping icon  to remove the SIR and MISP attribute mapping association. **Note:** For more information on MISP attribute types, see the MISP documentation.
Filter observables based on security tags	Option to filter the observables based on the selected security tags. **Security tags**: Add tags to filter the observables. For example, if you are adding a tag called 'Block from sharing' or 'TLP: White' then if one of the observables has any of these tags associated then these observables will not be added as an attribute

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	to the MISP event during the MISP event creation.
Set attribute IDS flag when observable finding is malicious	Option that lets you know that if an observable is marked as malicious in SIR, then the corresponding attribute in MISP has the IDS flag enabled. If the IDS flag is not set, the attribute is considered as contextual information and is not used for automatic intrusion detection.

The following example shows how to navigate to the additional options page. On this page, you can enable the SIR observables and MISP attribute types mapping, add new SIR observable types, such as the IPV6 network and IPV4 network, and map it to the MISP attribute type domain IP address.

Mapping SIR observables and MISP attribute types



Synchronize MITRE-ATT&CK information to MISP events

Synchronize the MITRE-ATT&CK information with MISP attributes for better security incident and threat analysis.

Before you begin

Role required: sn_sec_misp.write

Procedure

On the Additional Options form, review the options to synchronize the MITRE-ATT&CK information with the MISP attributes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Advanced Options form

Field	Description
Sync Security Incident MITRE-ATT&CK™ techniques as local galaxies to MISP event	Option to synchronize the ServiceNow AI Platform SIR security incident MITRE-ATT&CK™ techniques as local galaxies in the MISP event. **Note:** To add local galaxies, the user who has configured the integration should belong to the host organization of the corresponding MISP server.
Sync Security Incident MITRE-ATT&CK™ techniques as global galaxies to MISP event	Option to synchronize the ServiceNow AI Platform SIR security incident MITRE-ATT&CK™ techniques as global galaxies in the MISP event.

Result
You created a profile that enables you to automatically create events in MISP from the ServiceNow AI Platform. You can now view the events in the Associated MISP Events related list.

Add MISP tags to events

Add MISP tags to the created MISP events.

Before you begin
Role required: sn_sec_misp.write

Procedure

1. On the Additional Options form, navigate to **Select MISP tags to add to the event** section on the form view.
2. Review the options to add tags to the created events.

Advanced Options form

Field	Description
Add tags to the created MISP event	Option that allows you to automatically add MISP tags to the events that are created from ServiceNow.
Tags (Local)	The selected tags will be added as local tags to the MISP event.
Tags (Global)	The selected tags will be added as global tags to the MISP event.

3. Click **Save**.

Result
Adding MISP tags helps in classification of the event.

MISP event data

You can review the MISP event data so that you can see detailed information about the MISP events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MISP event data in the list view

Access the list view from **MISP** > **MISP Event Data**.

Use the list view to get a quick overview of the MISP event data.

MISP Events list view

Field	Description
Event ID	Event ID that is assigned by MISP when the event was first created or imported into the MISP server.
Info	Short description of the event.
Analysis	Current stage of the analysis for the event with the following possible options: • Initial: The analysis is just beginning • Ongoing: The analysis is in progress • Completed: The analysis is complete
Threat Level	Risk level of the event. Incidents can be categorized into three different threat categories (low, medium, high). This field can be left as undefined. The following are the options: • Low: General mass malware • Medium: Advanced Persistent Threats (APT) • High: Sophisticated APTs and 0-day attacks
MISP Tags	Tags that are associated with the MISP event.
MISP Galaxies	Galaxies that are associated with the MISP event.
Owner Org	Organization that owns the event on the MISP instance. This field is visible only to administrators.
Creator Org	Organization that created the event on the MISP instance.
Distribution	Distribution of the individual attribute. An attribute can have a different distribution level than the event.
MISP Event Hyperlink	Link to the MISP event that is stored on the MISP server.
MISP Source	MISP source where the event is created.

MISP event data in the form view

Use the form view to get detailed information about the MISP events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MISP Event form view

Field	Description
Event ID	Event ID that is assigned by MISP when the event was first created or imported into the MISP server.
UUID	ID that uniquely identifies events and attributes.
Creator Org	Organization that created the event on the MISP instance.
Owner Org	Organization that owns the event on the MISP instance. This field is visible only to administrators.
Creator User	User who created the event in MISP.
Last Change	Date that the event was last modified.
MISP Source	MISP source where the event is created.
Created date (in MISP)	Date that the event was created or first imported in the MISP server.
Threat Level	Risk level of the event. Incidents can be categorized into three different threat categories (low, medium, high). This field can be left as undefined. The following are the options: • Low: General mass malware • Medium: Advanced Persistent Threats (APT) • High: Sophisticated APTs and 0-day attacks
Analysis	Current stage of the analysis for the event with the following possible options: • Initial: The analysis is just beginning • Ongoing: The analysis is in progress • Completed: The analysis is complete
Distribution	Distribution of the individual attribute. An attribute can have a different distribution level than the event.
Published	Status of whether the event has been published or not. Publishing allows the attributes of the event to be used for all eligible exports and notifies users that have subscribed to the event alerts.
MISP Event Hyperlink	Link to the MISP event that is stored on the MISP server.
Info	Short description of the event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MISP Event form view (continued)

Field	Description
Tags (Local)	Tags that are available on the host organization's MISP instance to enable tagging for synchronization and export filtering. MISP events are not modified when you use local tags. Local tags are always stripped before being synchronized with other MISP instances and sharing communities.
Tags (Global)	Tags that are available globally to be shared and synchronized with other MISP instances and sharing communities. When you add global tags to MISP instances, you can modify events.
Galaxies (Local)	Galaxies that are available on the host organization's MISP instance for synchronization and export filtering. MISP events are not modified when you use local galaxies. These local galaxies are always stripped before being synchronized with other MISP instances and sharing communities.
Galaxies (Global)	Galaxies that are available globally to be shared and synchronized with other MISP instances and sharing communities. When you add global galaxies, MISP you can modify events.

Associated MISP events

You can use the associated MISP events list view to view the events that have been created manually or automatically in the context of a security incident.

Associated MISP Events

Field	Description
Security Incident	SIR security incident. Click the security incident to view the security incident.
MISP Event	MISP event ID. Click the MISP event to view the MISP event in the ServiceNow AI Platform.
MISP Source	MISP source where the event is created. Click the MISP source to view the source.
Event Creation Mode	Status of whether the event was created manually or automatically with the event creation profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Associated MISP Events (continued)

Field	Description
	Click the MISP event to view the associated MISP event.
Automatic Event Creation Profile	Event creation profile that is used to create the automatic event. Click the profile to view the Automatic MISP Event Creation Profile.

MISP user information

You can use the MISP user information page to view all the associated users for the ServiceNow AI Platform MISP integration for Security Operations.

MISP User Information

Field	Description
Source	User account's MISP source.
User ID	User ID that is assigned by the MISP server when a user account is created.
User Email	Email address of a user. Only organization administrators can see the email addresses of their own organization's users.
Organisation	Organization that a user belongs to.
Role Name	Role name that defines the user privileges that are attributed to a user. For more information about roles in MISP, see the MISP documentation.
Role ID	User role ID in MISP. For example, Perm Admin, Perm Audit, or Perm Tagger, and so on.
Permission	Permissions that a user has. The permissions that are available in MISP are as follows: • Read Only • Manage Own Events • Manage Organization Events • Manage Publish Organisation Events
Sighting Permission	Permission that enables a user to perform sighting searches.
Tagger Permission	Permission that enables a user to do tagging.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Domain separation and MISP

Domain separation is supported in MISP. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with MISP

Follow these steps to achieve domain separation:

- Create a user with the required roles in your domain.
- Perform the MISP integration for Security Operations procedures in your domain.

Troubleshooting MISP integration

This section covers important troubleshooting tips that can help you resolve common issues you can encounter when setting up or running MISP integration.

SSL issues

When connecting through the MISP integration, ensure that you've installed a valid CA certificate on the MISP server, which hasn't expired. You can import RSA or your own certificates into the platform and ensure that the common name of the certificate matches the host name. For more information, see Install and configure the MISP integration for Security Operations and MISP user roles and permissions.

Using MISP to investigate and analyze threats

You can use the MISP data across the ServiceNow AI Platform Threat Intelligence module and the ServiceNow AI Platform SIR module to investigate and analyze threats to your organization.

Sighting searches in MISP

You can perform sighting searches on observables in the MISP instance to determine how often certain types of attacks, such as phishing attacks or communications with a malicious IP or URL, occur in your network. Each occurrence is considered a sighting.

Sightings in MISP

Sightings denote that an indicator, object, or attribute, was seen and its validity is confirmed. Sightings in MISP is a system that allows you to respond to attributes on an event. It is designed to provide an easy method for your users to confirm that they have seen a given attribute, giving it more credibility. You can sight an attribute multiple times.

Note: Observables are known as attributes in MISP.

Some attributes are considered as false positives, which means that they are not valid sightings. Other attributes are valid for only a certain duration, such as a phishing campaign that runs for only one week. You can assign an expiration date to the attributes that are valid for a certain duration, but each organization can assign only one valid expiration date to an attribute.

Sightings that are created in MISP by users of organizations that are marked as local in the corresponding MISP server are known as internal sightings. Sightings that are created in MISP by users of organizations that are marked as remote in the corresponding MISP server are known as external sightings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sighting searches in SIR

The Security Operations Integration - Sightings Search workflow executes the sightings search. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries that are based on the sighting search configurations, and executes the searches that are based on the configured workflow.

Sighting searches helps analysts to determine the prevalence of a threat over time. You can select individual or multiple observables and the date range for your search from a security incident. Results are included in the Security Incident Sightings, Sightings Search Results, and Sightings Search Details related lists.

As you start to analyze an incident, you can set up your ServiceNow AI Platform to automatically perform a sightings search or manually perform an observable sightings search to identify other users in your organization who are impacted by the same phishing attack.

Enable automatic sighting searches in MISP

Enable the sighting search in MISP to run automatically so that the Security Operations Integration - Sightings Search workflow is triggered whenever new observables are associated with a security incident.

Before you begin

Verify that the Sightings Search Configuration profile for MISP is active.

Role required: sn_si.analyst

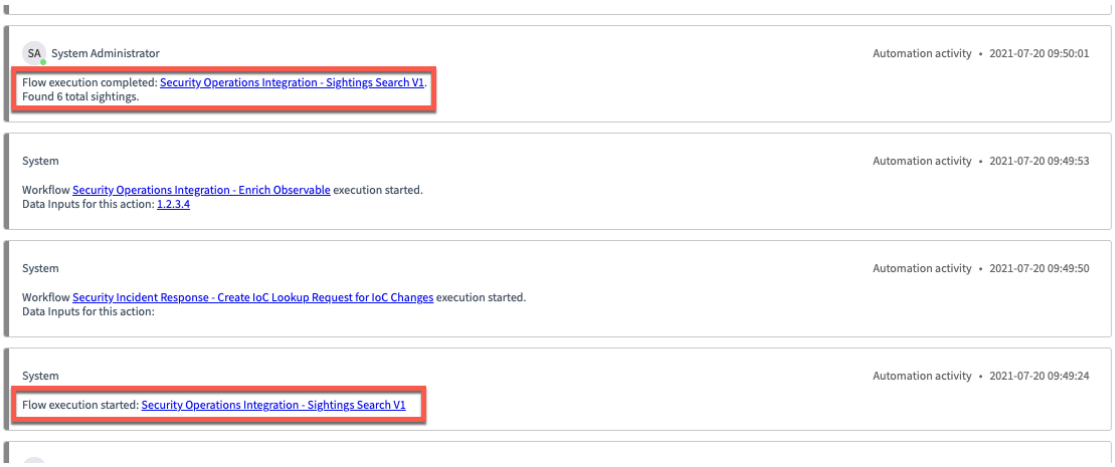
About this task

If you enable the sighting search capability to run automatically in the MISP integration configuration, the sighting search in MISP triggers when new observables are associated with a security incident. By default, the **Run Sighting Search automatically when new observables are associated with the security incident** option is enabled.

Procedure

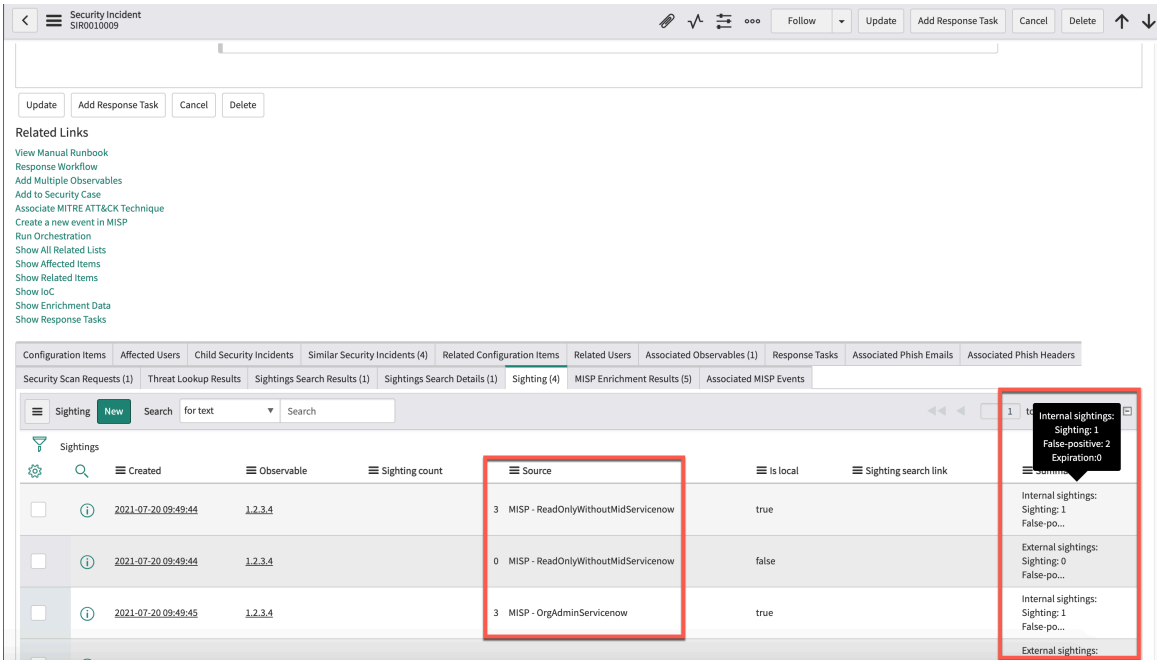
1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to view in the MISP sightings search data.
3. Review the work notes after new observables have been associated with the security incident. A work note is posted when the Security Operations Integration - Sightings Search workflow has triggered.

   The following example shows the work notes section.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. View the aggregated information of observables that are seen across all the events (global) and categorized by their internal or external sightings after the workflow execution has completed.
   View the information in the Sightings, Sightings Search Results and Sightings Search Details related lists.The following example shows the sightings search record that was created in the Sightings related list.



Sightings Search record

Field	Description
Created	Date and time that the sightings search record was created.
Observable	Observable that is searched for by the query.
Sighting count	Count of internal and external sightings.
Source	Source of the observable. If the observable is from a MISP organization, the record is preceded with the words `MISP`.
Is local	Status of whether the sighting was reported by an internal user.
Sighting search link	Sighting search link in the MISP instance.
Summary	Type of sightings that are associated with the record. The three types of Sightings are Sighting, False-positive, and Expiration. The Summary column appears only when the MISP integration for Security Operations is installed. If sources other than MISP appears, the Summary column entry is empty for that record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Perform a manual sighting search in MISP

Select individual or multiple observables and perform a manual sighting search in the ServiceNow AI Platform MISP integration for Security Operations application to determine the prevalence of a threat over time.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Role required: sn_si.analyst

Procedure

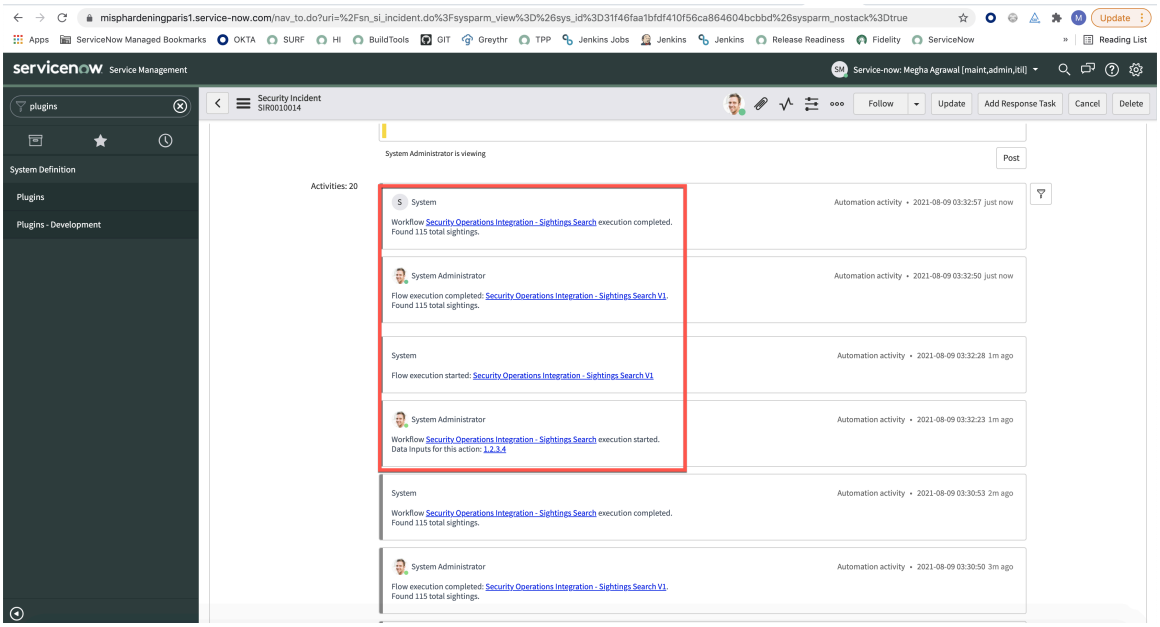
1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to run the MISP sightings search for.
3. Click **Show All Related Lists** and the **Associated Observables** tab.
4. Select the observable and then from the Actions menu, click **Run Sightings Search**.
   You can select multiple observables for a sighting search.
   The Run Sightings Search dialog box opens.
5. Specify the date range to search for the sightings search data.

Run Sightings Search dialog box

Field	Description
Last	Number of hours or days prior to the creation of the incident to search. The default is 7 days. The limit is 99 hours or days.
between	Range of dates to search. Default dates are as follows: ○ The date and time that the incident was created. ○ The date and time that is seven days prior to the opening of the incident.

6. Click **Search**.
   The following example shows the manual sighting search results in the work notes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Result

A Sightings Search record is created. After the workflow execution has completed, you can view the aggregated information of observables that are seen across all the events (global) and categorized by their internal or external sightings. Aggregate and associated sightings data are displayed in the security incident under the Sightings, Sightings Search Results, and Sightings Search Details related lists.

Report sightings to MISP

Report threat data sightings so that you can react to false positives in your data and increase your awareness when a true positive threat occurs. You can also add an expiration date for a particular observable or attribute.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Role required: sn_si.analyst

About this task

The MISP integration for Security Operations enables you to report sightings to MISP globally across all events. To report a sighting to a specific event, you must use the MISP instance and report the sighting locally.

To report a sighting to MISP, the observable or the attribute must be available in the MISP instance.

Procedure

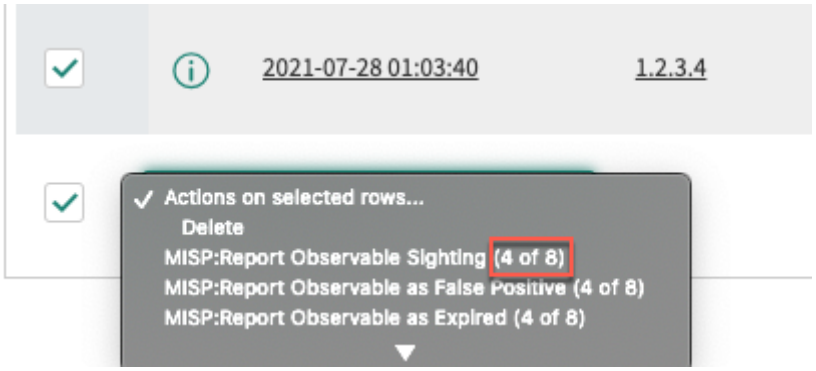
1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to report the sightings to MISP for.
3. Click **Show All Related Lists** and the Sightings related list.
4. Select the observable and from the Actions menu, select one of the following options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
MISP: Report Observable Sighting	Report the observable as sighted to MISP. If the observable is associated with multiple events, it is updated in all the events.
MISP: Report Observable as False Positive	Report the observable as a false positive to MISP.
MISP: Report Observable as Expired	Report the observable as expired to MISP.

If you select observables that are not specific to a MISP source, the Actions menu shows the count of relevant MISP sources. The following example shows four out of eight observables as relevant to MISP.The following example shows the actions menu and the relevant observables for submission.

Actions menu that shows the relevant observables for submission



5. **Optional:** If you selected the **MISP: Report Observable Sighting** option, you should fill in the fields of the Report Observable Sighting to MISP dialog box.

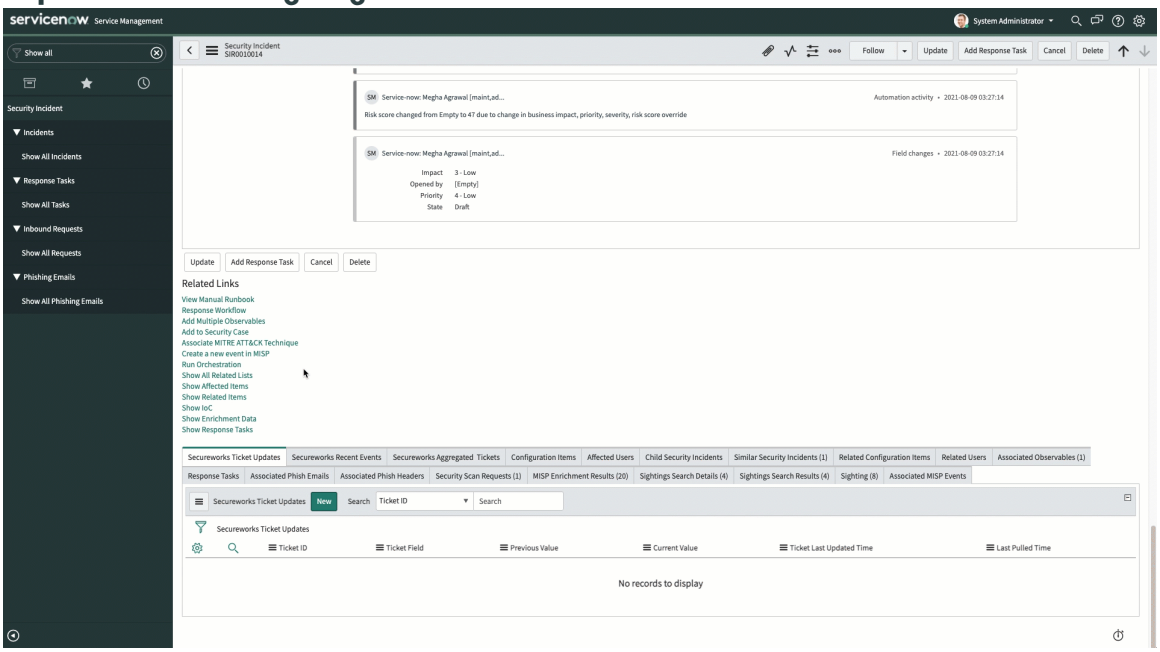
Report Observable Sighting to MISP dialog box

Field	Description
Source	Source field that corresponds to the MISP source of the sighting.
Date	Date field that corresponds to the date that the observable is sighted. If the date is empty, the current date and time is populated in MISP.

The following example shows how to navigate to the Sightings related list in the security incident. From that list, you can select an observable and report the observable sighting to MISP. The success message shows that the sighting was successfully submitted to MISP.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reports observable sighting to MISP



a. Click **Report Sighting**.

6. **Optional:** If you selected the **MISP: Report Observable as False Positive** option, you should fill in the fields of the Report Observable as False Positive to MISP dialog box.

Report Observable as False Positive to MISP dialog box

Field	Description
Source (optional)	Source field that corresponds to the MISP source. Use this field to declare the observable as a false positive.
Date	Date field that corresponds to the date that the observable was found to be a false positive. If the date is empty, the current date and time is populated in MISP.

a. Click **Report False Positive**.

7. **Optional:** If you selected the **MISP: Report Observable as Expired** option, you should fill in the fields of the Report Observable Expiration to MISP dialog box.

Report Observable Expiration to MISP dialog box

Field	Description
Source	Source field that corresponds to the MISP source. Use this field to set an observable as expired.
Date	Date field that corresponds to the date that the observable has expired on. If the date is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	empty, the current date and time is populated in MISP.

a. Click **Report Expiry**.

Result
The sightings successfully update to the MISP server.

Observable enrichment in MISP

By enriching observables with additional information from various MISP sources during incident response investigations, you can contain identified threats.

Enable automatic observable enrichment in MISP

Enable automatic observable enrichment in the ServiceNow AI Platform MISP when new observables are associated with the security incident.

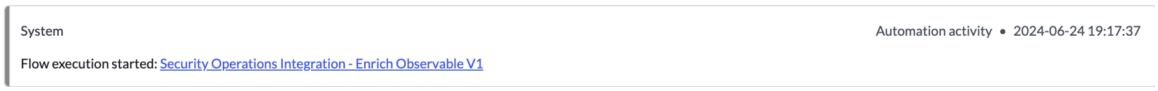
Before you begin

- Enable the Security Incident Response system property for the **Enables or Disables the scheduled job, Lookup Security Incident Observables** option to trigger the observable enrichment capability in SIR.
- Role required: sn_si.analyst

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to enrich the observable data in MISP for.
3. Review the work notes after new observables have been associated with the security incident.

   The following example shows that a work note posts when the Security Operations Integration - Enrich Observable flow triggers.

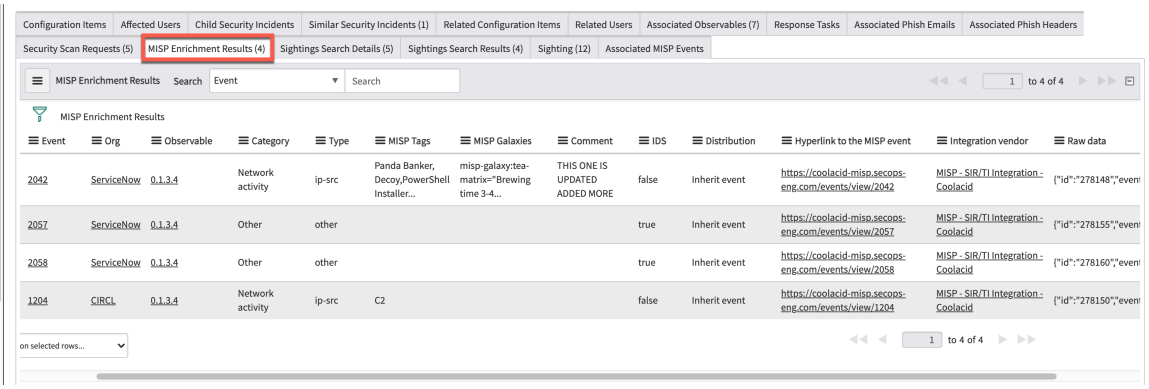
4. In the MISP Enrichment Results related list of the security incident, view the enrichment results after the flow execution completes.

   Note: You must configure that the MISP Enrichment Results related list appears in the security incident related lists. For more information, see related list configuration.

   The following example shows the enrichment results in the MISP.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The following table shows the MISP enrichment results.

MISP Enrichment Results

Field	Description
Event	ID of the event. Click open to view the record in the ServiceNow AI Platform instance.
Org	Organization that has originally created the event.
Observable	Observable that is associated with the event.
Category	Category of the attribute. View the list of categories in the MISP documentation.
Type	Type of the attribute. View the list of types in the MISP documentation.
MISP Tags	List of tags that are associated with the MISP attribute.
MISP Galaxies	List of galaxies that are associated with the MISP attribute.
Comment	Contextual comment to further describe the attribute. These comments are not used for correlation and are purely informative.
IDS	Indicator of compromise, which allows it to be included in all the eligible exports.
Distribution	Distribution of the attribute after it is published. An attribute can have a different distribution level than the event. In either case, the lowest distribution level is used.
Hyperlink to the MISP event	Link to the MISP event, which is stored on the MISP server.
Integration vendor	Integration vendor who provides the data for enrichment.
Raw data	Raw data that is associated with the MISP attribute.

Perform a manual observable enrichment in MISP

Select individual or multiple observables and perform a manual observable enrichment so that you can enrich observables with additional information from various MISP sources.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

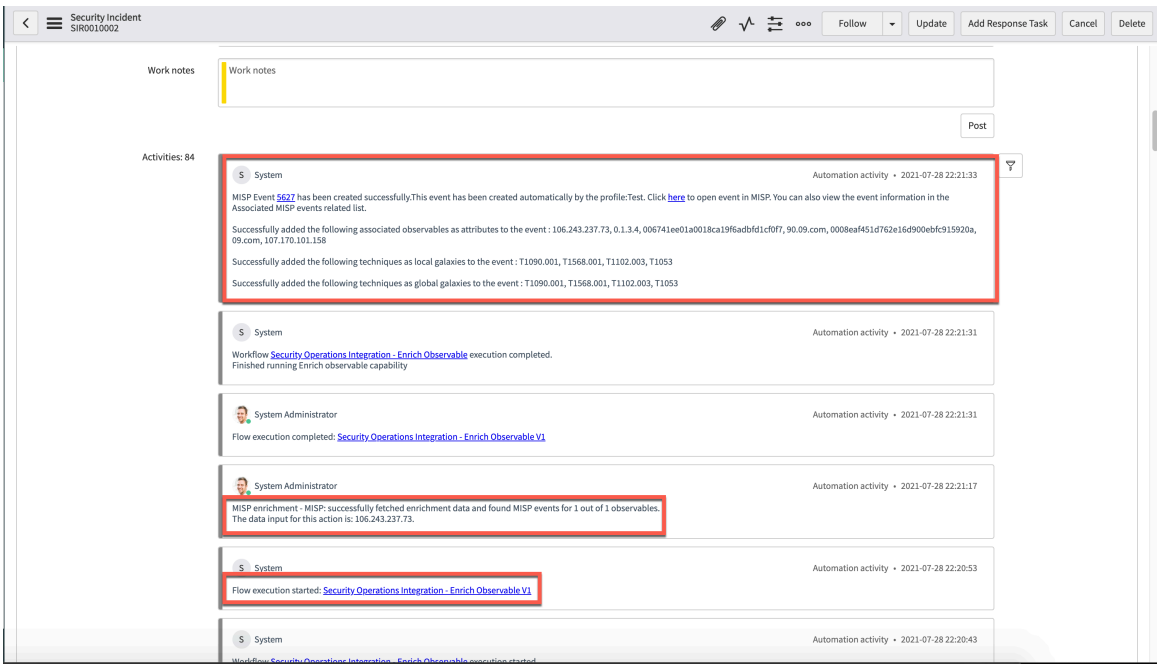
- Review the MISP user role and permissions for using the MISP bi-directional features.
- Role required: sn_si.analyst

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to perform the enrichment for.
3. Click **Show All Related Lists** and the **Associated Observables** tab.
4. Select the observable and from the Actions menu, click **Run Observable Enrichment**.
   You can select multiple observables for a sighting search.
   The Run Observable Enrichment dialog box appears.
5. Select a MISP source and in the Selected column, select an implementation to enrich the selected observables.
6. Click **Submit**.
   A work note shows that the Security Operations Integration - Enrich Observable workflow has triggered. The associated implementation workflows execute to perform the enrichment. You can view the work notes in the security incident to view the status.

   The following example shows how to view the work notes for a manual observable enrichment.

Work notes for manual observable enrichment



The enrichment message lists the created event. You can view the event in the ServiceNow AI Platform or in the MISP instance and view the details of the record in the MISP Enrichment Results tab.

Add or remove tags to MISP attributes

Add or remove tags in MISP to classify events or attributes. You can use tagging globally to enable your classification or use tags locally when you don't want MISP events to be modified during your classification.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Verify that the attribute that you are editing belongs to the same organization as the MISP user.
- Note that the tags and galaxies that are available to you are based on the MISP source and its distribution permissions.
- Role required: sn_sec_misp.write

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables, attributes, or events that you want to add the tags for.
3. Click **Show All Related Lists** and the MISP Enrichment Results related list.
4. Click the preview icon ⓘ next to a record, and then click **Open Record**.
   The following example shows how to review the **MISP Enrichment Results** and how to open a MISP enrichment record.

   MISP Enrichment Result record

5. Review the MISP Enrichment Result record.

MISP Enrichment Result

Field	Description
Observable	
Event	Event ID that is assigned by the MISP server when the event was first created or imported into MISP. Preview the event or click the record to view the event data in the MISP Event Data page.
Org	Organization that created the MISP attribute.
Category	Category of the attribute that you add to the specific event in MISP. You can select an option such as an internal reference, network activity, financial fraud, and so on.
Type	Type of MISP attribute.
Integration vendor	Integration vendor that provides the data for the observable enrichment.
Created date (in MISP)	Date that the event was first created or imported into MISP.
IDS	Status of whether an observable is marked as malicious in SIR. The corresponding attribute in MISP is also marked as true.
Distribution	Distribution option controls, such as who can view this event after it is published. This option also controls whether the event is synchronized to other servers. The

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	distribution is inherited by the attributes, and the most restrictive setting wins. The distribution options are as follows: ○ Your organization only: Enables only members of your organization to view this event. The event can be pulled to another instance by one of your organization members where only your organization has the access to view it. Events with this setting are not synchronized. ○ This community only: Enables users that are part of your MISP community to view the event, including your own organization, organizations on this MISP server, and organizations that run MISP servers that synchronize with this server. Any other organizations that are connected to these linked servers are restricted from viewing the event. ○ Connected communities: Enables users that are part of your MISP community to view the event, including all organizations on this MISP server, all organizations on MISP servers that synchronize with this server, and the hosting organizations of servers that connect to any server that is two hops away). Any other organizations that are connected to the linked servers that are two hops away are restricted from viewing the event. ○ All communities: Shares the event with all MISP communities, which allows the event to be freely available.
Hyperlink to the MISP event	Link to the MISP event that is stored on the MISP server.
Raw data	Raw details for the observable enrichment data record.
Comment	Comments that you add for the attributes. These comments are for informational purposes only and not used for correlation.
Tags (Local)	Tags that are available on the host organization's MISP instance to enable tagging for synchronization and export filtering. MISP events are not modified when you use local tags. These tags are always stripped before being synchronized with other MISP instances and sharing communities.
Tags (Global)	Tags that are available globally to be shared and synchronized with other MISP instances

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	and sharing communities. When you add global tags to MISP instances, you modify events.
Galaxies (Local)	Galaxies that are available on the host organization's MISP instance for synchronization and export filtering. MISP events are not modified when you use local galaxies. These galaxies are always stripped before being synchronized with other MISP instances and sharing communities.
Galaxies (Global)	Galaxies that are available globally to be shared and synchronized with other MISP instances and sharing communities. When you add global galaxies, MISP events are modified.

6. To edit either a local or global tag, click the edit icon in one of the following options:

   - **Tags (Local)**
   - **Tags (Global)**

7. In The MISP Attribute Tags dialog box, enter the name of the tag to search and to add it.
8. Click **Update Tags to MISP Attribute**.

   The following example shows that by clicking the edit icon for the local tags, you can search and add the C3, Adware, C2, and Botnet 3101 tags, and update the MISP server with the tags. The confirmation message shows that all tags have been updated in MISP.

   The tags update successfully in the MISP server.
9. To view the changes in the record, click **Reload Form** in the success message.

Add or remove galaxies to a MISP event or attribute

Add or remove galaxies in MISP so that you can classify these objects as a cluster in MISP and attach them to MISP events or attributes.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- To add local galaxies, the user who has configured the integration should belong to the host organization of the corresponding MISP server.
- Note that the tags and galaxies that are available to you are based on the MISP source and its distribution permissions.
- Role required: sn_sec_misp.write

Procedure

1. Click the edit icon in one of the following options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Galaxies (Local)**
- **Galaxies (Global)**

2. In The MISP Event Galaxies dialog box, fill in the details.

MISP Event Galaxies dialog box

Field	Description
Event ID	Event ID that is assigned by the MISP server when the event was first created or imported into MISP.
Namespace	Namespace where the galaxy is stored. You can use namespaces to group similar galaxies.
Galaxies	Galaxy where you store the cluster information.
Clusters	Information about the clusters in the galaxy.

3. Click **Update Galaxies to MISP Attribute**.
   The following example shows that by clicking the edit icon for the local galaxies, you can select the deprecated namespace, select the Enterprise Attack - Attack Pattern galaxy, and add the cluster information. After the galaxy information is updated, you can view the success message.

4. To view the changes in the record, click **Reload Form** in the success message.

Result
The galaxy information is successfully updated in the MISP server.

Add comments to MISP attribute

Add comments for the MISP attributes. The comments that you add are for informational purposes only and are not used for correlation of MISP data.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Verify that the attribute that you are editing belongs to the same organization as the MISP user.
- Role required: sn_sec_misp.write

Procedure

1. Click the edit icon on the Comment field.
2. Enter your comment in the Attribute Comment field.
3. Click **Update Comment to MISP Attribute**.
   The following example shows that by clicking the edit icon next to the comment field, you can add a comment and then update the MISP attribute. After the comment is updated, you can view the success message.

4. To view the changes in the record, click **Reload Form** in the success message.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The comment is successfully updated in the MISP server.

Managing events in MISP

You can create events in MISP automatically or manually from the ServiceNow AI Platform. You can also edit the event data in MISP from the ServiceNow AI Platform.

Verifying automatically created events in MISP

You can verify the automatically created events after you configure the event creation profile in your ServiceNow AI Platform instance.

Automatic event creation profile

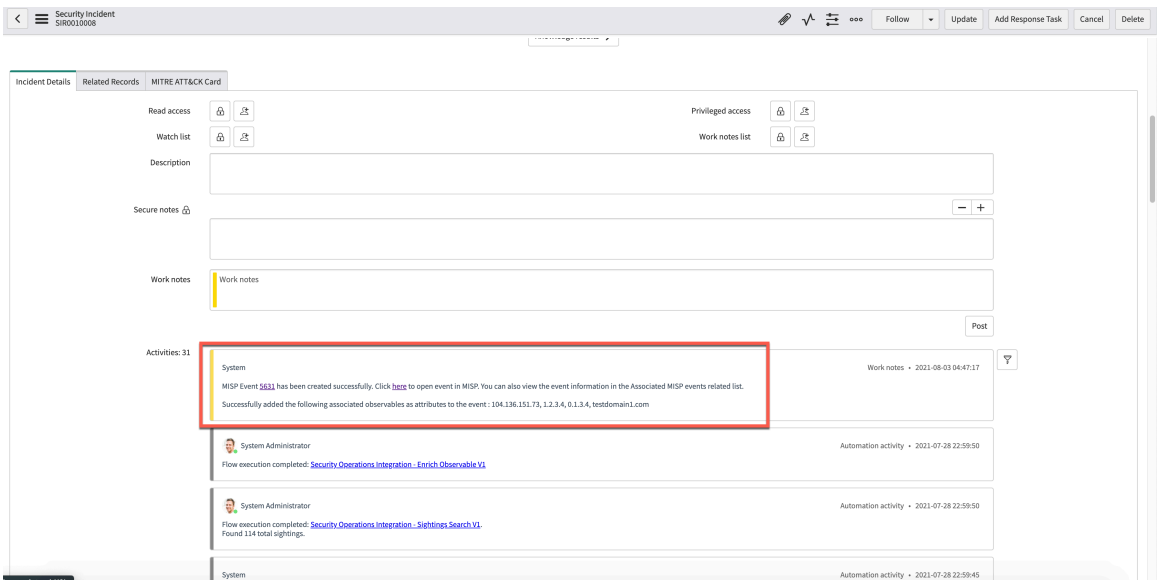
Configuring the automatic event creation profile is done by the sn_si.admin or the sn_ti.admin user roles in the **MISP Integration** > **Automatic Event Creation Profiles** module.

Viewing the MISP event data

You can view the created events in the following ways:

- View the work notes for the created events. You can view the event details in the ServiceNow AI Platform instance and also as it appears in the MISP server as shown in the following example.

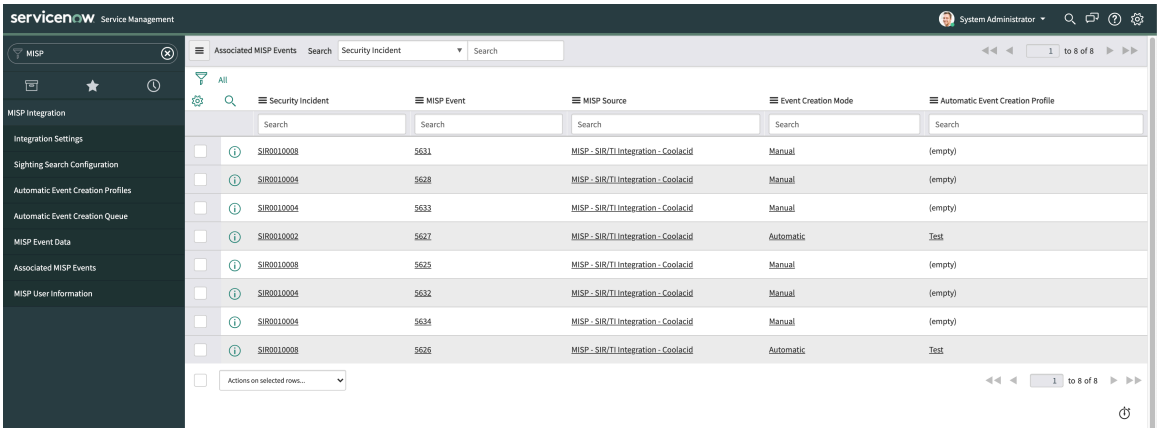
Work notes for created events



- Click the Associated MISP Events related list. Here, you can view the event in relation to the security incident and the MISP resources as shown in the following example.

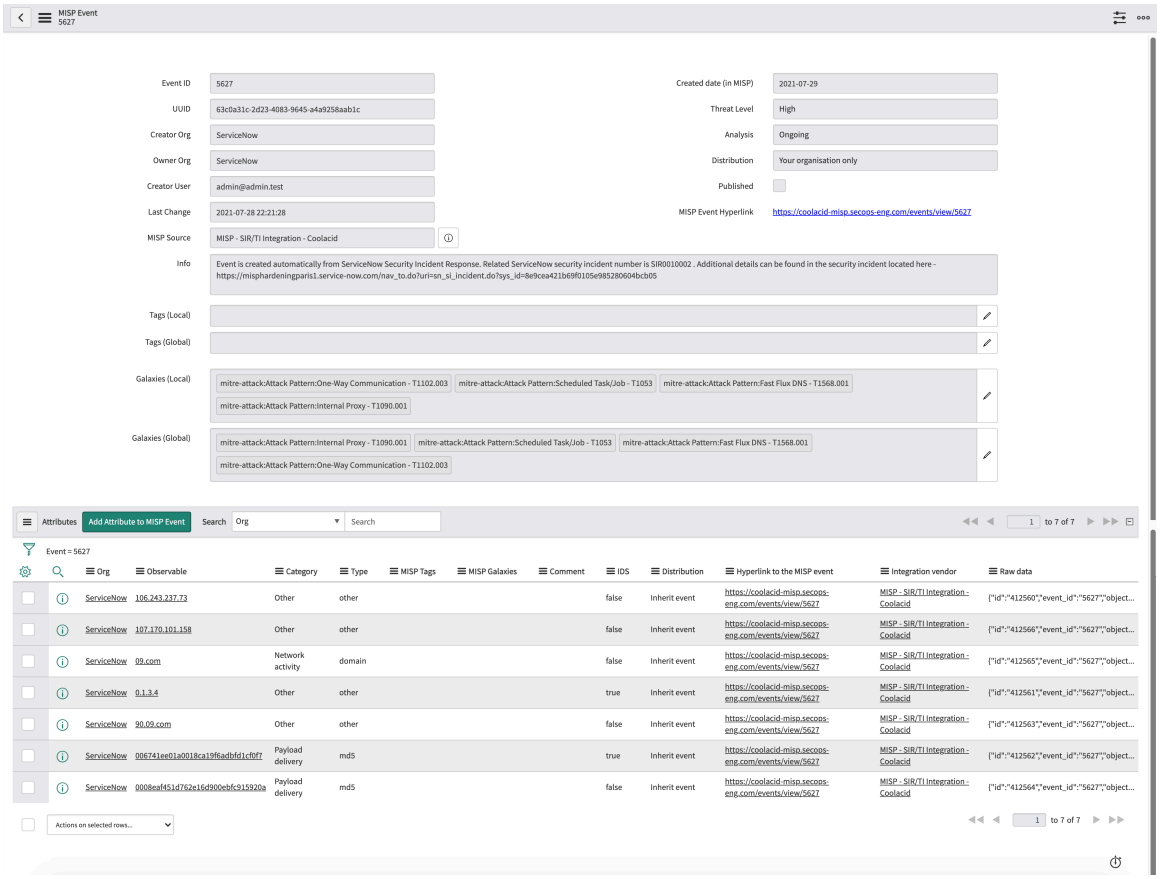
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

List of associated events



- View the MISP event data in the form view to review the detailed information about the MISP events as shown in the following example.

Event data in the form view



Manually create an event in MISP

Manually create events in MISP from the ServiceNow AI Platform to capture contextually related information represented as attributes and objects.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Role required: sn_sec_misp.write

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the observables that you want to create an event for.
3. Click **Create a new event in MISP**.
4. In the Create a new event in MISP dialog box, fill in the details.

Create an event in MISP dialog box

Field	Description
Date	Creation date of the event in MISP.
Event Info	Event information that is automatically created from the ServiceNow AI Platform Security Incident Response.
Threat Level	Risk level of the event. You can categorize the incidents into three different threat categories (low, medium, high). This field can also be left as undefined. The following are the options: ○ Low: General mass malware ○ Medium: Advanced Persistent Threats (APT) ○ High: Sophisticated APTs and 0-day attacks
Source	MISP source for the event creation.
Distribution	Option that controls who can view this event after the event is published. This option also controls whether the event is synchronized to other servers. The distribution is inherited by the attributes. The most restrictive setting wins. The distribution options are as follows: ○ Your organization only: Enables only the members of your organization to view this event. The event can be pulled to another instance by one of your organization members where only your organization has the access to view it. Events

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field		Description
		with this setting are not synchronized. ○ This community only: Enables users that are part of your MISP community to view the event, including your own organization, organizations on this MISP server, and organizations that run MISP servers that synchronize with this server. Any other organizations that are connected to linked servers are restricted from viewing the event. ○ Connected communities: Enables users that are part of your MISP community to view the event, including all organizations on this MISP server, all organizations on MISP servers that synchronize with this server, and the hosting organizations of servers that connect to any server that is two hops away. Any other organizations that are connected to the linked servers that are two hops away from this server are restricted from viewing the event. ○ All communities: Shares the event with all MISP communities.
Analysis		Current stage of the analysis for the event with the following possible options: ○ Initial: The analysis is just beginning ○ Ongoing: The analysis is in progress ○ Completed: The analysis is complete
Advanced Options	Add SIR associated observables as attributes to MISP Event	Option to add available observables in a security incident to a MISP event as attributes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

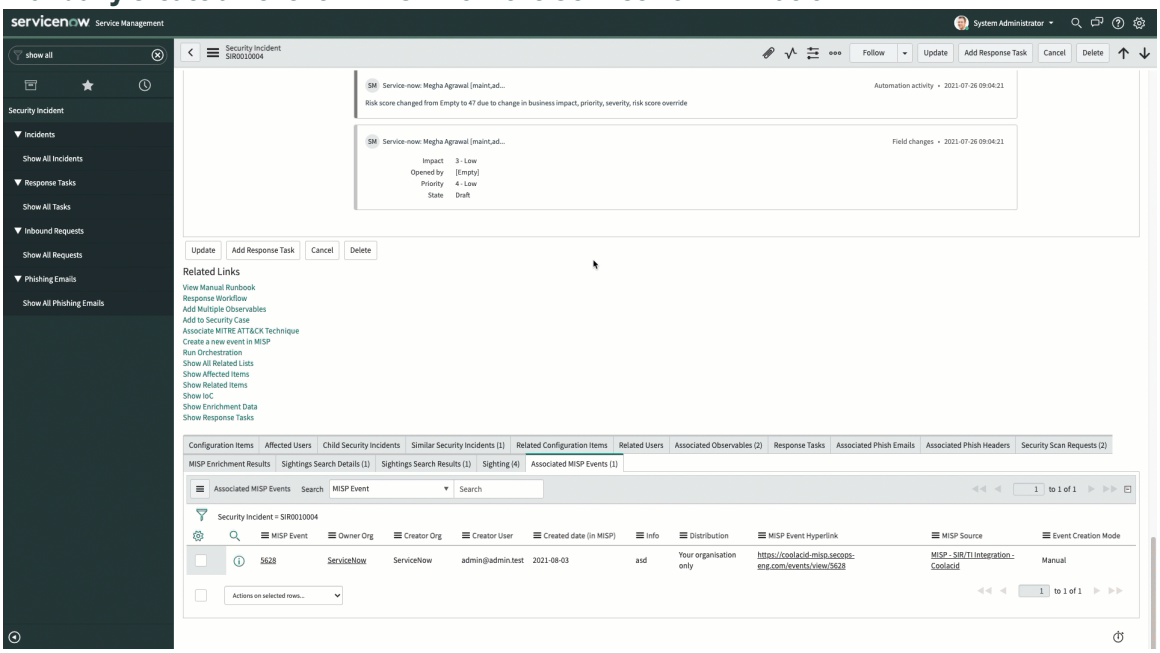
Field		Description
		This option enables the **Set attribute IDS flag when observable finding is malicious** option.
	Set attribute IDS flag when observable finding is malicious	Observable that is marked as malicious in SIR. The corresponding attribute in MISP is also marked as true.
	Filter observables based on security tags	Option to filter the observables based on the selected security tags. This option provides the capability to distinguish and manage the MISP events in threat intelligence. **Security tags**: Add tags to filter the observables. For example, if you are adding a tag called 'Block from sharing' or 'TLP: White' then if one of the observables has any of these tags associated then these observables will not be added as an attribute to the MISP event during the MISP event creation.
	Synch Security Incident MITRE ATT&CK techniques as local galaxies to MISP event	Option to synchronize the ServiceNow AI Platform SIR security incident MITRE-ATT&CK™ techniques as local galaxies in the MISP event.
	Sync Security Incident MITRE ATT&CK techniques as global galaxies to MISP event	Option to synchronize the ServiceNow AI Platform SIR security incident MITRE-ATT&CK™ techniques as global galaxies in the MISP event.
	Add tags to the MISP event	Option that allows you to add MISP tags to the events that are created from ServiceNow. This option displays the following options: ○ **Local (Tags):**The selected tags will be added as local tags to the MISP event. ○ **Global (Tags):**The selected tags will be added as global tags to the MISP event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Create New MISP Event**.

   The following example shows that by creating an event in MISP, you can view the results in the security incident. You also can view the work notes, the event in the ServiceNow AI Platform instance, and the event in the MISP server as shown in the following example.

   Manually create an event in MISP from the ServiceNow AI Platform



   You can view the results in the following ways:

   - A success message appears at the top of the security incident page. You can view the event details in the ServiceNow AI Platform instance and also as it appears in the MISP server.
   - In the work notes, you can view the success message with more details. You can also view the event details in the ServiceNow AI Platform instance and also as it appears in the MISP server.
   - In the Associated MISP Events related list, you can view the event in relation to the security incident and the MISP resources.

Add attributes to a MISP event

Add attributes to an event, such as the type, category, and other contextual information about the event.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Verify that the event that you are adding or updating the attribute belongs to the same organization as the MISP user.
- Role required: sn_sec_misp.write

Procedure

1. Navigate to **All** > **MISP** > **Associated MISP Events**.
   You can also navigate to the Associated MISP Event related list in any security incident.
2. Click the MISP event that you want to add an attribute for.
3. Click **Add Attribute to MISP Event**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the Add Attribute to Event dialog box, fill in the details.

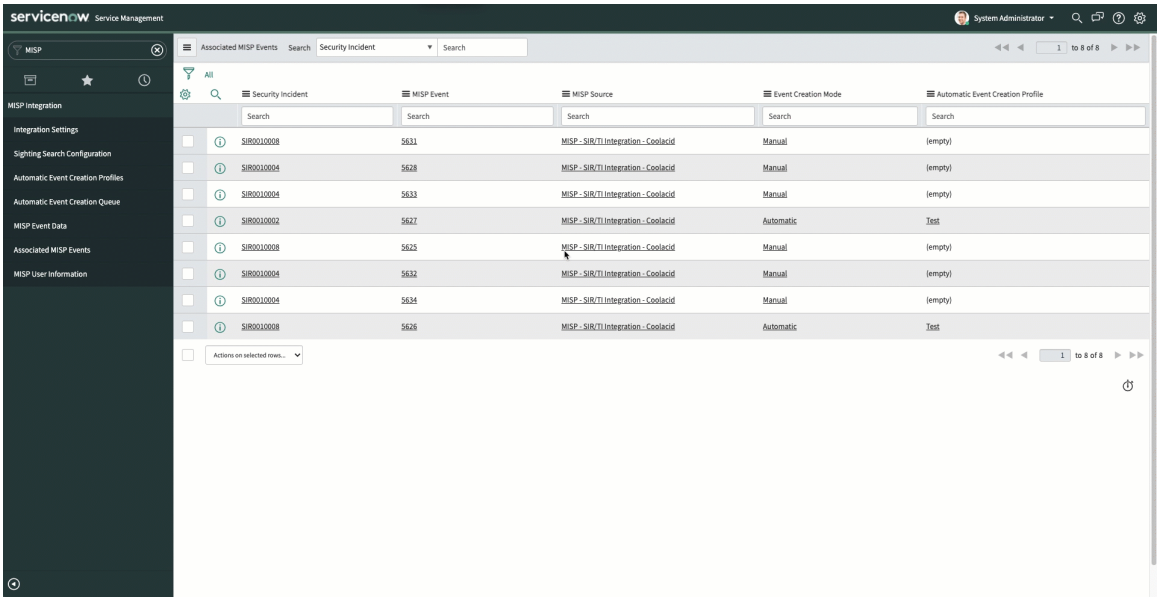
Add Attribute to Event dialog box

Field	Description
Value	Actual value of the attribute. Enter data about the value that is based on what is valid for the chosen attribute type. For example, for an attribute of type ip-src (source IP address), 11.11.11.11 is a valid value. **Note:** You can only select attributes or observables that share context with the event. The observables can't already have an attribute in MISP.
Category	Category of the attribute. The category describes the aspect of the malware for this attribute. An example would be the persistence mechanisms of the malware or network activity.
Type	Type that explains the category. For example, if an attacker uses an IP address for an attack, a source email address or a file sent through an attachment can all describe the payload delivery of a malware. These types of attributes have the category of payload deliver.
Distribution	Users who can view this attribute. The distribution is inherited by attributes. The most restrictive setting wins.
Use Attribute as an IDS signature	Observable that is marked as malicious in SIR. The corresponding attribute in MISP is also marked as true.
Comments	Comments that you add for the attributes.

The following example shows that by navigating from the Associated MISP Events list, you can view the event record 5627 and add attributes to the event. The attributes include the value (testdomain.com), category as external analysis, type as domain. You can also enable IDS. The success message on the event record shows that the attribute is added to the event as shown in the following example.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add attribute to a MISP event



5. Click **Add Attribute to MISP Event**.

Result

You can view the added attribute in the Attributes section.

Add tags to a MISP event

Add tags in ServiceNow AI Platform MISP to classify events or attributes. You can use tagging globally to enable your classification or use tags locally when you don't want MISP events to be modified during your classification.

Before you begin

- Review the MISP user role and permissions for using the MISP bi-directional features.
- Verify that the event you are editing belongs to the same organization as the MISP user.
- Note that the tags and galaxies that are available to you are based on the MISP source and its distribution permissions.
- Role required: sn_sec_misp.write

Procedure

1. Navigate to **All** > **Security Incident** > **Show All Incidents**.
2. Select the security incident that contains the event that you want to add tags for.
3. Click **Show All Related Lists** and the MISP Enrichment Results related list.
4. Click the Event ID from the list of enrichment results.
   You can also navigate from the **MISP** > **Associated MISP Events** module.
5. Review the MISP Event record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

MISP Event form view

Field	Description
Event ID	Event ID that is assigned by MISP when the event was first created or imported into the MISP server.
UUID	ID that uniquely identifies events and attributes.
Creator Org	Organization that created the event on the MISP instance.
Owner Org	Organization that owns the event on the MISP instance. This field is visible only to administrators.
Creator User	User who created the event in MISP.
Last Change	Date that the event was last modified.
MISP Source	MISP source where the event is created.
Created date (in MISP)	Date that the event was created or first imported in the MISP server.
Threat Level	Risk level of the event. Incidents can be categorized into three different threat categories (low, medium, high). This field can be left as undefined. The following are the options: ○ Low: General mass malware ○ Medium: Advanced Persistent Threats (APT) ○ High: Sophisticated APTs and 0-day attacks
Analysis	Current stage of the analysis for the event with the following possible options: ○ Initial: The analysis is just beginning ○ Ongoing: The analysis is in progress ○ Completed: The analysis is complete
Distribution	Distribution of the individual attribute. An attribute can have a different distribution level than the event.
Published	Status of whether the event has been published or not. Publishing allows the attributes of the event to be used for all eligible exports and notifies users that have subscribed to the event alerts.
MISP Event Hyperlink	Link to the MISP event that is stored on the MISP server.
Info	Short description of the event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Tags (Local)	Tags that are available on the host organization's MISP instance to enable tagging for synchronization and export filtering. MISP events are not modified when you use local tags. Local tags are always stripped before being synchronized with other MISP instances and sharing communities.
Tags (Global)	Tags that are available globally to be shared and synchronized with other MISP instances and sharing communities. When you add global tags to MISP instances, you can modify events.
Galaxies (Local)	Galaxies that are available on the host organization's MISP instance for synchronization and export filtering. MISP events are not modified when you use local galaxies. These local galaxies are always stripped before being synchronized with other MISP instances and sharing communities.
Galaxies (Global)	Galaxies that are available globally to be shared and synchronized with other MISP instances and sharing communities. When you add global galaxies, MISP you can modify events.

6. To edit either a local or global tag, click the edit icon in one of the following options:

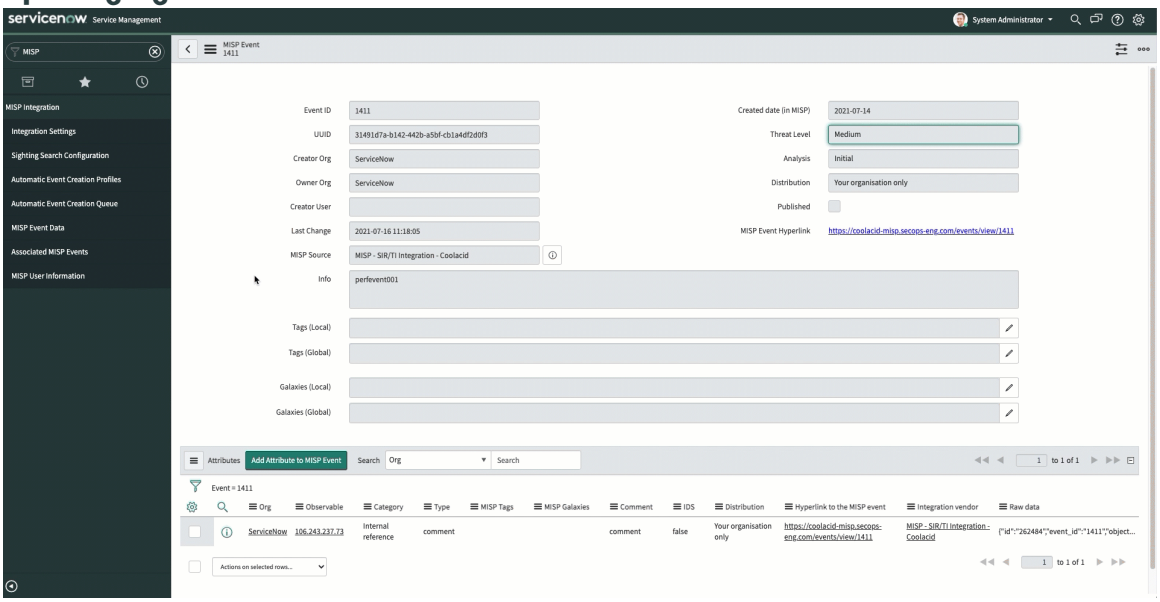
   - **Tags (Local)**
   - **Tags (Global)**

7. In The MISP Event Tags dialog box, enter the tag name to search and add the tags.
8. Click **Update Tags to MISP Event**.

   The following example shows that by clicking the edit icon for the local tags, you can search and add the C3, Adware, C2, and Botnet 3101 tags, and update the MISP server with the tags. The confirmation message shows that all the tags are updated in MISP.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Updating tags to MISP event



9. Click **Reload Form** in the success message to view the changes in the record.

Result

The tags are updated successfully in the MISP server.

Update galaxies to a MISP event or attribute

Add or remove galaxies in ServiceNow AI Platform MISP so that you can classify these objects as a cluster in the MISP instance and attach them to MISP events or attributes.

Before you begin

- Review the MISP user role and permissions required for using the MISP bi-directional features.
- To add local galaxies, the user who has configured the integration should belong to host organization of the corresponding MISP server.
- The tags and galaxies available to you are based on the MISP source and its distribution permissions.
- Role required: sn_sec_misp.write

Procedure

1. Click the edit icon in one of the following options.

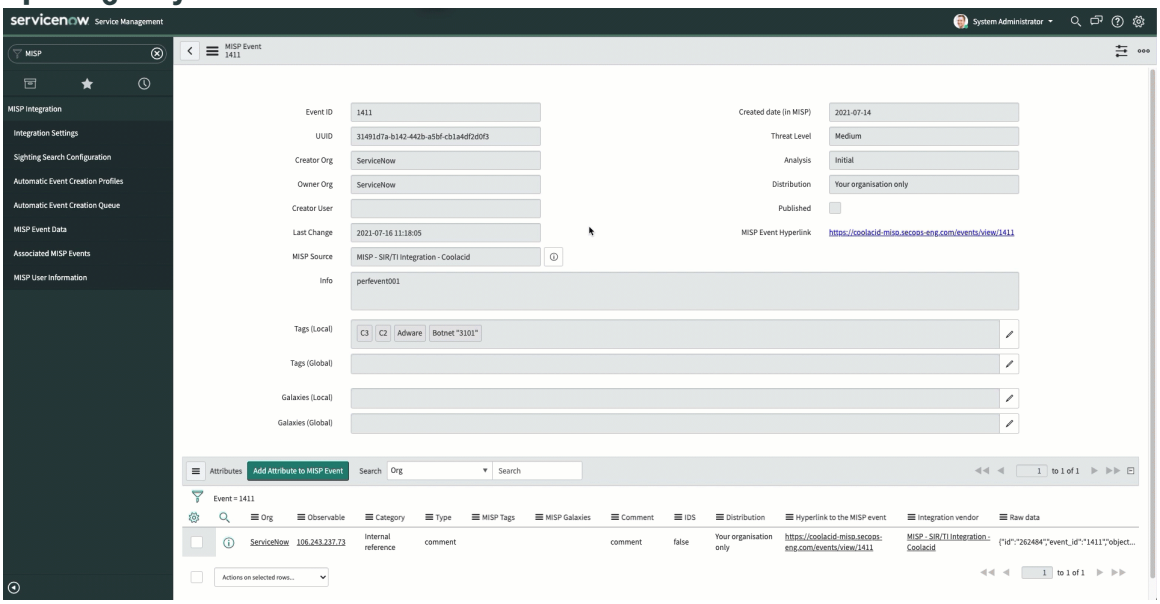
   - **Galaxies (Local)**
   - **Galaxies (Global)**

2. In The MISP Event Galaxies dialog, type and search to add the tags.
3. Click **Update Galaxies to MISP Event**.

   The following example shows how to click the edit icon for the local galaxies, select the deprecated namespace, select the Enterprise Attack - Attack Pattern galaxy, and add cluster information. After the galaxy information is updated, you can view the success message.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Update galaxy information to MISP event



The galaxies are updated successfully in the MISP server.

4. Click **Reload Form** in the success message to view the changes in the record.

Roll up MITRE-ATT&CK information using MISP enrichment results

Roll up the MISP enrichment results manually if you haven't enabled the automatic rollup of MISP information.

Before you begin

Role required: sn_si.analyst

About this task

Use the base system auto-extraction rules to import the MITRE-ATT&CK information from the MISP integration. The MISP integration for Security Operations introduces two base system MITRE-ATT&CK technique extraction rules for MISP - MISP galaxies and MISP tags. For more information on auto-extraction rules in MITRE-ATT&CK, see auto-extract technique rules for importing MITRE-ATT&CK information.

If you have enabled automatic rollup of MITRE-ATT&CK information using MISP enrichment results to a security incident, the information is automatically rolled up. If you have not enabled automatic rollup, you can do this task manually.

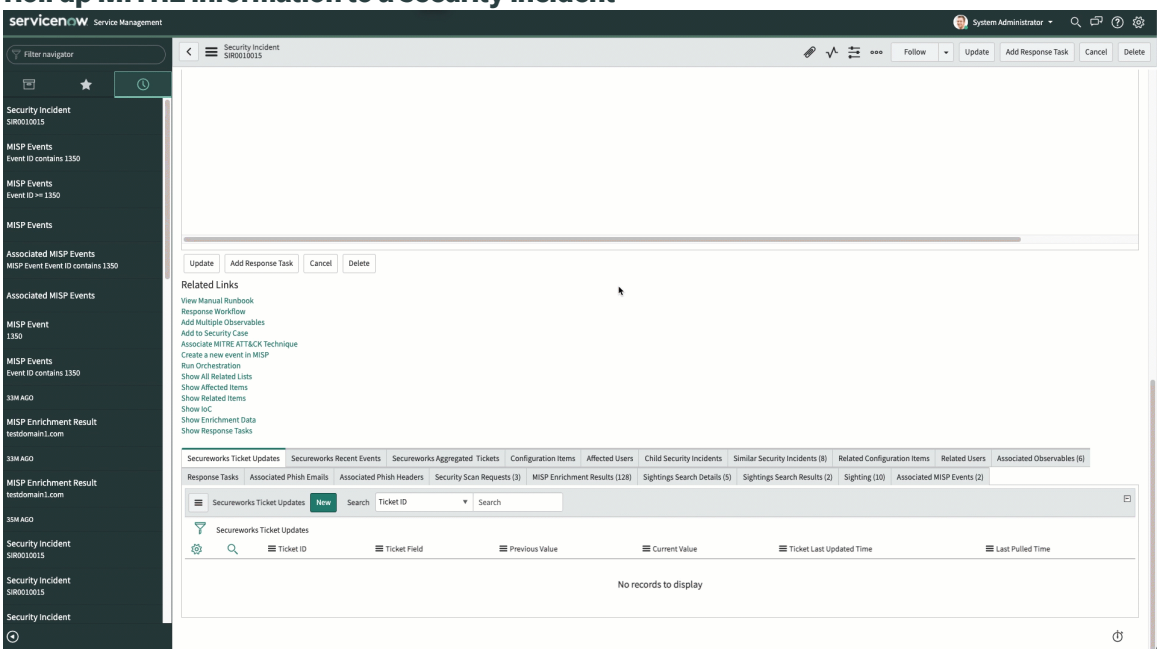
Procedure

1. Navigate to **All** > **Security Incidents** > **Show All Incidents**.
2. Select the security incident that you want to enrich with the MITRE-ATT&CK information.
3. Click **Show All Related Lists** and the **MISP Enrichment Results** tab.
4. Select the observable and from the Actions menu, click **Roll up MITRE ATT&CK Information to SI**.
   You can select multiple observables and then roll up the information.
5. To confirm the changes, click **Reload**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows how to select an observable and roll up the MISP enrichment results to the security incident.

Roll up MITRE information to a security incident



Result

You can view the MITRE-ATT&CK Card to confirm that the MISP Enrichment Results have been rolled up to the security incident.

OPSWAT Metadefender Integration

OPSWAT Metadefender allows threat data, detected by the third-party Metadefender scanner, to be downloaded to the Threat Intelligence application for tracking, prioritization, and resolution.

Explore	Setup
• OPSWAT Metadefender integration overview • Threat Intelligence integrations	Activate and configure the OPSWAT Metadefender integration
Use	**Develop**
Perform lookups on observables	• ServiceNow Security Operations integration development guidelines • Tips for writing integrations • Developer training • Developer documentation • Find components installed with an application
Troubleshoot and get help	
• Integration troubleshooting • Ask or answer questions in the Security Operations community	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

OPSWAT Metadefender integration overview

OPSWAT Metadefender is a security solution that provides access to multiple anti-malware machines and easily integrates with Security Operations.

Before you can use the OPSWAT Metadefender integration, you must activate the plugin and configure the integration. If necessary, you can also update your X509 SSL certification.

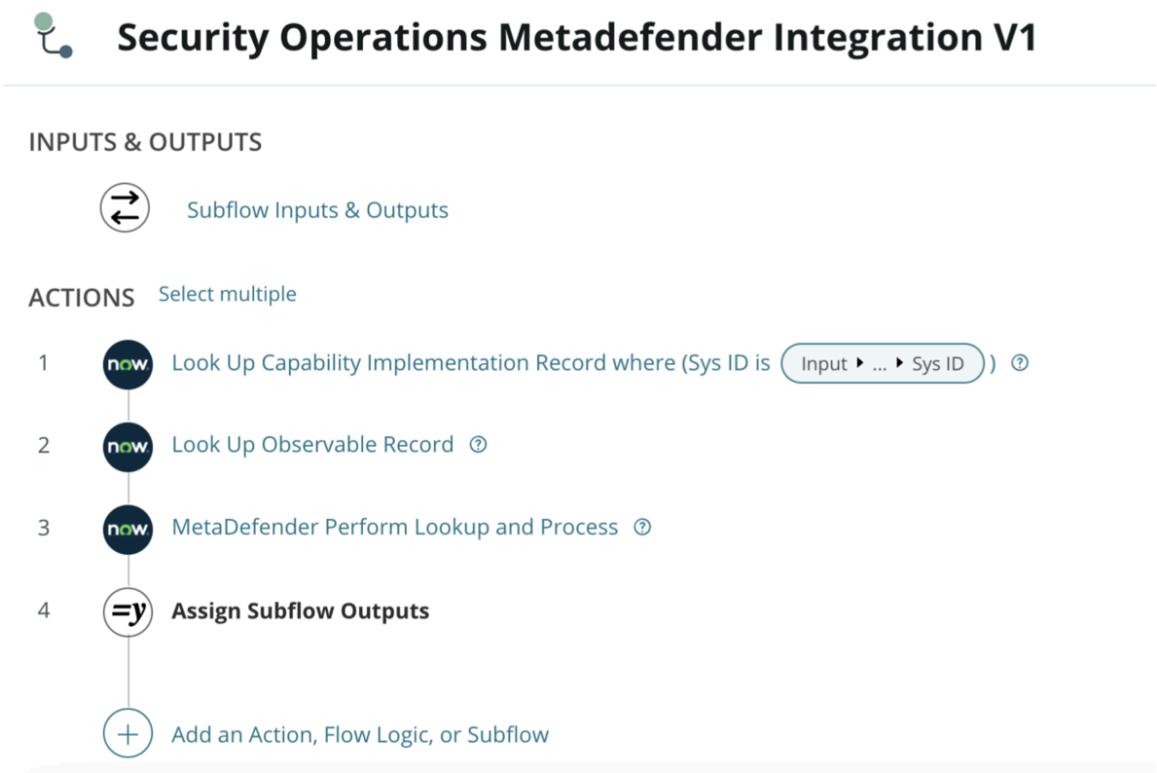
Threat Lookup - OPSWAT Metadefender flow

The Threat Lookup - OPSWAT Metadefender flow performs a lookup on selected observables. If the observables are of a type recognized by OPSWAT Metadefender, the observables are scanned for malware, and the results are returned.

This flow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the OPSWAT Metadefender implementation is selected. For more information, see Perform lookups on observables.

Role required: sn_si.admin

Threat Lookup - OPSWAT Metadefender flow



For information on the activities used by this flow, see Common Security Operations integration flows and orchestration Flow Actions.

Activate and configure the OPSWAT Metadefender integration

Before you can use the OPSWAT Metadefender integration, you must download it from the ServiceNow Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the integration is complete, access the OPSWAT portal and obtain the Metadefender Cloud API Key
3. In your instance, navigate to **Security Operations** > **Integrations** > **Integration Configuration**. The available security integrations appear as a series of cards.
4. In the OPSWAT Metadefender card, click **Configure**.
5. Enter (or paste) the **API Key** you acquired from the OPSWAT portal.
6. Click **Submit**.

Result
After it is configured, OPSWAT Metadefender can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related topics

Perform lookups on observables

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin
Role required: admin

Procedure

1. Acquire the SSL certificate from the third-party vendor.
   For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.

   a. Enter the endpoint URL into the browser address bar.
      For example: `https://<3rdparty>/`.

   b. Click the lock icon in the address line.

   c. Click **More Information** and click the **Security** tab.

   d. Click **View Certificate** and click the **Detail** tab.

   e. Click **Export** to save the PEM into your local file system.

   f. Open the saved file in any text editor tool and copy the content to the clipboard.
      It must begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

2. Navigate to **System Definition** > **Certificates**.
3. Click **New** and create a new record for the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In **PEM Certificate**, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Add the certificate to the Identity Provider record.
   a. Navigate to **Multi-Provider SSO** > **Identity Providers**.
   b. Select the active default identity provider for which you created the new certificate.
   c. Scroll down to **X.509 certificates** related list, and click **Edit**.
   d. Move the newly created certificate to the **Selected** column.
6. Click **Save**.
   The other fields in the record are generated automatically.

> **Note:** If you have a certificate that has expired, you need to remove it. For information on how to remove the expired certificate, refer to KB0691439 Replacing an expiring SAML certificate.

VirusTotal integration

The VirusTotal integration enables you to request the analysis of suspicious IP addresses, files, file hashes, and URL addresses to aid in your investigation to determine if they are malicious.

Explore	Set up
Threat Intelligence integrations	• VirusTotal integration setup • Activate and configure the VirusTotal integration
Use	**Develop**
• Perform lookups on observables • Threat Lookup - VirusTotal workflow	• ServiceNow Security Operations integration development guidelines • Tips for writing integrations • Developer training • Developer documentation • Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

VirusTotal integration setup

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. It integrates easily with Security Operations.

Before you can use the VirusTotal integration, you must activate the plugin and add the appropriate API key. If necessary, you can also update your X509 SSL certification.

If the VirusTotal lookup source is used and malware is encountered, an observable is created. For IP lookups, an additional list of URLs that share the IP address is created, and observables are created for each of the URLs.

Note:

- The Threat Intelligence plugin is required in order to implement VirusTotal integration.
- The VirusTotal integration has been upgraded to Version 3 APIs.

Activate and configure the VirusTotal integration

Before you can use the VirusTotal integration, you must download it from the ServiceNow Store.

Before you begin

Role required: admin
Threat Intelligence must be installed and activated before you can use VirusTotal. The VirusTotal integration has been upgraded to version 3 APIs.

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, access VirusTotal and obtain the API Key under your VirusTotal profile.
3. In your instance, navigate to **Security Operations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
4. In the VirusTotal card, click **Configure**.

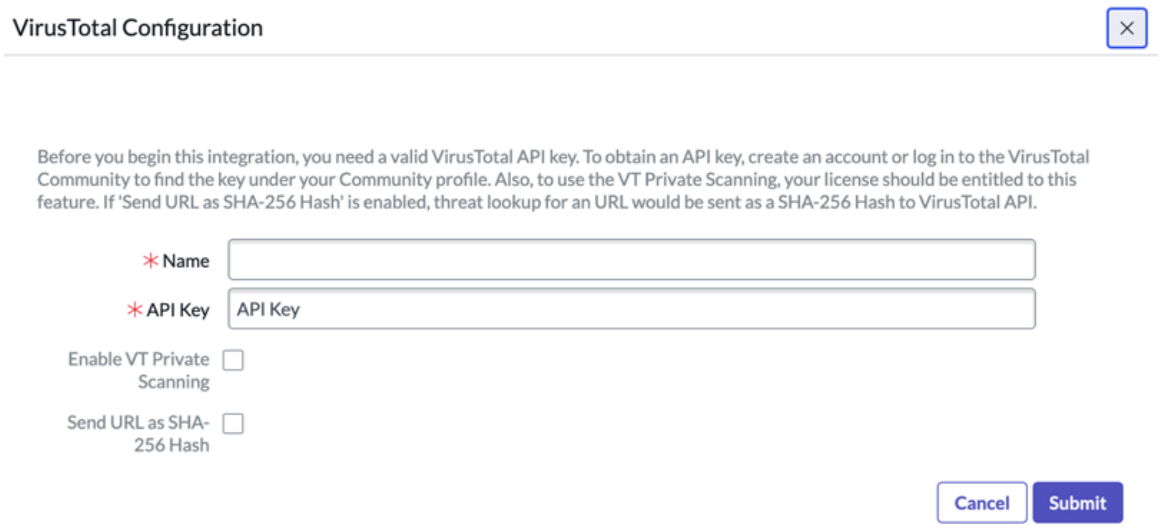
VirusTotal Configuration

Field	Description
Name	Name of the integration. For example, VirusTotal.
API Key	Enter (or paste) the **API Key** you acquired from the VirusTotal site.
Enable VT Private Scanning	Select this check box to analyze files with VirusTotal in a privacy preserving fashion. The files uploaded via this offering won't be shared with anyone beyond your organization, and will remain in VirusTotal only for a brief period of time. The resulting analyses will be ephemeral too and only visible to your VirusTotal group.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Important: To use the VT Private Scanning, your VirusTotal license should be entitled to this feature.
Send URL as SHA-256 Hash	Select this check box to send the URLs as hashes for threat lookup and protect the users' privacy on the integration. **Note:** If disabled, the URL is sent as Base64 encoding to the VirusTotal API.

5. Click **Submit**.



Result
After it is configured, VirusTotal can be selected for performing lookups on observables in Threat Intelligence and on observables in security incidents.

Related topics
Perform lookups on observables

Threat Lookup - VirusTotal workflow

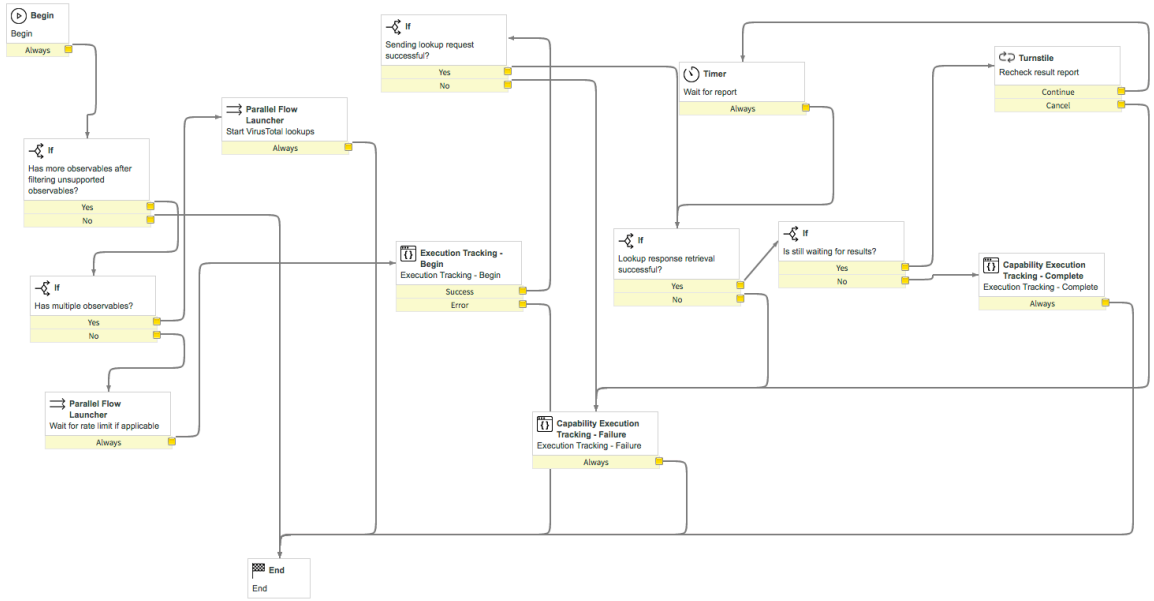
The Threat Lookup - VirusTotal workflow performs a lookup on selected observables. If the observables are of a type recognized by VirusTotal, the observables are scanned for malware, and the results are returned.

Before you begin
Role required: admin

About this task
This workflow is triggered by the Security Operations Integration - Threat Lookup capability when you perform a threat lookup on one or more observables, and the VirusTotal implementation is selected. For more information, see Perform lookups on observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Lookup - VirusTotal workflow



For information on the activities used by this workflow, see Common Security Operations integration flows and orchestration Flow Actions.

WhoisXML API integration

The WhoisXML API integration enables you to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

Explore

Threat Intelligence integrations

Set up

- WhoisXML API integration setup
- Activate and configure the Security Operations Whois integration

---

Use

Threat Intelligence - Run IoC Lookup workflow

Develop

- ServiceNow Security Operations integration development guidelines
- Tips for writing integrations
- Developer training
- Developer documentation
- Find components installed with an application

Troubleshoot and get help

- Integration troubleshooting
- Ask or answer questions in the Security Operations community

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

WhoisXML API integration setup

Before you can use the Whois integration, you must activate the plugin and add the credentials. If necessary, you can also update your X509 SSL certification.

The Threat Intelligence and WhoisXML API Integration plugins are required to implement the WhoisXML API integration.

Activate and configure the Security Operations Whois integration

The Integration Configuration feature allows you to quickly activate and set up third-party security integrations, including the Security Operations Whois integration. Before you can use the Security Operations Whois integration, you must download it from the ServiceNow Store, and you must have a valid account from WhoisXML API.

Before you begin

Threat Intelligence must be installed and activated before you can use the Security Operations Whois Integration.

Role required: admin

Procedure

1. Download the integration from the ServiceNow Store.
2. When the installation is complete, navigate to **Security Operations** > **Integration Configuration**.
   The available security integrations appear as a series of cards.
3. In the Whois API card, click **Configure**.
4. Enter the Username and Password from your WhoisXML API account.
5. Click **Submit**.

Update your X.509 certificate

If you require an SSL connection for the integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. This task is optional.

Before you begin

Role required: admin

Procedure

1. Acquire the SSL certificate from the third-party vendor.
   For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.

   a. Enter the endpoint URL into the browser address bar.
      For example: `https://<3rdparty>/`.

   b. Click the lock icon in the address line.

   c. Click **More Information** and click the **Security** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Click **View Certificate** and click the **Detail** tab.

e. Click **Export** to save the PEM into your local file system.

f. Open the saved file in any text editor tool and copy the content to the clipboard.
It must begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

2. Navigate to **System Definition** > **Certificates**.
3. Click **New** and create a new record for the integration.
4. In **PEM Certificate**, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Add the certificate to the Identity Provider record.
   a. Navigate to **Multi-Provider SSO** > **Identity Providers**.
   b. Select the active default identity provider for which you created the new certificate.
   c. Scroll down to **X.509 certificates** related list, and click **Edit**.
   d. Move the newly created certificate to the **Selected** column.
6. Click **Save**.
   The other fields in the record are generated automatically.

> **Note:** If you have a certificate that has expired, you need to remove it. For information on how to remove the expired certificate, refer to KB0691439 Replacing an expiring SAML certificate.

Enrich Observable WhoIs workflow

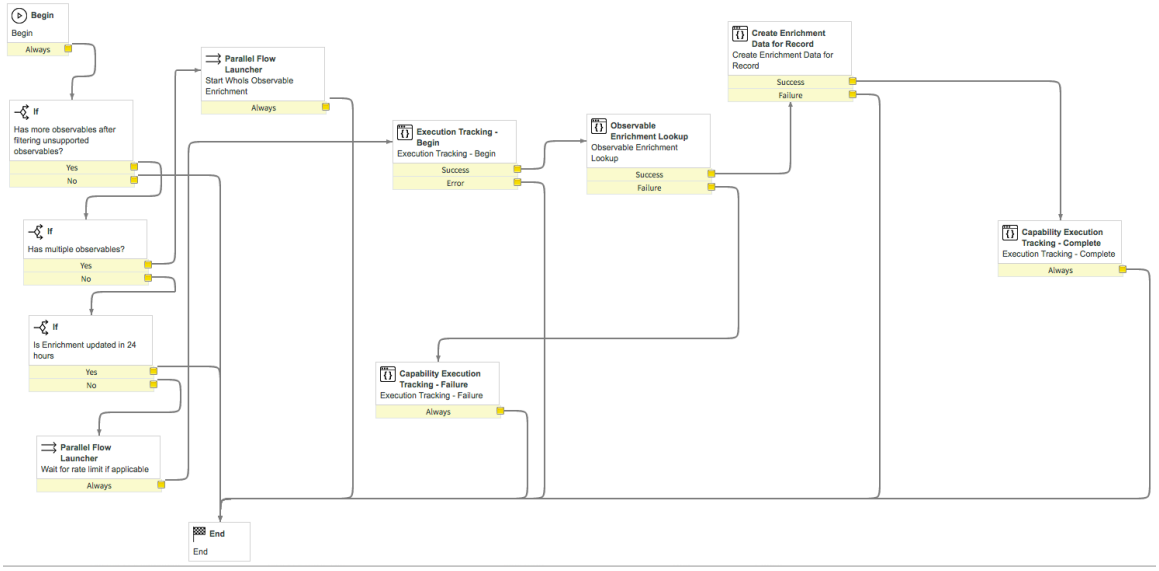
The **Enrich Observable WhoIs** workflow performs enrichment on selected observables. If the observables are of a type recognized by the WhoisXML API Integration, the observables are enriched.

Before you begin
Role required: admin

About this task
This workflow is triggered by the Security Operations Integration- Enrich Observable capability when you perform enrichment on one or more observables, and the WhoIs implementation is selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enrich Observable WhoIs workflow



Activities specific to this integration are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Observable Enrichment Lookup activity

The **Observable Enrichment Lookup** workflow activity initiates the observable enrichment process.

The **Observable Enrichment Lookup** activity can be used with any observables workflow to begin enrichment.

Results

Possible results for this activity are:

Results

Result	Description
Success	The lookup is successful.
Fail	An error occurred while attempting to perform the lookup. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
implementation_id	System identifier of the implementation used to perform the lookup.
domain_id	The domain identifier for the domain within which the lookup is being performed.
observable_ids	One or more observables to perform the desired action against. The IDs are used as a workflow input.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
capabilityExcutionId	System identifier of the capability that launched the implementation workflow. Only required for Integration Capability implementation workflows such as Splunk, Elasticsearch.
task_sys_id	System identifier for any task associated with the workflow.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response_data	Raw data returned by the implementation's API endpoint for the given domain.
mapping_id	The identifier for the enrichment mapping. For example, the WhoIs integration returns data in two different format, IP and URL, with a mapping id for each.

Threat Intelligence Orchestration

Threat Intelligence Orchestration activities allow users to determine whether a threat has been seen before in other security incidents or on other systems using workflow orchestration.

For more information on editing Security Incident Response Orchestration workflows or creating custom workflows, see Getting started with workflows and Workflow editor Workflow editor.

Set up Threat Intelligence Orchestration

Prior to using Threat Intelligence Orchestration, perform steps to set up various parts of the system, including populating the CMDB, configuring the MID Server, and configuring credentials.

Before you begin

Role required: admin

To use Threat Intelligence Orchestration you need a fully populated CMDB with domain names. For more information, see Discovery.

About this task

Procedure

1. Activate the Threat Intelligence plugin.
2. Configure the MID Server
3. Configure MID Server service credentials
   You are now ready to use Threat Intelligence Orchestration activities within a workflow.

Threat Intelligence Orchestration workflows and activities

The base system includes workflows and workflow activities you can use to automate actions on your instance.

Threat Intelligence - Run IoC Lookup workflow

The **Threat Intelligence - Run IoC Lookup** workflow checks whether there is an unexpired observable and if so, the lookup is set to **Complete** and updated with the data from the observable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_si.basic

Note: This workflow replaces Threat Intelligence Orchestration business rules (**Populate with existing IoC tables**, **Queue the lookup**, and **Update observable**) with activities.

If a lookup is inserted or updated and meets the conditions, the Lookup business rule triggers this workflow.

About this task

The **Threat Intelligence - Run IoC Lookup**workflow checks whether there is an unexpired observable and if so, the lookup is set to **Complete** and updated with the data from the observable. Any indicators associated with the observable are reactivated.

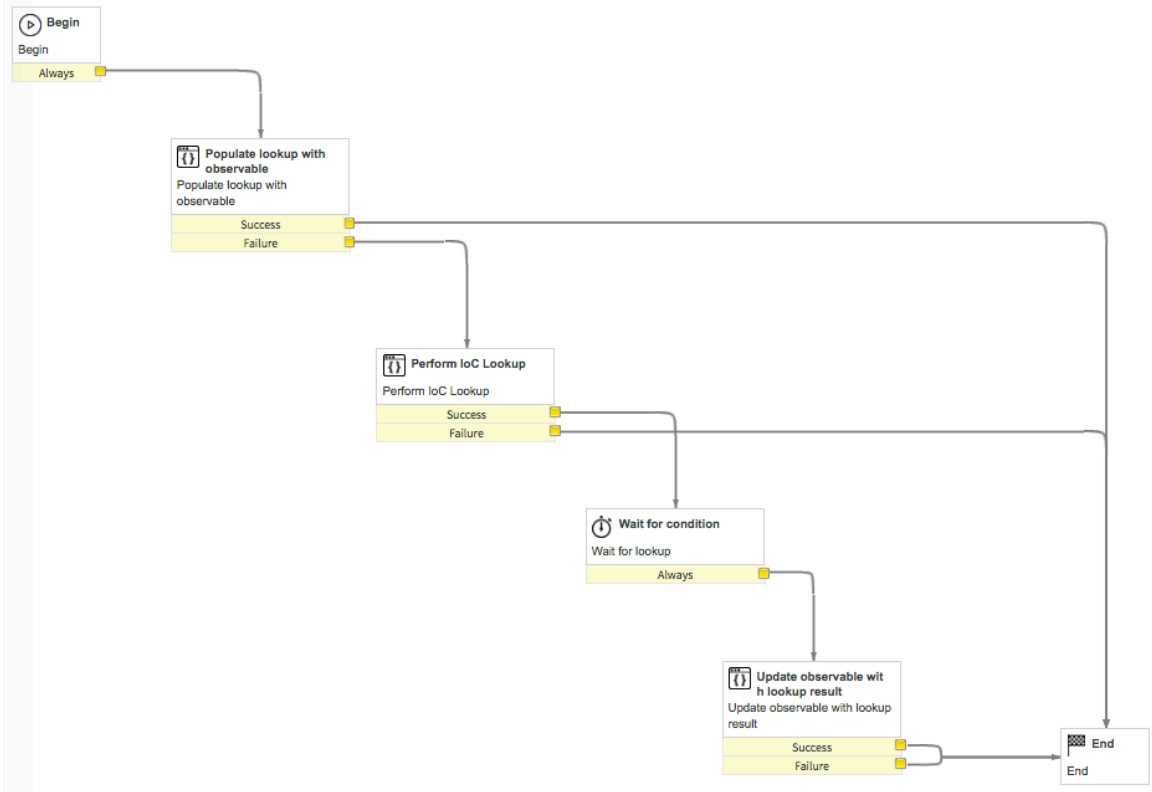
If the observable is expired, the workflow runs the lookups and increments the **Sighting count** in the existing, expired observable.

If no correlating observable exists, a new observable with indicator is created.

Workflow process activities include:

- Populate lookup with observable activity
- Perform IoC Lookup activity
- Wait for lookup (core activity)
- Update observable with lookup result activity

Threat Intelligence - Run IoC Lookup workflow



Populate lookup with observable activity

If an unexpired observable is found, the **Threat Intelligence Orchestration - Populate lookup with observable** workflow activity supplies data from an existing observable to a lookup. This activity can accelerate the investigation and remediation process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When triggered by a workflow **Populate lookup with observable** attempts to find an existing observable for a lookup that matches the **value** and **type** of the lookup provided to the activity as input.

If the observable exists and is not expired, this activity:

- Updates the lookup with the information found in the observable
- Reactivates an indicator if it is inactive, increments the **Encountered count**, and updates the **Last seen** date
- Sets **State** to Complete.

Input variables

Input variables determine the initial behavior of the activity.

Input variable	Description
scanID[string]	lookup identifier

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables	Description
True	Found valid observable and updated lookup.
False	Did not find valid observable. Observable is either missing or expired.

Perform IoC Lookup activity

The **Threat Intelligence Orchestration - Perform IoC Lookup** workflow activity performs a given lookup. This activity can accelerate the investigation and remediation process.

When triggered by a workflow, **Perform IoC Lookup** takes a scanID, looks up the lookup record, and adds the lookup to the queue by creating a lookup queue entry.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
scanID[string]	lookup identifier

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
True	Triggered the lookup.
False	Did not trigger the lookup.

Update observable with lookup result activity

The **Threat Intelligence Orchestration - Update observable with lookup result** workflow activity updates the observable record. If one does not exist, it creates a new observable. This activity is useful for logging information.

When triggered by a workflow **Update observable with lookup result** updates an existing observable to include the new **Sighting count**, adds a note, and, if inactive, reactivates any indicators. The **Encountered count** and **Last seen** date in the indicator are also updated.

If no correlating observable exists, the workflow creates a new observable with indicator as follows:

- Runs the IoC lookups
- Creates a new observable
- Creates an indicator for the observable
- Adds a **Sighting count** to the observable
- Adds an **Encountered count** and **Last seen** date to the indicator
- Adds a message indicating from which lookup it was created

.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
scanID[string]	Lookup identifier.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
True	Update or creation of observable is successful.
False	Update or creation of observable failed.

Run Default IoC Lookup Sources activity

When triggered by a workflow, Threat Intelligence - **Run Default IoC Lookup Sources** takes in a lookup request ID and creates multiple lookups depending on the entered data values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For each data type, the **include_in_bulk scan** column of the supported lookup type table of each lookup source is evaluated. If true, a lookup is added to the lookup request.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
scan_request_id	Lookup request system identifier

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
Number of scans created	Integer

Security Case Management

Security Case Management provides a means for security analysts who are engaged in threat hunting to gather information on suspicious activity in their environment. Case-related records, such as security incidents, observables, CIs, and affected users can be added to cases to accommodate broad and specific analysis.

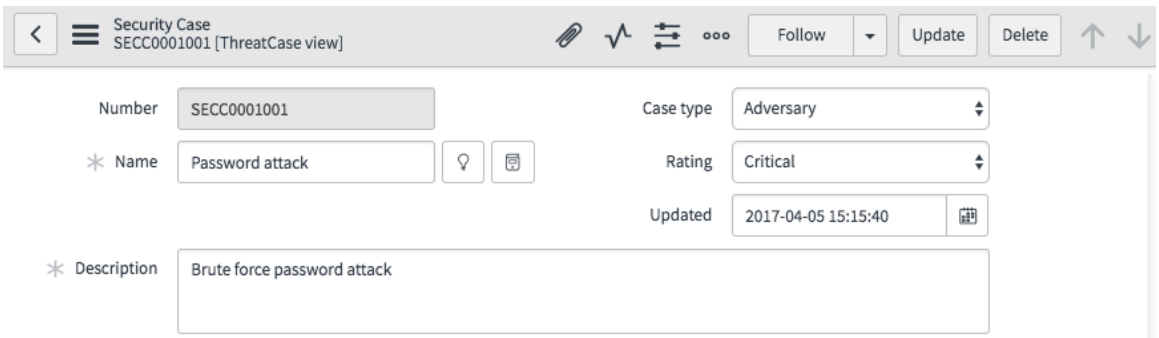
With the ability to easily pivot through the records and related information, analysts can assess whether they are facing a targeted campaign, advanced persistent threat, and so forth.

Security cases can be created from various sources on your instance, including Security Case Management, Security Incident Response, and Threat Intelligence. You can also create cases from configuration items and affected users in the Configuration Items [cmdb.ci] and Users [sys.user] tables, respectively. After cases have been created, each of these sources can be also used to add valuable analysis resources to existing cases.

Each security case consists of three main sections, a header section, a section with additional case details, and a case artifacts section containing a collection of records that aid in building an argument for identifying and dealing with particular threats.

Case header

Case header section

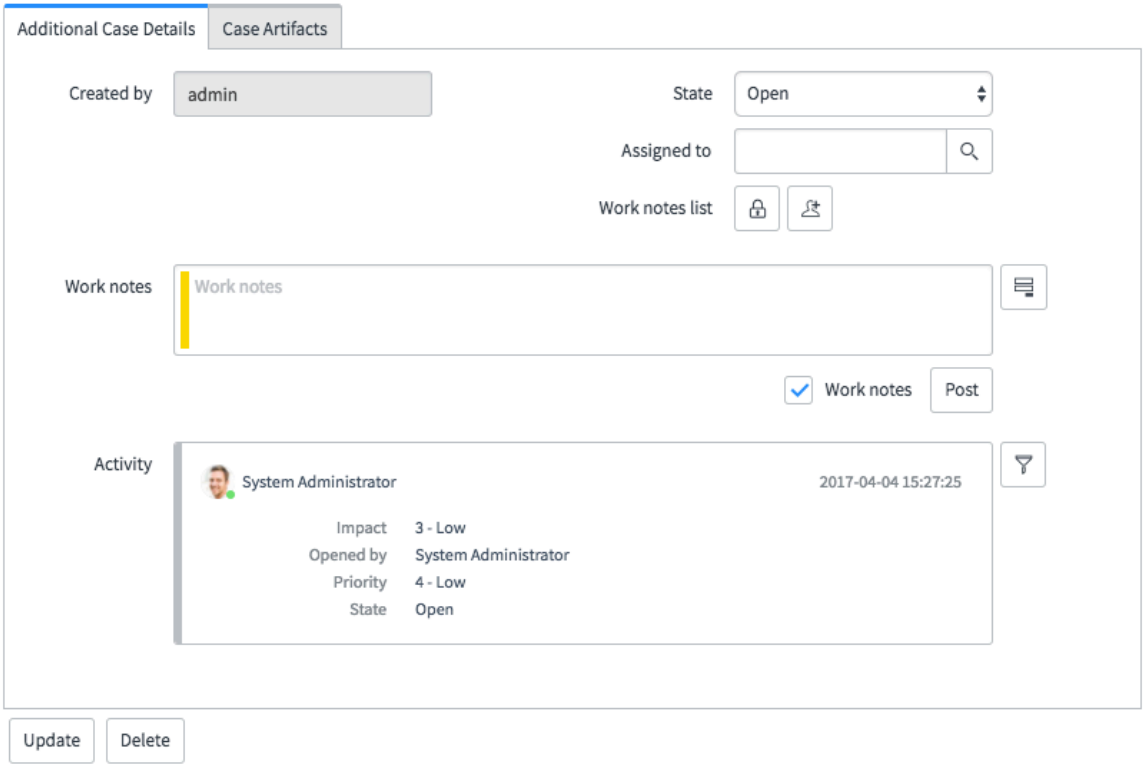


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The case header provides basic information used to identify and classify the security case. The case number uses the SECC prefix.

Additional case details

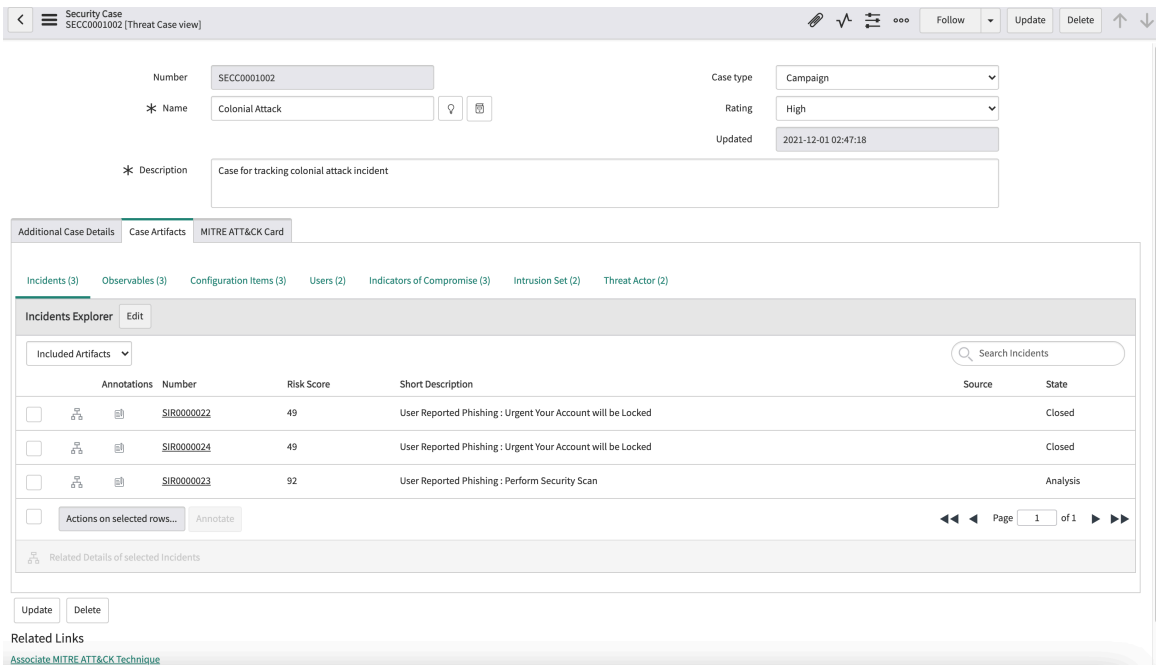
Additional Case Details section



The **Additional Case Details** section provides information specific to the analysis that has already been performed on the case, including its current state, and work notes and activities recorded for the case.

Case artifacts

Case Artifacts section

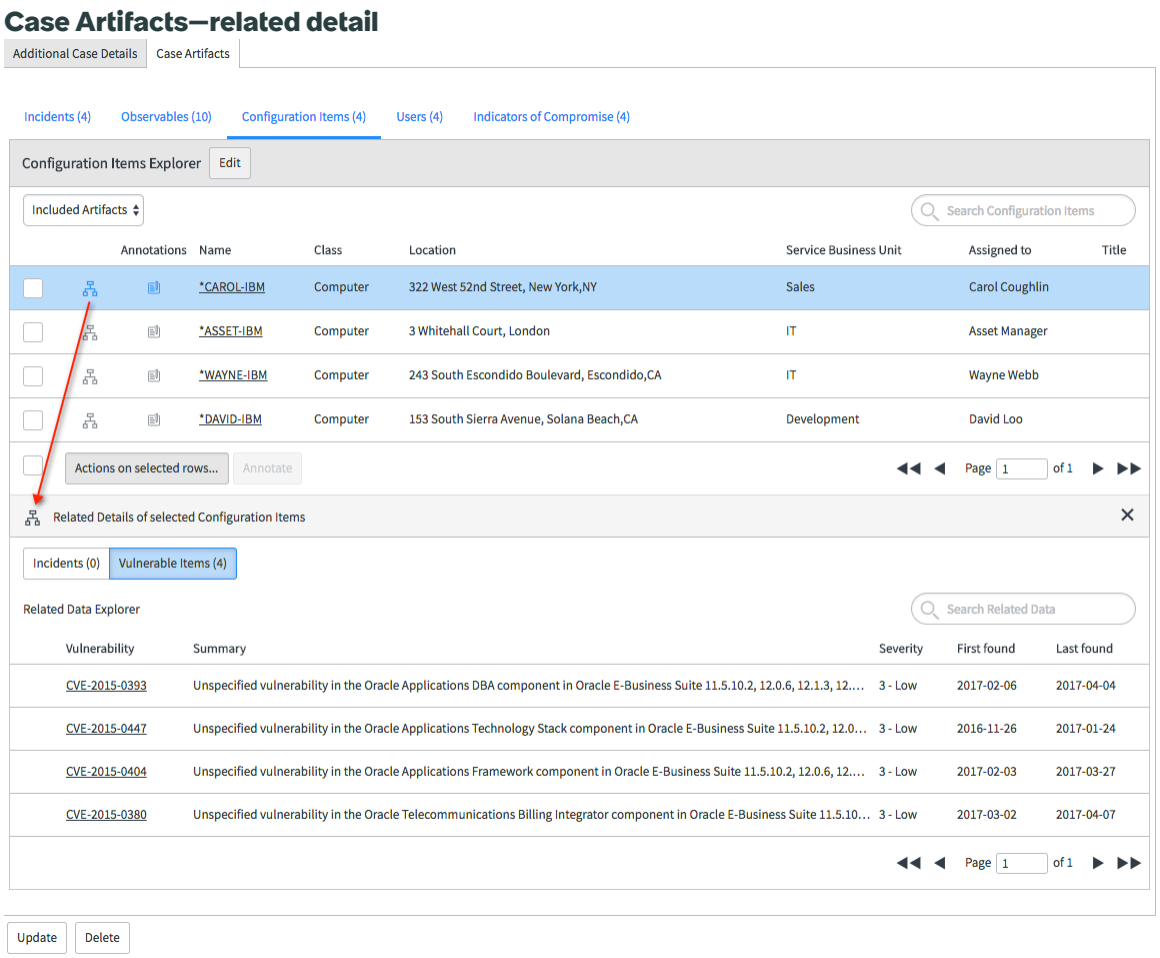


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Case Artifacts** section provides a series of tabs of information contained in the security case.

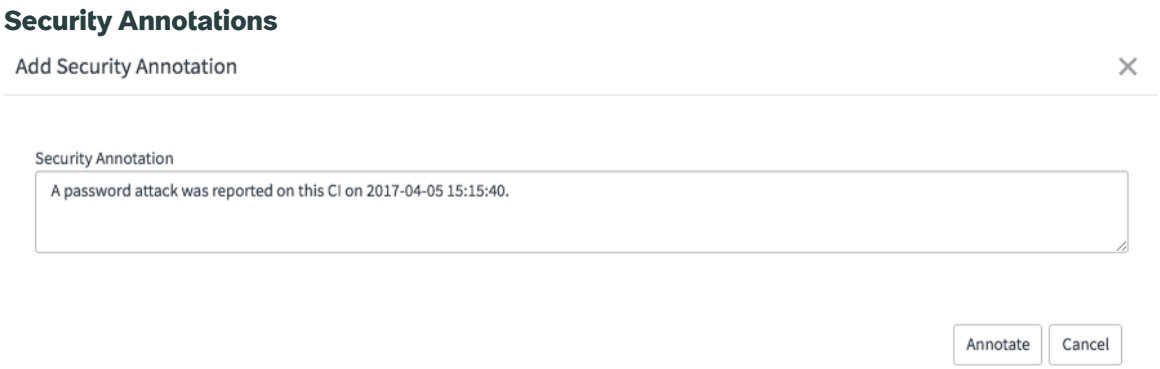
You can perform searches within the contents of each tab. You can also exclude specific records you have already evaluated as being safe or which are of no value in your investigation. The excluded records are not deleted, but are hidden from view. If needed, you can view excluded records and add them back.

Within each tab, you can click the Additional Details icon to show related information for the selected record. For example, if you click the **Configuration Items** tab to view the Configuration Items Explorer, and click Additional Details for a specific CI, you can view incidents, vulnerable items, and annotations associated with that CI.



You can also select a record and click the **Annotate** button for a case-related artifact to add annotations to the record. Annotations are simply notes that each analyst can make on a particular artifact.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Other tools the analyst can use for examining cases include:

- Run a sightings search on observables in a case
- Search for security artifacts

Create cases in Security Case Management

Cases are used to track information about a campaign or state actor threatening your organization. After a case is created, you can add artifacts that allow you to review and analyze all related information within a single case record.

Before you begin

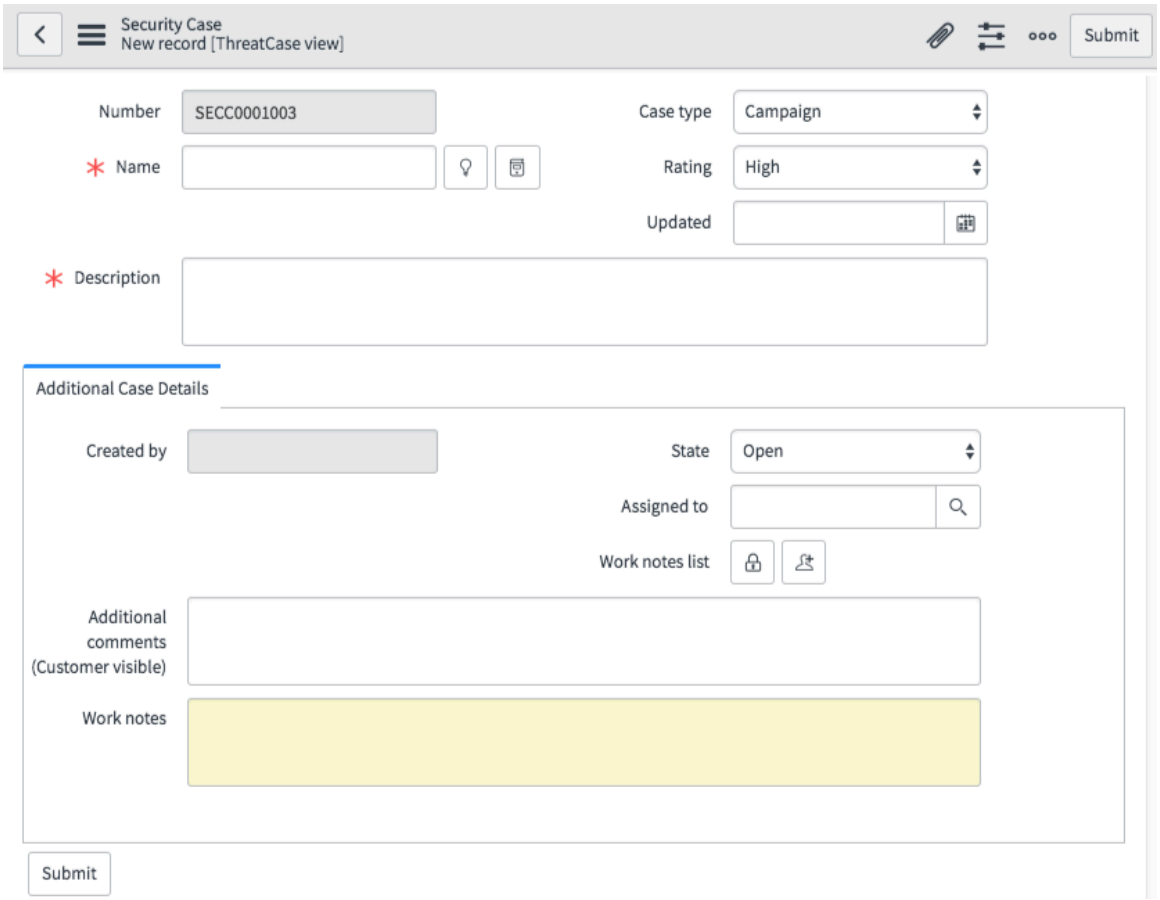
Role required: sn_ti.case_use

r

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Case Management** > **All Cases**.
   The Security Cases list opens.
2. Click **New**.
   The Security Cases screen opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

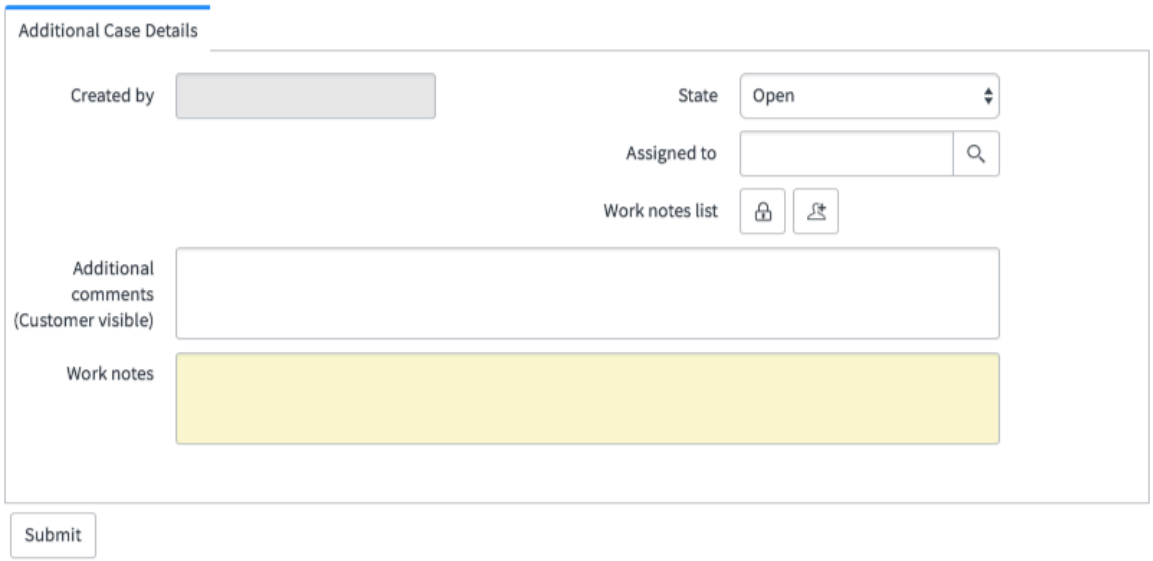


3. Fill in the fields as appropriate.

Field	Description
Case Number	[Read only] The case number.
Case Name	Enter a descriptive name for the case.
Case Type	Select the type of case being investigated.
Rating	Select the importance of this case (from Critical to Low).
Last Updated	[Read only] The date and time the case was last updated.
Short Description	A brief description of the case.

4. Click the **Additional Case Details** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Fill in the fields as appropriate.

Field	Description
Created by	[Read only] The name of the user who created this case.
State	The current state of the case. At case creation, the State defaults to Draft.
Assigned to	Click the lookup icon and assign the case to an analyst.
Work notes list	Click the lock icon and add internal users who can view work notes.
Additional comments	As needed, enter notes on the case that will be visible to the customer.
Work Notes	If needed, type a work note for the case.

6. Click **Submit**.
   After the record has been saved, you can click the **Case Artifacts** tab and add artifacts to the case.

Add artifacts to a case

After you have created a case, you can add artifacts, such as security incidents, CIs, and indicators of compromise, to the case. These artifacts act as clues in solving the case.

Before you begin

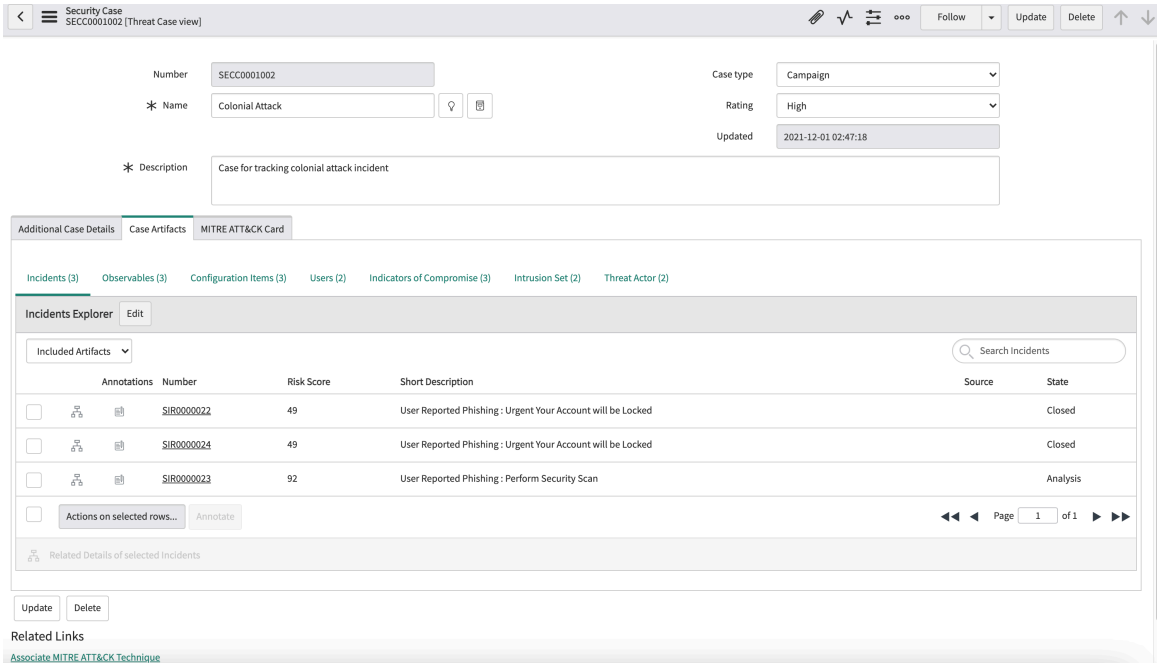
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

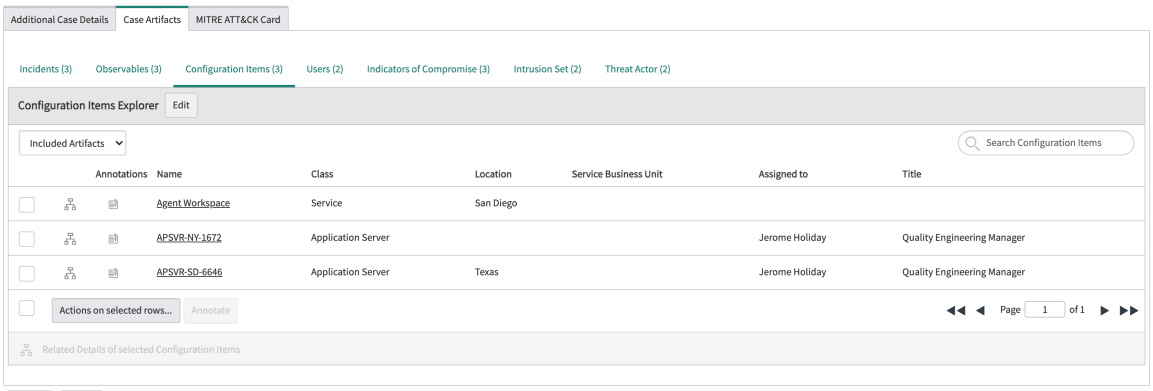
Procedure

1. Open a case to which you want to add artifacts.
2. Click the **Case Artifacts** related list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

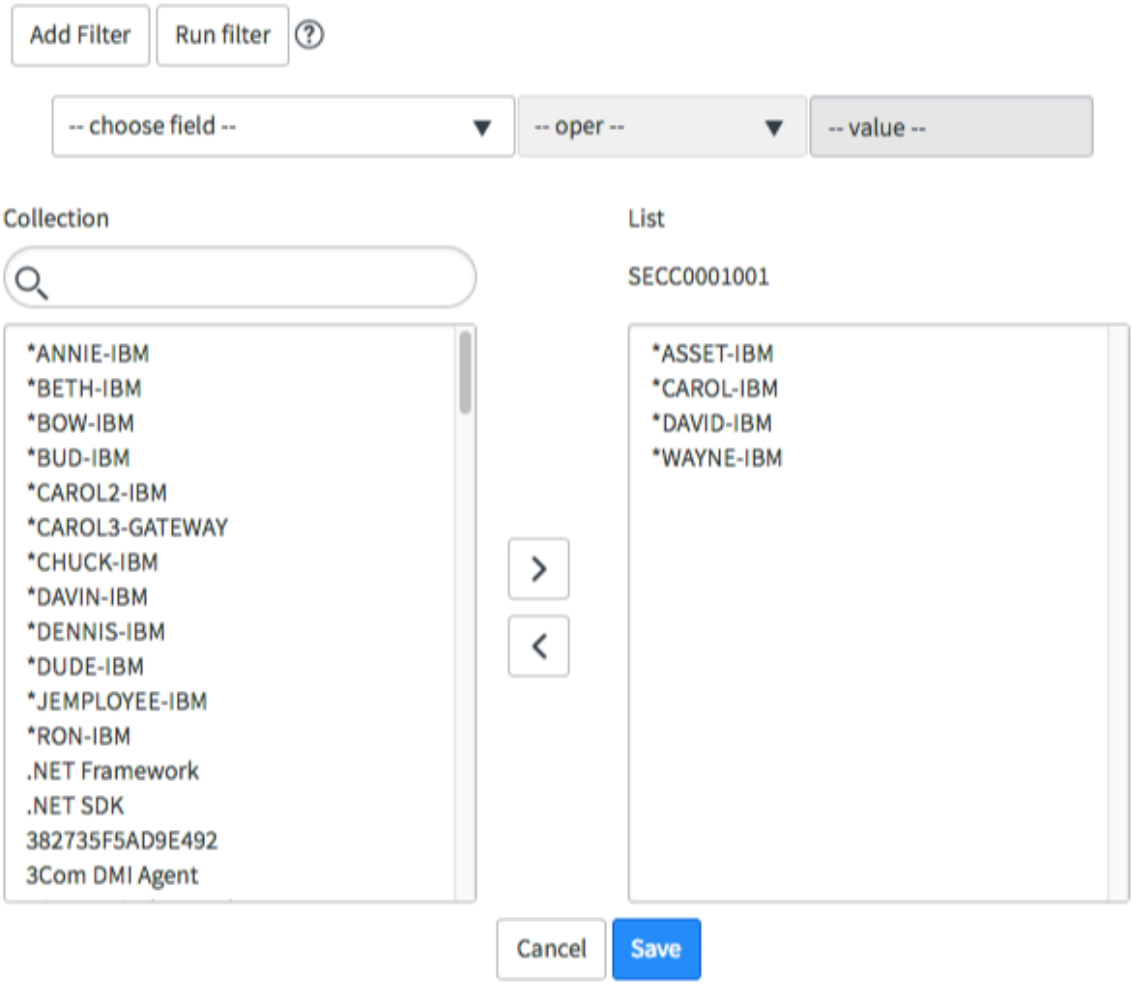


3. Click the tab associated with the type of artifact you want to add to the case. For example, click **Configuration Items** to add one or more CIs to the case.



4. Click **Edit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Using the slushbucket and filters, locate the artifact records you want to add to the case and move them from the Collection bucket to the List bucket, and click **Save**.
   The list appears in the selected tab and the selected artifacts are added to the list.

Related topics

- Add IoCs and observables to an existing case
- Add security incidents to an existing case
- Add CIs to existing cases
- Add affected users to existing cases

Associate MITRE-ATT&CK information with security case

Associate MITRE-ATT&CK tactics and techniques to a security case for better security case management and threat analysis at a granular level.

Before you begin

Role required: sn_si.analyst

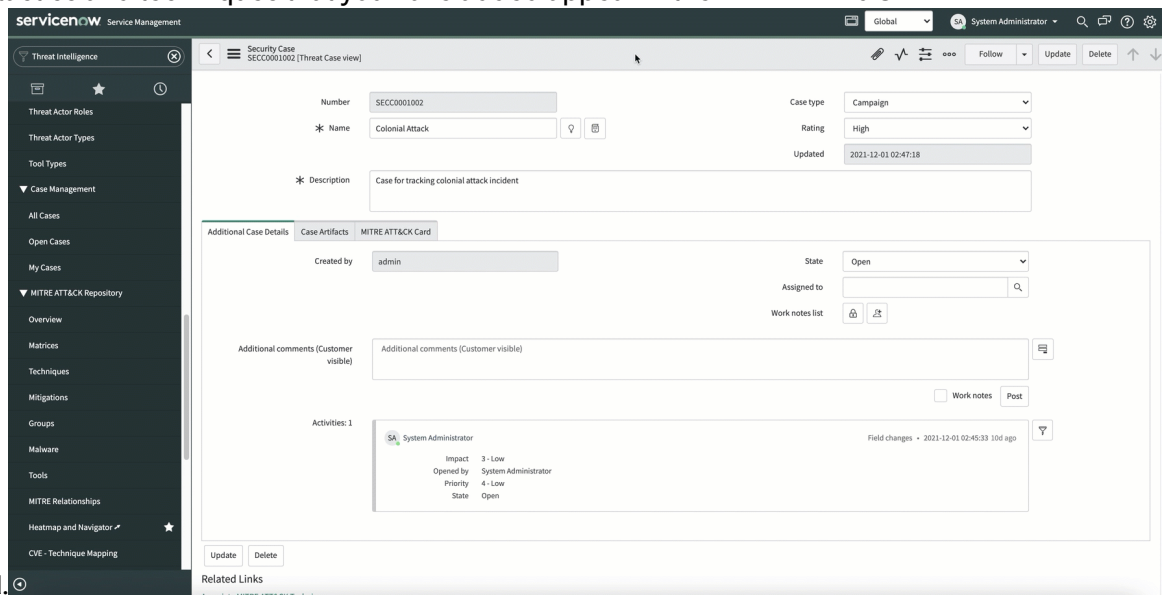
Procedure

1. Navigate to **All** > **Threat Intelligence** > **Case Management** > **All Cases**.
2. Select the security case that you want to enrich with the MITRE-ATT&CK information.
3. From the related list, click **Associate MITRE ATT&CK Technique**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the following illustration, you can see how to navigate from the related list to **Associate MITRE ATT&CK Technique**, review the source, and add a tactic and technique.

4. In the source lists, review the **Source**.
5. Review the **Tactic** and **Techniques**, and add or remove them based on the relevance with the case.
6. Click **Save**.
   The tactics and techniques that you have added appear in the MITRE-ATT&CK Card.



Case creation from security artifacts

In addition to creating cases manually from Security Case Management, you can also create cases from security artifacts, such as security incidents, indicators of compromise, affected users, and configuration items.

IoCs and observables in cases

In Threat Intelligence, you can create cases from IoCs and observables, as well as add IoCs and observables to existing cases. You can also create observables directly from a case.

Create a case from IoCs or observables

In Threat Intelligence, you can create a case from artifacts (IoCs or observables). After the IoCs or observables have been used to create a case, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

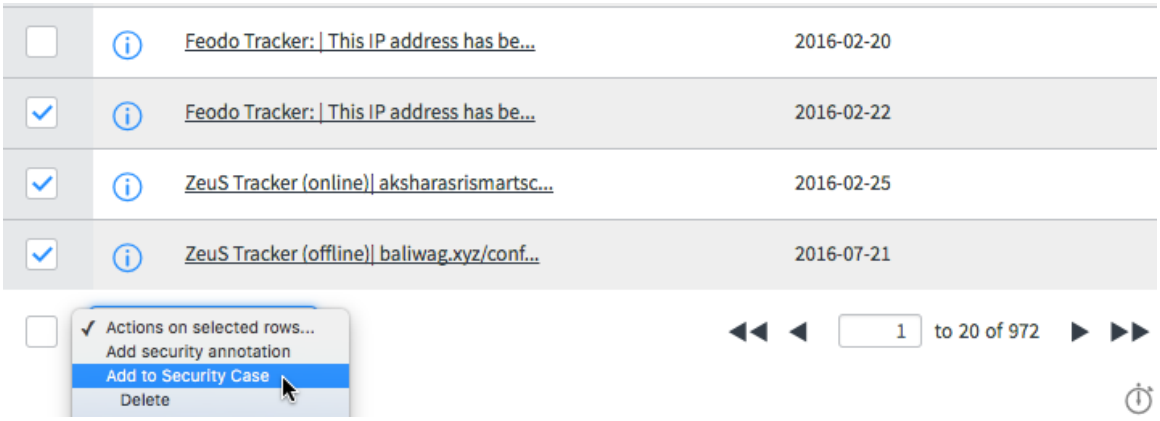
Procedure

1. Navigate to the artifacts (IoCs or observables) you want to use to create a case.
   - To create a case from IoCs, navigate to **Threat Intelligence** > **IoC Repository** > **Indicators**.
   - To create a case from observables, navigate to **Threat Intelligence** > **IoC Repository** > **Observables**.
2. In the list, select the artifacts you want added to a new case.

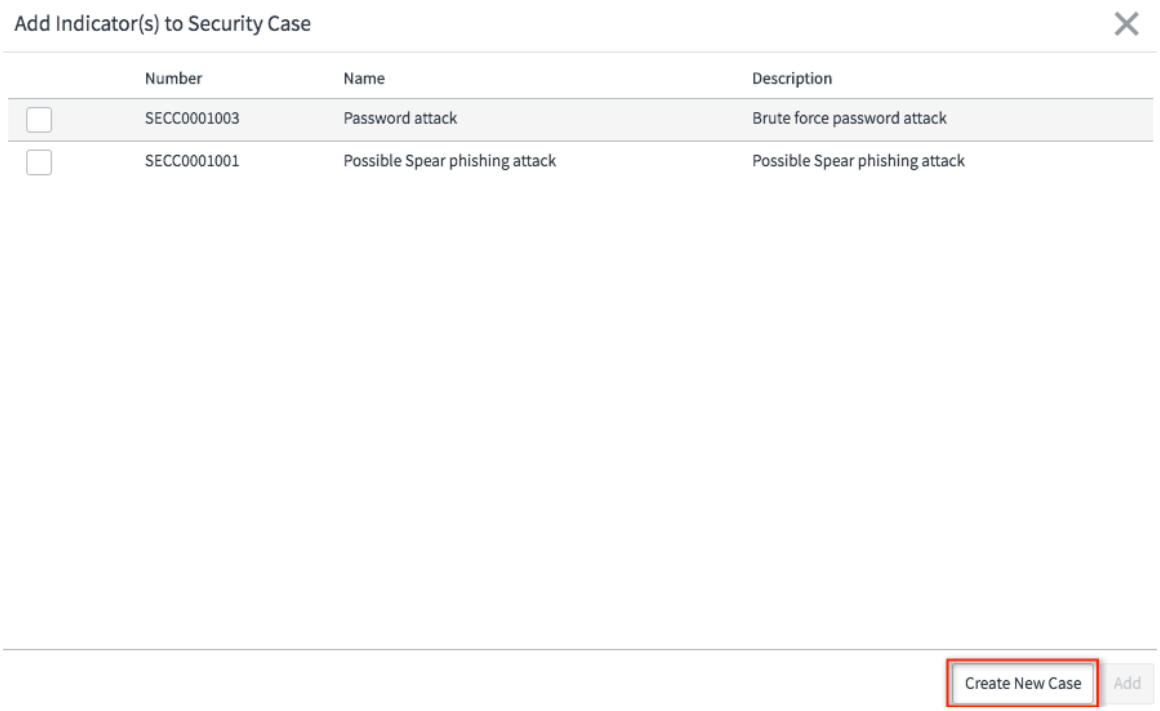
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you select multiple IoCs or observables, they are all added to the case.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.



The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.



4. Click **Create New Case**.
5. Fill in the fields.

Field	Description
Case Name	Enter a name for this case.
Description	Enter a description that would be of value to the case analyst.

6. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.

7. Click the link to view the new case.

Add IoCs and observables to an existing case

You can add IoCs and observables to existing cases. After the security incidents have been added to cases, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

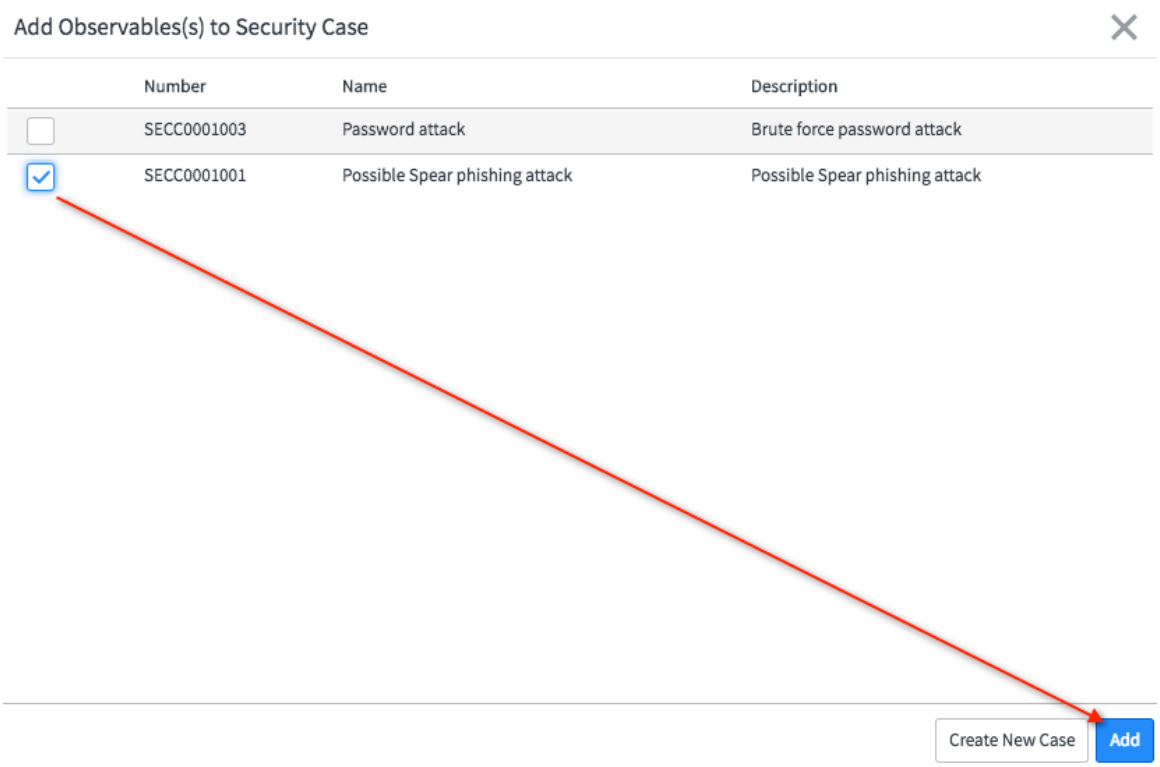
Role required: sn_ti.case_user_write

Procedure

1. Navigate to the artifacts (IoCs or observables) you want to add to existing cases.
   - To add IoCs to one or more cases, navigate to **Threat Intelligence** > **IoC Repository** > **Indicators**.
   - To add observables to one or more cases, navigate to **Threat Intelligence** > **IoC Repository** > **Observables**.
2. In the list, select the artifact records you want added to existing cases.

   Note: If you select multiple cases, the selected IoCs or observables are added to each of the selected cases.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.
   The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.
4. Select the cases into which you want to add the selected IoCs or observables.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Add**.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

Create an observable from a case

New observables can be created from cases in Security Case Management.

Before you begin

Role required: sn_ti.case_user

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Case Management** > **All Cases**.
   The Security Cases list opens.
2. Either open an existing case or click **New** to create a new case.
3. Click the **Case Artifacts** related link and click the **Observables** tab.
4. Click **New** and enter the requested information.

Field	Description
Value	[Read only] The case number.
Observable type	Enter a descriptive name for the case.
Observable type category	Select the type of case being investigated.
Incident count	Select the importance of this case (from Critical to Low).
Finding	[Read only] The date and time the case was last updated.
Notes	A brief description of the case.

5. Click the **Additional Case Details** tab.
6. Fill in the fields as appropriate.

Field	Description
Created by	[Read only] The name of the user who created this case.
State	The current state of the case. At case creation, the State defaults to Draft.
Work notes list	Click the check box to display the work notes in the Additional Case Details section of the case record.
Work Notes	If needed, type a work note for the case. If the **Work notes list** is selected, the work note appears in the Additional Case Details section of the case record.

7. Click **Submit**.
   As needed, you can click the **Case Artifacts** tab and add artifacts to the case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run a sightings search on observables in a case

You can search for observables using the Sighting Search feature to determine how often they occur. Each occurrence is considered a sighting. You can limit the search to the number of sightings within a selected number of days or within a date range.

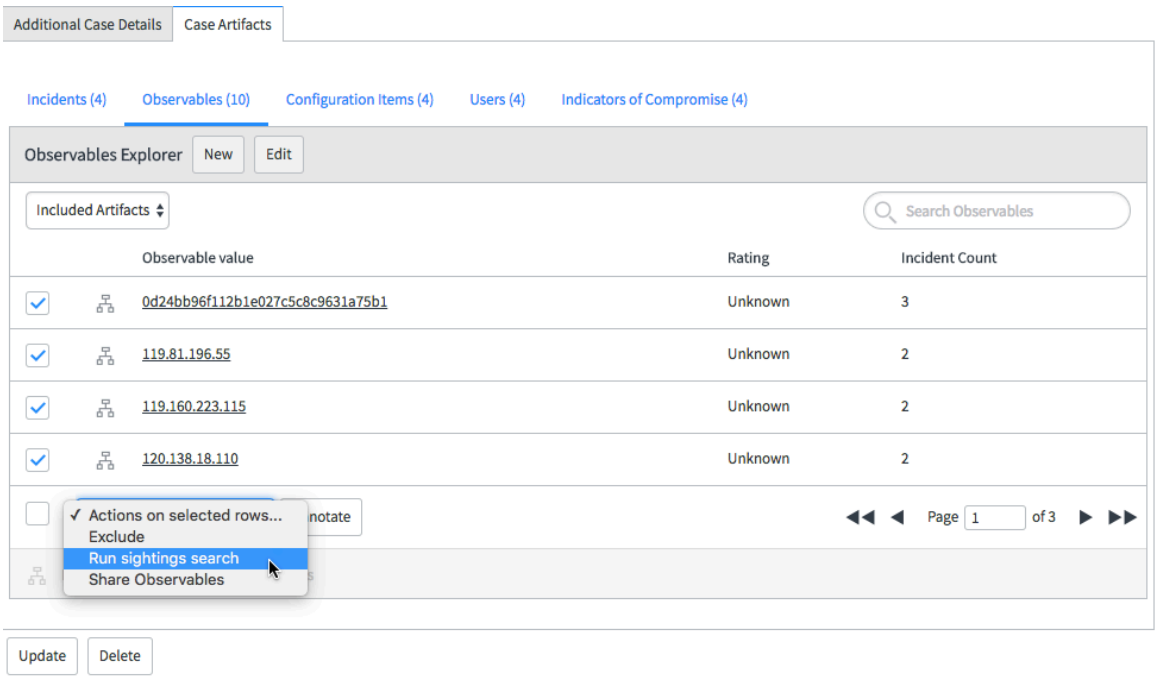
Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

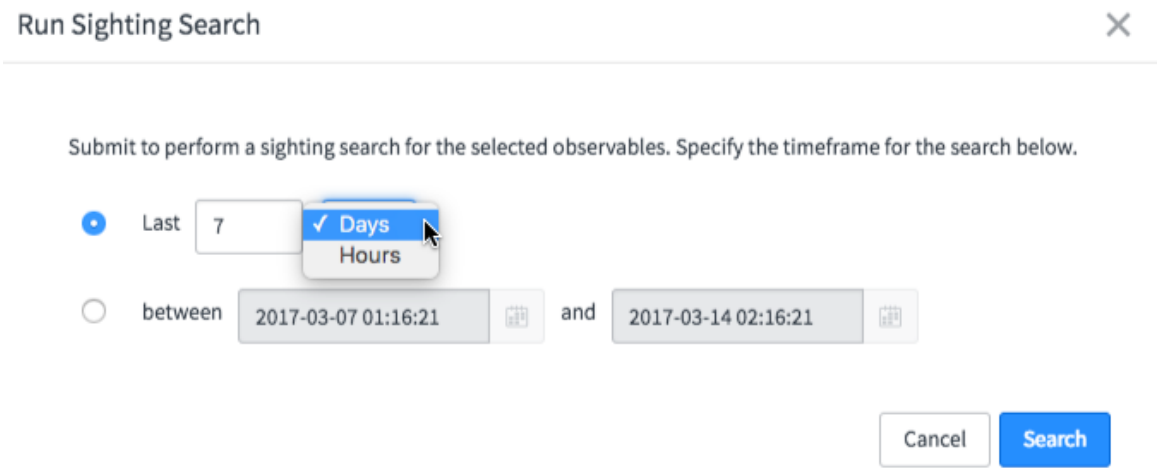
Procedure

1. Navigate to **All** > **Threat Intelligence** > **Case Management** > **All Cases**.
2. Open the case that contains observables for which you want to run a sightings search.
3. Click the **Case Artifacts** related link.
4. Click the **Observables** tab.
5. Select one or more observables for which you want to search for sightings.



6. From the **Actions on selected items** drop-down list, select **Run sightings search**.
   The **Run Sighting Search** dialog box appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Either enter the number of days or hours you want to search for sightings of the selected observables, or select a date range.
8. Click **Search**.

Security incidents in cases

In Security Incident Response, you can create cases from security incidents, CIs, and affected users, as well as add those artifacts to existing cases.

Create a case from security incidents

In Security Incident Response, you can create cases from security incidents. After the security incidents have been used to create a new case, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

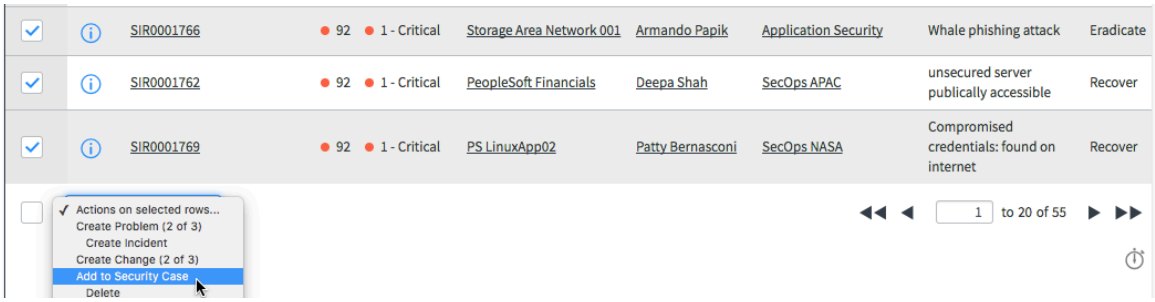
About this task

You need to navigate to the security incidents you want to use to create cases.

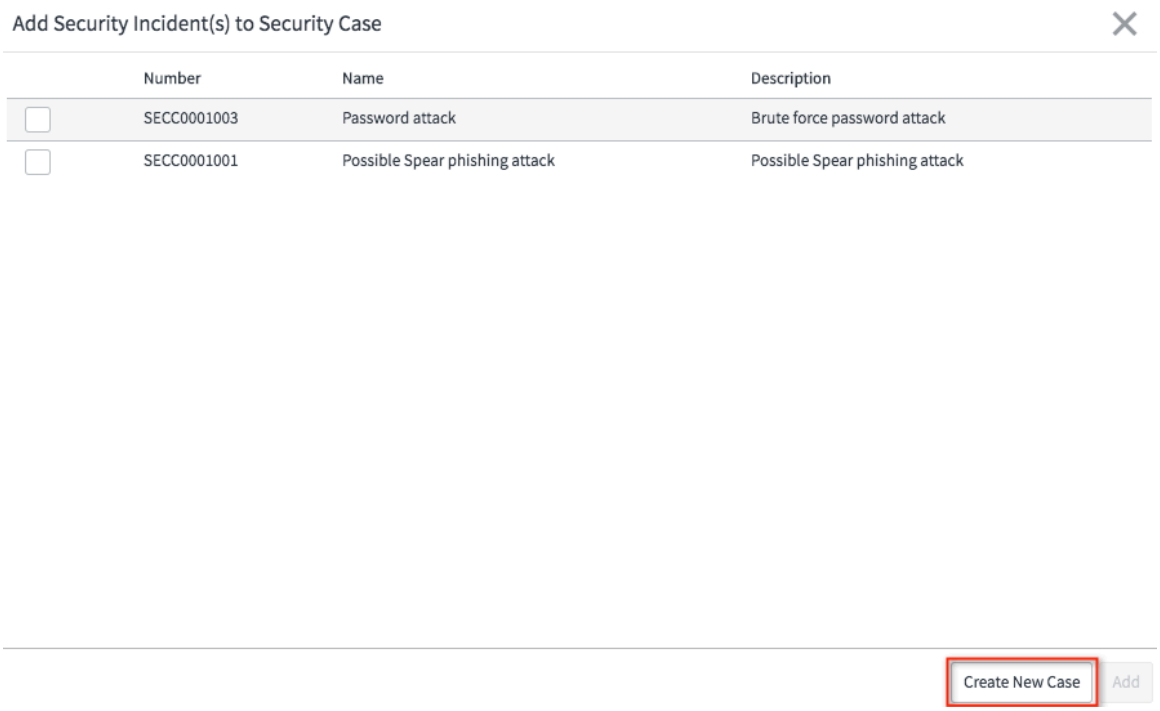
Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show Open Incidents**.
   The Security Incidents list opens. From the list, you can create a new case from one or more security incidents, or you can select a specific security incident and create a new case from the form.
2. To create a case from the list, select the artifacts you want added to a new case.
3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.



4. Click **Create New Case**.
5. Fill in the fields.

Field	Description
Case Name	Enter a name for this case.
Description	Enter a description that would be of value to the case analyst.

6. Click **Submit**.
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.
7. Click the link to view the new case.

Add security incidents to an existing case

You can add security incidents to one or more existing cases. After the security incidents have been added to cases, you can use Security Case Management to analyze the data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

About this task

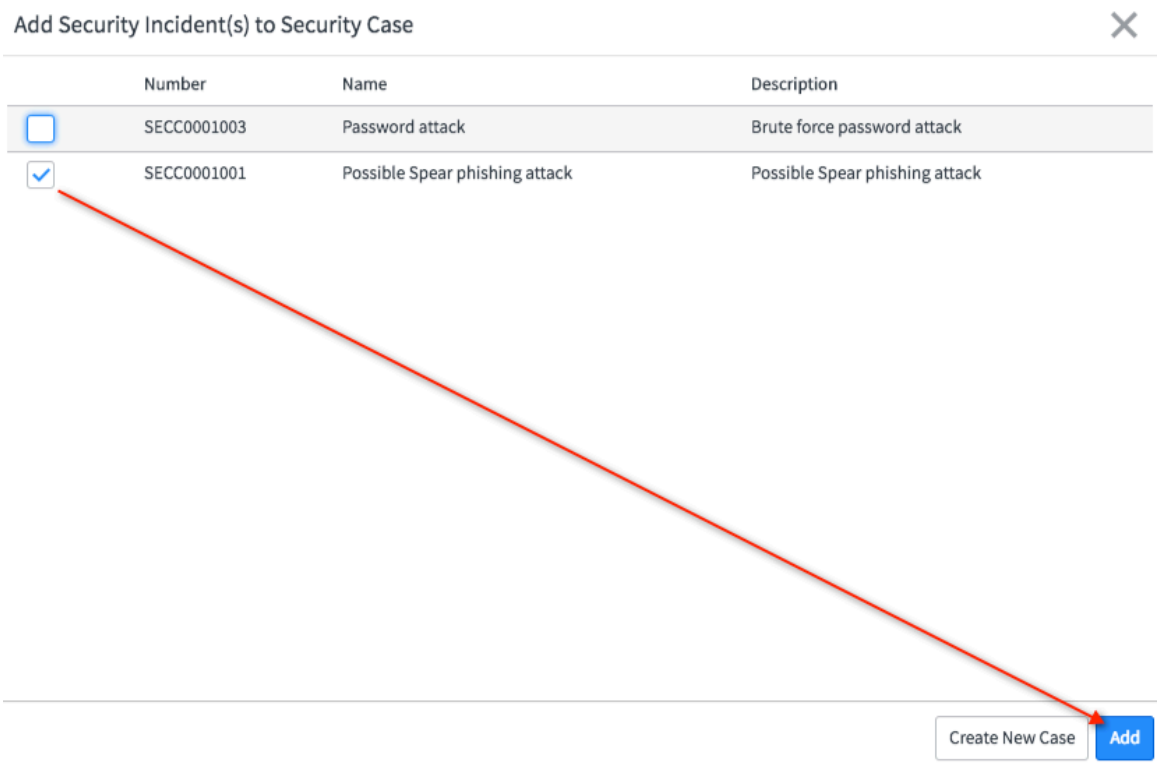
You need to navigate to the security incidents you want to add to existing cases.

Procedure

1. Navigate to **All** > **Security Incident** > **Incidents** > **Show Open Incidents**.
   The Security Incidents list opens.
2. In the list, select one or more security incidents that you want to add to existing cases.

   Note: If you select multiple security incidents, the selected security incidents are added to each of the selected cases.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.
   The **Add to Security Case** dialog box opens and displays the cases assigned to you.



4. Select the cases into which you want to add the selected security incidents.
5. Click **Add**.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

Configuration items in cases

You can create a new case from one or more configuration items (CI) in the Configuration Item [cmdb_ci] table. You can also add CIs to existing cases.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a case from CIs

You can create a security case from configuration items in the Configuration Item [cmdb_ci] table. After the CIs have been used to create a new case, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

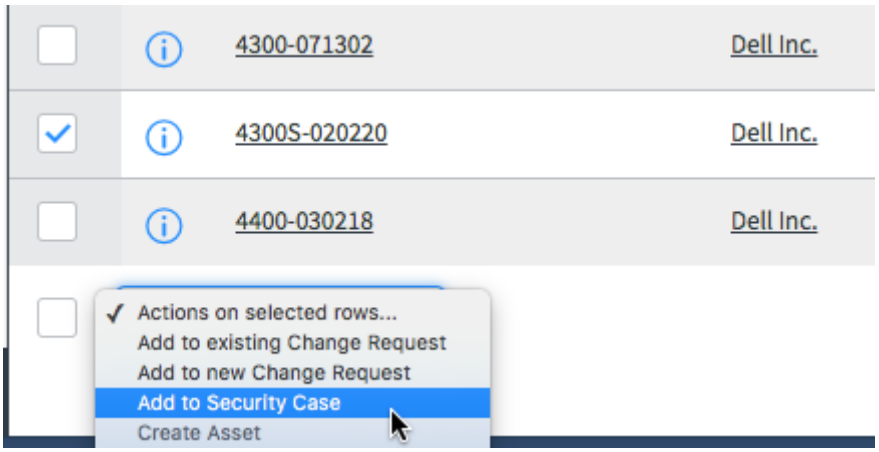
Role required: sn_ti.case_user_write

About this task

You need to navigate to the configuration items you want to use to create a case.

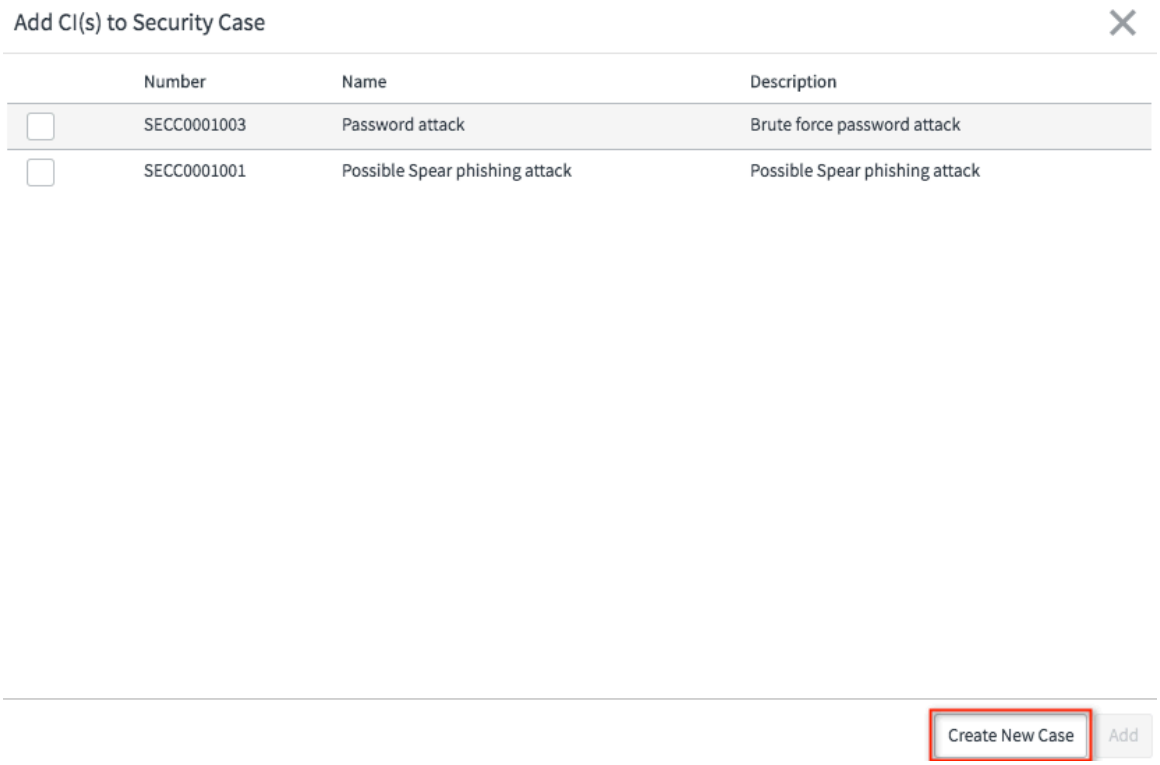
Procedure

1. Navigate to **All** > **Configuration** > **Base Items** > **Computers** to view CIs for computers.
   The list for the selected CI type opens. From the list, you can create a new case from one or more CIs, or you can select a specific CI and create a new case from the form.
2. From the list, select the CIs you want added to a new case.
3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.



The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click **Create New Case**.
5. Fill in the fields.

Field	Description
Case Name	Enter a name for this case.
Description	Enter a description that would be of value to the case analyst.

6. Click **Submit**.
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.
7. Click the link to view the new case.

Add CIs to existing cases

You can add configuration items to one or more existing cases. After the CIs have been added to cases, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

About this task

You need to navigate to the CIs you want to add to the existing cases.

Procedure

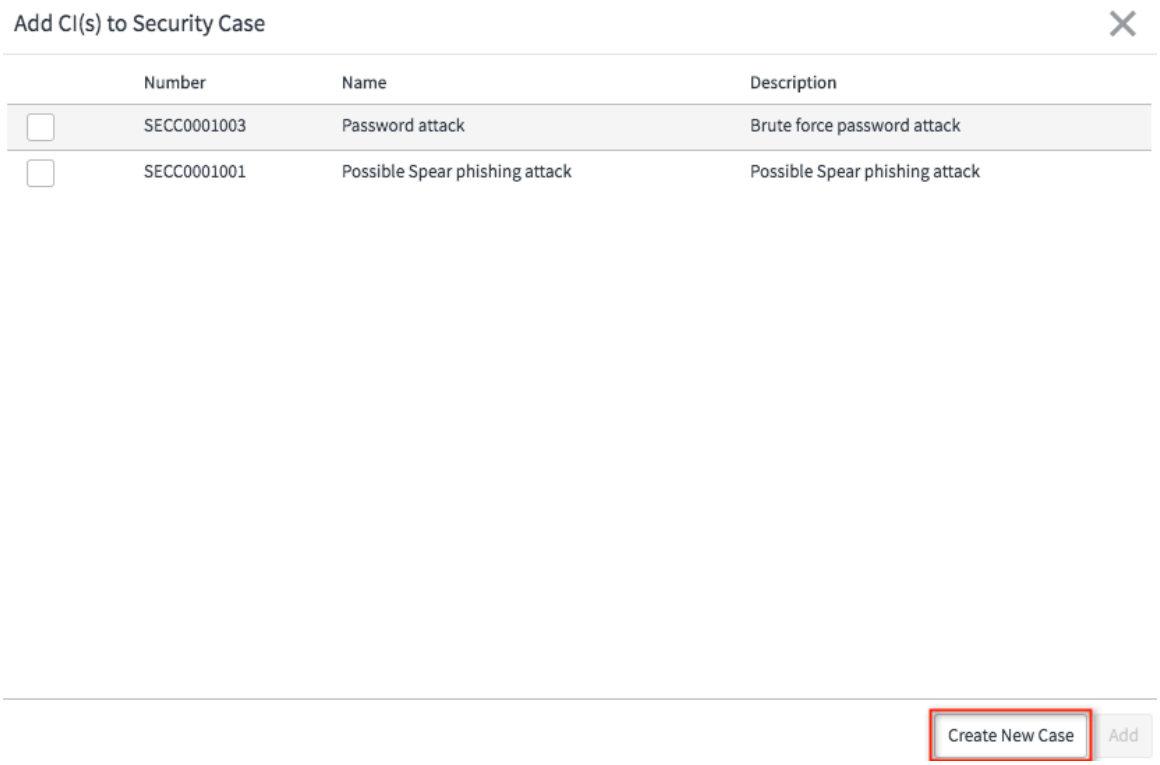
1. Navigate to **All** > **Configuration** > **Base Items** > **Computers** to view CIs for computers.
   The list of the selected CIs opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. In the list, select one or more CIs that you want to add to existing cases.

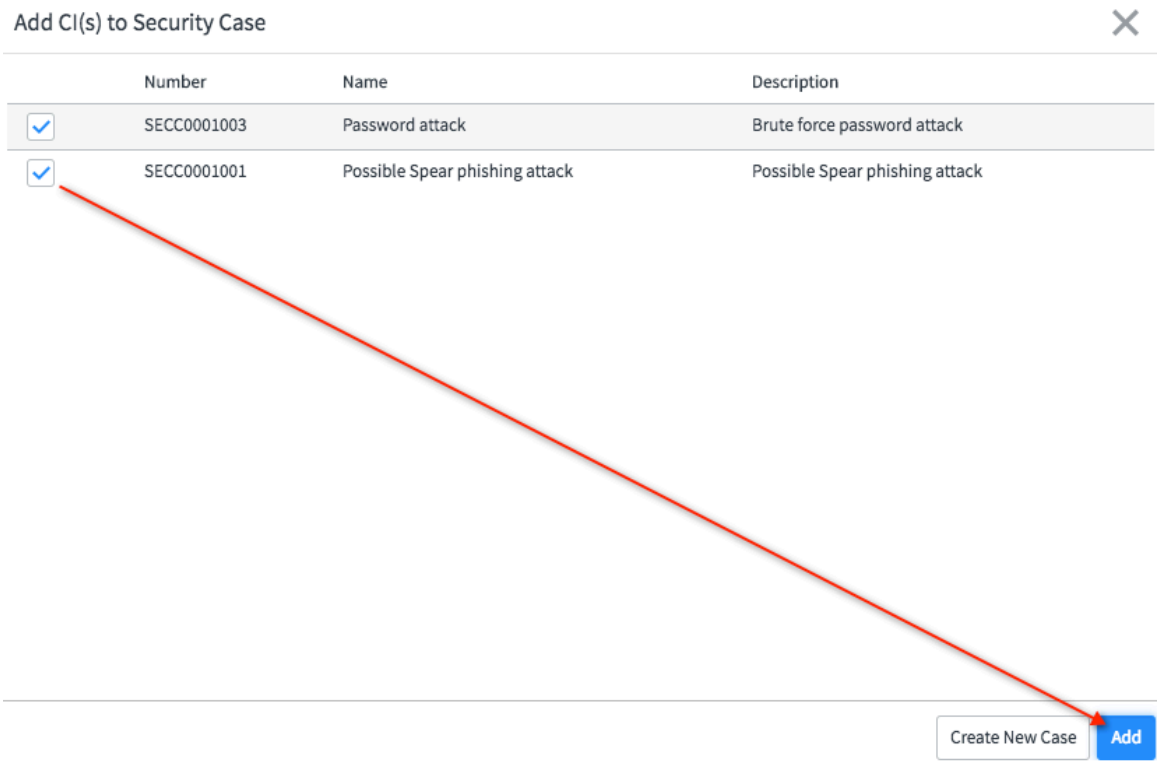
   Note: If you select multiple CIs, the selected CIs are added to each of the selected cases.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.
   The **Add to Security Case** dialog box opens and displays the cases assigned to you.



4. Select the cases into which you want to add the selected CIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Add**.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

Affected users in cases

You can create a new case from one or more affected users in the User [sys_user] table. You can also add users to existing cases.

Create a case from affected users

You can create a security case from affected users in the User [sys_user] table. After the affected users have been used to create a new case, you can use Security Case Management to analyze the data.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

About this task

You need to navigate to the users you want to use to create a case.

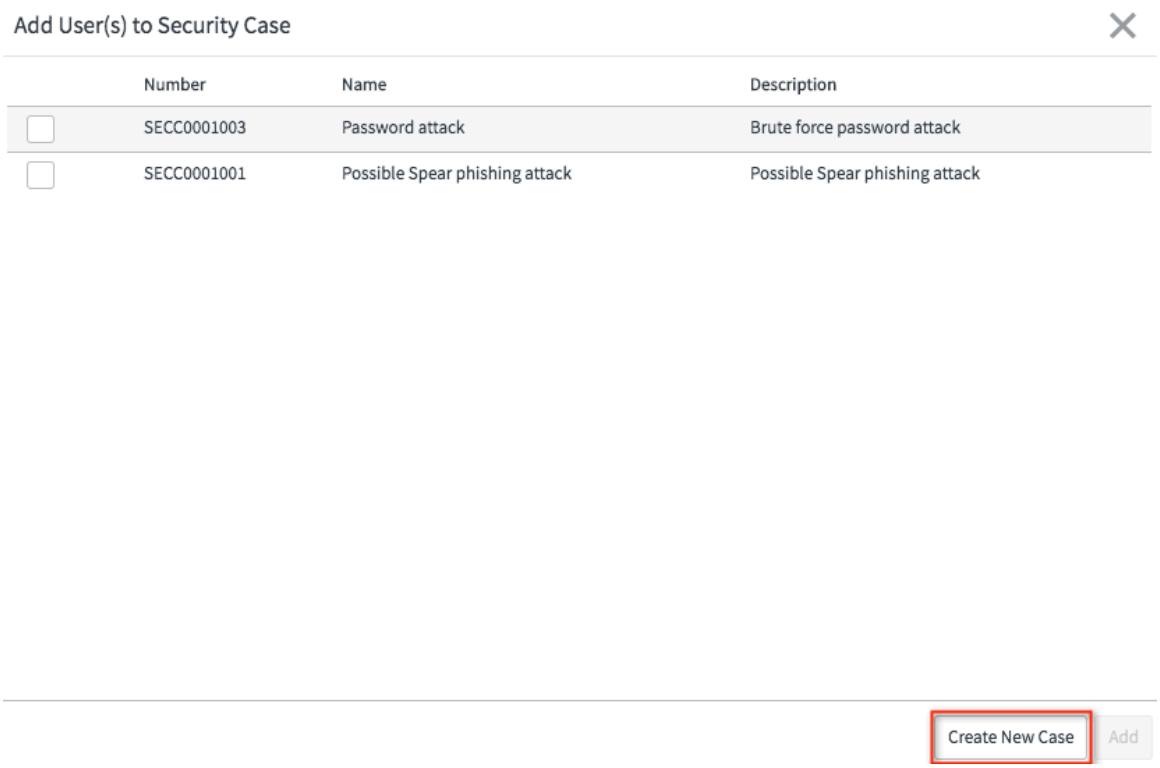
Procedure

1. Navigate to **All** > **User Administration** > **Users**.
   The list for the selected users opens. From the list, you can create a new case from one or more user records, or you can select a specific user record and create a new case from the form.
2. From the list, select the users you want added to a new case.
3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Add to Security Case** dialog box opens. If you already have cases assigned to you, they display in the list.



4. Click **Create New Case**.
5. Fill in the fields.

Field	Description
Case Name	Enter a name for this case.
Description	Enter a description that would be of value to the case analyst.

6. Click **Submit**.
   A message at the top of the list indicates that a new case has been created, along with a link to the case in Security Case Management.
7. Click the link to view the new case.

Add affected users to existing cases

You can add affected users to one or more existing cases. After the user records have been added to cases, you can use Security Case Management to analyze the data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

About this task

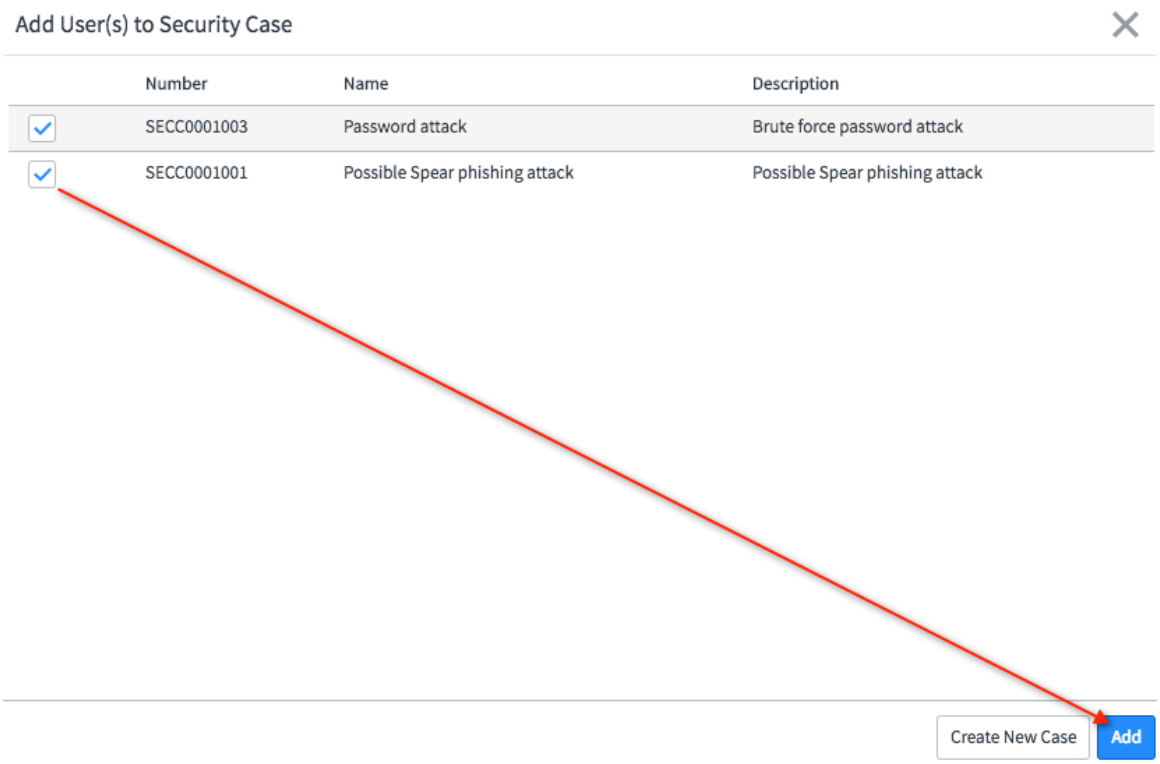
You need to navigate to the user records you want to add to existing cases.

Procedure

1. Navigate to **All** > **User Administration** > **Users**.
   The list of user records opens.
2. In the list, select one or more users that you want to add to existing cases.

   Note: If you select multiple users, the selected user records are added to each of the selected cases.

3. From the **Actions on selected items** drop-down list, select **Add to Security Case**.
   The **Add to Security Case** dialog box opens and displays the cases assigned to you.



4. Select the cases into which you want to add the selected users.
5. Click **Add**.
   A message indicates that the selected records have been added to the cases, along with a link to the cases in Security Case Management.

Security artifact analysis

After you have created cases, either using Security Case Management, or from artifacts such as IoCs, observables, security incidents, and so forth, you can continue to add artifacts to aid in anaysis of the threats identified.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related details for case artifacts

As you add artifacts to a case, additional related details for each artifact may also be automatically added. For example, if you add a security incident, it may contain affected CIs and user records. You can quickly view the related details for a selected artifact without leaving the list of artifacts.

View related details for a security incident artifact

If your case includes security incident artifacts, you can view any related details contained in each security incident referenced by the case.

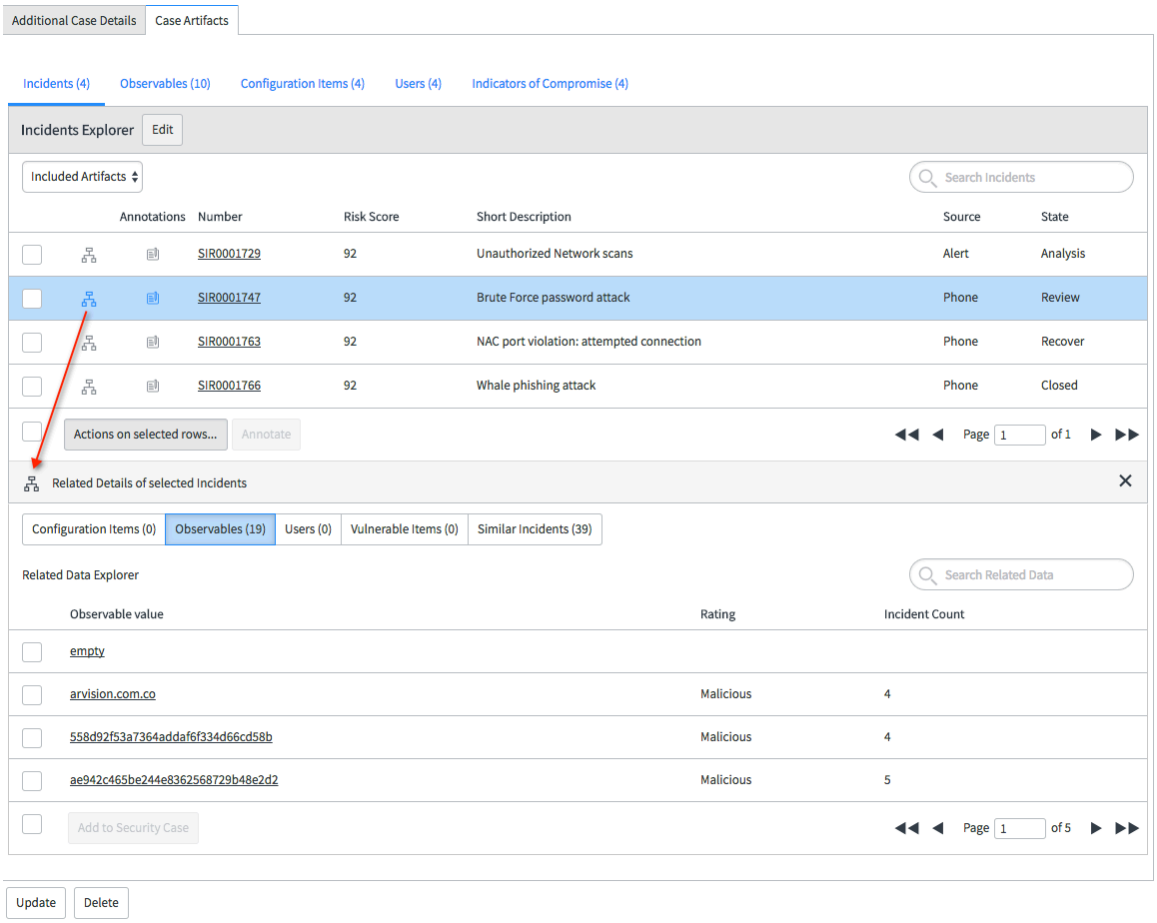
Before you begin

- The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains security incident artifacts.
2. Click the **Incidents** tab.
3. Click the Additional Details icon for the security incident you want to view related details for.



4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View related details for a configuration item artifact

If your case includes configuration item artifacts, you can view any related details contained in each CI referenced by the case.

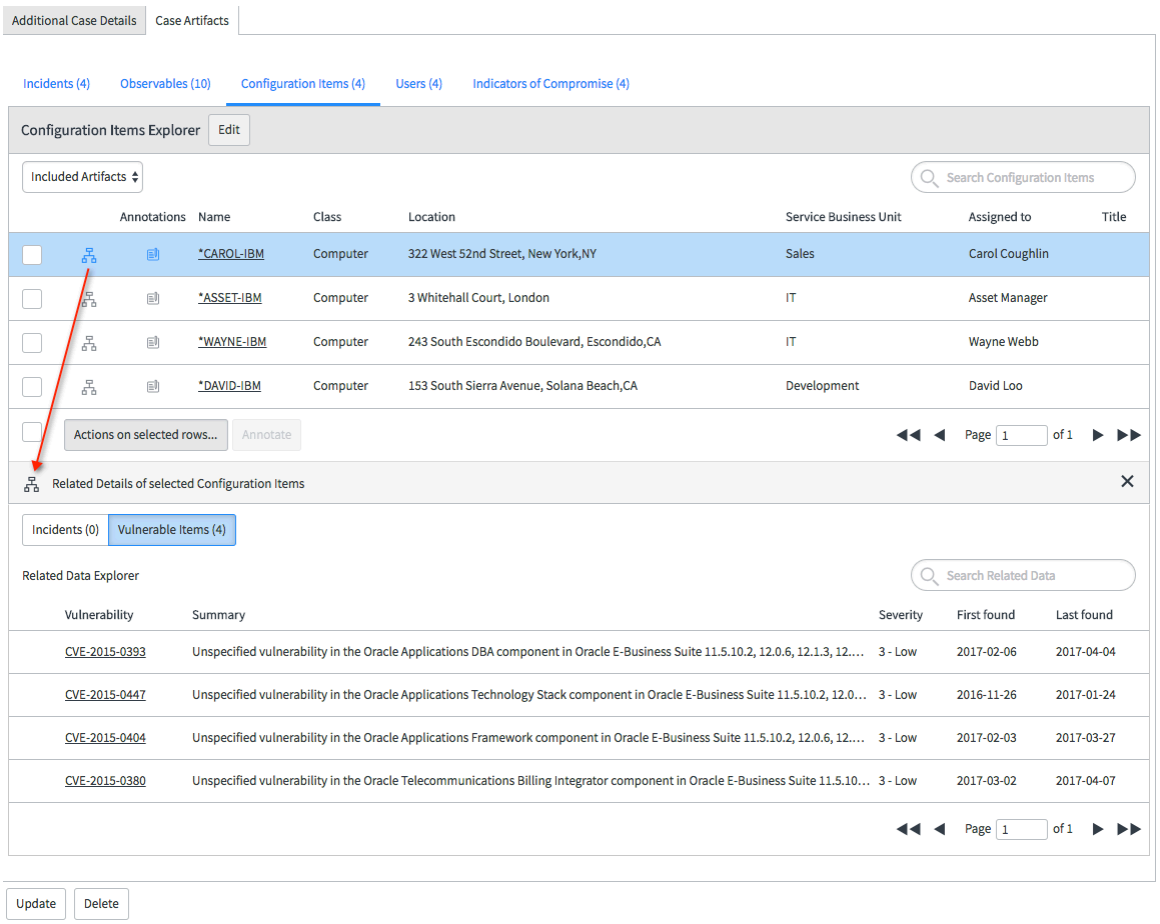
Before you begin

- The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains CI artifacts.
2. Click the **Configuration Items** tab.
3. Click Additional Details for the CI artifact you want to view related details for.



4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click the **Security Annotation** tab to view annotations for the selected artifact.

View related details for an IoC artifact

If your case includes indicators of compromise (IoC) artifacts, you can view any related details contained in each IoC referenced by the case.

Before you begin

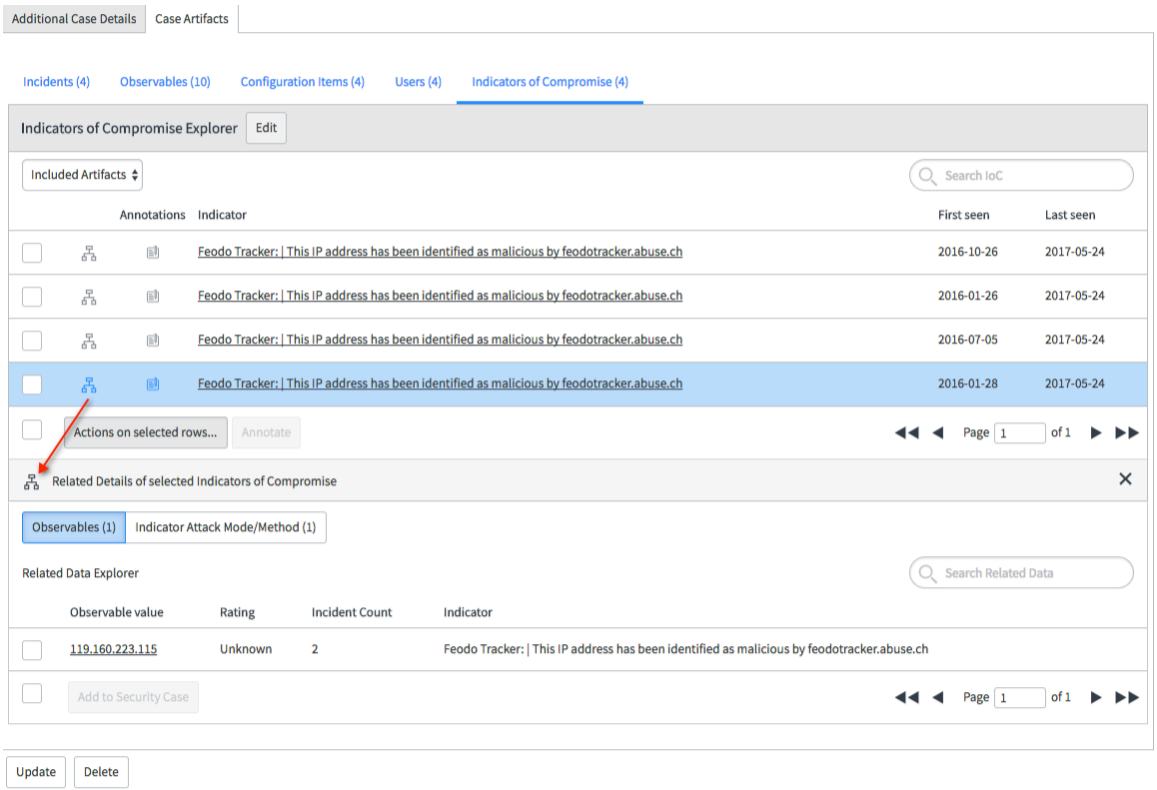
- The Threat Intelligence plugin must be activated to use Security Case Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains IoC artifacts.
2. Click the **Indicators of Compromise** tab.
3. Click Additional Details icon for the IoC artifact you want to view related details for.



4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

View related details for an affected user artifact

If your case includes affected user artifacts, you can view any related details contained in each affected user referenced by the case.

Before you begin

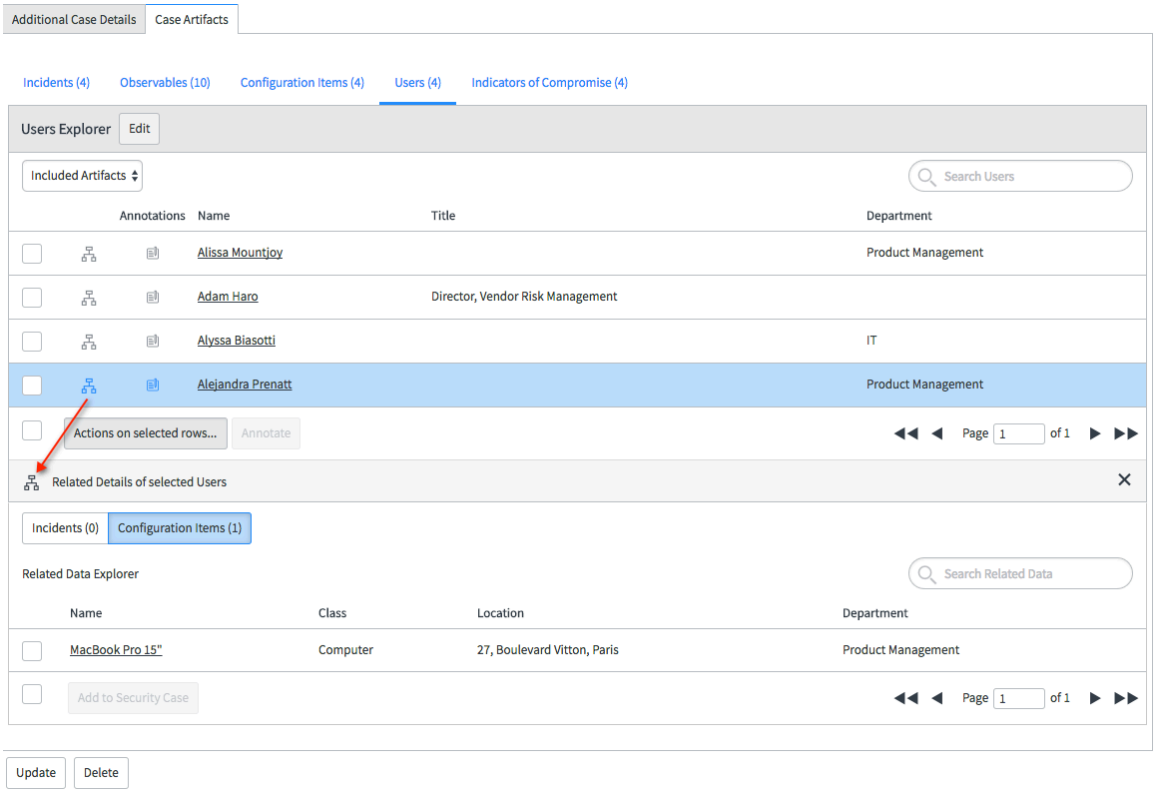
- The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains affected user artifacts.
2. Click the **Users** tab.
3. Click Related Details for the affected user artifact you want to view related details for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

View related details for an observable artifact

If your case includes observable artifacts, you can view any related details contained in each observable referenced by the case.

Before you begin

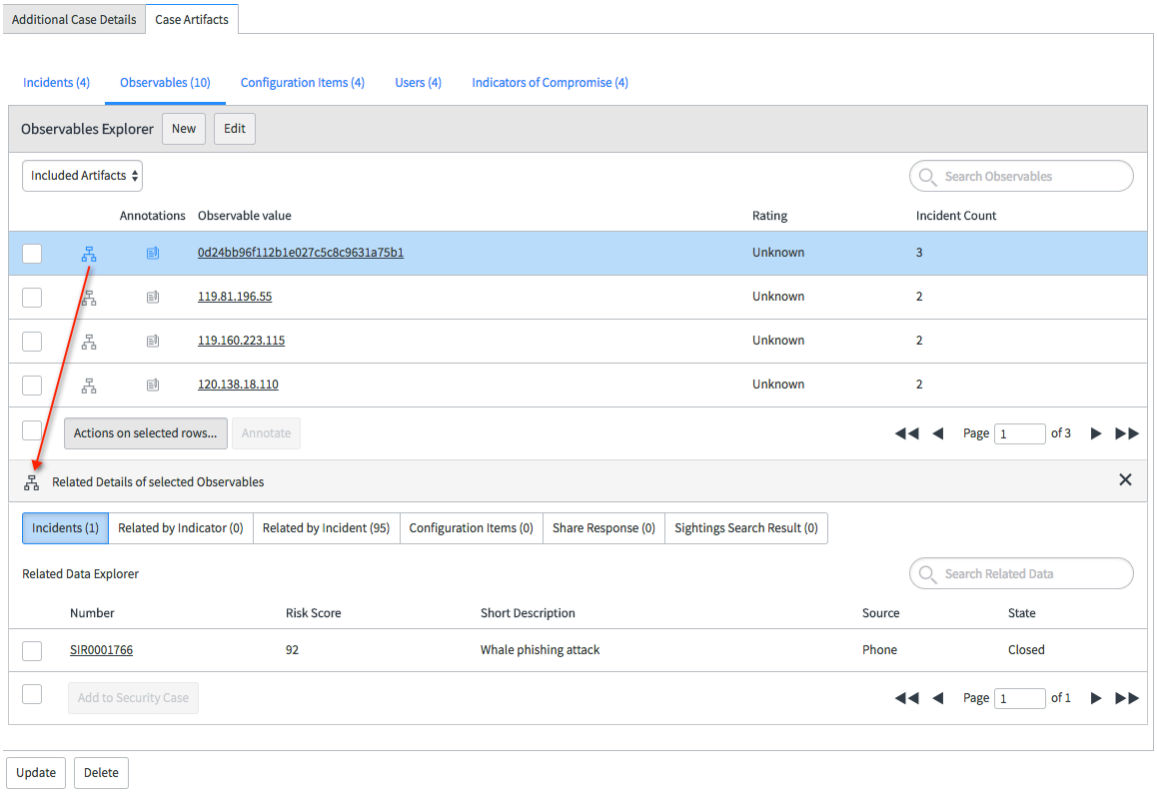
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains observable artifacts.
2. Click the **Observables** tab.
3. Click Additional Details icon for the observable artifact you want to view related details for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click any of the tabs to view specific types of details for the selected artifact.
5. You can also click **Security Annotation** tab to view annotations for the selected artifact.

Security artifact exclusion and inclusion

The lists of supporting artifacts assigned to a case can sometimes get long and there may be instances where you want to remove particular artifacts from a list. Rather than permanently remove the artifacts, you can exclude them from the list and, as needed, return them to the list at a later time.

Exclude security artifacts from a case

You can remove artifacts from the lists of supporting artifacts. They are not permanently removed and can be returned to the case as needed.

Before you begin

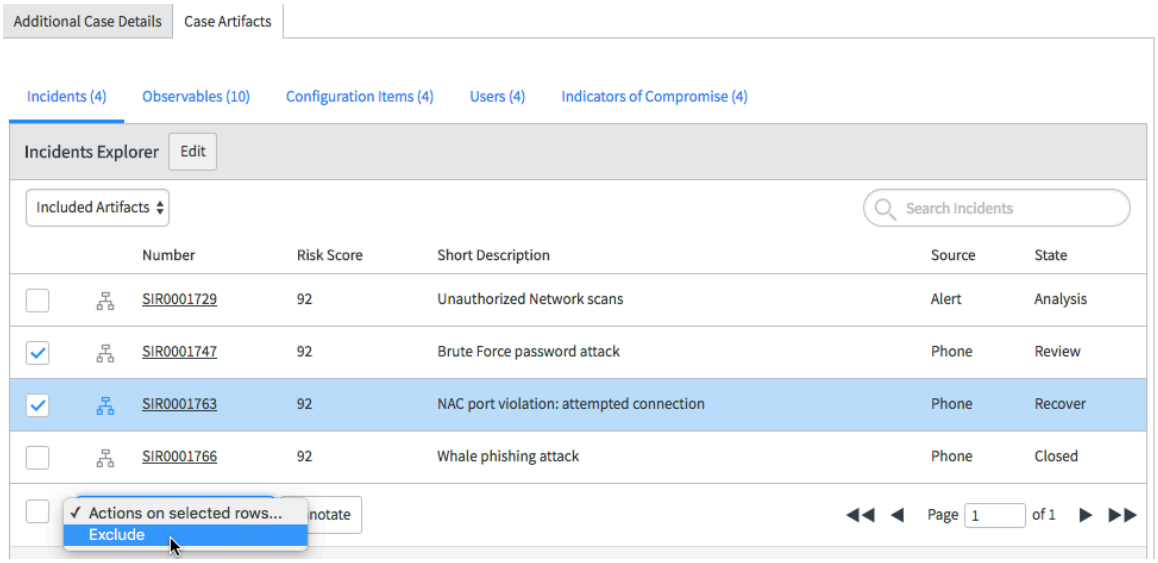
- The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains artifacts that you want to exclude from a list.
2. Click the **Case Artifacts** related list.
3. Click the tab associated with the artifacts you want to exclude.
   For example, click **Incidents** to exclude security incidents from the list.
4. Select one or more artifact records that you want to exclude.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. From the **Actions on selected items** drop-down list, select **Exclude**.
6. Click **Exclude** in the confirmation box.
   The selected artifacts are removed from the list.

Return excluded security artifacts to a case

After you have excluded artifacts from a list in a case, you can return them to the case you can continue to work on them.

Before you begin

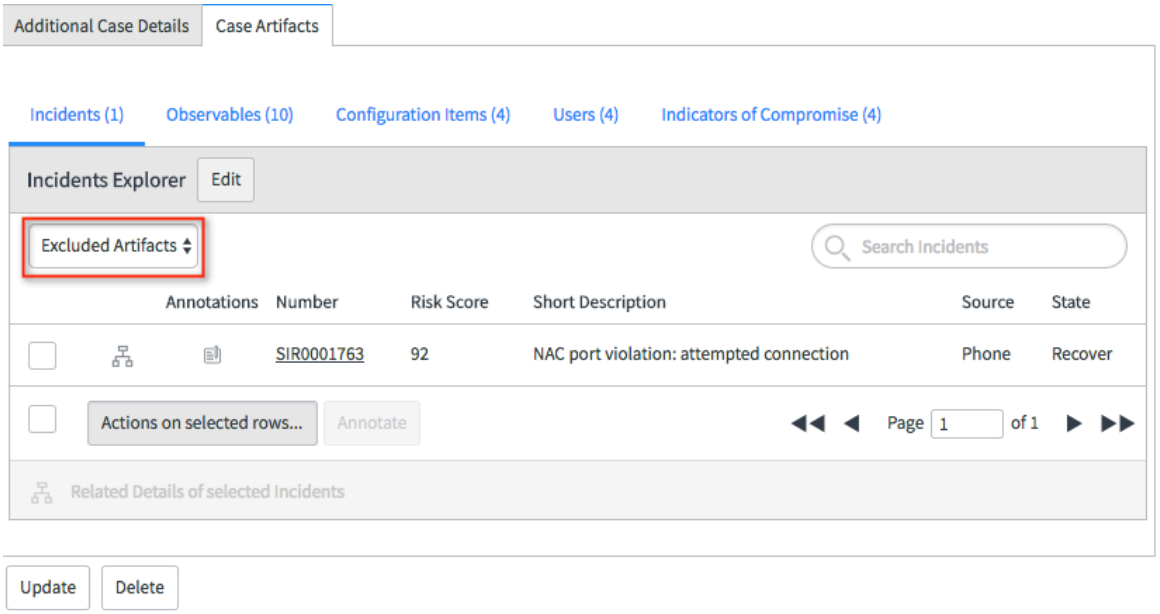
The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

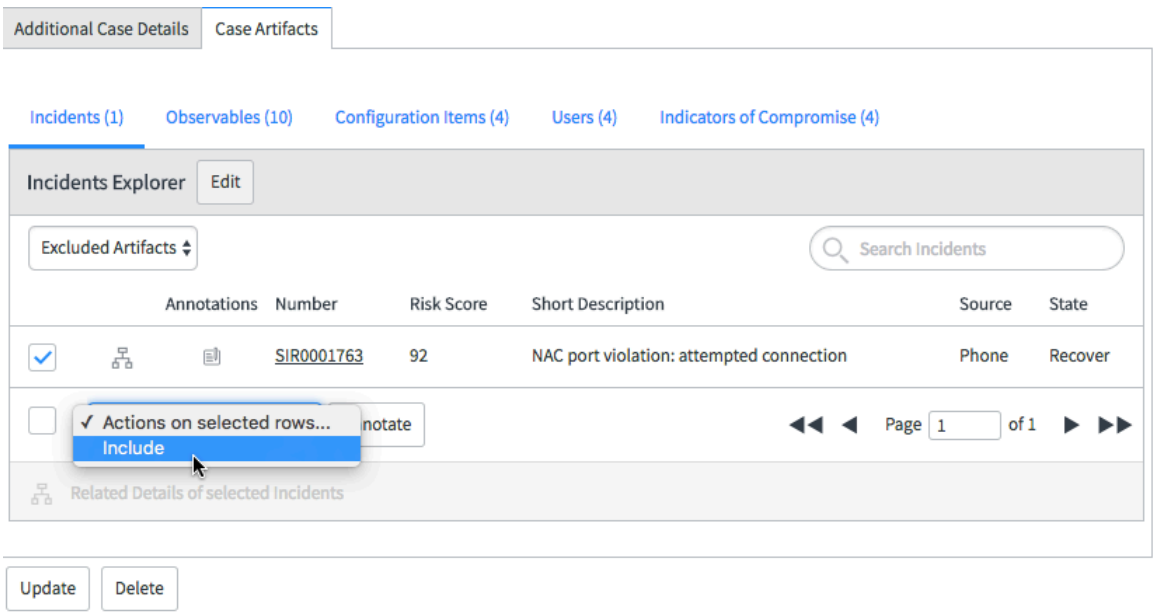
Procedure

1. Open a case that contains artifacts that you previous excluded from a list that you want to return to the list.
2. Click the **Case Artifacts** related list.
3. Click the tab associated with the artifacts you want to return to the list.
4. Click the Artifact Filter drop-down list and select **Excluded Artifacts**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Select one or more artifact records that you want to return to the Include list.
6. From the **Actions on selected items** drop-down list, select **Include**.



7. Click **Include** in the confirmation box.
   The selected artifacts are removed from the list of excluded artifacts and returned to the list of artifacts included in the case.

Annotate security artifacts

As you are analyzing a case, you can add annotations to any artifact.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

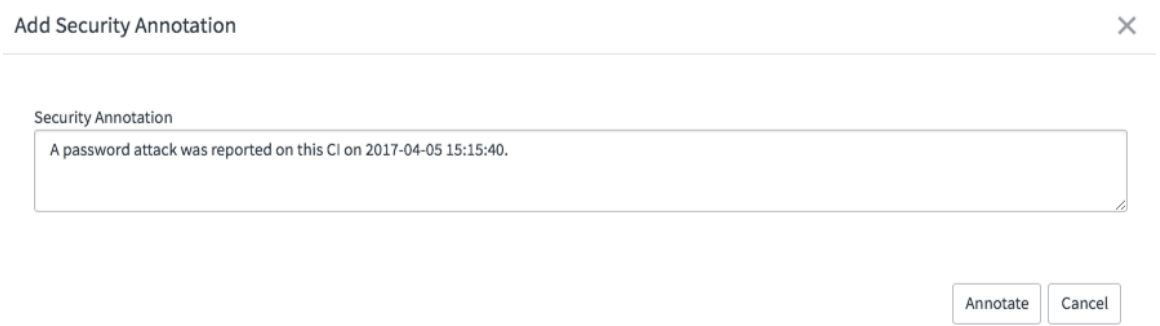
- sn_ti.case_user_write for adding annotations
- sn_ti.case_user_read to view annotations

Procedure

1. Open a case that contains artifacts that you want to annotate.
2. Click the **Case Artifacts** related list.
3. Click the tab associated with the artifacts you want to annotate.
   For example, click **Indicators of Compromise** to add annotations to IoCs.
4. To add an annotation to one or more artifacts, perform the following steps:

   a. Select the artifacts to which you want to add an annotation.

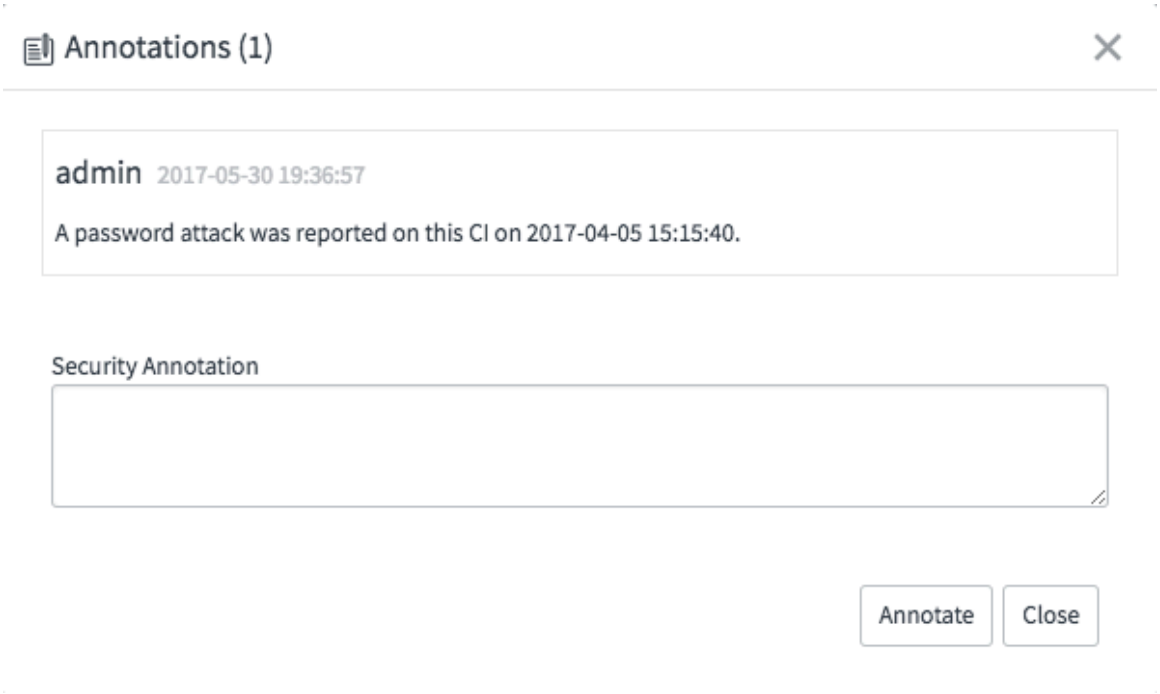
   b. Click **Annotate**.



   c. Type the annotation and click **Annotate**.
   The annotation is added to the selected artifacts.

5. To view annotations for an artifact, click the View annotations ( ) icon.
   The existing annotations appear in the Annotations dialog box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. You can also enter a new annotation for the artifact in the **Security Annotation** box, and click **Annotate**.

Search for security artifacts

You can perform a keyword search on any security artifact list.

Before you begin

The Threat Intelligence plugin must be activated to use Security Case Management.

Role required: sn_ti.case_user_write

Procedure

1. Open a case that contains security artifacts.
2. Click the tab for the security artifacts you want to perform a keyword search on.
3. In the **Keyword search** box, begin to type the name of the artifact you want to locate. When artifacts that match your entry are found, they are displayed.

Security Posture Control

Gain visibility into your enterprise asset inventory and security tool coverage. Use policies provided with the product or create your own to identify assets missing key security tools, such as endpoint protection, configuration management, and vulnerability scanning. Monitor assets for security tool configurations specific to your environment and automate the remediation workflow for security gaps in the Configuration Compliance application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

Explore  Learn about Security Posture Control concepts and features	Install  Install Security Posture Control applications	Integrate  Integrate Service Graph Connectors with Security Posture Control
Use  Learn how to use the workspace to search your assets and identify security gaps	Mitigations Controls Monitoring  Gain insight into which threats to your assets are mitigated by available mitigation controls	Reference  Get details about scenarios that help you identify specific types of tool coverage gaps. See examples of base, child, and cloned policies, and see a list of supported hardware and software service graph connectors.

Troubleshoot and get help

- Security Operations Resource Library
- Security Operations community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Exploring Security Posture Control

Security Posture Control enables cybersecurity teams to get visibility into their complete enterprise asset inventory and determine their overall security posture.

Security analysts gain insights into how well security tools are deployed and covering their assets based on their asset inventory and imported data from service graph connectors and ServiceNow products such as Hardware Asset Management (HAM) and ITOM Discovery.

Security analysts can also create custom policies and configure insights to monitor the compliance of assets with internal security standards. Vulnerability managers can use insights from Security Posture Control (SPC) to prioritize remediation of vulnerabilities on high-risk assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The SPC product is based on Cloud Security Posture Management (CSPM) and Cyber Asset Hygiene Management (CAHM). Security Posture Control consists of two applications that are available by separate subscription from the ServiceNow® Store.

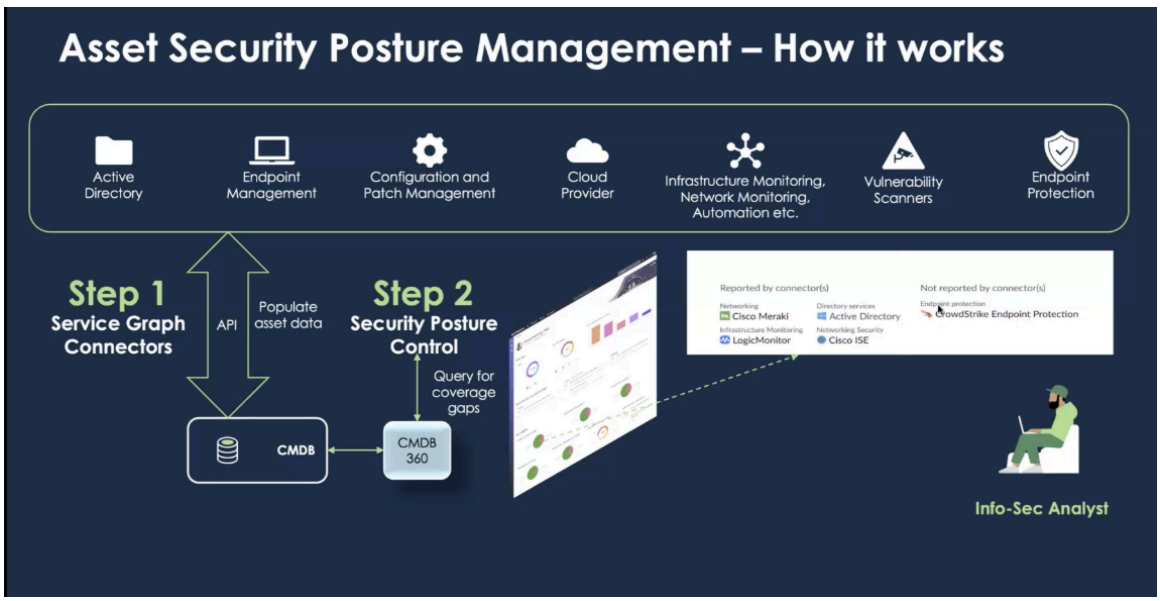
Release version	Release notes
Security Posture Control Core: v6.2, v6.1, v6.0.	For compatibility information, see KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes Security Posture Control release notes
Asset Security Posture Management: v5.3, v5.1, v5.0	
Mitigation Controls Monitoring v4.0, v3.0, v2.0	

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

With the SPC product, Info-Sec teams can perform the following tasks:

- View security posture insights for your on-premise and cloud assets. SPC helps your Info-Sec teams identify assets that are missing endpoint protection, unmanaged assets, assets exposed to the internet, and any high-risk combinations involving vulnerabilities.
- Monitor your assets for their compliance with internal security tool configuration standards. For example, ensure that the latest version of an endpoint protection product is being used.
- Automate your remediation workflow for the security posture gaps you find with the ServiceNow Configuration Compliance application.
- Create custom policies and insights based on asset metadata, security tool coverage data, and vulnerability data.
- Gain insight into which threats to your assets are mitigated by available mitigation controls based on how various security tools are configured with Mitigation Controls Monitoring.

How Asset Security Posture Management works



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Asset Security Posture Management (ASPM) identifies security tool coverage gaps in assets by using API integrations with various third-party tools (Service Graph Connectors) along with ServiceNow products.

ASPM relies on data populated in your CMDB about your assets. The asset data is imported by various categories of monitoring tools and compared to identify any potential security gaps.

For example, say there is asset data populated in the CMDB that is reported by tools that cover infrastructure monitoring and networking tools. However, this data for those same assets is not populated or reported by endpoint protection tools. If you compare the asset data reported by these different tools you can see that there are assets missing an endpoint protection agent.

Asset Security Posture Management identifies security tool coverage gaps in assets by using API integrations with various tools (Service Graph Connectors) and ServiceNow products. Categories include but are not limited to the following:

- Digital Employee Experience
- Discovery
- Endpoint Management
- IT Asset Management
- Infrastructure Monitoring
- Networking
- Network Security
- Network Performance Monitoring
- Configuration and Patch Management
- Endpoint Protection
- Cloud Provider
- Application Performance Monitoring
- Directory Services
- Vulnerability Assessment

The Security Posture Control workflow

Identifying security tool gaps involves the following steps:

1. Set up and activate API connections with any of the tools that you are using in various categories. You can use Service Graph Connectors for products that are available from the ServiceNow Store for the API connections that are required. For more information about the supported service graph connectors, see Service Graph Connectors. Supported service graph connectors are available from the ServiceNow® Store with separate subscriptions.
2. Activate the policies shipped with the Security Posture Control application. The Security Posture Control product finds security tool gaps by performing the following tasks:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Identifies the list of all unique assets populated by various Service Graph Connectors in the CMDB.

b. Identifies assets that are not reported by specific categories from this asset pool, for example, Endpoint Protection. Assets are identified based on the active policy that is being evaluated.

c. Assets identified as not reported by specific categories are reported as 'Findings' or 'Test Results' in the Configuration Compliance application.

3. Automatically assign 'Findings' to different teams for remediation with the Configuration Compliance application.

High-risk combinations

With Asset Security Posture Management, you can also identify assets that have high-risk combinations. An example of a high-risk combination might show assets that are missing security tools, have critical vulnerabilities, and are exposed to the internet.

Some of the policies shipped with the Security Posture Control application look for these high-risk combinations of critical vulnerabilities and security tool coverage gaps. However, for these combination policies to work, you must have the Vulnerability Response application and at least one vulnerability scanner integration product such as Qualys, Rapid7, or the Tenable Vulnerability Integration application installed. These applications are available with separate subscriptions from the ServiceNow Store.

Mitigation Controls Monitoring

From within in the Security Posture Control (SPC) Workspace, gain insight into which threats to your assets are mitigated by available mitigation controls based on how various security tools are configured. See Mitigation Controls Monitoring for more information.

Install the supported applications for Security Posture Control

The applications required for this integration are available on the ServiceNow Store. Some applications have dependencies that you must download and install separately.

Before you begin

Role required: admin for download, installation, and activation of all applications.

Procedure

1. Download the required applications from the ServiceNow Store into your ServiceNow instance.

   The Security Posture Control (SPC Core) application provides the core framework and is required for Asset Security Posture Management (ASPM). The Configuration Compliance application and its dependencies permit you to create remediation tasks for the security control gaps you find using Asset Security Posture Management.

Asset Security Posture Management applications

Application	App ID
Asset Security Posture Management	(Plugin id: sn_sec_caasm)
ITOM Discovery License	(Plugin id: com.snc.itom.discovery.license)
Security Posture Control Core	(Plugin id: sn_sec_spc_core)
Mitigation Controls Monitoring	(Plugin id: sn_sec_mit_ctr)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	App ID
Configuration Compliance (includes child app secops_shared_components)	(Plugin id: sn_vulc)
Vulnerability Response Licensing and Usage	(Plugin id: sn_vul_licensing)

Cloud Security Posture Management applications

Application	App ID
Discovery Plugin	(Plugin id: com.snc.discovery)
Cloud Configuration Governance	(Plugin id: sn_itom_ccg)
CCG Content Pack	(Plugin id: sn_itom_ccg_cp)
CMDB CI Class Models	(Plugin id: sn_cmdb_ci_class)
Cloud Action Library	(Plugin id: com.sn.itom.cal)

Required applications for the SPC Connector Framework

Application	Application ID and version
Security Posture Control API Connectors	sn_spc_cxf v1.0.3
Security Posture Control	sn_sec_spc_core v6.3.2
Asset Security Posture Management	sn_sec_caasm v5.4.1
Mitigation Controls Monitoring	sn_sec_mit_ctrl v4.1.0

Plugin dependencies

Plugin	Plugin ID
ServiceNow IntergationHub Action Template - Data Stream	com.glide.hub.action_type.datastream

See Creating your own API connectors in Security Posture Control for more information.

For more information about downloading and activating applications, see the following topics:

- Download an application from the ServiceNow Store for the first time.
- Activate a ServiceNow Store application.

2. After you have downloaded the applications, navigate to **All** > **System Applications** > **All Available Applications** > **All**.
3. Locate the applications that you downloaded and select **Install** to activate them along with their dependencies.
   Any dependency applications that are also installed automatically along with an application are displayed in the Application installation dialog. However, if you are prompted to install dependency plugins during the installation, follow the prompts provided. Verify you have all the applications and dependencies listed in the previous table installed and activated.

   A dialog is displayed after an application is successfully activated.

   For more information about downloading and installing applications from the ServiceNow Store:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To Opt in to ServiceNow products, follow the steps in Opt in to the ServiceNow Store products.
- To install an application that you have purchased from the ServiceNow Store, follow the steps in Install a ServiceNow Store application.
- Alternatively, if you want to manage your entitlement for the applications on other ServiceNow AI Platform instances, follow the steps in Manage entitlements from your ServiceNow instance.

4. After you have installed and activated the applications, assign users to the following Security Posture Control groups:

   These groups inherit all the roles necessary to read and edit SPC records.

   SPC Admin Group

   Users in this group have full read and write access to all the records for the product, including licensing information. Granular roles for this group include: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin, and sn_sec_spc_core.configure].

   SPC Analyst Group

   Users in this group have full read and write access to all the records for the product but cannot view licensing information. Granular roles for this group include [pa_power_user and sn_sec_spc_core.analyst].

   SPC Analyst Read Only Group

   Users in this group have full read access to all the records for the product but cannot view licensing information. Granular roles for this group include [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read, and cmdb_ms_user].

   Supporting application roles

   The following roles are required by the applications listed in the preceding table that support SPC and Asset Security Posture Management.

   - Configuration Compliance Admin [sn_vulc.admin] - Configures the Configuration Compliance application, has visibility to all records, and can modify properties. Assigns roles in the Configuration Compliance application.
   - Vulnerability Response Admin [sn_vulc.admin] - Configures the Vulnerability Response application and the vulnerability risk calculators.
   - MID Server [mid_server] - Configures a MID Server.

5. Set the glide.identification_engine.multisource_enabled system property to **true**. Security Posture Control relies on data from service graph connectors that is populated in the CMDB 360 Data [cmdb_multisource_data] table. This data is populated only when the glide.identification_engine.multisource_enabled system property is set to true. You must have the cmdb_ms_admin role to modify property values. To set the property, navigate to **All** > **Configuration** > **CMDB 360 Properties**.
6. **Optional:** Set the **ignoreCIClass** [sn_sec_cmn.ignoreCIClass] system property to ignore some configuration item (CI) classes when running CI Lookup Rules.

   (Optional) As an SPC Admin and SPC Analyst, you might need to ignore certain hardware or virtual classes so that you do not ingest information about assets you do not want to control. See Create a Vulnerability Response CI lookup rule and Ignore CI classes for more information.

7. Modify reconcilation and recompute CMDB data sources to set the source of truth for attribute values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The CMDB 360 dashboard provides aggregations and analysis of CMDB 360 data. CMDB 360 collects data about all the discovery sources reporting attribute values for CIs. Use the CMDB 360 view in Configuration Management Database (CMDB) Workspace to track activities and identify potential issues of discovery sources. See CMDB 360 view in CMDB Workspace for more information.

Service Graph Connectors for Security Posture Control

Security Posture Control relies on API integrations or Service Graph Connectors as a key source for the asset data used to identify security gaps.

Security Posture Control currently supports service graph connectors (SGC)s that can provide you with a wide variety of data about your assets. These integration applications are available from the ServiceNow Store.

Choose the connectors you want to use and download the applications and activate them. The list of supported connectors in the Store will grow as Security Posture Control supports more connectors.

To take full advantage of Security Posture Control features, you might want to download and activate the following Service Graph Connector products to support the categories listed below.

Service graph connectors supported by Security Posture Control currently include the following categories:

- Digital Employee Experience
- Discovery
- Endpoint Management: Microsoft Intune or Jamf Device and Endpoint Management.
- IT Asset Management
- Infrastructure Monitoring
- Networking
- Network Security
- Network Performance Monitoring
- Configuration and Patch Management: Microsoft SCCM or IBM Bigfix.
- Endpoint Protection: CrowdStrike or SentinelOne.
- Cloud Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

> **Note:** If Cloud Discovery is activated, these service graph connector products are not required.

- Application Performance Monitoring
- Directory Services (Active Directory) Microsoft Active Directory
- Vulnerability Assessment: Qualys, Rapid7, or Tenable.

After you install them, you can view the connectors and their categories on the connector table [sn_sec_spc_core_connector] in your instance.

You can view Asset types and how they map to CI classes and Connectors on the [sn_sec_spc_core_asset_type_connector] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Supported hardware service graph connectors for Security Posture Control and Supported software service graph connectors for Security Posture Control for more information and examples of these tables. Although not extensive lists, you can see how the supported connectors provide a wide variety of data.

Security Posture Control supports ServiceNow products such as Software Asset Management (SAM) and Hardware Asset Management (HAM) that you can use along with service graph connectors to help you to look for any discrepancies that exist between the installed software reported by your vulnerability scanner products and the software reported by scanners that is already accounted for in SAM and other ServiceNow products.

For more information about downloading, configuring, and activating supported applications for service graph connectors, see the following topics:

- Service Graph Connectors .
- Download an application from the ServiceNow Store for the first time.
- Activate a ServiceNow Store application.

Policies for Security Posture Control

Policies audit your assets based on data imported from your service graph connectors to help you find potential violations.

Policies

Security Posture Control policies are built on an asset-relationships-properties data model. There are policies that are included with the application, and you can create your own policies to look for specific criteria.

The criteria for policies can be specified either in the form of conditions on that asset's properties or on a related entity's properties. From the policy builder in the Policy and findings module in the workspace, you can define policies to look for an asset type (Hardware, Software) and a Connection (Reported by, Not reported by), or an Entity (Asset source, service graph connector product, or CMDB Metadata), or you can match other types of specific criteria.

To help you with modifying or creating policies:

- Set your conditions in the Asset search module and search for assets by specific service graph connector products or for assets that have specific data reported by a connector. You can save your searches as policies.
- Clone the policies that are included with the application to create more expansive policies. You copy and then refine an existing policy's conditions without having to re-enter them.
- Create new policies (child policies) using base policies you select as a starting point for new policies.

Asset types and policies

You use these primary, or top-level asset types as a starting point for defining policies.

Hardware Asset

Hardware Asset is an abstraction that represents any device that includes personal computing devices, servers, network devices, cloud virtual machines, and other hardware. Policies audit your assets for potential violations based on the imported data from service graph connector products and ServiceNow® products such as Software Asset Management (SAM) and ITOM Discovery.

Software Asset

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Software Asset permits you to look for any discrepancies that exist between the installed software reported by imported data from service graph connectors, your vulnerability scanner products, and the software reported by scanners that is already accounted for in Software Asset Management (SAM) and other ServiceNow products.

Entities and their relationships to secondary entities

Entity	Relationship	Target entity	Description
Hardware Asset	Reported by	Asset Source	Represents a source that reported this asset into CMDB.
Hardware Asset	Reported only by	Asset Source	Represents the only source reporting this asset into CMDB.
Hardware Asset	Not reported by	Asset Source	Represents a source that did not report this asset into CMDB.
Hardware Asset	With IRM Exception	IRM Exception	Represents an exception record in Integrated Risk Management.
Hardware Asset	With vulnerability	Vulnerability	Represents a vulnerability found on this asset.
Hardware Asset	Has configuration finding	Configuration	Represents a configuration and a compliance issue found on this asset.
Hardware Asset	With CMDB metadata	CMDB Metadata	Represents the collection of CMDB CI properties on this asset.
Hardware Asset	With connector data	Service Graph Connector	Represents collection of properties reported by selected service graph connector for this asset.
Hardware Asset	With aggregated data	Aggregated data	Collection of properties with aggregated values reported by different sources for a given asset. An example is OS.
Hardware Asset	From CI Class	CMDB CI Class	Used for defining conditions on specific CI class properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Entities and their relationships to secondary entities (continued)

Entity	Relationship	Target entity	Description
Hardware Asset	Has cloud metadata	Cloud Metadata	Represents cloud metadata (applicable for cloud VMs).
Hardware Asset	Has port exposed to internet	OpenPort	Represents a port open to the internet (applicable for cloud VMs).
Software	Reported by	Asset Source	Represents a source that reported this software.
Software	Reported only by	Asset Source	Represents the only source reporting this software.
Software	Not reported by	Asset Source	Represents a source that did not report this software.
Software	With software details	Software	Represents the collection of software properties such as publisher and version, for example.

Example policy audit and data population: CI classes in the CMDB

If a policy tries to retrieve an asset class that is reported or not-reported by a specific Service Graph Connector, Security Posture Control maps all the relevant configuration item (CI) classes that are related to that asset class in the CMDB that are populated or not-populated by that Service Graph Connector or connector Category.

For example, say a policy looks for all the hardware assets that are reported by the Service Graph Connector Jamf Pro. The following logic applies.

1. Security Posture Control identifies which CI classes in the CMDB are mapped to the class 'Hardware Asset' for Jamf Pro.

   Note: Different Service Graph Connectors populate different CI classes in the CMDB, and the mapping to CI classes from 'Hardware Asset' varies from one Service Graph Connector to another.

2. Security Posture Control determines that the CI classes, Computer, Server, and Printer in the CMDB are mapped to the ‘Hardware Asset’ asset class for the Service Graph Connector Jamf Pro.
3. Security Posture Control then queries for any asset records populated in any of these three CI classes: Server, Computer, and Printer by the Jamf Pro Service Graph Connector in the CMDB and returns those assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The 'CI classes supported by SPC' column in the following table indicates which classes of CI records are considered during a query by the Security Posture Control product as part of a policy evaluation. This table is not a comprehensive list, but you can use it to see how ingested data from various categories and sources is generally mapped and queried.

Policies included with the application

Activate the asset profiles and policies in the Security Posture Control workspace that are Included with the application so that you can identify gaps in configuration or coverage for security tools.

Creating your own policies

See Creating your own policies in the Security Posture Control application for more information about how to create your own policies.

For example policies, see Examples of base, child, and cloned policies for Security Posture Control.

See Create and activate custom policies for Security Posture Control for more information about the steps required to create a policy.

Supported SGCs

For a list of some of the supported service graph connectors, see Supported hardware service graph connectors for Security Posture Control and Supported software service graph connectors for Security Posture Control.

Mitigation Controls policies

From within in the Security Posture Control (SPC) Workspace, gain insight into which threats to your assets are mitigated by available mitigation controls based on how various security tools are configured. See Mitigation controls policies for more information.

Policies included with the Security Posture Control application

There are a few policies that are included with the Security Posture Control application that are tied to important use cases and are ultimately shown as key insights on the dashboard on the landing page (Home module) in the SPC Workspace.

Viewing policies

To view these policies, navigate to **Workspaces** > **Security Posture Control** > **Policies and findings** > **All**.

These policies are deactivated by default. You must activate them before you can view returned results (Findings). You cannot edit these policies, but you can use them to help you create other policies by cloning their conditions as a starting point. See Clone a policy or create a child policy in Security Posture Control for more information.

You can clone these policies to create your own custom policies but note that any policies you clone are not reflected as key insights on the dashboard on the Home landing page with the key insights that are included with the application. However, you can configure findings for these cloned policies and see the returned results from these policies.

You can configure custom insights or reports for the cloned policies, or, alternatively configure findings for these cloned policies to manage remediation. You can also create your own custom policies from scratch to monitor security controls coverage as per your internal requirements.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The policies shipped with the application include the following categories:

- Policies that monitor security controls coverage (endpoint protection and vulnerability scanner).
- Policies that identify unmanaged devices.
- Policies that monitor toxic combinations that involve critical combinations such as missing security controls, internet exposure, and so on.
- Policies for SPC API Integrations for Mitigation Controls Monitoring.

After you clone and activate any policies you create, you must create your own custom insight record on the Custom insight builder module in the workspace (the last module in the navigator panel). Only then can you view the data from your policies on the Custom insights dashboard (the second icon from the top in the workspace).

Policies and asset profiles included with the application

Get insights into your overall security posture and configuration gaps in your security tools using the policies and asset profiles that are included with the application. Activate these asset profiles and policies in the Security Posture Control workspace so that you can identify gaps in configuration or coverage of the following tools:

- CrowdStrike
- Microsoft Intune, Defender, and SCCM
- HCL Big Fix
- Qualys
- Rapid7

Creating your own policies

See Creating your own policies in the Security Posture Control application for more information about how to create your own policies.

For example policies, see Examples of base, child, and cloned policies for Security Posture Control.

See Create and activate custom policies for Security Posture Control for more information about the steps required to create a policy.

See Mitigation controls policies for more information for more information about policies used for mitigation controls monitoring.

Creating your own policies in the Security Posture Control application

You can create your own custom policies to monitor data that is specific to the assets in your environment. You base these policies on data you will import from the various Service Graph Connectors you have installed and activated.

How to start

You can clone existing policies and add more conditions to them or create a policy from scratch. For your custom policies, you can include criteria for common CMDB properties populated by various Service Graph Connectors.

Alternatively, you can use a base policy as a starting point and include conditions for approved exceptions with polices for the Governance, Risk, and Compliance (GRC) application, for

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

example. These exceptions are for assets that you don't want to monitor and include in your asset counts.

For your custom policies, you can include conditions for metadata such as OS, OS version, and FQDN, for example to help you monitor assets with older software. Note that these properties are common CMDB properties populated by various Service Graph Connectors for any given asset.

See Policies included with the Security Posture Control application for more information about top-level Asset Types and their relationships in the policy condition builder for you policies.

For example policies, see Examples of base, child, and cloned policies for Security Posture Control.

See Create and activate custom policies for Security Posture Control for more information about the steps required to create a policy.

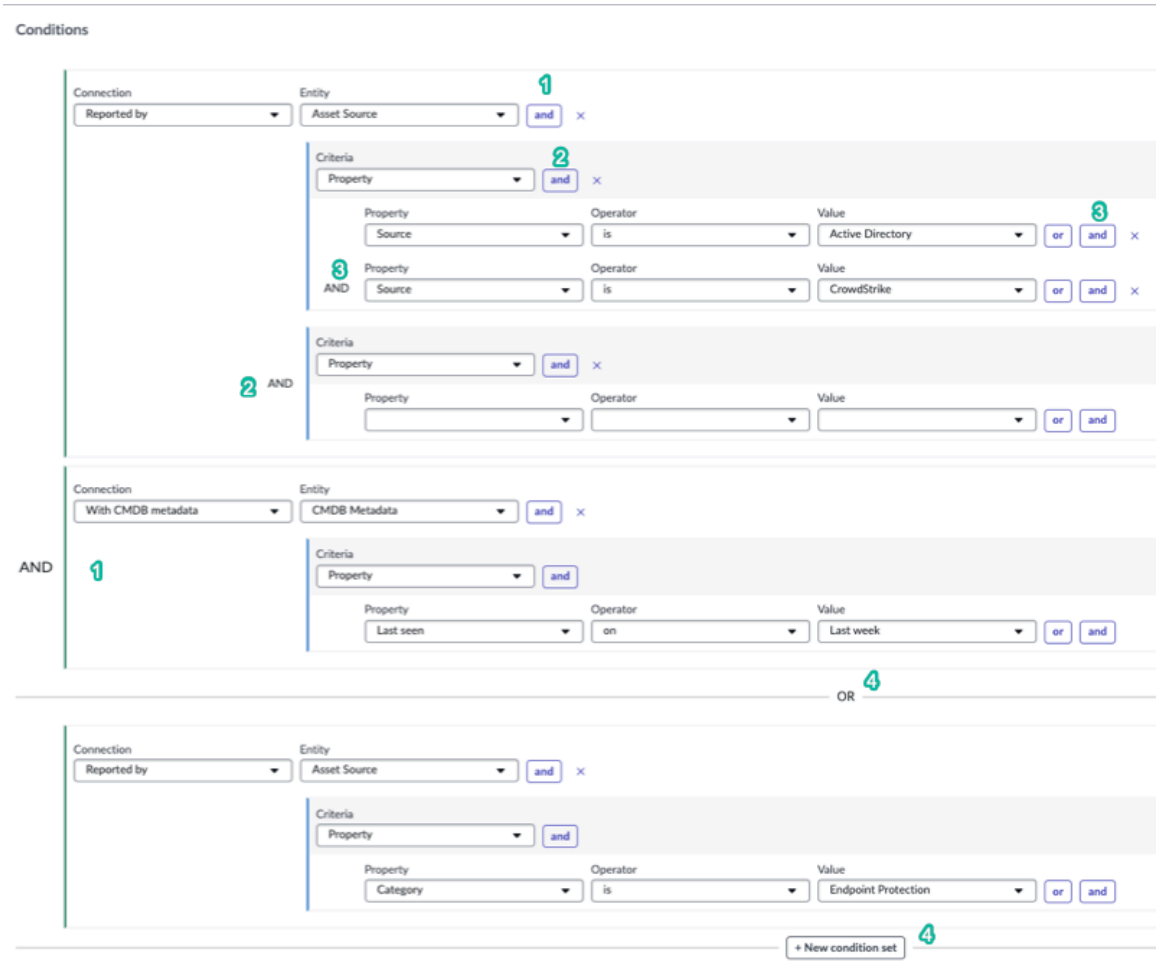
Using the AND, OR decorators in the condition builder

You navigate from the top-level asset types for hardware and software to their secondary entities by using the condition builder in the Policies and findings module in the workspace. Depending on your choices, fields are displayed for you and you modify or add criteria.

The AND, OR decorators in the condition builder permit you to set up the logic for the returned data you want returned for the policy.

Decorator	Description	Number referenced in the image
Select **AND** next to the top-most Connection and Entity fields for new set of conditions.	Adds a logical AND between the current Connection-Entity criteria, and new criteria from another Connection-Entity.	1
Select **AND** to the right of a Criteria or Property field for new set of Criteria and Property conditions.	Adds a logical AND between the current Connection-Entity criteria, and a new criteria under the same Connection-Entity.	2
Select **OR/AND** to the right of a Property field for new set of Property conditions.	Adds a logical OR/AND between current Property, and a new Property from the same Connection-Entity-Criteria.	3
Select **+ New condition set** for a new set of conditions.	Adds a logical OR between the Condition Set of all current Criteria, and a new Condition Set.	4

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Using base policies, cloning, and child policies

You can use multiple policies to evaluate your assets and create your own custom insights. You have the following options to help you create custom or edit existing policies quickly:

- Clone policy - Create a copy of a policy. The name of the policy and its conditions are displayed with a 'copy' in the title. The conditions are displayed, and you can edit them. See Edit an activated policy in Security Posture Control.
- Create child policy - The name of the policy you started from is displayed as the "Base policy" on the new record. Conditions of your base policy are inherited in the new policy, and a new, empty condition set is displayed. See Clone a policy or create a child policy in Security Posture Control.
- Exclusion policies – Add policies to your custom policies so that asset findings from the policies you select are excluded from your results. See Create and activate custom policies for Security Posture Control.

Metadata and CMDB filtering

It might be important for your security teams to monitor assets with older software. You can specify policy criteria starting with the Connection 'With CMDB Metadata' after the Hardware Asset type to include the common properties listed below. This is not an all-inclusive list. In order to gather this metadata, the properties must be available from the CMDB Metadata connection populated by your service graph connectors.

- RAM
- Host name

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Serial number
- OS Domain
- OS Version
- Disk Space
- Last seen
- OS
- First seen
- CPU Count
- MAC Manufacturer
- NIC
- IP Address
- Location
- FQDN
- Netmask
- IP Version
- Serial Number Type
- OS Service Pack

Starting with v3.0 of Security Posture Control:

The Connection ‘With CMDB Metadata’ permits you to add the Host name Property and use the matches regex Operator to help you type in regular expressions in your conditions for the Hardware Asset type. For example, if you enter ‘lp’, you can look for all laptops with 'lp' as the second and third characters in the host name.

'First seen': Assets that have been discovered for the first time by any source within the time frame you select with the 'First seen' timestamp Property.

'Last seen': Assets that were 'Last seen Within the last n days' by any source. Enter the number of days up to 30 as a Value. For example, enter 3 as a Value to monitor assets by 'last logon' from Active Directory in the last three days.

Software Asset type: Look for software publishers or use SGCs you have installed that import software data and metadata you want if you start with the Connection ‘With software details’.

For Hardware asset types, you can use the Connection ‘Has model info’ with the Connection ‘With CMDB Metadata’ for devices based on specific models and model information.

Hardware Asset types also permits you to search for all assets reported by a Source, Qualys, for example, but that are not reported by ServiceNow ITOM Discovery.

See Policies for Security Posture Control for more information about the Security Posture Control policy schema.

Exceptions with the Governance, Risk, and Compliance (GRC) application

An Integrated Risk Management (IRM) exception is an asset with an approved exception from the Governance, Risk, and Compliance (GRC) product. You have the option in a policy to add a condition for an exception so you don’t monitor these assets and include them in your counts.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, some assets might have exceptions approved for certain control objectives with IRM. To reduce your returned matches, information security teams might want to exclude those assets from monitoring for security controls with IRM exceptions that are already approved.

Key insights and configured insights for Security Posture Control

Key and configured (custom) insights provide you with visual reports that are created and updated by the assessment criteria that match your assets. Insights help you monitor security controls metrics on a dashboard.

Key insights

The criteria used for the assessments of your assets are provided by the policies that are included with the application.

- Key insights use the policies that are included with the application.
- Configured insights can be created using the policies included with the application, your own custom policies, or a combination of both.

On the Home (landing page) in the Security Posture Control workspace, the Key insights section below the Overview displays visual reports that are created and updated by the policies that are included with the application. These insights are also included with the application and display the following information:

- Endpoint protection agent installed: Total number of assets that have or do not have endpoint protection.
- Managed device coverage: Number of managed assets compared to those that are unmanaged.
- Vulnerability scan coverage: Total number of scanned assets compared to the those that are not scanned for known vulnerabilities by a third-party vulnerability scanner.
- Assets with critical vulnerabilities: Number of assets out of the total number of assets that have critical vulnerabilities.
- Vulnerable items by criticality: Total number of vulnerable items broken down by their severity. A known vulnerability that matches an asset in your CMDB results in a vulnerable item. This insight requires you to install the Vulnerability Response application and at least one scanner integration: Qualys, Rapid7, or the Tenable Vulnerability Integration. All these applications are available on the ServiceNow® Store.
- Top 3 policies by findings: Policies that return the most findings (matches) on your assets.

Configured insights

You can create your own insights if you want more information not found in the Key insights. You can create these configured insights and use existing policies or your own custom policies for assessment. Your configured insights are displayed on the Configured insights dashboard module, the second icon from the top in the workspace.

Following types of insights can be configured.

- Comparison chart: Compare results between multiple policies with bar charts.
- Policy match count widget: View the number of devices that match a policy.
- Policy match percentage chart: View the percentage of devices that match a policy in a pie chart. You can choose the total asset pool as either all the assets monitored by SPC or the assets that match the base policy from which the current selected policy is created.
- Policy trend chart: View the trends of assets that match various policies.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Create and activate a configured insight for Security Posture Control for more information about the steps for creating a configured insight.

Groups

You must create or assign groups to your configured insights when you create new records in the Custom insight builder module. Groups allow you to organize your reports on the Configured insights dashboard.

Insights can be organized into groups. Each group can have 21 widgets or insights.

Using the Security Posture Control workspace

The Security Posture Control workspace contains the modules you use for configuring, using, and monitoring the imported data about your assets.

Roles

SPC Admin Group

Users in this group have full read and write access to all the records for the product, including licensing information. Granular roles for this group include: [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin, and sn_sec_spc_core.configure].

SPC Analyst Group

Users in this group have full read and write access to all the records for the product but cannot view licensing information. Granular roles for this group include [pa_power_user and sn_sec_spc_core.analyst].

SPC Analyst Read Only Group

Users in this group have full read access to all the records for the product but cannot view licensing information. Granular roles for this group include [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read, and cmdb_ms_user].

Supporting application roles

The following roles are required by the applications that support SPC and Asset Security Posture Management.

- Configuration Compliance Admin [sn_vulc.admin] - Configures the Configuration Compliance application, has visibility to all records, and can modify properties. Assigns roles in the Configuration Compliance application.
- Vulnerability Response Admin [sn_vulc.admin] - Configures the Vulnerability Response application and the vulnerability risk calculators.
- MID Server [mid_server] - Configures a MID Server.

The modules of the workspace

To access the workspace, navigate to **Workspaces** > **Security Posture Control** The Home (landing page) is displayed. The Security Posture Control workspace contains the following modules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Modules

Module	Description
Home	View data visualizations and other information in the Overview, Key insights, and Key use case coverage sections to help you monitor your assets. The information provided on this page permits you to report on the status of your overall security posture to IT, IT and security managers, and other key stakeholders. See Key insights and configured insights for Security Posture Control and Policies for Security Posture Control.
Configured insights	View the data visualizations about your assets that you create, configure, and activate. See Key insights and configured insights for Security Posture Control.
Asset search	Quickly search for assets in your environment based on conditions you set. Verify that you can locate assets with a set of conditions before you commit those conditions to a policy. You can refine these searches so you get a preview of assets that meet your search criteria. When you are ready, you can save your conditions as a policy. See Create an asset search in Security Posture Control.
Asset profiles	Create and define asset profiles to monitor different categories of devices with your SPC policies. Incorporate your asset profiles into your policies so you can run policies for specific types of assets. Filter the insights in the Configured Insights dashboard so they are based on your asset profiles. See Create an asset profile in Security Posture Control.
Policies and findings	Create, clone, edit, and activate policies. There are policies that are included with the application, and you can create your own. Policies audit your assets to find matches for potential violations. Insights, visualizations, and use cases depend on policies. See Policies for Security Posture Control.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Modules (continued)

Module	Description
	Assets that match policy conditions are reported as Findings and are mapped to the Configuration Compliance application for remediation. See View findings for Security Posture Control.
Connectors and use cases setup	Activate and view the status of installed service graph connectors (SGC)s and API integrations. Service Graph Connectors and API integrations are sources you use for importing data about your assets.#A wide variety of (SGC)s are supported and are available from the ServiceNow® Store. Set up and monitor key use cases. Use cases are different scenarios that you configure to help you identify specific types of tool coverage gaps. Each use case requires a policy or policies to audit your assets for potential violations. See Use cases, policy examples, and supported service graph connectors in Security Posture Control.
Custom insight builder	Create your own data visualizations. Custom insights provide you with visual reports that are updated by the audit results of your policies and imported data. Once you activate them, your custom insights are displayed on the dashboard in the Configured insights module. You can determine where data for an insight is displayed on the dashboard by using Groups. See Create and activate a configured insight for Security Posture Control.

Using the modules of the workspace to identify gaps in tool coverage

Identifying security tool gaps requires you to perform the following steps.

1. Set up and activate API connections with any of the tools that you are using in various categories. You can use Service Graph Connectors for products that are available from the ServiceNow Store for the API connections that are required. For more information about the supported service graph connectors, see Service Graph Connectors for Security Posture Control and Service Graph Connectors. Supported service graph connectors are available from the ServiceNow® Store with separate subscriptions.
2. Perform one or more asset searches based on specific criteria to get an inventory.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Activate the policies shipped with the Security Posture Control application. You can also or create your own policies and activate them based on the results of your asset searches.
4. Create and activate your own configured insights to help you monitor your assets.
5. To gain insight into which threats to your assets are mitigated by available mitigation controls based on how various security tools are configured, see Using mitigation controls monitoring with Security Posture Control.
6. Set up rules to automate the remediation workflow in the Configuration Compliance application.

Identifying security tool gaps involves the following steps:

1. Activate the policies shipped with the Security Posture Control application. The Security Posture Control product finds security tool gaps by performing the following tasks:
   a. Identifies the list of all unique assets populated by various Service Graph Connectors in the CMDB.
   b. Identifies assets that are not reported by specific categories from this asset pool, for example, Endpoint Protection. Assets are identified based on the active policy that is being evaluated.
   c. Assets identified as not reported by specific categories are reported as 'Findings' or 'Test Results' in the Configuration Compliance application.
2. Automatically assign 'Findings' to different teams for remediation with the Configuration Compliance application.

Creating your own policies

See Creating your own policies in the Security Posture Control application for more information about how to create your own policies.

See Create and activate custom policies for Security Posture Control for more information about the steps required to create a policy.

For example policies, see Examples of base, child, and cloned policies for Security Posture Control.

Activate a policy included with the Security Posture Control application

Policies that are included with the application must be activated before Security Posture Control can monitor the assets that match that policy. By default, none of the policies included with the application are activated.

Before you begin

You must verify that all the required prerequisites are met before you activate the policies that are included with the application.

- Verify required Service Graph Connectors activated.
- Verify any required applications such as Vulnerability Response are installed and activated, if applicable.
- For more information about policies used for mitigation controls monitoring, see Mitigation controls policies.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

You cannot edit the policies that are included with the application, but you can create new policies based on their criteria with the **Clone policy** and **Create child policy** features. These features are available in the More options menu (three vertical dots).

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Policies and findings** > **All**.

   To determine if a policy is activated, confirm its status (`true` or `false`) in the Active column.

2. Select a policy record to open it.
3. You have the following options on policy records that are included with the application:

Option	Description
Activate policy	Activate a policy if you want to monitor any assets that match the policy conditions and generate findings. If available, select Deactivate policy to stop asset evaluations and findings generation for this policy.
Configure findings	Select **Yes** in the modal to generate findings for the policy. Select the **Configure assignment rules** link to set up assignment rules in the Configuration Compliance application to assign any findings for your policy for resolution. **Note:** For policies you create with 'Software' as the Asset type, you can save the policy and create custom insights, but you cannot configure findings from the policy record.
Clone policy	Create a new policy with all the conditions from the displayed policy as a starting point. See Create and activate custom policies for Security Posture Control for more information.
Create a child policy	Create a child policy that inherits the conditions of the current policy. The current policy conditions are displayed in the 'Base policy' field on the new record, and you add more conditions.
Deactivate policy (Displayed on activated policies only)	Deactivate an active policy if you don't want any assets to be monitored or evaluated

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	against that policy. This editing option is only visible on activated policy records.
View findings	Open a new tab and view the matching assets if available. Findings are also referred to CTRs, or test result records for the policy.

Create and activate custom policies for Security Posture Control

Create your own custom policies to monitor assets for tool coverage and other high-risk combinations.

Before you begin

To help you understand the steps required to create a policy with more details, refer to Examples of base, child, and cloned policies for Security Posture Control. The examples walk you through the steps required to create a base policy, use the base policy to create a child policy, and clone a policy.

For example policies, see Examples of base, child, and cloned policies for Security Posture Control.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **List** > **Policies** > **All**.
2. Select **New policy**.
3. Select the pencil icon next to the name at the top to modify the metadata.

   Fill out the fields.

Field	Description
Name	A unique name for your policy.
Criticality	Select one from the list.
Short description	A unique description for your policy.

4. Select **Save metadata**.
5. For Asset type select on from the list.

Entity option	Entity description
Hardware	Locate IP devices that include personal computing devices, cloud virtual machines, servers, network devices, and other hard ware.
Software	Locate installed software on devices report ed by from SGCs and your vulnerability scan ners.

6. **Optional:** Choose none, one or both.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Base policy	The conditions of your base policy choice are inherited in the new policy.
Exclusion policies	Select any policies you want to exclude from the asset findings for this policy. Any findings from these policies are ignored.

(Optional) The Connection and Entity fields are displayed.

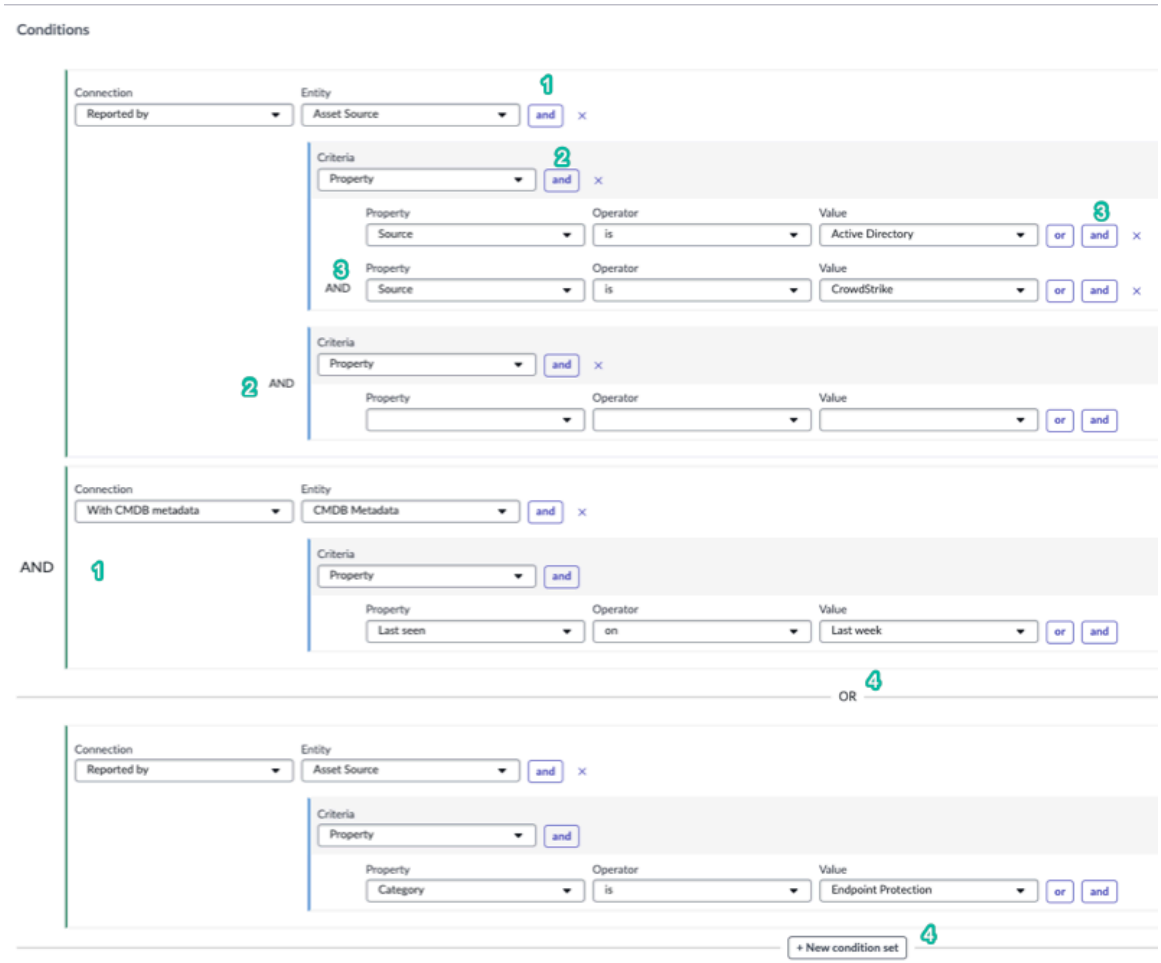
7. Select one from the list for the Connection field.
   The target Entity field is auto populated based on your choice. A new Criteria field is displayed along with Property, Operator, and Value fields. For more information about asset types and the schema for relationships, see Policies for Security Posture Control.
8. Select one from the list for Property.
9. Select **Category** or **Source**.
10. Select an operator and enter a connector category, for example, Endpoint management, or a category product name (source).
11. **Optional:** Use the condition builder and add more conditions or condition sets.

    (Optional) You navigate from the top-level asset types for hardware and software to their secondary entities by using the condition builder. Depending on your choices, fields are displayed for you and you modify or add criteria.

    The AND, OR decorators in the condition builder permit you to set up the logic for the returned data you want returned for the policy. Refer to the following table and image for more information.

Decorator	Description	Number referenced in the image
Select **AND** next to the top-most Connection and Entity fields for new set of conditions.	Adds a logical AND between the current Connection-Entity criteria, and new criteria from another Connection-Entity.	1
Select **AND** to the right of a Criteria or Property field for new set of Criteria and Property conditions.	Adds a logical AND between the current Connection-Entity criteria, and a new criteria under the same Connection-Entity.	2
Select **OR/AND** to the right of a Property field for new set of Property conditions.	Adds a logical OR/AND between current Property, and a new Property from the same Connection-Entity-Criteria.	3
Select **+ New condition set** for a new set of conditions.	Adds a logical OR between the Condition Set of all current Criteria, and a new Condition Set.	4

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



12. Select **Save policy** after you are done editing.
    Your policy is saved. You can choose to activate it now or return later to activate it.
13. From the more options menu next to **Save policy**, select configure findings.
14. Fill in the fields.

Option	Description
Generate findings for this policy?	Choose **Yes** to generate findings for matching assets. After data is imported, select View finds is displayed on the policy record. Choose **No** if you don't want to generate findings.
Configure assignment rules	Select the link to set up assignment rules to assign findings for remediation in the Configuration Compliance application. There is a default assignment rule in the [sn_vulc_assignment_rule_list] table you can use in Configuration Compliance.

15. Select **Save configuration**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you save and activate a policy, it evaluates the imported data from the service graph connector scheduled in the next run. If you want to display the data on the Configured insights dashboard in the workspace, you must create a New insight in the Custom insight builder module. After you activate the configured insight, its data is displayed on the Configured insights dashboard in the workspace.

Edit an activated policy in Security Posture Control

You can edit activated policies to help you customize their conditions to better match your assets.

Before you begin

You cannot edit the policies that are included with the application, but you can clone and create child policies from them. See Clone a policy or create a child policy in Security Posture Control.

If you edit policies and publish your changes, versions are tracked and version numbers are displayed on the policy record and its related test results.

Before you edit an activated policy, you might prefer to deactivate it so that the policy does not continue to evaluate your assets while you edit.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **List** > **Policies** > **All**.
2. Select a policy record to open it.
3. Select **Edit policy**.
   If you are editing for the first time, two deactivated buttons are displayed next to the active **Exit edit mode** button: **Save changes** and **Publish changes**. If you have previously edited this policy and saved it as a draft, the notification, `You have an unpublished edit` is also displayed.
4. Make your edits and choose one to continue.

Option	Description
Save changes	Save your changes as a draft and return to editing mode. Your changes are not published at this point, and you can return to the policy and continue editing later.
Publish changes	Publish your changes as a new version of the policy and automatically exit edit mode. It may take some time for findings to display on your new version of the policy on the View findings button on the policy. If you publish a new version of a policy, you have the option to close any existing findings for the policy that you changed. You might prefer to close any existing findings from the original policy if you only want to view findings for your changed policy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	If you cancel at this point or exit edit mode, a message is displayed that you have an unpublished edit for this policy. If you choose to close its existing related test results (findings), test result and remediation task states transition in accordance with the state transition processes of the Configuration Compliance application. See Test result and remediation task state transitions in the Security Posture Control application for more information.
View version history	For published changes, versions are tracked and version numbers are displayed on the policy record and its related test results.
Exit edit mode	Exit without saving your changes or save your changes and exit without publishing. If you save your changes and don't publish them, you must publish your new version before it can create findings.
Deactivate policy (Displayed on activated policies only)	Deactivate an active policy if you don't want any assets to be monitored or evaluated against that policy. This editing option is only visible on active policy records.
View findings	Open a new tab and view the matching assets if available. Findings are also referred to CTRs or test result records for the policy.

5. After you save the policy as a draft and exit edit mode, select from the following options:

Option	Description
Edit policy	Return to edit mode.
Deactivate policy (Displayed on activated policies only)	Deactivate an active policy if you don't want any assets to be monitored or evaluated against that policy. This option is only visible on active policy records.
More options menu	
Configure findings	Select **Yes** in the modal to generate findings for the policy. See View findings for Security Posture Control.
Clone policy	Create a copy of the policy record. See Clone a policy or create a child policy in Security Posture Control.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Create child policy	Create a new policy using this policy as a base. See Clone a policy or create a child policy in Security Posture Control.
Delete policy	Remove the policy record from the policy list.
View findings	Open a new tab and view the matching assets if available. Findings are also referred to test result records (CTRs) for the policy.
View linked records	For published policies, view custom insights if available. See Create and activate a configured insight for Security Posture Control

Clone a policy or create a child policy in Security Posture Control

Clone an existing policy and add conditions to it to create your own custom policy. You can also create child policies from existing policies.

Before you begin

You can clone policies to create your own custom policies. You can clone a policy or create a child policy using any policy as a base to help you extend the existing policies without having to enter in the conditions again. All the conditions in the base policy are also inherited in the child policy. See Clone a policy or create a child policy in Security Posture Control for more information.

You can clone any policies that are included with the application but policy matches are not reflected as key insights on the dashboard on the Home landing page. Only key insights for policies that are included with the application are displayed on the Home landing page.

After you clone and activate any policies you create, you must create your own configured insight record in the Custom insight builder module in the workspace (the last module in the navigator panel). Only then can you view the data from your policies on the Configured insights dashboard (the second icon from the top in the workspace).

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **List** > **Policies** > **All**.
2. Select the policy record that you want to clone.
3. Select one from the more options menu next to **Activate policy**.

Option	Description
Clone policy	Select this option if you want to use the conditions of an existing policy as a starting point for your new policy. A new tab with the cloned policy record is displayed with 'copy' in the name. (Optional) Select Base policy and add one from the list for your new policy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Create child policy	Select this option if you want to create a new policy using the current policy as a starting point. A new tab with a blank policy record with a base policy you choose is displayed.

4. **Optional:** Select **Base policy** and select a policy as the base for your new policy.

   (Optional) You might choose this option if you want to inherit the conditions of an existing policy as a starting point for your new policy.

5. **Optional:** Select **Exclusion Policies** and select policies that you want to exclude from the findings of this policy.
   Any findings in your new policy that match any excluded policies are not included in your findings.
6. For a cloned policy, edit the conditions.
   For more information about the Asset-connection-entity relationships in the condition builder, see Policies for Security Posture Control. For more information about the decorators in the condition builder, see Creating your own policies in the Security Posture Control application.
7. Edit and Save your policy with **Save changes**.
   Your policy is displayed on the All list in the List module in the workspace.
8. To activate a policy, follow the steps described in Create and activate custom policies for Security Posture Control.
9. **Optional:** Select Delete policy to delete a policy.
   The delete option is not supported for any policies that come with the application or for any policies that have generated findings. You can only deactivate policies with findings.

Create and activate a configured insight for Security Posture Control

You can create your own insights. Configured insights are insights that you can create either using existing policies or your own custom policies.

Before you begin

You must create an insight record and activate it before you can view your data on the Configured insights dashboard. You can have up to six insights and 21 charts on the Configured insights dashboard module in the workspace.

Any policies you use for a custom insight must be activated.

For policies you create with 'Software' as the Asset type, you can save the policy and create custom insights, but you cannot configure findings from the policy record.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Insight builder**.

   On this landing page, there are three tabs:

   Active

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your activated custom insights. Activated custom insights are displayed on the Configured insights landing page (second icon from the top in the workspace).

Inactive

Your inactive custom insights. Deactivated insights are not displayed on the Configured insights landing page until the insights and their supporting policies supporting them are activated.

All

All your active and inactive configured insights.

2. Select **New Insight** on the right of the page to create a new record.
3. In the Type field select an insight from the choice list.

Option	Description
Comparison chart	Compare counts for matching assets for up to five policies.
Policy match count widget	The total number of your assets that match a policy or policies.
Policy match percentage chart	The percentage of your total assets that match or do not match a policy.
Policy match trend chart	Historical trend of assets that match a policy or policies.

4. Select one.
   - Hardware asset or Cloud virtual machine
   - Software
5. Select groups for your insight.
   An insight must belong to at least one group. You must create or assign groups to your configured insights when you create new records in the Custom insight builder module. Groups allow you to organize your reports on the Configured insights dashboard.
6. Select the policies and the corresponding labels you want for your insight data.
7. Select **Save**.
   Your insight is saved on the Inactive insight tab.
8. To activate your new insight, open the record on the Inactive list and select **Activate**.
   Data is gathered from the next scheduled import for the Service Graph Connectors that are associated with the insight's policies, and data is displayed on the Custom insights dashboard module in the workspace.

Create an asset profile in Security Posture Control

Create an asset profile with conditions to group assets. You can use these asset profiles in your policies.

Before you begin

Roles required: SPC Admin Group or SPC Analyst Group

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Asset profiles**.
2. Select **New**.
   The condition builder is displayed. Note that the name includes the date and time you created the profile.
3. Select the pen icon to edit the profile name with a unique name.
4. Select **Save metadata**.
5. Select one from the list for Connection:

   The asset profile supports three Connection types.

   - **With CMDB metadata** - Collection of CMDB CI properties such as Host name, OS, OS version, First and Last seen, for example, or connections that have network adaptors or installed software.
   - **With aggregated data** - Collection of properties with aggregated values reported by different sources for a given asset. An example is the various ways sources might report an OS version: `windows11`, `Win11`, `Windows 11`, and so on.
   - **From CI class** - Collection of CI classes that includes Computer, Server, Virtual Machine Instance and others.

   The operators and logic for this asset profile policy builder is similar to the one described in Creating your own policies in the Security Posture Control application.

6. Select **Create**.
   Your profile is displayed on the Asset Profiles list.

   You can associate asset profiles to any policies.

7. Navigate to **All** > **Security Posture Control Workspace** > **Policies and findings**.
8. Select a policy.
9. In the Policies and profiles section, select one or more asset profiles.
10. Select **Save changes**.
    The policy audits your assets based on data imported from your service graph connectors and includes the conditions of the asset profiles that you added. You can Create and activate a configured insight for Security Posture Control and add asset profiles as a filter.
11. Navigate to **All** > **Security Posture Control Workspace** > **Configured insights**.
    You must Create and activate a configured insight for Security Posture Control before data is displayed on this page.

    Since the visualizations on this page are configured by policies, you can filter them with asset profiles. Filter the data for the visualizations by following these steps:

12. Select the filter icon.
13. Select **Select**.
14. Select and move any of the asset profiles in the Available column to the Applied column.
15. Select **Apply**.
    The custom insights visualizations are filtered to show data for the policies that included the asset profiles you chose. A message in the Filter pane indicates how many configured insights are filtered out as a result of the asset profiles you added. There might be a delay for updates to trending data, because the Run SPC Policy scheduled job must complete to update trending data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Delete an asset profile in Security Posture Control

You can delete asset profiles. You delete asset profiles if they are associated to policies so the asset profile's conditions are not included in the next policy audit.

Before you begin

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Asset profiles**.
2. Select a profile record.
3. Select the more actions menu icon (⋮) and select **Delete asset profile**.
4. **Optional:** In the dialog select **Review policies** to view any policies this profile is linked to. Policies that contain the asset profile are listed in the Linked policies tab.
5. Select the tab with the asset profile that you want to delete.
6. Select the more actions menu icon and select **Delete asset profile**.
   This is a hard delete. The conditions of the asset profile are removed from any policies and are not included in the next nightly policy audits to get the latest results.

View findings for Security Posture Control

You can view the findings generated by the evaluation of policies in Security Posture Control in the Security Posture Control Workspace.

Findings

You can configure findings to be generated from the execution of policies so that they can be assigned to various teams for remediation or used for reporting. See Activate a policy included with the Security Posture Control application for more information about generating findings directly from your policies.

Security Posture Control publishes these findings as 'Test Results' in the Configuration Compliance module. All administrative controls in the Configuration Compliance application that are related to the assignment, grouping (remediation task generation), remediation targets, and exceptions are supported for findings that are generated by Security Posture Control.

The labels used for findings:

Tool coverage

This type represents a security tool coverage gap. This finding type is applicable for policies using 'Reported by' and 'Not reported' connector relationships.

Internet exposure

This type represents internet exposure of a cloud asset. This finding type is applicable for policies using the 'Has port exposed to internet' relationship or connection.

High-risk combination

This type represents an issue having more than one associated risk factor, for example, assets with critical vulnerabilities and a missing endpoint protection agent.

Integrated Risk Management (IRM) exception

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This type represents an asset with an approved exception from the Governance, Risk, and Compliance (GRC) product. If indicated, these exceptions are not included in your findings counts.

Has vulnerability

This type represents assets with associated vulnerable items (VITs) that have known vulnerabilities.

Security posture labels are generated and attached to test results. A label of an appropriate type, 'Tool coverage', for example, is automatically assigned to test results based on the type of policy. Multiple labels are displayed on records for assets that have more than one label.

By using security posture labels associated with the findings, you can write assignment rules in Configuration Compliance to route these issues to teams for remediation. For example, you can send ‘Tool coverage’ findings to an IT ops team, and ‘Internet exposure’ to an application team.

Where to view findings

You have these options to view the findings generated by the evaluation of policies.

Roles required: SPC Admin Group or SPC Analyst Group

- Navigate to **Security Posture Control Workspace** > **Policies and findings** > **Findings** > **All.**
- On a policy record, select **View findings**. The list displays groups of findings that organize them into general categories such as 'High-risk combination', 'Internet exposure', and so on, but these groups are not formal groupings that can be used for remediation. You need to set up remediation and assignment rules in Configuration Compliance for findings.
- In the Configuration Compliance application, select **Test Results** and filter the records by **Source is ServiceNow SPC**.

The dashboard

In the Security Posture Control Workspace, the Home (landing page) displays these visualizations:

Overview

- Assets: Number of assets monitored on-premise and in the Cloud.
- Findings by criticality: Number of critical findings out of your total assets.
- Assets monitored by top 5 sources: Top five Service Graph Connectors reporting on assets.
- Cloud accounts: Number of Cloud accounts monitored by AWS and Azure.
- Open vs closed findings: Comparison of records still in process or awaiting resolution and those that are resolved.

Key insights

- Endpoint protection agent installed: Total number of assets have or do not have endpoint protection.
- Managed device coverage: Number of managed assets compared to those that are unmanaged.
- Vulnerability scan coverage: Total number of scanned assets compared to the number that are not scanned for known vulnerabilities by a third-party vulnerability scanner.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Assets with critical vulnerabilities: Number of assets out of the total number of assets that have critical vulnerabilities.
- Vulnerable items by criticality: Total number of vulnerable items broken down by their severity. A known vulnerability that matches an asset in your CMDB results in a vulnerable item.
- Top 3 policies by findings: Policies that return the most findings (matches) on your assets.

Key use case coverage

Select a use case and select **Help activate** or **Help improve** to view which service graph connectors and policies should be activated for the key use cases.

Test result and remediation task state transitions in the Security Posture Control application

The states on findings (configuration test records) and their associated remediation tasks are impacted if you modify your policies in the Security Posture Control application.

State transition scenarios between test results and remediation tasks

With some exceptions, states generally transition between your findings (test results) and their associated remediation tasks in Security Posture Control the same way they transition between test results and remediation tasks in the Configuration Compliance application. However, if you modify your policies in Security Posture Control, your changes impact how states transition on your findings and their associated remediation tasks.

The following tables illustrate how states transition on your findings if you edit and publish a new version (edit), deactivate, or delete your policies.

For more information about state changes in Configuration Compliance, see Test result and remediation task state transitions in the Configuration Compliance application.

Note: Starting with v14.9 of Configuration Compliance, the following terms have been renamed:

Changes in terminology

Terminology prior to v14.9	Terminology v14.9 onwards
Test Result Group	Remediation Task
Group Rules	Remediation Task Rules
Policy	Test group

Enhancements to policy audits ensure that retired assets are not evaluated by activated policies. If the state of an asset transitions from **Retired** back to **Active**, it is included in the next policy evaluation.

If a policy is...	Field values on existing finding records for...	Transition to...
Deactivated	Result	Retain original values
	State	Closed
	Resolution	Stale

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a policy is...	Field values on existing finding records for...	Transition to...

If a policy is...	Field values on existing finding records for...	Transition to...
Edited with the option to close any existing findings selected	Result	Retain original values
	State	Closed
	Resolution	Result Invalid

If a policy is...	Field values on existing finding records for...	Transition to...
Edited with the option to retain any existing findings selected	Result	Valid (Passed) test cases retain original values and invalid test cases (Failed) are closed.
	State	Closed
	Resolution	Result Invalid

If a policy is...	Field values on existing finding records for...	Transition to...
Deleted	Results	Retain original values
	State	Closed
	Resolution	Result Invalid

Creating your own API connectors in Security Posture Control

Create your own Security Posture Control (SPC) API connectors using the connector framework that is included with the application.

Overview for the connector builder framework

Benefits

Create your own SPC API connectors quickly to help you integrate with security tools and import asset data that is based on the unique requirements of your environment. Use imported data to help you monitor your overall security posture and identify assets that are missing key security tools.

The connector framework includes the following features.

- A step-by-step process to guide you through the connector builder.
- A single place to build and maintain all your SPC integrations to import custom data into your CMDB.
- After you publish them, monitor your API connectors on the SPC API Integrations tab in the **Security Posture Control** workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The API connector builder

You use the Connector builder in the Security Posture Control workspace to create and publish your customized API connectors.

Prerequisites

Before you start creating your API connector, you might prefer to set up any credentials for the service (vendor) that you want to implement with and have their API documentation and credentials handy as you work through the Connector builder. See Enter metadata for more information.

Required applications and plugins

The following applications and plugins are required.

For more information about applications in the ServiceNow® Store, see Exploring the ServiceNow Store and downloading and activating applications Download an application from the ServiceNow Store for the first time.

Note: If you're downloading applications to non-production or development instances, it's not necessary to get entitlements.

Role required: admin for download, installation, and activation of all applications and plugins.

Required Applications

Application	Application ID and version
Security Posture Control API Connectors	sn_spc_cxf v2.0.0
Security Posture Control	sn_sec_spc_core v7.0.1
Asset Security Posture Management	sn_sec_caasm v5.5.1
Mitigation Controls Monitoring	sn_sec_mit_ctrl v4.1.4
Integrations Commons for CMDB	sn_cmdb_int_util v2.20.0

Plugin dependencies

Plugin	Plugin ID
IntergationHub Action Template - Data Stream	com.glide.hub.action_type.datastream

Required roles

Role required: admin

Assign the sn_sec_spc_core.developer role to the users who you want to view and configure SPC API connectors with the Connector builder in the Security Posture Control workspace.

Assign the sn_spc_cxf.admin role if you want users to configure SPC API connectors with advance scripting with the Connector builder.

See Install the supported applications for Security Posture Control for information about assigning roles to Security Posture Control groups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enter metadata

Fill in the metadata for your service graph connector.

Before you begin

Role required: sn_sec_spc_core.developer

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Connector builder**.
   The Custom API connectors are displayed.
2. **Optional:** Select an existing connector record from the Connector name column to edit it.
3. To create a record, select **New connector**.
   A tab opens in your browser and the required fields for the Enter metadata step are displayed.
4. Fill in the fields.

Field	Description
Connector name	A unique name. You might prefer to add 'CXF' in the title to help you easily distinguish the API connectors that you create from the API connectors from other services (vendors).
Vendor	Connector's vendor name from the list. The templates in the connector builder provide you with options that are based on popular API integrations from security tool vendors. You can choose a vendor to base your connector on. Alternatively, select the  to add a vendor name and URL. Select the refresh icon () to see your vendor on the list.
Connector category	Select one for your connector type.
Description	A unique description for this API connector to help you easy identify its data imports from your other connectors.

5. Select **Save and continue** to save your edits.
   You must save your changes before you can continue.

Create connector alias and connection credentials

Enter the connection URL and credential alias details for your API connector.

Before you begin

You must have a set of test credentials handy to configure your API connector and test the connection. Note that you use these test credentials for building and testing the connector. These aren't the connection URL and credentials that the system uses once your API connector is published. You must complete this step before you can proceed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select the **Learn how to create a connection and credential alias** link for more information before you start. You can keep this page open in your browser as a tab as you fill in the fields for this step. You can create and share these credentials across APIs so that you don't have to create and enter multiple sets of credentials if you want more than one instance of an API connector.

Role required: sn_sec_spc_core.developer

Procedure

1. Fill in the Alias and Connection fields.

   Note: If a message is displayed that prompts you to change your application scope, update it to the `Security Posture Control API Connectors` scope as directed.

2. Select the **Create new** link to the right of the Alias field to create a (Credential) alias.

   a. In the Connection and Credential Aliases record, enter a unique name for your API connector's alias.

   b. **Optional:** Select the search icon on the Parent Alias field and select one.
   If you select a parent alias from the list, this record points to another alias record. If you select a parent alias some fields on the form are no longer displayed, and you can submit your changes.

   c. Select **Submit**.

   d. Select the refresh icon ( ) to see your alias on the list.

   e. Select your alias.

   f. Select the **Create new** link next to the Connection field.
   A new HTTP(s) Connection record is displayed. Fill out the fields to create a connection for your alias.

Field	Description
Name	Unique name for the connection.
Active	Record is activated by default.
Credential	You must select a credential from the list.
Domain	(Optional) Global is displayed.
Connection Alias	Select a credential alias from the list. Alternatively, enter an alias. The connection alias must match the associated alias that you created or selected for the Alias field in the previous step.
Connection URL	If the URL builder is not selected, enter the connection URL in HTTP : / / or HTTPS : / / format.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Use MID Server	A MID Server isn't required. If you select this check box, fill out the fields for your MID Server.
Connection timeout	This value isn't required. Leave this field empty to use the system default connection timeout value. Don't enter 0 as a value. Alternatively, enter a value for the number of milliseconds the system waits for a successful host connection. If a successful connection doesn't occur during this time, the connection request times out.

g. Select **Submit**.

h. Select the refresh icon ( ) for the Connection field to see your connection on the list.

i. Select your connection.

The base URL and credential are displayed in read-only fields. These connections are associated with the alias that you choose. This list isn't a complete list.

If you don't see the Credential field, you can select the view connection link ( ) icon next to the Connection field.

In the form that is displayed, add the Credential in the Credential field. You must have the credential field populated before you can save the record.

3. Select **Update**.
4. Select **Save and continue** to save your edits.
   You must save your changes before you can continue.
   After you save your edits, the Select template step is displayed and highlighted on the stepper.

Trouble?

Select the view connection link ( ) if you see the following message: `There are no credentials associated with the selected connection. Please update the connection via the View connection button.`

Select a connector template

Select a template to support your API's structure.

Before you begin

These templates provide you with options that are based on API structures that are widely used by security tool vendors. When you select a template, you're choosing a configuration that aligns with industry-standard ways of organizing and communicating with APIs. By selecting a common response format (JSON), HTTP methods (GET or POST), and well-known pagination strategies, connecting with a wide variety of security tools is easier, because you're using familiar and widely adopted API patterns.

Role required: sn_sec_spc_core.developer

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Select one option from a list and **Apply** to view the template cards that match your selections.

   a. Select **Clear filters** to reset.

      The cards with available templates change as you apply your choices in the modals.

      Response type - JSON is supported.

      HTTP method - Select **GET** or **POST**.

      Pagination type - Select one. Select the information icon (ⓘ) to the right of the Pagination type list above the template cards for more information. Pagination strategies and sample requests and responses are also provided.

   b. Select the information icon (ⓘ) on a card for more information about the template.

   c. To choose a template from the available results, select **Select**.

      The name of the selected template is displayed above the cards, for example, CXF0000008.

2. Select one option from each list and **Apply** to view the template cards that match your selections.

Template option	Description
Response type	JSON is supported.
HTTP method	**GET** or **POST** is displayed.
Pagination type	View the information (ⓘ) icon for more information on pagination strategies you select.

3. Select **Save and continue** to save your template.
   You must save your changes before you can continue.

Provide input values for your API connector

Provide input parameters to make a valid API call, test the connection, and receive a sample response.

Before you begin

For all templates, you can select the information icon (ⓘ) to learn more about each parameter. You can use the API samples provided with each template. After you define your input parameters, you must test your connection.

Roles required:

- sn_sec_spc_core.developer
- sn_spc_cxf.admin - required for advanced scripting

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Fill in the fields.

> **Note:** If you change any input parameters after testing the connection, you must test the connection again before you can continue on to Map API response to SPC attributes.

Field	Description	Example
Object list path	Path to the list of assets in the response payload.	An example: `$.list`
API endpoint relative path	This is the path to the API without the host URL.	An example: `/r2`
API query parameters	Key-value pairs that are appended to the API URL for filtering. Values can be strings, scripts, or references to fields in the credential table.	An example: Name [name of query parameter] Value type [Static values] Value [a string]
Pagination parameters	Dynamic parameters used to retrieve subsequent pages of API data. Specify the parameter name, its location in the request (Query, Header, or Body), the path to extract its next value from the API response, and an optional default value.	An example of pagination type Offset: Offset Parameter name [start] Location in API request [Query parameters] Default value [0] Limit Parameter name [count] Location in API request [Query parameters] Default value [5]
(Optional) Add parameter	Add custom parameters	Select **Add parameter** to define your own parameters. For example, you might want to determine if there are additional pages of data that are included in the API response. Parameter name [hasMore] Path in API response [$.hasMore]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description	Example
		Location in API request [Header parameters] Default value [1]

2. When you're satisfied with your API input, select **Get sample response**.
   After a few moments, a message is displayed if the connection was successful.

   If you entered your parameters manually for this step, the data imported from the connection test that is rendered in the sample response is authentic and you can use it in the next step to help you map parameters.

3. Select **Save and continue** to save your edits.
   You must save your changes before you can continue.

Map API response to SPC attributes

Map API response properties to SPC attributes.# After you have mapped the attributes, you publish your connector so it imports data.

Before you begin

For this step, you map parameters to SPC attributes and policies from the data you imported with your API connector.

- Select and use the API response sample in the list in the Reference section for SPC attributes.
- Select the API response schema sample in the list for API attributes to help you map the properties to dedicated SPC attributes.

These schema and samples are provided for you after you enter values and save your edits in the previous step. The response schema is aggregated. To see all observed properties, change the reference list to **API response schema**.

Note: Regardless of whether you enter your parameters manually, or if you choose use Now Assist to generate your parameters automatically, you must Validate your API connector before you can publish it.

Roles required:

- sn_sec_spc_core.developer
- sn_spc_cxf.admin - required for advanced scripting

Procedure

1. Add required attributes.

   Select the tooltips for more information and context about the fields on this page.

   The Host name attribute and Asset identifier attributes are required. Other fields are optional. All attribute values can be scripted with the script toggle. To commit your script, you must select **Save and Close script**. If you no longer want to script an attribute, select the scripting toggle to deactivate it.

   The Collection field applies the same collection to all attributes, and this value helps you fill out the form quickly. This field auto-populates any fields that aren't yet mapped.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Add an Asset identifier.

   An asset identifier is a unique combination of properties returned by the API to identify configuration items.

b. Add a Host name attribute.

c. **Optional:** Create an SPC custom attribute if you want to add a property.
   Only create custom properties if they aren't included as part of the default attributes that are provided. Use the following steps to create custom properties.

2. As an example, create an attribute, `osName` for an asset's operating system from the reference samples.

   a. Select **API response sample** in the Reference window.

   b. Locate the object, for example, `"operatingSystem"`, and note it might have a property such as `"osName"`.

   c. Select **Add attribute**.

   d. Select the Collection field to apply a filter to the API attribute list, in this example, this might be something like, **$.operatingSystem**.

   e. Select the API attribute field and select **osName** from the list.

      The Type list persists the mapped value to that type. Select the type that you want this attribute to be stored as. This field is required.

      Use the Transformer field to augment the value coming back from the API. For example, if you select **Date** for the Type, you can use the Transformer field to cast between types. Using the transformer is optional.

   f. **Optional:** Add properties so you can filter data so that it identifies specific types of assets with this attribute.

   g. Select the Asset identifier attributes field and add the properties you want, for example, **address** and **assetType**.
      Adding these properties not only helps you identify specific assets, but additionally it might help you identify an asset that is reported differently by multiple security tools. One tool might import it using **address**, for example, and another might report the **assetType**. Adding these attributes can help you avoid creating duplicate findings for the same asset.

3. After you have completed the mapping, select **Save and continue** to save your changes.
   You must save your changes before you can continue.

Validate your API connector

Test the connection for your API connector. You must pass both checks before you can publish your connector. You must review your input and mapping to be sure that it is accurate before publishing your connector.

Before you begin

Roles required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_sec_spc_core.developer
- sn_spc_cxf.admin - required for advanced scripting

Procedure

1. Select **Validate**.
   A modal is displayed that tracks the progress for the two validation steps. Your connector, at a minimum, must pass this check before you can publish your connector. If you fail one or both of the validation checks, the **Publish connector** UI action isn't activated.

   Note: Passing this validation so the **Publish connector** UI action is activated doesn't necessarily mean your mapping is accurate. Review your mapping, address any errors and warnings, and resolve any issues. A passing validation check means that you can successfully connect to the endpoint you specified with the credentials and basic parameters that you have provided. You must review your mapping for accuracy.

2. Select the icons in the stepper to return and edit your entries.
3. Select **Save and continue** to move to the next step.

   Note: If you edit information in the stepper, your template, input fields, and mapping response fields might change.

4. When you're satisfied with your template, select **Publish connector**.

   Note: After you publish your API connector, custom attributes can't be edited or deleted. You can edit the other fields.

5. In the modal that is displayed, copy the information for scope, table, label, and value.

   Keep this information handy and note that a new record is displayed.

6. Select **Create discovery source**.
7. Fill in the fields with the information that you copied.
8. Select **Submit and close the window**.

Create an instance and set the import schedule

Create an instance and determine when and how often you want your connector to import data.

Before you begin

Role required: sn_sec_spc_core.developer

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Connectors and use case setup**.
2. Select the **SPC API Integrations** tab.
3. Locate the card for your connector with the integrations used for mitigation controls data.
4. Look for connectors with CXF in the name and select the card.
5. Select **New** to create an instance.
6. In the New instance modal, enter a unique name and select **Create Instance**.
7. With the integration tile selected, select the instance you created in the previous step in the Name column.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. In step one in the modal, enter the alias and connection information and select **Next**.
9. In step two in the modal, set how often and when you want the integration to import data.
10. Select **Save and exit**.
11. **Optional:** Add instances for the integration.
    Add more instances for the integration. The alias and connection credentials you created during the setup permit you to share credentials across multiple instances (accounts). You can have a maximum of five active instances for your API Integration.
12. To view and edit the import schedule, navigate to **All** > **System Import Sets** > **Administration** > **Scheduled imports**.

Create an asset search in Security Posture Control

Set your conditions and search for assets by specific service graph connector products or for assets that have specific data reported by a connector.

Before you begin

As an example search, say you want to identify your assets that have Windows servers and a specific version found in CrowdStrike metadata details.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Asset search**.
2. Choose one.

Option	Description
Hardware Asset	Search for any device that includes personal computing devices, servers, network devices, cloud virtual machines, and other hardware.
Software	Search for installed software on your assets reported by service graph connectors, your vulnerability scanner products, and the soft ware reported by scanners that is already ac counted for in Software Asset Management (SAM) and other ServiceNow products.

   For this example, select **Hardware Asset** for Asset type.
3. **Optional:** Select **Base policy** and **Exclusion policies** if you want to use an existing policy's conditions as a start and you want to exclude assets that match existing policies, respectively. The policies you select are displayed.
4. Select **With connector data** for the Connection field.
5. Select **CrowdStrike Device Details** for the Entity.
6. For Property, Operator, and Value, select **[Agent Version][is]** and enter the version, for example, **6.26.14003.0**.
7. Select the and operator to the right of the Entity field with CrowdStrike Device Details as the value for another condition.
8. Select **With CMDB metadata** for the Connection field.
   The Entity field is populated with CMDB Metadata.
9. Select **Property** for the Criteria field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. For Property, Operator, and Value, select **[OS][contains]** and enter **Windows server**.
11. Select **View assets**.
    After a few moments, results are displayed on the Matching assets tab. If you see no matches, you can refine your search. After you are satisfied you have set the conditions correctly, you can save the search as a policy and activate it. Like other policies, it searches your assets with a background job continuously after you activate it.

Resolving duplicate configuration items in Security Posture Control

Resolving duplicate entries for configuration items (CIs) in your Configuration Management Database ensures that you get accurate audits with your SPC policies.

Duplicate configuration items overview

In certain cases, your asset discovery sources, that is, your service graph connector products (SGCs), import asset data that might create duplicate entries in your Configuration Management Database (CMDB) for assets (configuration items). These duplicate CI records occur when two or more assets are listed in your CMDB with the same names, but the CMDB references are different.

An example might be an asset that named by its IP address, `10 . 0 . 2 . 11`, that is listed twice on the CMDB 360 Data [cmdb_multisource_data] table. One entry for `10 . 0 . 2 . 11` is listed in the CMDB reference column as `10 . 0 . 2 . 11`, and another is listed as `10 . 0 . 65 . 159`. These assets might be from the same Discovery source, an SGC product, or they might be from two or more Discovery sources. In either case, to avoid problems with SPC policies and your asset inventories, you must remove the duplicate CIs.

Identifying and removing duplicate configuration items

You can identify duplicate CIs by filtering on the Name column on the [sn_sec_spc_core_asset_cache] table and noting which assets have the same name.

If you identify duplicates, the CI deduplication process incorporates a deduplication template that you must publish, a system property that you activate, and a scheduled job that removes duplicate CIs in the SPC Cached Assets [sn_sec_spc_core_asset_cache] table. The process removes duplicates and preserves the master, or canonical, CI record that has the most related items.

Resolve duplicate configuration items in Security Posture Control

Use this process to remove duplicate configuration items in the SPC Cached Assets [sn_sec_spc_core_asset_cache] table. This process removes duplicate records and preserves the master, or canonical, asset record that has the most related items.

Before you begin

Roles required: sn_cmdb_user for access to the CMDB Workspace and sn_sec_spc_core.admin to initiate the scheduled job

Procedure

1. Navigate to **All** > **System Properties** > **All Properties**.
2. Locate the sn_sec_spc-core.is_ci_name_unique system property.

   This is a configurable value on the property that specifies whether all configuration items listed in your CMDB or Asset Cache table have unique names.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See Resolving duplicate configuration items in Security Posture Control for more information about how to identify duplicate CIs.

3. Select the record to open it and set the Value field to **true**.
4. Update the record.
5. Navigate to **CMDB Workspace** > **Management** and select the De-duplication template library link under Management tools on the right.

   Note: The sn_cmdb_user role is required for access to the CMDB Workspace.

6. In the De-duplication templates pane, expand **SPC deduplication templates** and select **Name flip-flop** to open it.
7. Select **Publish**.
8. Select **Publish** in the modal.

   You have published the deduplication template and activated the sn_sec_spc-core.is_ci_name_unique system property. You must execute the Generate deduplication task scheduled job to generate the tasks that resolve the duplicated CIs.

9. Navigate to **All** > **System Definition** > **Scheduled Jobs** > **Generate deduplication task** and select the record to open it.
10. Select **Execute Now**.
    Verify the background job is queued and processing.
11. Navigate to the **Background Jobs [sn_sec_cmn_background_job]** table to monitor the Generate deduplication task scheduled job.
    When the scheduled job is successfully completed (Complete), you can initiate the template you published.
12. Navigate to **CMDB Workspace** > **Management** and select **View deduplication dashboard**.
13. Select **Running** to load the template.
14. Select the **Completed** tab to view the completed tasks.

    You must verify that the deduplication tasks have completed before you check the SPC Cached Assets [sn_sec_spc_core_asset_cache] table for duplicates.

    You might have to refresh your screen to view the completed tasks.

15. When the scheduled job is successfully completed, and you have verified that the deduplication tasks are complete, navigate to the SPC Cached Assets [sn_sec_spc_core_asset_cache] table and filter the Name column and check for duplicates. The master, or canonical, is the CI record that has the most related items. It is preserved on the table. If there no duplicates, check the CMDB 360 Data [cmdb_multisource_data] table for duplicates.
16. Navigate to the CMDB 360 Data [cmdb_multisource_data] table.
17. Group by Col0 and check if different CMDB references exist for assets that correspond to the Name column of the SPC Cached Assets [sn_sec_spc_core_asset_cache] table.
    If you find any duplicates, run the Generate deduplication task scheduled job again.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using mitigation controls monitoring with Security Posture Control

From within in the Security Posture Control (SPC) Workspace, gain insight into which threats to your assets are mitigated by available mitigation controls based on how various security tools are configured.

Mitigation controls monitoring

For supported applications for Security Posture Control and Mitigation Controls Monitoring, see Exploring Security Posture Control.

The Security Posture Control application focuses on three core problem areas:

- Asset inventory - Identifying all your enterprise assets that include unmanaged or unknown assets.
- Security controls coverage and health - Identifying any coverage gaps with your security controls
- Vulnerability and threat mitigation visibility - Identifying which threats or vulnerabilities to your assets are mitigated by applicable mitigation controls.

Mitigation controls monitoring describes the features in Security Posture Control that fall under vulnerability and threat mitigation visibility.

Roles required:

- admin - Installs applications from the ServiceNow® Store and activates plugins (ITOM Discovery).
- SPC Admin Group and SPC Analyst Group - Users in this group have full read and write access to all the records for the product and the workspace.
- SPC Analyst Read Only Group - Users in this group have full read access to all the records for the product.

Mitigation controls monitoring users and benefits

Users

User	Description
Cybersecurity teams, Security analysts and managers	• Gain visibility into all your enterprise assets that include unmanaged or unknown assets. • Identify coverage gaps with your security controls, toxic combinations of problems such as critical vulnerabilities and internet exposure on your assets, and deviations from your internal security standards.
Vulnerability management teams	Gain insights in mitigations available for vulnerabilities on the assets and dynamically adjust risk score for those vulnerabilities.
Threat defense teams	Gain insights into gaps in mitigations or security controls configuration against specific attack techniques.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Posture Control and the mitigation controls monitoring workflow

Security Posture Control uses API integrations with security tools such as web-application-firewalls and endpoint protection tools to import additional configuration data about your assets and analyze it to identify the applicable mitigation controls for a given asset. These API integrations are separate from the service graph connector integrations that are supported by SPC and import different data. You configure these API integrations from within the SPC Workspace.

Service graph connector integrations or ITOM Discovery are still required for mitigation controls monitoring. For example, both the CrowdStrike Service Graph Connector and the CrowdStrike API integration supported by SPC must be activated to import additional insights about which mitigation controls are enabled by the CrowdStrike endpoint protection configuration.

Mitigation controls policies

The Security Posture Control and the Mitigation Controls applications are required to view the mitigation controls and mitigation controls policies in the SPC. Both applications are available from the ServiceNow Store.

Refer to the following topics for more information about downloading and installing applications from the ServiceNow® Store.

- Download an application from the ServiceNow Store for the first time
- Install a Security Operations integration

To view the mitigation controls policies, users in the SPC Admin Group and SPC Analyst Group can navigate to **Workspaces** > **Security Posture Control** > **Policies and findings** > **All** in the SPC Workspace navigation panel.

The following mitigation controls policies are included with the application and are displayed along with the other SPC policies:

- SEH Overwrite
- Heap spray
- CrowdStrike NULL Page Allocation
- CrowdStrike Force DEP
- CrowdStrike Force ASLR
- Microsoft Defender Control Flow Guard
- Microsoft Defender force ASLR
- Microsoft Defender Mandatory ASLR and Bottom-up ASLR
- SentinelOne Application Control
- SentinelOne Data Files
- SentinelOne Executables
- SentinelOne Exploits
- SentinelOne IDR
- SentinelOne Detect Interactive Threat
- SentinelOne Detect Lateral Movement
- SentinelOne Static AI
- SentinelOne Static AI - suspicious

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- SentinelOne Potentially unwanted applications
- SentinelOne Remote shell
- SentinelOne Reputation

Mitigation controls categories

The following categories of mitigation controls are currently supported with the SPC.

- Mitigation controls and policies required for Exploit Protection (EDR) mitigation controls.
- Exploit Protection (WAF) mitigation controls. You must create policies for AWS WAF. See Create a policy for the AWS WAF integration for mitigation controls monitoring for more information.

Mitigation controls and policies required for Exploit Protection (EDR) mitigation controls

This category of mitigation controls covers mitigations available on your assets in the form of endpoint protection agent configuration. This applies to endpoint protection agents such as CrowdStrike and SentinelOne.

Exploit mitigation settings such as 'Force Address Space Layout Randomization' and 'Force DEP' can be enabled in endpoint protection tools like CrowdStrike. SPC automatically detects this configuration on devices with the help of the policies included with the application and the API integration with endpoint protection tools.

Roles required: SPC Admin Group and SPC Analyst Group.

Prerequisites for CrowdStrike Exploit Protection (EDR) mitigation control detection

1. Verify that you have activated the CrowdStrike Service Graph Connector. This application is available in the ServiceNow Store. The installation and configuration information is included on the app listing. See Install and configure the CrowdStrike integrations for mitigation controls monitoring for more information.
2. Verify that the CrowdStrike API integration is activated in the Security Posture Control Workspace.

Prerequisites for Microsoft Exploit Protection (EDR) mitigation control detection

Microsoft SCCM credentials that include the Script Authors role. The Script Authors role provides required permissions to create a script that is required to import mitigation information on the SCCM server.

You must activate the SCCM integration to identify mitigation controls configured in Microsoft Defender.

See Install and configure the Service Graph Connector for Microsoft SCCM and the Microsoft Defender Mitigation Control Integration for more information.

- Defender – Exploit Mitigation – CFG

  Microsoft Defender Control Flow Guard.

- Defender – Exploit Mitigation – DEP

  Microsoft Defender Data Execution Prevention.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Defender – Exploit Mitigation – Mandatory ASLR and Bottom-Up ASLR

  Microsoft Defender force ASLR.

- MITRE tactics addressed: Initial Access, Execution, Credential Access, Defense Evasion, Privilege Escalation, Lateral Movement.

1. Verify that you have activated the SentinelOne Service Graph Connector.

   This application is available in the ServiceNow Store. The installation and configuration information is included on the app listing. See Install and configure the Service Graph Connector for SentinelOne and the SentinelOne Mitigation Control Integration for more information.

2. Verify that the SentinelOne API integration is activated in the Security Posture Control Workspace.

Install and configure the CrowdStrike integrations for mitigation controls monitoring

The CrowdStrike Service Graph Connector and API integrations require separate configuration steps. You configure the CrowdStrike Service Graph Connector to import asset details. You configure the CrowdStrike API Integration to gather mitigation data about the assets that are monitored by CrowdStrike.

Before you begin

- Verify you have installed and activated the Security Posture Control and the Mitigation Controls Monitoring applications in your instance. These applications are available in the ServiceNow Store.
- The CrowdStrike Service Graph Connector must be installed and configured before you configure the CrowdStrike API integration.

Roles required: admin for installation of plugins, and SPC Admin Group and SPC Analyst Group for configuration of integrations in the workspace.

Procedure

1. To install and configure the CrowdStrike Service Graph Connector integration, follow these steps:

   Note: If you have installed the Service Graph Connector for CrowdStrike, proceed to step 2 for how to configure the CrowdStrike API Integration.

   a. Navigate to **Connectors and use cases setup** > **Service graph connectors tab**.

   b. Locate the CrowdStrike Endpoint Protection service graph connector.

   c. Select the link that takes you app listing for the Service Graph Connector for CrowdStrike in the ServiceNow® Store.

   d. Follow the prompts to install the application.

   e. Download the installation guide from the Supporting Links and Docs section on the app listing before you exit to help you with configuration and activation.

   f. Navigate to **CrowdStrike** > **Setup** in your instance.

   g. Follow the prompts in the guided setup and refer to the documentation to configure and activate the SGC.

2. Navigate to **Connectors and use cases setup** > **SPC API Integrations**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This tab lists the mitigation controls sources (CrowdStrike, F5 Big Ip, and SCCM), and the tab is displayed in the workspace only if you have installed the Mitigation Controls Monitoring application.

On the source cards, you can view the status of the mitigation source (`Active` or `Inactive`) and the number of mitigation controls and their associated policies that are monitored by CrowdStrike (6). You can select the number to view the list.

Note the Active column in Sources displays, `Active`. This indicates the source (CrowdStrike SGC) is active, but you must configure the CrowdStrike API Integration before you can monitor mitigation controls.

3. Select **Next**.
4. Select CrowdStrike in the Name column.
5. Select Edit and fill out the fields.

Note: Enter the same CrowdStrike account information and server details for the API Integration that you provided for the CrowdStrike Service Graph connector. This information ensures that you import mitigation data that matches the asset data that you imported with the service graph connector.

Field	Description
Name	Instance name. You can change this name to help you save credentials without testing them. If you change any fields under the Name field, you must test the connection prior to saving and exiting.
Asset Size Limit	Number of assets monitored.
Client ID	CrowdStrike ID
Client Secret	CrowdStrike Secret
API URL	API URL, for example, https://api.crowdstrike.com

6. When you are ready, select **Test connection**.
   A message is displayed if the connection is successful.
7. Select **Save and exit**.
8. Select **View details** on the CrowdStrike card on the SPC API Integrations tab and note the source and API are activated, and the configuration progress bar is completed.
9. **Optional:** If the credential test is not successful, you can select **Revert to previous credentials** to insert credentials you've previously validated.
10. Follow these steps to run the CrowdStrike integrations.

    a. Navigate to **CrowdStrike Mitigation Control** > **Integrations**.
    There are three integrations:

    - CrowdStrike Prevention Policy Integration
    - CrowdStrike Device Control Policy Integration
    - CrowdStrike Asset Insight Integration

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The integrations are chained and run in a specific order. Successful completion of one integration initiates the next.

b. Select the CrowdStrike Prevention Policy Integration in the Name column to initiate the integration runs.

c. On the record, select the **Active** check box and select **Execute Now**.

You can view the integration run status on the Integration Run tab from the integration records.

The integration is scheduled to run daily by default.

The CrowdStrike Asset Insight Integration imports only information about assets that have changed since the last integration run. The CrowdStrike Device Control Policy Integration and the CrowdStrike Prevention Policy Integration import all data for each run.

Install and configure the Service Graph Connector for Microsoft SCCM and the Microsoft Defender Mitigation Control Integration

The Service Graph Connector for SCCM and the Microsoft Defender Mitigation Control Integration require separate configuration steps.

Before you begin

You must install, activate, and configure the Service Graph Connector for SCCM to import asset details. You configure the Microsoft Defender Mitigation Control Integration, that also uses SCCM, to gather additional data about mitigation controls configured on the assets to that are monitored by the Service Graph Connector for SCCM.

Roles required:

- admin for installation and activation of plugins
- SPC Admin Group and SPC Analyst Group for configuration of integrations in the workspace
- Microsoft SCCM credentials that include the Script Authors role. The Script Authors role provides required permissions to create a script that is required to import mitigation information on the SCCM server.

  Note: This role must be created and assigned with the following permissions:

  Script Authors role

Category	Permission	State
Collection	Run Script	No
Site	Read	Yes
SMS Scripts	Create	Yes
SMS Scripts	Read	Yes
SMS Scripts	Delete	Yes
SMS Scripts	Modify	Yes

- Microsoft SCCM credentials that include the Script Approvers role. The script created to import mitigation information requires approval in your Microsoft SCCM console by user with the Script Approvers role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: This role must be created and assigned with the following permissions:

Script Approver

Category	Permission	State
Collection	Run Script	No
Site	Read	Yes
SMS Scripts	Read	Yes
SMS Scripts	Approve	Yes
SMS Scripts	Modify	Yes

Procedure

1. To install and configure the Service Graph Connector for Microsoft SCCM integration, follow these steps:

   Note: If you have installed the Service Graph Connector for Microsoft SCCM integration, proceed to step 2 to configure the Microsoft Defender Mitigation Control Integration.

   a. Navigate to **Connectors and use cases setup** > **Service graph connectors tab**.
   b. Locate the Service Graph Connector for Microsoft SCCM integration.
   c. Select the link that takes you to the app listing for the application in the ServiceNow® Store.
   d. Follow the prompts to install the application.
   e. Download the installation guide from the Supporting Links and Docs section on the app listing before you exit to help you with configuration and activation.
   f. Navigate to **Setup** in your instance.
   g. Follow the prompts in the guided setup and refer to the documentation to configure and activate the SGC.
2. Navigate to **Connectors and use cases setup** > **SPC API Integrations** to configure the Microsoft Defender Mitigation Control Integration.

   This tab lists the mitigation controls sources (CrowdStrike, F5 Big Ip, and Defender), and the tab is displayed in the workspace only if you have installed the Mitigation Controls Monitoring application.

   On the source cards, you can view the status of the mitigation source (`Active` or `Inactive`).

   Note the Active column in Sources displays, `Active`. This indicates the source (Service Graph Connector for Microsoft SCCM) is active to retrieve asset data, but you must configure the Microsoft Defender Mitigation Control Integration that fetches additional data about defender configurations on these assets using SCCM before you can monitor mitigation controls.
3. Select **Next**.
   The SCCM Configuration page is displayed with one Microsoft SCCM Mitigation Control instance link.
4. Select the instance link that is provided in the Name column.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Fill out the fields for the SCCM credentials configuration Microsoft SCCM Mitigation Control Integration modal.

Field	Description
Name	Field is populated automatically with the instance name.
Connection	Field populated automatically with connection information.
Host	Host name for the SCCM server inside the connection information provided in the previous field.
User name	User name to access the SCCM server.
Password	Password to access the SCCM server.
MID Server	Select a ServiceNow-managed MID Server from the list.
Validation status	Field populated after validation attempt. If the connection successful, the integration instance state is **Valid**.
SG connector connection	Select one Connection and Credential Aliases option from the list for the Service Graph Connector for Microsoft SCCM. You set this connection up during the Guided Setup steps for Microsoft SCCM SGC.
Validation detail	Details about the validation attempt.

6. Select **Save and Test Credentials**.
   A `Valid` response for a successful connection is required to proceed to the next step.
7. Select **Next**.
   A PowerShell script is created automatically to retrieve mitigation details. A modal is displayed with the option to Validate script approval.
8. To approve the script, log in to your Microsoft SCCM console with the Script Approver role.

   A PowerShell script has been generated in your SCCM Configuration manager to retrieve mitigation details. You must log in with the appropriate credentials with a user role that has the script approver permission in order to approve the script. After it is approved, you can validate it in your ServiceNow AI Platform instance.

9. In your console, locate the **[Servicenow Secops]: Get System Mitigations** script and approve it.

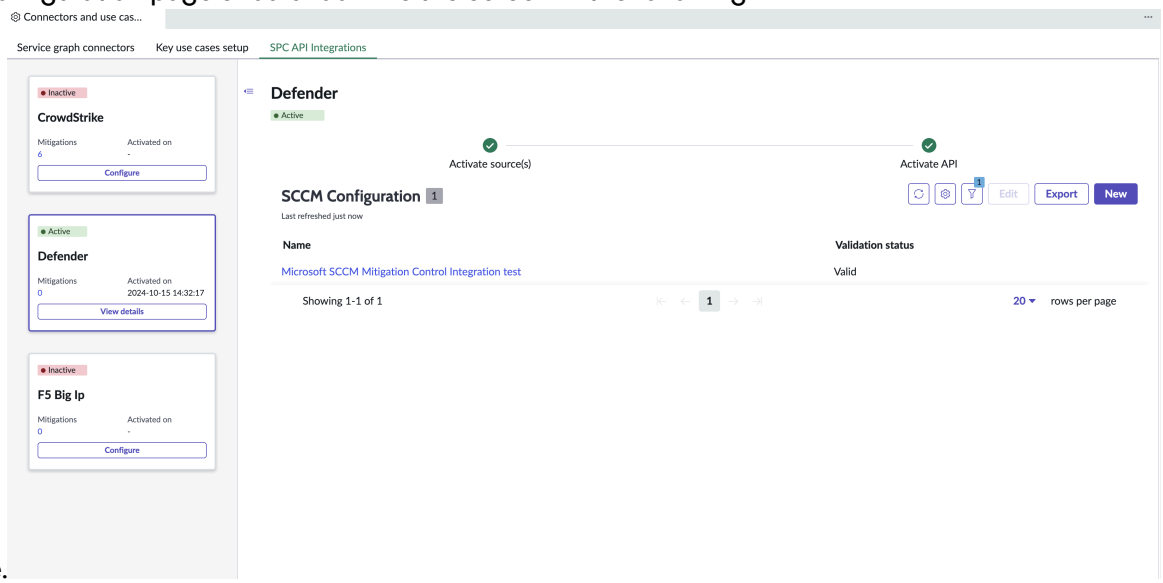
   Note: In your SCCM configuration manager, the Script section is located under the software library. Locate: [Servicenow Secops]: Get System Mitigations script to approve it.

   This script remains in the **Waiting for approval** state until you approve it.

   You can validate the script in your ServiceNow AI Platform instance without approving it as described above, but the error message, `Script is not approved is displayed`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. To validate the approval, return to your ServiceNow AI Platform instance and in the Approve PowerShell script modal select **Validate script approval**.
11. Select **Done**.
    The configuration page should look like the screen in the following image.



Create multiple instances for the Microsoft Defender Mitigation Control Integration

You can configure multiple instances for the Microsoft Defender Mitigation Control Integration.

Before you begin

Roles required:

- SPC Admin Group and SPC Analyst Group for configuration of new integration instances in the workspace
- Microsoft SCCM credentials that include the Script Authors role. The Script Authors role provides required permissions to create a script that is required to import mitigation information on the SCCM server.

  Note: This role must be created and assigned with the following permissions:

Script Authors role

Category	Permission	State
Collection	Run Script	No
Site	Read	Yes
SMS Scripts	Create	Yes
SMS Scripts	Read	Yes
SMS Scripts	Delete	Yes
SMS Scripts	Modify	Yes

- Microsoft SCCM credentials that include the Script Approvers role. The script created to import mitigation information requires approval in your Microsoft SCCM console by user with the Script Approvers role.

  Note: This role must be created and assigned with the following permissions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Script Approver

Category	Permission	State
Collection	Run Script	No
Site	Read	Yes
SMS Scripts	Read	Yes
SMS Scripts	Approve	Yes
SMS Scripts	Modify	Yes

Procedure

1. Navigate to **Connectors and use cases setup** > **SPC API Integrations**.
2. Select **New**.
   The New Defender instance modal is displayed.
3. Enter a name for your new instance and select **Create instance**.
   The SPC API Integrations page is displayed with the instance provided with the application and your new instance.
4. Select the link for your new instance.
5. Fill out the fields in the SCCM credentials configuration modal for your new instance.

Field	Description
Name	Field is populated automatically with the instance name.
Connection	Create a new connection. **a.** Select **Create Connection and Alias** at the top of the modal. **b.** In the Connection and Credential Aliases form, fill out the mandatory fields. ▪ **Name** - Unique name ▪ **Type** - Connection and Credential ▪ **Connection type** - Basic **Note:** Do not select **Submit** at this time. **c.** Right-click anywhere in the gray header and select **Save**. The page refreshes and related links and tabs are displayed at the bottom of the page after you save it. **d.** With the Connections tab selected, select **New** at the right of the tab. The Connection form is displayed. Fill out the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

	▪ **Name** - Unique name
	▪ Credential - Select the search icon. Locate the Windows credentials and select the link. On the Windows Credentials form, fill out the fields.
	  ▪ **Name** - Unique name
	  ▪ Username - User name for the credentials. This is the user name that will be referenced for the Username field in the SCCM credentials configuration modal after you save it on this page.
	  ▪ Password - Password for the credentials. This is the password that will be referenced for the password field in the SCCM credentials configuration modal after you save it on this page.
	▪ Host - This is the Host for the SCCM server that will be referenced in the Host field in the SCCM credentials configuration modal after you save it on this page.
	e. Select the **Use MID Server** check box. Select Specific MID Server for **MID Selection** and select one from the MID Server list.
	f. Right-click anywhere in the gray header and select **Save**. These are the credentials you enter on the Connection form described above in step d.

Host	This is the Host for the SCCM server referenced from the Host field after you save it on the Connection page as described above.
User name	This is the user name referenced from the Username field after you save it on the Connection page as described above.
Password	This is the password referenced from the Password field after you save it on the Connection page as described above.
MID Server	This is the MID Server referenced from the MID Server fields after you save it on the Connection page as described above.
Validation status	Field populated after validation attempt. If the connection successful, the integration instance state is **Valid**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
SG connector connection	Select one Connection and Credential Aliases option from the list for the Service Graph Connector for Microsoft SCCM. You set this connection up during the Guided Setup steps for Microsoft SCCM SGC.
Validation detail	Details about the validation attempt.

6. Navigate to **Connectors and use cases setup** > **SPC API Integrations**.
7. Select the link for your new instance.
8. In the SCCM credentials configuration modal, select the connection from the list that you created in step 5 for the Connection field.

   Note that the fields listed below are auto-populated based on the information you entered for your new connection.

Host	This is the Host for the SCCM server referenced from the Host field after you save it on the Connection page as described above.
User name	This is the user name referenced from the Username field after you save it on the Connection page as described above.
Password	This is the password referenced from the Password field after you save it on the Connection page as described above.
MID Server	This is the MID Server referenced from the MID Server fields after you save it on the Connection page as described above.
Validation status	Field populated after validation attempt. If the connection successful, the integration instance state is **Valid**.
SG connector connection	Select one Connection and Credential Aliases option from the list.
Validation detail	Details about the validation attempt.

9. Select **Save and Test Credentials**.
   A `Valid` response for a successful connection is required to proceed to the next step.
10. Select **Next**.
    The PowerShell script is created as described in Install and configure the Service Graph Connector for Microsoft SCCM and the Microsoft Defender Mitigation Control Integration. Follow the steps in that topic to approve the scripts for your new instances.

Install and configure the Service Graph Connector for SentinelOne and the SentinelOne Mitigation Control Integration

The Service Graph Connector for SentinelOne and the SentinelOne Integration for Mitigation Control Integration require separate configuration steps. You install and configure the Service Graph Connector for SentinelOne to import asset details. You configure the SentinelOne

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integration for Mitigation Control Integration to gather mitigation data about the assets that are monitored by the Service Graph Connector for SentinelOne.

Before you begin

Roles required:

- admin for installation and activation of plugins.
- SPC Admin Group and SPC Analyst Group for configuration of integrations in the workspace.
- SentinelOne credentials.

Procedure

1. To install and configure the Service Graph Connector for SentinelOne integration, follow these steps:

   Note: If you have installed the Service Graph Connector for SentinelOne, proceed to step 2 to configure the SentinelOne Integration for Mitigation Control Integration.

   a. Navigate to **Connectors and use cases setup** > **Service graph connectors tab**.

   b. Locate the Service Graph Connector for SentinelOne integration.

   c. Select the link that takes you to the app listing for the application in the ServiceNow® Store.

   d. Follow the prompts to install the application.

   e. Download the installation guide from the Supporting Links and Docs section on the app listing before you exit to help you with configuration and activation.

   f. Navigate to **Setup** in your instance.

   g. Follow the prompts in the guided setup and refer to the documentation to configure and activate the SGC.

2. Navigate to **Connectors and use cases setup** > **SPC API Integrations** to configure the SentinelOne Integration for Mitigation Control Integration.

   This tab lists the mitigation controls sources: CrowdStrike, F5 Big Ip, Defender, SentinelOne. The tab is displayed in the workspace only if you have installed the Mitigation Controls Monitoring application.

   On the source cards, you can view the status of the mitigation source (`Active` or `Inactive`).

   Note the Active column in Sources displays, `Active`. This indicates the source, in this case, the Service Graph Connector for SentinelOne, is active to retrieve asset data, but you must configure the SentinelOne Integration for Mitigation Control Integration before you can monitor mitigation controls on the imported assets.

3. Select **Next**.
   The SentinelOne Configuration page is displayed with one SentinelOne Integration for Mitigation Control instance link.
4. Select the instance link that is provided in the Name column.
5. Fill out the fields for the SentinelOne Integration for Mitigation Control Integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

Enter the same SentinelOne account information and server details for the SentinelOne Integration for Mitigation Control Integration that you provided for the Service Graph Connector for SentinelOne. This information ensures that you import mitigation data that matches the asset data that you imported with the service graph connector.

Select the pen icon if you need to edit the fields.

Field	Description
Instance name	Field is populated automatically with the instance name.
API Key	Field populated automatically with the API key information.
API URL	Host name for the SentinelOne server, for example: https//usea1-na.sentinelone.net

6. Select **Save and Test Credentials**.
   A `Valid` response for a successful connection is required to proceed to the next step.
7. Select **Save and Exit**.
8. Select **View details** on the SentinelOne card on the SPC API Integrations tab.
   Note that the source and API are activated, and the configuration progress bar is completed.
9. **Optional:** Select **Revert to previous credentials** to insert credentials that you've previously validated.
10. Follow these steps to run the SentinelOne Asset Import Integration.

    a. Navigate to **SentinelOne Mitigation Control** > **Integrations**.
    There is one integration: SGC SentinelOne Asset Import.

    b. Select the **SentinelOne Prevention Policy Integration** in the Name column to initiate the integration.

    c. On the record, select the **Active** check box and select **Execute Now**.

    You can view the integration run status on the **Integration Run** tab from the integration records.

    The integration is scheduled to run daily by default.

    The SentinelOne Asset Import Integration imports only information about assets that have changed since the last integration run.

Exploit Protection (WAF) mitigation controls

This category of mitigation controls covers mitigations available in the form of Web Application Firewall.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploit Protection (WAF)

Security Posture Control detects servers that are running behind the web application firewall (WAF) by using the API integration with WAF tools such as F5 BIG-IP (F5) and network traffic data from ITOM IP-based Discovery, if necessary.

Mitigation control imports the Web ACL rules and all associated load balancers to determine which rules are protecting your virtual machines with the help of Discovery and Service Mapping patterns.

Roles required: SPC Admin Group and SPC Analyst Group.

Prerequisites for Exploit Protection (WAF) with F5 BIG-IP

1. Verify that you have activated ITOM IP-based Discovery in the environment where F5 BIG-IP F5 WAF and associated application servers are setup.
2. Verify that the API integration for F5 BIG-IP F5 is activated in the Security Posture Control Workspace.

Prerequisites for Exploit Protection (WAF) with Amazon Web Services AWS

Data for this integration is imported by the Discovery and Service Mapping Patterns [sn_itom_pattern] and the Mitigations Controls Monitoring [sn_sec_mit_ctrl] application. Both applications are required. Follow the steps below in the order they are listed so that you can import all the Web ACLs, the Web ACL rules, and the mitigation data required to help you confirm that a virtual machine is protected. See Amazon AWS Cloud components discovery using patterns for more information about AWS discovery patterns.

1. Define Web ACLs and rules in your AWS service account you want to use. See Using web ACLs in AWS WAF for more information.

   Note: You can create your own Web ACL rules, however, you might prefer to use the AWS manged rules that are designed specifically to work with their Web ACLs. If you choose to create your own custom rules for Web ACLs, note that this integration with AWS WAF supports only attack types that match Contains SQL injection attacks and Contains XSS (cross site scripting) injection attacks. Load balancers are the assets (resources) supported by this integration.

2. Install and activate the Discovery and Service Mapping Patterns [sn_itom_pattern] application in your instance so the names and default actions of the Web ACLs you defined in step 1 can be discovered. For more information, see Install the supported applications for Security Posture Control.
3. Verify the sn_itom_pattern.discover_aws_app_pool_members MID Server system property is set to `true`. To activate this property, navigate to **All** > **MID Server** > **Properties**.
4. Verify you have installed and activated the Mitigation Controls Monitoring [sn_sec_mit_ctrl] application. This application includes a pattern extension, Web ACL Rules and Associated Resources. This pattern extension permits you to import the actual Web ACL rules and their associations (relationships) to your resources (assets) into your instance.

Configure the F5 BIG-IP integrations for mitigation controls monitoring

The ITOM IP-based Discovery application and the F5 BIG-IP API integrations require separate configuration steps. You configure the ITOM IP-based Discovery application to import asset details. You configure the F5 BIG-IP API Integration to gather mitigation data about the assets that are monitored by ITOM IP-based Discovery.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- ITOM IP-based discovery must be up and running in the environment where F5 BIG-IP and any associated application servers are setup.
- For on-premise assets, you must provide a MID Server.
- Activate the source (ITOM) to gather data about the assets being monitored.
- Activate the API Integration to gather mitigation data about the assets.

Roles required: admin for installation of plugins and creating system properties, and SPC Admin Group and SPC Analyst Group for configuration of integrations in the workspace.

Procedure

1. To install and configure the integration, follow these steps:

   Note: If you have installed and activated ITOM, proceed to step 2 for how to configure the F5 BIG-IP (F5) API Integration.

   a. Navigate to **Connectors and use cases setup** > **Service graph connectors tab**.

   b. Select the F5 BIG-IP card.

   c. Select the **ITOM Plugin** link to activate the ITOM plugin.

   d. Follow the prompts.

2. Navigate to **Connectors and use cases setup** > **SPC API Integrations**.

   This tab lists the mitigation controls sources (CrowdStrike and F5 Big Ip, and SCCM), and the tab is displayed in the workspace only if you have installed the Mitigation Controls Monitoring application.

   On the source cards, you can view the status of the mitigation source (`Active` or `Inactive`.

3. Select **Next**.

   Note that the source (ITOM) is active, but you must configure and activate the F5 BIG-IP API Integration before you can monitor mitigation controls.

4. Select F5 BIG-IP in the Name column.
5. Select Edit and fill out the fields.

Field	Description
Name	Instance name. You can change this name to help you save credentials without testing them. If you change any fields under the Name field, you must test the connection prior to saving and exiting.
Username	F5 BIG-IP username
Password	F5 BIG-IP password.
MID Server	Select a MID Server from the list.
API URL	API URL with port 8443, for example, https://bigip.example.com:8443.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. When you are ready, select **Test connection**.
   A message is displayed if the connection is successful.

   If the following error results from testing the connection during the configuration steps, `Session contains no certificates - Untrusted: Session contains no certificates - Untrusted`, set the following system properties to `false`:

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   A user with the admin role must create these system properties in the global scope if they are not listed on the System Property [sys_properties] table. The system properties is Type, True/False (Boolean).

7. Select **Save and exit**.
8. On the F5 BIG-IP card on the SPC API Integrations tab and note the source and API are activated, and the configuration progress bar is completed.
9. **Optional:** If the credential test is not successful, you can select **Revert to previous credentials** to insert credentials you've previously validated.
10. To run the API integrations, follow these steps:

    a. Navigate to **F5 Big Ip Mitigation Control** > **Integrations**

       There are Five integrations. The integrations are chained and run in a specific order. Successful completion of one integration initiates the next one:

       - F5 Big IP Device Integration
       - F5 Big IP Policy Integration
       - F5 Big IP Attack Signature Integration
       - F5 Big IP Virtual Server Integration
       - F5 Big IP Pool Member Integration

    b. To initiate the integration chain, select the **F5 Big IP Device Integration** in the Name column.

    c. On the record, select the **Active** check box and select **Execute Now**.

    d. View the status of the integration runs on the Integration Run tab from the integration records.
       The integration is scheduled to run daily by default.

Configure the AWS WAF integration for mitigation controls monitoring

Determine if your virtual machines are protected with the AWS WAF integration for mitigation controls monitoring.

Before you begin

Data is imported by two separate applications:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Discovery and Service Mapping Patterns application imports the names and the default actions, allow or block, of the Web ACLs that you define in your AWS Service Account. The Discovery Pattern `Amazon AWS - Web ACL (LP)` is activated with the application.
- The Mitigations Controls Monitoring application imports the actual Web ACL rules and the relationships between associated resources like an application load balancer. This extension is included as a part of the Mitigations Controls Monitoring application.

Verify you have completed the steps to define Web ACLs and rules and activated the required applications for the AWS WAF Integration described in Exploit Protection (WAF) mitigation controls prior to activating the applications.

Roles required:

- admin for installation of plugins in your ServiceNow AI Platform® instance.
- SPC Admin Group for configuration of integrations in the workspace.
- AWS credentials for the AWS service account you want to use.

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Connectors and use cases setup** > **SPC API Integrations tab**.
2. Select the **AWS WAF** tile.
3. Select one.

Option	Description
View service accounts	View the available AWS service accounts that are configured in your instance. To create a new account: **a.** Select **View service accounts**. **b.** Select **New**. **c.** Fill in the fields. ▪ Name - Name of your AWS service account. This is the account you use for your Discovery schedule and credentials. ▪ Account id - Account ID for your AWS service account. ▪ Datacenter type - Select **AWS Datacenter [cmdb_ci_aws_datacenter]** **d.** Select **Submit**.
Configure service account	Configure an AWS service account in your instance.

4. Create the Discovery schedule for the AWS service account you want to use.
   a. Navigate to **All** > **Discovery** > **Home**.
   b. Select **View Active Schedules**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select **Add Schedule**.

d. Select **Add Cloud Schedule** and fill in the fields.

Field	Description
Provider	AWS
Schedule name	Enter a unique name for your schedule to help you distinguish it from other AWS schedules.
Add Account	Select to create a Service Account.
Select Account	Select to edit an existing Service Account.
Account ID	Account ID for your AWS service account.
MID Selection Type	You must provide a MID Server. Select one: ▪ Auto-select MID Server ▪ Specific MID Cluster ▪ Specific MID Server To import rules data for individual virtual machines with your MID Server, you must activate a MID Server property. To verify or set this property, navigate to **All** > **MID Server** > **Properties** > **sn_itom_pattern.discover_aws_app_pool_members**. Set the Value to `true`.
Credentials	These are the Discovery credentials for your service account.
URL	
Access Role Name	
Select account for access	

e. Select **Test Account**.
You must have a successful validation before you can continue.

f. Select **Next**.

g. Select the datacenters you want to discover.

h. Select the **Discover VMs by IP address** toggle and select the MID Server you selected in step d from the list.

i. Select **Next**.

j. Select how often and when you want to run your discovery.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

k. Select **Finish and Run**.

After the discovery schedule you set has run, the discovery pattern **Amazon AWS - Web ACL (LP)** runs and the data from both applications is imported.

Create a policy for the AWS WAF integration for mitigation controls monitoring

Create a policy so you can audit your assets based on data imported from the integration.

Before you begin

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **Workspaces** > **Security Posture Control** > **Policies and findings** > **All**.
2. Select **Hardware Asset** for Asset type.

   Properties also work for Asset search and Asset Profiles.
3. For Connection select **Security control configuration**.
4. For Entity select **AWS Insight**.

   A Criteria field is displayed auto-populated with `Connection`.
5. For the new Connection field select **With AWS managed rule**.

   The Entity field is auto-populated with `Managed Rule` and a Criteria field is displayed auto-populated with `Property`. Blank Property, Operator, and Value fields are displayed.

   If you created a custom AWS rule, select **With custom match statement**. The Entity field is populated with `Match Statement`.
6. Select properties from the list.

   You can add more than one.

   For example, for a Web ACL for SQL database in your AWS Service Account, you might see the following rules:

   - SQLiExtendedPatterns_QUERYARGUMENTS
   - SQLiQUERYARGUMNETS
   - SQLi_BODY
   - SQLi_COOKIE
   - SQLi_URIPATH

   From the policy builder, this property displays as: SQLRuleSet-SQLi_BODY is Allow. You can select **Allow** or **Block** from the list.
7. Select **or** to add properties.
   See Create and activate custom policies for Security Posture Control for more information about using the policy builder to create policies.
8. Select **Save changes** when you have completed your policy.
9. **Activate** the policy if you want to view findings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. See View findings for Security Posture Control for more information about viewing the findings from your policy.
11. Open a record on the list and select the Mitigation controls Mitigated vulnerable items tabs.

    The Mitigated vulnerable items tab lists all the mitigated vulnerable items that include information about the CVEs that are mitigated as a result of the mitigation rules that are found on your assets.

    - Verified source(s) - AWS APIs, ITOM Discovery
    - Protected by Web Application Firewall (WAF) - Yes
    - WAF type - AWS
    - Vulnerable items fully mitigated - number of associated vulnerable items mitigated.
    - Vulnerable items partially mitigated - number of associated vulnerable items in process.
    - Managed Rules categorized by actions - Managed Rules with 'Block' and 'Allow' actions.

      You might see more rules than you entered for your policy. These rules are identified with `CommonRuleSet` (CRS) in the rule.

    - Custom Rules - any of your custom rules categorized by 'Block' and 'Allow' actions.
    - On the Home page dashboard, the Assets with mitigations tile lists the assets that are protected by WAF in the Exploit Protection (WAF) visualization.

View detected mitigations

You must activate policies before you can view which threats to your assets are mitigated by available mitigation controls.

Before you begin

Verify you have completed the requirements listed in Install and configure the CrowdStrike integrations for mitigation controls monitoring, Install and configure the Service Graph Connector for Microsoft SCCM and the Microsoft Defender Mitigation Control Integration and Configure the F5 BIG-IP integrations for mitigation controls monitoring.

Roles required: SPC Admin Group and SPC Analyst Group.

Procedure

To view assets with mitigations detected by Security Posture Control with the ‘Assets with MITRE mitigations’ widget on the dashboard, follow these steps.

a. Navigate to **Workspaces** > **Security Posture Control** > **Home**.

b. Under the Key insights section, review the Assets with MITRE mitigations widget.

c. Select a mitigation category, **Exploit Protection (EDR)** or **Exploit Protection (WAF)** in the widget.

d. You can see the list of assets with mitigations detected in that mitigation category.

e. Select an asset.

f. Select the **Mitigation controls** tab to see the details of the mitigation control detected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

g. Select the **Mitigated vulnerable items** tab to see the list of vulnerable items mitigated by this mitigation control.

> **Note:** For this tab to be populated, the Vulnerability Response application must be installed and activated.

Mitigation controls to vulnerable item mapping

Mitigation controls data is mapped to vulnerable items. You can view a list of mitigation controls that are used to mitigate the vulnerabilities and underlying Common Vulnerabilities and Exposures (CVEs) associated with the vulnerable items.

After identifying a specific mitigation control on an asset, Security Posture Control automatically identifies any vulnerable items that are mitigated by that control. For example, any vulnerable items with CVEs that are part of signatures in Web Application Firewall (WAF) policies are marked as mitigated vulnerable items. This identification might be useful for vulnerability management teams to help them automatically reduce risk scores for vulnerable items that are mitigated.

Vulnerable item mitigation controls table

The Vulnerable item mitigation controls [sn_vul_vulnerable_item_mitigation_control] table has been created to map mitigation control data to mitigated vulnerable items (VITs). This table lists mitigated VITs and the detected mitigation controls that were used to mitigate the vulnerabilities and their underlying CVEs associated with the vulnerable items. The mitigated CVE records contain references to the mitigation control used for the assets, for example, Exploit Protection (EDR).

Example data is shown in the following table.

Vulnerable item mitigation controls data

Mitigation control exists	Mitigation control effectiveness	Detected mitigation control type	CVEs mitigated	Vulnerable item
Yes/No	Moderate	Exploit Protection (EDR)	CVE-2009-3373	VIT0018323

Open a mitigation control record (Detected mitigation control type) on the table to review details about how a CVE and its related Common Weakness Enumeration (CWE) vulnerability is mitigated by the mitigation control associated with an asset. The mitigation control record contains details about the CWEs that have been mitigated, for example, how a mitigation setting satisfies vulnerabilities specified in a CWE.

Risk calculator and risk calculator rules

Mitigation information might be used to help you set up customized risk calculator rules to help you recalculate the risk scores on VITs that have specific types of vulnerabilities and mitigation controls associated with them. For this example rule, which is based on the preceding table, the default risk calculator calculates a risk score of 60 for VITs that have the mitigation control type, Exploit Protection (EDR) on detected assets. This calculation score is due to the moderate risk that is associated with the vulnerability with this mitigation in place.

Example risk calculator rule with the following conditions:

[Mitigation control details] [is not] [empty] AND [Mitigation control details, Detected mitigation control type] [is] [Exploit Protection (EDR)].

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Values:

[Risk score][is][60]

See Define fields and weights for the risk rule for Vulnerability Response Risk Calculators for more information.

Use cases, policy examples, and supported service graph connectors in Security Posture Control

Use cases are different scenarios that you configure to help you identify specific types of tool coverage gaps. Each use case requires a policy or policies to audit your assets for potential violations. You can also define your own policies to help you fulfill requirements for your specific internal security standards.

Use cases

The Security Posture Control application supports various use cases that are included with the application. Use cases help you identify specific types of tool coverage gaps in your assets, internet exposure of cloud assets, and combinations with vulnerabilities. The policies that you need for the supported use cases are also included with the product.

You can view the coverage status for some of the key use cases on the Home (landing) page in the Security Posture Control Workspace at **Workspaces** > **Security Posture Control** > **Home** on the Home module (landing page).

Alternatively, you can view the supported service graph connectors and coverage status for some of the key use cases on the 'Service graph connectors supported' and 'Key use case setup' tabs at **All** > **Workspaces** > **Security Posture Control** > **Connectors and use cases setup** (the gear icon).

Note:

The Key use cases tab on the Home landing pages does not list all the possible use cases. It provides you with a few important use cases that you activate to help you get started with Security Posture Control product deployment.

Before you activate policies for the supported use cases provided with the application verify you have completed the following tasks.

- You have installed and configured all the required applications described in Install the supported applications for Security Posture Control.
- You have met one or more of the following prerequisites for each use case.

1. You are currently using or you install and activate service graph connectors for various categories.

   Categories for the use cases include service graph connectors that you must activate to get initial insights, and #service graph connectors that you have the option to activate for improved coverage for the assets Security Posture Control#s monitoring.

2. You are currently using or you install and activate the Vulnerability Response application.
3. You are currently using or you configure the Cloud Account Scan for your AWS and Azure accounts under ‘Cloud Security Posture Management’.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Specific requirements for each supported use case are described in the following sections. Additionally, you must activate one or more of the policies shipped with Security Posture Control for a use case. This concept is also covered in the following sections.

Examples of base, child, and cloned policies

See Examples of base, child, and cloned policies for Security Posture Control and how you can reuse the conditions of a base policy when you create other policies. Create base, child policies and cloning existing policies in these examples. These examples also help you see how the policy builder works in the Policies and findings module.

Supported service graph connectors

See tables of supported service graph connectors, their tool categories, and the types of data they import in Supported hardware service graph connectors for Security Posture Control and Supported software service graph connectors for Security Posture Control.

Security Posture Control use case: Detecting assets with missing endpoint protection

To detect assets missing an endpoint protection agent, the following prerequisites are required.

Depending on your use case, you can choose to activate only the required connectors.

1. Activate at least one Service Graph Connector from the Endpoint Protection category.
2. Activate at least one Service Graph Connector for ONE of the following categories.
   a. Directory Services (Microsoft Active Directory).
   b. Endpoint Management: Microsoft Intune or Jamf Device and Endpoint Management.
   c. Configuration and Patch Management: Microsoft SCCM or IBM Bigfix.
   d. Cloud Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

   Note: If Cloud Discovery is activated, these service graph connector products are not required.

3. [Optional] You can activate Service Graph Connectors for any of the following categories to improve overall coverage, that is, the number of assets that are reported and monitored by Security Posture Control.
   a. Network Security
   b. Infrastructure Monitoring
   c. Networking
   d. Application Performance Monitoring#.

After you verify you have met these prerequisites, you must activate the following policy, Assets missing endpoint protection###.#For more information on policies, please refer to Policies for Security Posture Control.

Security Posture Control use case: Detecting assets missed by vulnerability assessment tools

To detect assets missed by vulnerability assessment tools, the following pre-requisites are required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For each Service Graph Connector in the list, you can see if that connector is required for monitoring on-prem assets or cloud assets. Depending on your use case, you can choose to activate only the required connectors.

1. Activate at least one Service Graph Connector from the Vulnerability Assessment category.
2. Activate at least one Service Graph Connector for ONE of the following categories.
   a. Directory Services (Microsoft Active Directory).
   b. Endpoint Management: Microsoft Intune or Jamf Device and Endpoint Management.
   c. Configuration and Patch Management: Microsoft SCCM or IBM Bigfix.
   d. Cloud Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

   Note: If Cloud Discovery is activated, these service graph connector products are not required.

3. [Optional] You can activate Service Graph Connectors for any of the following categories to improve overall coverage, that is, the number of assets that are reported and monitored by Security Posture Control.
   a. Network Security#.
   b. Networking.
   c. Infrastructure Monitoring.
   d. Application Performance Monitoring#.

After you verify you have met these prerequisites, you must activate the following policy, Assets not scanned for vulnerabilities. For more information on policies, please refer to Policies for Security Posture Control.

Security Posture Control use case: Detecting unmanaged assets

This use case includes two parts, detecting assets that are missing configuration and patch management agents.

To detect assets missing configuration and patch management tools, the following pre-requisites are required.

For each Service Graph Connector in the list, you can see if that connector is required for monitoring on-premise assets or cloud assets.

Depending on your use case, you can choose to activate only the required connectors.

1. Activate at least one Service Graph Connector from the Configuration and Patch Management categories.
2. At least one Service Graph Connector must be enabled for ONE of the following categories.
   a. Directory Services (Microsoft Active Directory).
   b. Endpoint Protection: CrowdStrike or SentinelOne.
   c. Vulnerability Assessment: Qualys, Rapid7, or Tenable.
   d. Configuration and Patch Management: Microsoft SCCM or IBM Bigfix.
3. [Optional] You can activate Service Graph Connectors for any of the following categories to improve overall coverage, that is, the number of assets that are reported and monitored by Security Posture Control.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Networking.

b. Infrastructure Monitoring

c. Network Security

d. Application Performance Monitoring#.

After you verify you have met these prerequisites, you must activate at least one of the following policies.#For any policy that starts with 'Cloud assets', Service Graph Connectors under the category 'Cloud Provider' must be enabled.#For more information on policies, please refer to Policies for Security Posture Control.

- Assets missing configuration and patch management.
- Cloud assets missing configuration and patch management.

Security Posture Control use case: Detecting assets missing an endpoint management solution

To detect assets missing an endpoint management solution, the following pre-requisites are required.

Depending on your use case, you can choose to activate only the required connectors.

1. Activate at least one Service Graph Connector from the Endpoint Management category.
2. At least one Service Graph Connector must be enabled for ONE of the following categories.
   a. Directory Services (Microsoft Active Directory).
   b. Endpoint Protection: CrowdStrike or SentinelOne.
   c. Vulnerability Assessment: Qualys, Rapid7, or Tenable.
   d. Configuration and Patch Management: Microsoft SCCM or IBM Bigfix.

After you verify you have met these prerequisites, you must activate the following policy, Assets missing endpoint management solution. For more information on policies, please refer to Policies for Security Posture Control.

Security Posture Control use case: Detecting assets with vulnerabilities and security tool coverage gaps

You can identify assets with critical vulnerabilities and missing critical security tools such as endpoint protection to prioritize those assets for remediation. Security Posture Control ships a few policies included with the product to support this use case.

This use case requires that you install the Vulnerability Response application and an integration with at least vulnerability assessment product such as Qualys, Rapid7, or Tenable.

The following policies are included with the Security Posture Control product to support this use case for assets with critical vulnerabilities that are also missing security tool coverage.

1. Assets with critical vulnerabilities and missing endpoint protection.
2. Assets with critical vulnerabilities and missing configuration and patch management.
3. Assets with critical vulnerabilities and missing endpoint management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Posture Control use case: Detecting internet exposure of cloud assets and high-risk combinations

It is critical to monitor potential internet exposure of Cloud assets (virtual machines) on various ports to ensure that vulnerabilities on these assets are not exploited remotely. This use case helps you identify these assets.

Security Posture Control permits you to evaluate the configuration of cloud assets to help you identify those assets that are internet-facing, that is, which assets are reachable from anywhere on the internet and from what ports they are exposed.

Security Posture Control combines these insights with security tool coverage gaps and vulnerability data from third-party scanners such as Qualys, Rapid7, or Tenable to identify high-risk combinations.

Currently, this use case supports AWS and requires the following pre-requisites.

1. The Service Graph Connector for AWS is activated for the same AWS accounts that you have configured.
2. You have activated one or more of the policies that are included with the product in Security Posture Control.
   - Cloud assets with SSH port 22 open to internet.
   - Cloud assets with SSH port 22 open to internet and missing endpoint protection.
   - Cloud assets with HTTP port 80 open to internet and missing endpoint protection.
   - Cloud assets with critical vulnerabilities and SSH port 22 open to internet (Requires Vulnerability Response).
   - Cloud assets with critical vulnerabilities, missing endpoint protection and SSH port 22 open to internet (Requires Vulnerability Response).
   - Cloud assets with HTTP ports open to internet, critical vulnerabilities, and missing endpoint protection (Requires Vulnerability Response).

Supported hardware service graph connectors for Security Posture Control

Supported Hardware service graph connectors with CI class, source (product), and tool categories. This list is not complete and is subject to change with the addition of more products.

For Discovery source for a connector listed, 'SG', 'SGO', or 'SGC' precedes the product name for third-party products, for example, SG-AWS, SGO-Datadog, or SGC-AD (Active Directory). For ServiceNow products, 'SN' or 'ServiceNow' precedes the product name, for example, SNAssetManagement for ServiceNow Hardware Asset Management.

After you install them, you can view the connectors and their categories on the connector table [sn_sec_spc_core_connector] in your instance.

You can view Asset types and how they map to CI classes and Connectors on the [sn_sec_spc_core_asset_type_connector] table.

Hardware service graph connectors

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_computer	Active Directory	Directory Services

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_server	AppDynamics	Application Performance Monitoring
Hardware Asset	cmdb_ci_server	Automox	Configuration and Patch Management
Hardware Asset	cmdb_ci_computer	Automox	Configuration and Patch Management
Hardware Asset	cmdb_ci_computer	BigFix	Configuration and Patch Management
Hardware Asset	cmdb_ci_server	BigFix	Configuration and Patch Management
Hardware Asset	cmdb_ci_printer	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_server	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_iot	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_hc_device	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_netgear	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_computer	Cisco Meraki	Networking
Hardware Asset	cmdb_ci_server	CrowdStrike	Endpoint Protection
Hardware Asset	cmdb_ci_server	Datadog	Infrastructure Monitoring
Hardware Asset	cmdb_ci_server	Dynatrace	Application Performance Monitoring
Hardware Asset	cmdb_ci_computer	Dynatrace	Application Performance Monitoring
Hardware Asset	cmdb_ci_computer	ExtraHop Reveal(x)	Network Security
Hardware Asset	cmdb_ci_hc_device	ExtraHop Reveal(x)	Network Security
Hardware Asset	cmdb_ci_server	ExtraHop Reveal(x)	Network Security
Hardware Asset	cmdb_ci_iot	ExtraHop Reveal(x)	Network Security
Hardware Asset	cmdb_ci_printer	ExtraHop Reveal(x)	Network Security
Hardware Asset	cmdb_ci_iot	Forescout	Network Security
Hardware Asset	cmdb_ci_hc_device	Forescout	Network Security
Hardware Asset	cmdb_ci_computer	Forescout	Network Security
Hardware Asset	cmdb_ci_server	Forescout	Network Security
Hardware Asset	cmdb_ci_printer	Forescout	Network Security
Hardware Asset	cmdb_ci_server	Intune	Endpoint Management

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_computer	Intune	Endpoint Management
Hardware Asset	cmdb_ci_printer	Jamf Pro	Endpoint Management
Hardware Asset	cmdb_ci_server	Jamf Pro	Endpoint Management
Hardware Asset	cmdb_ci_computer	Jamf Pro	Endpoint Management
Hardware Asset	cmdb_ci_server	Lansweeper	IT Asset Management
Hardware Asset	cmdb_ci_computer	Lansweeper	IT Asset Management
Hardware Asset	cmdb_ci_printer	Lansweeper	IT Asset Management
Hardware Asset	cmdb_ci_hc_device	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_printer	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_server	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_vm_instance	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_iot	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_computer	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_netgear	LogicMonitor	Infrastructure Monitoring
Hardware Asset	cmdb_ci_server	Microsoft Defender	Endpoint Protection
Hardware Asset	cmdb_ci_server	New Relic	Application Performance Monitoring
Hardware Asset	cmdb_ci_computer	Nexthink	Digital Employee Experience
Hardware Asset	cmdb_ci_computer	Netskope	Data Loss Prevention
Hardware Asset	cmdb_hardware_product_model	Netskope	Data Loss Prevention
Hardware Asset	cmdb_ci_network_adapter	Netskope	Data Loss Prevention
Hardware Asset	cmdb_software_instance	Netskope	Data Loss Prevention
Hardware Asset	cmdb_sam_sw_install	Netskope	Data Loss Prevention
Hardware Asset	sn_sec_sgc_netskop_client_attribute	Netskope	Data Loss Prevention

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_server	Open Telemetry	Application Performance Monitoring
Hardware Asset	cmdb_ci_computer	Puppet	Configuration and Patch Management
Hardware Asset	cmdb_ci_server	Puppet	Configuration and Patch Management
Hardware Asset	cmdb_ci_computer	Qualys	Vulnerability Assessment
Hardware Asset	cmdb_ci_server	Qualys	Vulnerability Assessment
Hardware Asset	cmdb_ci_vm_instance	Qualys-ServiceNow	Vulnerability Assessment
Hardware Asset	cmdb_ci_server	Qualys-ServiceNow	Vulnerability Assessment
Hardware Asset	cmdb_ci_hardware	Rapid7	Vulnerability Assessment
Hardware Asset	cmdb_ci_computer	SCCM	Configuration and Patch Management
Hardware Asset	cmdb_ci_server	SCCM	Configuration and Patch Management
Hardware Asset	cmdb_ci_printer	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_iot	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_server	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_computer	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_hc_device	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_vm_instance	ScienceLogic	Infrastructure Monitoring
Hardware Asset	cmdb_ci_hardware	ServiceNow HAM	Hardware Asset Management
Hardware Asset	cmdb_ci_hardware	ServiceNow ITOM Discovery	Discovery
Hardware Asset	cmdb_ci_aws_datacenter	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_azure_datacenter	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_availability_zone	SentinelOne	Endpoint Protection

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_google_datacenter	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_cloud_service_account	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_cloud_subnet	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_compute_template	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_network	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_vm_instance	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_key_value	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_os_template	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_server	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_computer	SentinelOne	Endpoint Protection
Hardware Asset	sn_sec_sgc_sntlone_asset_tags	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_ip_address	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_network_adapter	SentinelOne	Endpoint Protection
Hardware Asset	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	Endpoint Protection
Hardware Asset	cmdb_ci_server	Tanium Asset	Endpoint Management
Hardware Asset	cmdb_ci_computer	Tanium Asset	Endpoint Management
Hardware Asset	cmdb_ci_ups	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_industrial_sensor	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_cnc	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_hardware	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_netgear	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_industrial_actuator	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ip_switch	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_hub_network	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_security	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_server	Tenable	Vulnerability Assessment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_ot_rtu	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_ews	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_plc	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_control	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_dcs	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_storage_server	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_hmi	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_control_module	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_industrial_robot	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_historian	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_industrial_drive	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_iot	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ip_firewall	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_computer	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_unclassed_hardware	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ids_network	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_ot_ied	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_printer	Tenable	Vulnerability Assessment
Hardware Asset	cmdb_ci_computer	VMWare Workspace ONE UEM	Endpoint Management
Hardware Asset	cmdb_ci_server	VMWare Workspace ONE UEM	Endpoint Management

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Hardware Asset	cmdb_ci_printer	VMWare Workspace ONE UEM	Endpoint Management
Hardware Asset	cmdb_ci_vm_instance	Wiz	Cloud Native Application Protection Platform
Hardware Asset	cmdb_ci_server	Wiz	Cloud Native Application Protection Platform
Hardware Asset	cmdb_ci_linux_server	Wiz	Cloud Native Application Protection Platform
Hardware Asset	cmdb_ci_win_server	Wiz	Cloud Native Application Protection Platform

Supported software service graph connectors for Security Posture Control

Supported Software service graph connectors with CI class, source (product), and tool categories. This list is not complete and is subject to change with the addition of more products.

After you install them, you can view the connectors and their categories on the connector table [sn_sec_spc_core_connector] in your instance.

You can view Asset types and how they map to CI classes and Connectors on the [sn_sec_spc_core_asset_type_connector] table.

Software service graph connectors

Asset type	CI class	Asset source	Connector category
Software	cmdb_ci_spkg	BigFix	Configuration and Patch Management
Software	cmdb_ci_spkg	Dynatrace	Application Performance Monitoring
Software	cmdb_ci_spkg	Forescout	Network Security
Software	cmdb_ci_spkg	Intune	Endpoint Management
Software	cmdb_ci_spkg	Jamf Pro	Endpoint Management
Software	cmdb_ci_spkg	New Relic	Application Performance Monitoring
Software	cmdb_ci_spkg	Nexthink	Digital Employee Experience
Software	cmdb_ci_spkg	Netskope	Data Loss Prevention

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Software service graph connectors (continued)

Asset type	CI class	Asset source	Connector category
Software	cmdb_ci_spkg	Qualys-ServiceNow	Vulnerability Assessment
Software	cmdb_ci_spkg	SCCM	Configuration and Patch Management
Software	cmdb_ci_spkg	ServiceNow ITOM Discovery	Discovery
Software	cmdb_ci_spkg	Tanium Asset	Endpoint Management
Software	cmdb_ci_spkg	VMWare Workspace ONE UEM	Endpoint Management

Examples of base, child, and cloned policies for Security Posture Control

You can create your own base policies that have broad sets of conditions that you can use as starting points for more complex policies.

Examples

The following examples will help you see how you can reuse the conditions of a base policy when you create other policies by creating child policies or cloning existing policies. These examples also help you see how the policy builder works in the Policies and findings module.

Start with the first example, the Base policy. The other examples use the base policy as a starting point.

Note: The CrowdStrike service graph connector is used as the service graph connector in these examples, but you can use any connector that you have installed. These examples have you create and activate the polices to look for asset matches. You can remove these policies at any time from the Policies and Findings module after you activate them.

Create a base policy for Security Posture Control (example)

An example of how to create a base policy that you can use to create other policies.

Before you begin

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Policies and findings**.
2. Select **New policy**.
3. Select the pen icon in the upper left and in the Edit metadata modal, fill in the fields.

Field	Description
Name	Type in, Base policy - Windows 10 devices.
Criticality	Select **Low**.
Short description	Type in, **Locate devices with Windows 10 in stalled**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **Save metadata**.
5. In the Condition builder select **Hardware Asset** for Asset type.

   For this policy, leave the Base policy and Exclusion policies options in their default (off) settings.

6. For Connection select **With aggregated data**.

   For this policy, aggregated data helps you the locate assets in your CMDB that have Windows 10 installed. For example, some records might have slight variations on how different scanners report 'Windows 10'. Aggregated data ensures that all these slight variations on 'Windows 10' will match this policy.

   The Entity and Criteria fields are filled in automatically based on your selection in the Connection field.

7. For Property select **OS**.
8. For Value type in `Windows 10`.
9. Select **Save changes**.
   Your base policy is displayed on the All list of the Policies and findings module but it is not activated.
10. Select **Activate policy** so your base policy monitors any assets that match the policy's conditions and generates findings.

Create a child policy from a base policy for Security Posture Control (example)

An example of how to create a child policy using the conditions of a base policy.

Before you begin

This child policy inherits the conditions of a base policy, and you will add more conditions to your child policy to help you focus on more specific asset details. You want a new policy to monitor all your devices that have Windows 10 installed that are reported by the CrowdStrike service graph connector, and you want to exclude any devices that match another policy. For this example, you will exclude assets that have been approved for Integrated Risk Management (IRM) exceptions from your findings.

Note: If you do not have the CrowdStrike service graph connector installed, you can use one that have installed.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Policies and findings**.
2. From the Active list, locate the Base policy - Windows 10 devices you created in the first example and select it to open the record.
3. Select the more options menu (three vertical dots) and select **Create child policy**.
   A new tab opens and with a new record and the Base policy - Windows 10 devices is displayed in the Base policy field.
4. Select the pen icon in the upper left and in the Edit metadata modal fill in the fields.

Field	Description
Name	Type in, `Child policy- Windows devices with CrowdStrike`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Criticality	Select **Medium**.
Short description	Type in, `Locate all devices with Windows 10 reported by CrowdStrike.`

5. Select **Save metadata**.
6. In the Condition builder select **Hardware Asset** for Asset type.
7. Select the Base policy toggle.
8. Select the policy you created for Example 1, **Base policy - Windows 10 devices** from the list.

   This child policy automatically inherits the conditions of the base policy.
9. Select the Exclusion policies toggle.
10. Select Assets with IRM exception approved from the list.

    Note: If you don't have this policy, you can select another policy from the list that you want to exclude from this policy.

    The assets that match this policy will be excluded from your child policy. Note that you can add more polices.
11. Select **Reported by**.
12. Select **CrowdStrike** from the list.
13. Select **Save changes**.
    Your new policy is displayed on the All list of the Policies and findings module but it is not activated.
14. Select **Activate policy** so your base policy monitors any assets that match the policy's conditions and generates findings.

Clone a policy for Security Posture Control (example)

An example of how to create a policy that copies the conditions from another policy.

Before you begin

Create a policy that copies the conditions from the policy you created in Example 2 so you do not have to re-enter them. You will clone these conditions and add more conditions to the copy of the child policy you created. For this example, you want this policy to locate devices with Windows 10 with CrowdStrike, exclude assets with IRM exceptions that have not been seen in the last 7 days.

Roles required: SPC Admin Group or SPC Analyst Group

Procedure

1. Navigate to **All** > **Security Posture Control Workspace** > **Policies and findings**.
2. From the Active list, locate the child policy- Windows devices with CrowdStrike you created for the second example and select it to open the record.
3. Select the more options menu (three vertical dots) and select **Clone policy**.
   A new tab opens and the policy name is displayed in a new record with ‘copy’ in the title: Windows devices with CrowdStrike-copy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select the pen icon in the upper left and in the Edit metadata modal fill in the fields.

Field	Description
Name	Type in, `Cloned policy - Windows 10 CrowdStrike IRM exceptions not seen 7 days.`
Criticality	Select **Critical**.
Short description	Type in, `Locate devices with Windows 10 with CrowdStrike IRM exceptions not seen last 7 days..`

5. Select **Save Metadata**.
6. To the right of the first Connection and Entity fields, select the **AND** operator for new fields. This adds a logical AND between the current Connection-Entity criteria, and new criteria from another Connection-Entity. In this case, you want to specifcy connector data for assets not seen by CrowdStrike in the last 7 days.
7. For Connection select **With connector data**.
8. For Entity, select **CrowdStrike: CrowdStrike Device Details**.
   The criteria filed is automatically filled based on your selection.
9. For Property select **Last Seen Time**.
10. For Value select **This week**.
11. Select **Save changes**.
12. Select **Activate policy**.
    You can remove these policies at any time from the Policies and Findings module.

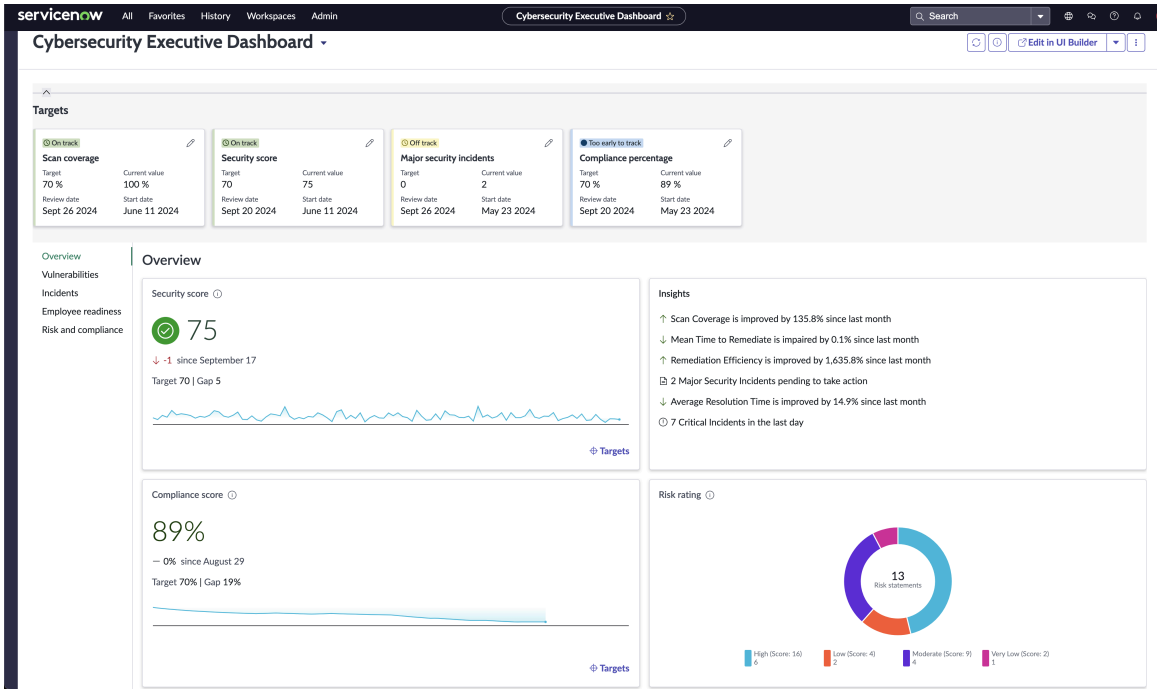
Cybersecurity Executive Dashboard

The Cybersecurity Executive Dashboard is a comprehensive solution that empowers Chief Information Security Officers (CISOs) and cybersecurity executives with visibility into the organization's security posture and initiatives. The dashboard consolidates data from various products within the ServiceNow Security Operations suite and Governance, Risk and Compliance (GRC).

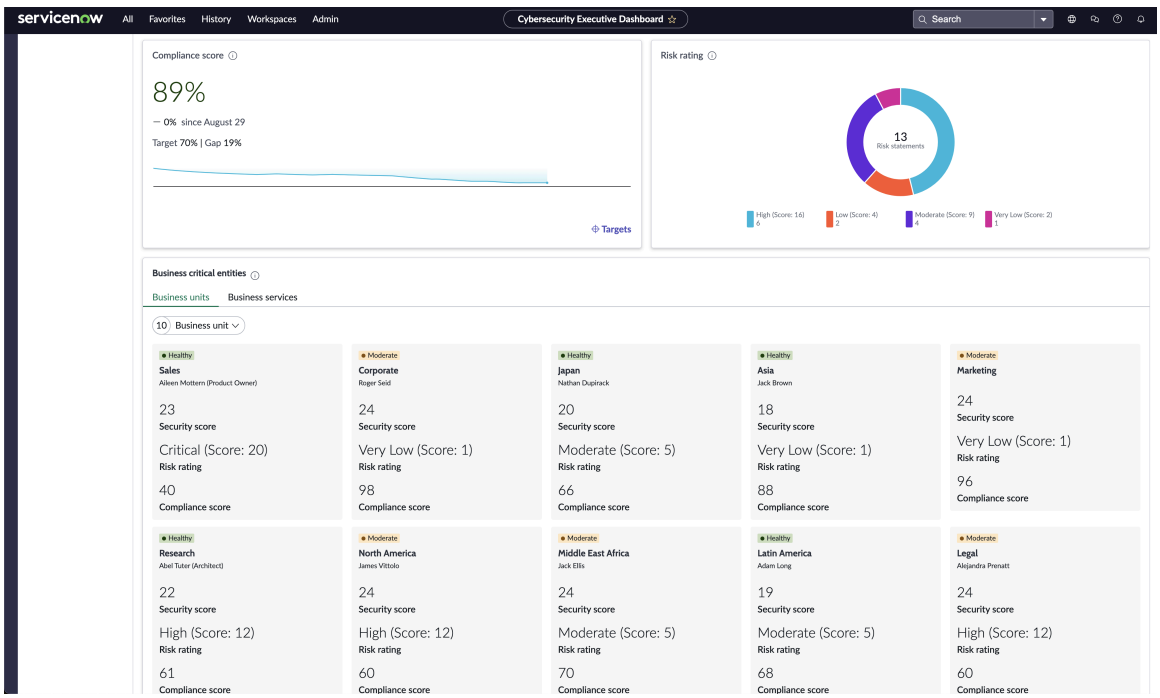
The dashboard provides the following features:

- Organization-wide security posture scoring
- Security, Risk, and Compliance scores by business unit
- Customizable monitoring
- Unified view of an organization's security landscape
- Benchmarking
- User-friendly interface
- Visibility into phishing simulation metrics from KnowBe4 and Microsoft Defender for Office 365

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



These features enable proactive decision making by providing quick access to critical security metrics. Thus, making it an indispensable tool for enhancing overall security resilience and readiness.



Required ServiceNow AI Platform roles

- CISO (sn_bod.ciso) to view and share the dashboard.
- sn_bod.ciso_admin to view, share the dashboard, configure weights for security posture rating.
- GRC CISO User (sn_grc_dashboards.grc_ciso_user) to view risk and compliance reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Access the Cybersecurity Executive Dashboard

To open the dashboard, navigate to **All** > **Cybersecurity Executive Dashboard** > **Cybersecurity Executive Dashboard**.

Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

User	Dashboard use
Chief Information Security Officers (CISOs)	CISOs gain insights on vulnerability management, incident management, organization security posture, phishing simulation metrics, and so on, for their organizations.

Data visualization

Note: To learn more about a widget, select the information icon .

Targets

Metrics	Type	Description
Targets	Percentage	Shows the set target to cover for a metric. The status of the targets is indicated through color coding. It shows all the targets whose review date is either within the past 30 days or upcoming. You can set the number of days for displaying targets using the *sn_bod.show_targets_from* system property. Additionally, these targets can be edited. See Set targets for more information.

Metrics	Type	Description
Security score	Single Score	Overall score of the organization's security posture by considering vulnerable items, security incidents, major security incidents, and misconfigurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Metrics	Type	Description
Insights	Highlights	Highlights of the entire dashboard.
Compliance score	Single Score	Provides compliance posture of the organization with the help of compliance score calculated based on the percentage of compliant controls out of the total number of controls.
Risk score	Single Score	Provides the count of risk statements based on the risk ratings. It helps organizations understand the potential impact and likelihood of various risks, enabling them to prioritize and manage these risks.
Business critical entities		
Business units	Single Score	Overall security score of the business units by considering the risk associated with vulnerabilities, misconfigurations, Operational Technology (OT) vulnerabilities, security incidents, and major security incidents. The health label of the business units is based on the security score only. To see how these labels are assigned, navigate to Risk Score Weights [sn_sec_cmn_risk_score_weight_list.do] table and search for business entity. Labels such as 'Healthy' are assigned based on predefined value ranges. For instance, a security score ranging from 0 to 39 is labeled as Healthy. The color coding for these labels is specified in the `UnifiedCISOutils` script include. You can configure both the value range as well as the colors for the labels. To see how the business unit and business unit head names are assigned, go to **All**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Metrics	Type	Description
		> **Organization** > **Business Units**. **Note:** Depending on the plugins you have enabled, you can access the Compliance score, Risk score, and Security score. To view the Compliance and Risk score, you must activate the GRC plugins. To view the Security score, you must activate the Security Operations related plugins. See Applications to active section for more information.
Business services	Single Score	Overall security score of the business services by considering the risk associated with vulnerabilities, misconfigurations, Operational Technology (OT) vulnerabilities, security incidents, and major security incidents. To see how these labels are assigned, navigate to Risk Score Weights [sn_sec_cmn_risk_score_weight_list.do] table and search for business entity. Labels such as 'Healthy', 'Moderate' and 'Critical' are assigned based on predefined value ranges. For instance, a security score ranging from 0 to 39 is labeled as Healthy. The color coding for these labels is specified in the`UnifiedCISOutils` script include. You can configure both the value range as well as the colors for the labels. To see how the business unit and business unit head name are assigned, go to **All** > **Organization** > **Business Units**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Metrics	Type	Description
		Note: Depending on the plugins you have enabled, you can access the Compliance score, Risk score, and Security score. To view the Compliance and Risk score, you must activate the GRC plugins. To view the Security score, you must activate the Security Operations related plugins. See Applications to active section for more information.

Vulnerabilities

Metrics	Type	Description
Mean time to remediate (monthly)	Line	Average time taken to close vulnerabilities and failed test results across all assets (hosts, containers, and applications) in a month. It also provides the following metrics: • Target: Target set in days to remediate the vulnerabilities. • Gap: Difference in days between the target and actual time taken to remediate the vulnerabilities. • Industry benchmark: Average of metrics from the peers in the same industry. • Global benchmark: Average of metrics from the peers in the global market See Opt-in for benchmark scores on how to view the benchmark scores.
Average age of active vulnerabilities (monthly)	Single Score	Monthly average age of all three types of vulnerable items. It also provides a

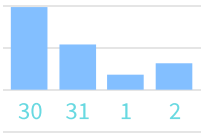
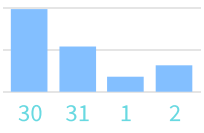
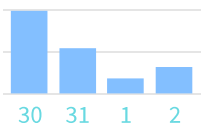
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerabilities (continued)

Metrics	Type	Description
		comparison of the current month age with the previous month. It also provides the following metrics: • Industry benchmark: Average of metrics from the peers in the same industry. • Global benchmark: Average of metrics from the peers in the global market • Target: Target set in days to remediate the vulnerabilities.
Remediation efficiency (monthly)	Single Score	Percentage of monthly closed vulnerable items to monthly active vulnerable items. It also provides the following metrics: • Percentage change from the previous month. • Target: Target set in percentage to remediate the vulnerabilities. • Gap: The gap between target and current score. • Industry benchmark: Average of metrics from the peers in the same industry. • Global benchmark: Average of metrics from the peers in the global market
Average age of active vulnerabilities by assignment group	Multiple line	Average age of active vulnerabilities for each assignment group.
Vulnerabilities by risk rating and age	Heatmap	Breakdown of active vulnerabilities across hosts, containers, and applications by risk rating and age.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerabilities (continued)

Metrics	Type	Description
Remediation target adherence by assignment group	Vertical  Bar	The ratio of the number of vulnerabilities and misconfigurations closed within remediation target to the total number of vulnerabilities and misconfigurations closed.
Scan coverage	Percentage	Percentage of the assets scanned in the last 90 days out of all assets in the CMDB.
Assets scanned vs unscanned	Horizontal bar	Breakdown of assets scanned in the last 90 days and total assets in CMDB by CI Class
Assets scanned	Horizontal bar	Assets scanned in the last 90 days for vulnerabilities versus configuration compliance.
Active critical and high findings trend	Multiple line	Daily trend of vulnerabilities and misconfigurations that have critical and high risk rating.
Vulnerabilities by asset category and risk rating	Vertical  Bar	Breakdown of active vulnerabilities and misconfigurations by asset category and risk rating (critical, high, and medium).
Deferred findings by reason and assignment group	Vertical  Bar	Breakdown of active vulnerabilities and misconfigurations deferred by deferral reason and assignment group.
Operational technology (OT)		
Active critical and high vulnerability trend	Line	Daily trend of OT vulnerabilities that are active with critical and high risk rating.
Mean time to remediate (monthly)	Single Score	Average time taken to close OT vulnerabilities. The ratio of total age of OT vulnerabilities closed to the total number of OT vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerabilities (continued)

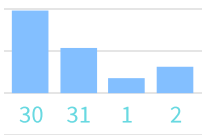
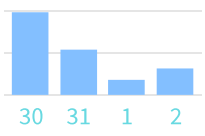
Metrics	Type	Description
		It also provides the following metrics: • Percentage change from the previous month. • Target: Target set in days to remediate the vulnerabilities. • Industry benchmark: Average of metrics from the peers in the same industry. • Global benchmark: Average of metrics from the peers in the global market See Opt-in for benchmark scores on how to view the benchmark scores.
Vulnerabilities by risk rating and age	Heatmap	Breakdown of active OT vulnerabilities by risk rating and age.
Average age of active vulnerabilities (monthly)	Line chart	Monthly average age of OT vulnerable items. It also provides a comparison of the current month age with the previous month.
Vulnerabilities by state and age	Heatmap	Breakdown of active OT vulnerabilities by state and age.

Incidents

Metrics	Type	Description
Major security incidents	Single Score	Number of major security incidents that are currently active.
Average security incidents resolution time (monthly)	Single Score	Monthly average resolution time in days of closed security incidents. It also provides the following metrics:

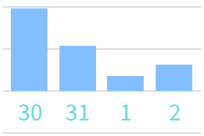
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incidents (continued)

Metrics	Type	Description
		• Percentage change from the previous month. • Target: Target set in days to remediate the security incidents. • Gap: The gap between the actual days taken to resolve and the target set to remediate. • Industry benchmark: Average of metrics from the peers in the same industry. • Global benchmark: Average of metrics from the peers in the global market
Average time to eradicate (monthly)	Line chart	Monthly average resolution in days to eradicate security incidents.
Average time to identify (monthly)	Single Score	Monthly average resolution in days to identify the security incidents.
Average time to contain (monthly)	Single Score	Monthly average resolution in days to contain security incidents.
Active incidents by priority and category	Heatmap	Count of active security incidents, which are categorized by priority and category.
Closed and open incidents trend	Vertical  Bar	Breakdown of closed and open incidents.
Active incidents by states	Vertical  Bar	Breakdown of active incidents based on their states.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Employee readiness

Metrics	Type	Description
Monthly phishing simulation overview	Vertical  Bar	Sum of users who performed the actions such as opened, clicked, and reported in the phishing simulation along with the sum of total users of each simulation for the past six months.

Risk and Compliance

To view Risk and Compliance widgets, you must activate the GRC plugins. For information on GRC plugins, see the Applications to activate section. For information on GRC widgets, see Risk and compliance dashboard for GRC: Metrics.

Indicators

Host SLA – Closed

This indicator is calculated daily. It considers the total age of all host vulnerabilities that were closed on the previous day at the time of calculation.

Container SLA – Closed

This indicator is calculated daily. It considers all the container vulnerabilities that were closed on the previous day at the time of calculation.

Application SLA – Closed

This indicator is calculated daily. It considers the total age of all the application vulnerabilities that were closed on the previous day at the time of calculation.

Test Result SLA – Passed

This indicator is calculated daily. It considers all the test result vulnerabilities that were passed on the previous day at the time of calculation.

Host SLA - Closed Count

This indicator is calculated daily. It considers the count of all host vulnerabilities that were closed on the previous day at the time of calculation.

Container SLA - Closed Count

This indicator is calculated daily. It considers the count of all container vulnerabilities that were closed on the previous day at the time of calculation.

Application SLA - Closed Count

This indicator is calculated daily. It considers the count of all application vulnerabilities that were closed on the previous day at the time of calculation.

Test Result SLA – Passed Count

This indicator is measured daily. It considers the count of all test result vulnerabilities that were last passed on the previous day at the time of calculation.

Scanned Assets

This indicator is calculated daily. It considers the sum of scanned CIs from the sn_vul_analytics_scan_coverage_config table, which includes those last scanned within the past 90 days, across all CMDB CI Classes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scannable Assets

This indicator is calculated daily. It considers the sum of total CIs from sn_vul_analytics_scan_coverage_config table for all the CMDB CI Classes present.

Vulnerable Items

This indicator is calculated daily. It considers the count of active vulnerable items at the time of calculation.

Application Vulnerable Item

This indicator is calculated daily. It considers the count of active application vulnerable items at the time of calculation.

Container Vulnerable Item

This indicator is calculated daily. It considers the count of active container vulnerable items at the time of calculation.

Summed Age of Vulnerable Items

This indicator is calculated daily. It considers the summed age of active vulnerable items at the time of calculation.

Summed Age of Application Vulnerable Items

This indicator is calculated daily. It considers the summed age of active application vulnerable items at the time of calculation.

Open Vulnerable Items

This indicator is calculated daily. It considers the open vulnerable items at the time of calculation.

Open Container Vulnerable Items

This indicator is calculated daily. It considers the open container vulnerable items at the time of calculation.

Open Application Vulnerable Items

This indicator is calculated daily. It considers the open application vulnerable items at the time of calculation.

Active Test Results

This indicator is calculated daily. It considers the open test results at the time of calculation.

Deferred VITs

This indicator is calculated daily. It has an indicator source as host vulnerable item.

Deferred AVITs

This indicator is calculated daily. It has an indicator source as an application vulnerable item.

Deferred CVITs

This indicator is calculated daily. It has an indicator source as a container vulnerable item.

Deferred Test Results

This indicator is calculated daily. It considers the test results that were in a deferred state.

Open Config Issues - Test results

This indicator is calculated daily. It has an indicator source as test result for the Unified Vulnerability Response Dashboard.

SI-Average Time To Identify

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This indicator is calculated daily. It considers the security incident where definition is time to identify at the time of calculation.

SI - Average Duration Time

This indicator is calculated daily. It considers the security incident where the definition is an incident state duration at the time of calculation.

Number of Open Major Security Incidents

This indicator is calculated daily. It considers open major security incidents at the time of calculation.

Number of closed security incidents

This indicator is calculated daily. It considers closed security incidents at the time of calculation.

Closed Application Vulnerable Items

This indicator is calculated daily. It considers closed application vulnerable items at the time of calculation.

Closed Container Vulnerable Items

This indicator is calculated daily. It considers closed container vulnerable items at the time of calculation.

Closed Vulnerable Items

This indicator is calculated daily. It considers closed vulnerable items at the time of calculation.

Get Max Risk Score for Vulnerable Items

This indicator is calculated daily. It considers the maximum risk score for vulnerable items at the time of calculation.

Get Max Risk Score for Container Vulnerable Item

This indicator is calculated daily. It considers the maximum risk score for container vulnerable items at the time of calculation.

Get Max Risk Score for Application Vulnerable Items

This indicator is calculated daily. It considers the max risk score for application vulnerable items at the time of calculation.

Summed Risk Score of VITs

This indicator is calculated daily. It considers the sum of risk scores of vulnerable items at the time of calculation.

Summed Risk Score of AVIs

This indicator is calculated daily. It considers the sum of risk scores of application vulnerable items at the time of calculation.

Summed Risk Score of CVIs

This indicator is calculated daily. It considers the sum of risk scores of container vulnerable items at the time of calculation.

Summed Risk Score of Misconfigurations

This indicator is calculated daily. It considers the sum of risk scores of test results at the time of calculation.

Get Max Risk Score for SI Incidents

This indicator is calculated daily. It considers the max risk scores of security incidents at the time of calculation.

Get Max Risk Score for Misconfigurations Test Results

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This indicator is calculated daily. It considers the maximum risk scores for misconfiguration of test results at the time of calculation.

Get Avg Risk Score for Misconfiguration Test Results

This indicator is calculated daily. It considers the average risk scores for misconfiguration of test results at the time of calculation.

Number of open security incidents

This indicator is calculated daily. It considers open security incidents at the time of calculation.

Phishing Overview

This indicator is calculated daily. It considers the count of Security Simulation Metrics at the time of calculation.

Aggregate MTTR

Calculates the average time taken to close vulnerabilities (hosts, containers, and applications) and the time taken to close the test results in days. [[Host SLA - Closed]] + [[Application SLA - Closed]] + [[Container SLA - Closed]] + [[Test Result SLA - Passed]]) / ([[Host SLA - Closed Count]] + [[Application SLA - Closed Count]] + [[Test Result SLA - Passed Count]] + [[Container SLA - Closed Count]])

Current Scan Coverage

Calculates the percentage by utilizing the ratio between the number of items scanned and the total number of items eligible for scanning during the same period. var scannedItems =[[Scanned Assets]];var scannableItems = [[Scannable Assets]];var res;if (scannedItems == 0)res = 0;elseres = scannedItems / scannableItems * 100;if (res > 100)res = 100;res;

Average Age of Active Vulnerable Items

Calculates the average age of all active vulnerable items (hosts, containers, and applications) in days. ([[Summed Age of Vulnerable Items]] + [[Summed Age of Application Vulnerable Items]] + [[Summed Age of Container Vulnerable Items]]) / ([[Vulnerable Items]] + [[Application Vulnerable Items]] + [[Container Vulnerable Items]])

Active VITs by age and risk rating

Calculates the total count of all active vulnerable items (hosts, containers, and applications) categorized by their age and level of risk assessment. [[Open Vulnerable Items]] + [[Open Container Vulnerable Items]] + [[Open Application Vulnerable Items]]

Deferred Issues

Calculates the total count of all vulnerable items (hosts, containers, applications, and test results) with the state as 'Deferred'. [[Deferred VITs]] + [[Deferred AVITs]] + [[Deferred Test Results]] + [[Deferred CVITs]]

Average resolution time of closed security incidents

Calculates the average time taken to close the security incidents in days. ([[Summed duration of closed security incidents]] / [[Number of closed security incidents]]) /24

Security Score

Calculates the overall security ratings daily. It's calculated based on the rolled up risk score. var secPostureRating = 100 - [[Security score]]; secPostureRating;

Security Score (Business Units)

Calculates the final rolled up risk score where the roll-up risk score of vulnerable items, misconfigurations, security incidents, and major security incidents are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

multiplied with the respective weights that are fetched from the security posture roll-up table. var numMajorIncidents = [[Number of Open Major Security Incidents]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Vulnerability and Misconfiguration Rolled up Risk Score]] * 20 + [[OT Vulnerability Rolled up Risk Score]] * 20 + [[Get Max Risk Score for SI Incidents]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

Security Score (Business Services)

Calculates the final rolled up risk score where the roll-up risk score of vulnerable items, misconfigurations, security incidents, and major security incidents are multiplied with the respective weights that are fetched from the security posture roll-up table. var numMajorIncidents = [[Number of Open Major Security Incidents - Services]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Vulnerability and Misconfiguration Rolled up Risk Score - Services]] * 20 + [[OT Vulnerability Rolled up Risk Score - Services]] * 20 + [[Get Max Risk Score for SI Incidents - Services]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

Vulnerability Rolled up Risk Score

Calculates the vulnerability rolled up risk score where the max risk score, average risk score of vulnerable items and count of vulnerable items are multiplied with their respective weights. var maxRiskScore = 100; var count = [[Active VITs by age and risk rating]]; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); else if (count > 100) countRiskScore = (maxRiskScore * 0.60); else if (count > 10) countRiskScore = (maxRiskScore * 0.40); else countRiskScore = (maxRiskScore * 0.20); var vulRiskScore = ([[Get Max Score form all Vulnerable Items]] * 0 + [[Average Risk Score of all Vulnerable Items]] * 100 + countRiskScore * 0)/100; vulRiskScore;

Get Max Score from all Vulnerable Items

Calculates the vulnerability rolled up risk score where the max risk score, average risk score of vulnerable items and count of vulnerable items are multiplied with their respective weights. var maxScoreForVI = [[Get Max Risk Score for Vulnerable Items]], maxScoreForCVI = [[Get Max Risk Score for Container Vulnerable Item]], maxScoreForAVI = [[Get Max Risk Score for Application Vulnerable Items]], maxScore; if (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; else if (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI; else maxScore = maxScoreForAVI; maxScore;

Average Risk Score of all Vulnerable Items

Calculates the average risk score from all vulnerable items (hosts, containers, and applications). var summedRiskScore = [[Summed Risk Score of VITs]] + [[Summed Risk Score of AVIs]] + [[Summed Risk Score of CVIs]], avgRiskScore; var totalVulCount = [[Open Vulnerable Items]] + [[Open Application Vulnerable Items]] + [[Open Container Vulnerable Items]]; if(summedRiskScore == 0) avgRiskScore = 0; else if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; avgRiskScore;

Misconfiguration Rolled up Risk Score

Calculates the misconfiguration rolled up risk score using the test outcomes categorized as Failed, Error, or Unknown. var maxRiskScore = 100; var count = [[Open Config Issues - Test results]]; var countRiskScore; if (0 == count) countRiskScore = 0; else if (count > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); else if (count > 100) countRiskScore = (maxRiskScore * 0.60); else if (count > 10) countRiskScore

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

= (maxRiskScore * 0.40); else countRiskScore = (maxRiskScore * 0.20); var misRiskScore = ([[Get Max Risk Score for Misconfigurations Test Results]] * 0 + [[Get Avg Risk Score for Misconfiguration test results]] * 100 + countRiskScore * 0)/100; misRiskScore;

Average Time to Eradicate

Calculates the average time taken to eradicate security incidents in days [[SI - Average Duration Time > Security Incident State = Eradicate]] / 1440

Average Time to Identify

Calculates the average time taken to identify security incidents in days. [[SI - Average Time To Identify]] / 1440

Average Time to Contain

Calculates the average time taken to contain security incidents in days. [[SI - Average Duration Time > Security Incident State = Contain]] / 1440

Remediation Target Adherence

Calculates the monthly percentage of remediation target adherence from test results, vulnerable items, container vulnerable items, and application vulnerable items. The target adherence is determined by the number of items that have fulfilled the set target. ([[Test Result SLA - Passed Count > Remediation status (unified) = Target Met]] + [[Container SLA - Closed Count > Remediation status (unified) = Target Met]] + [[Application SLA - Closed Count > Remediation status (unified) = Target Met]] + [[Host SLA - Closed Count > Remediation status (unified) = Target Met]]) / ([[Test Result SLA - Passed Count]] + [[Container SLA - Closed Count]] + [[Application SLA - Closed Count]] + [[Host SLA - Closed Count]]) * 100

Monthly Remediation Efficiency (All Vulnerable Items)

Calculates the monthly percentage of closed vulnerable items, containers vulnerable items, and application vulnerable items in contrast to newly identified ones. var closedItems = [[Host SLA - Closed Count]] + [[Container SLA - Closed Count]] + [[Application SLA - Closed Count]] + [[Test Result SLA - Passed Count]];

var newItems = [[Host VITs opened/reopened yesterday]] + [[Container VITs opened/reopened yesterday]] + [[Application VITs opened/reopened yesterday]] + [[Test results opened/reopened yesterday]];

var res = 0;if (closedItems == 0) res = 0;else if (newItems .=0)res = closedItems / newItems * 100;if (res > 1000) res = 1000; res;

Host VITs opened/reopened yesterday

This indicator is calculated daily. It considers the host vulnerable items that were last opened on the previous day at the time of calculation.

Application VITs opened/reopened yesterday

This indicator is calculated daily. It considers the application vulnerable items that were last opened on the previous day at the time of calculation.

Container VITs opened/reopened yesterday

This indicator is calculated daily. It considers the container vulnerable items that were last opened on the previous day at the time of calculation.

Test results opened/reopened yesterday

This indicator is calculated daily. It considers the test results that were last seen on the previous day at the time of calculation.

OT Vulnerable Items

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This indicator is calculated daily. It considers active OT vulnerable items present at the time of calculation.

OT Summed Duration of Closed Vulnerable

This indicator is calculated daily. It considers the total age of all OT vulnerabilities that are closed on the day of calculation.

OT Closed Vulnerable Items

This indicator is calculated daily. It considers the OT vulnerable items that are closed on the day of calculation.

Average age of OT active vulnerable items

Calculates the average age of OT vulnerable items ([[Summed age of OT vulnerable Items]] / [[OT Vulnerable Items]])

Breakdowns

- Business Unit
- Business Services
- Risk Rating
- Age Range
- Assignment Group (unified)
- Remediation Target Status (Closed)
- Asset Class
- Asset Category
- Risk Rating (unified)
- Deferred Reason (unified)
- Security Incident State
- Security Incident Priority
- Security Incident Category
- Phishing Event
- Deferred Reason Non Closed (unified)

Applications to activate

You must activate the following applications to populate the score in the widgets. Based on the application you're using, you must activate the dependent applications.

If you're using	Activate
Vulnerability Response	• Performance Analytics for Vulnerability Response • Vulnerability Response Common • Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you're using	Activate
	• Vulnerability Response and Configuration Compliance for Containers • Configuration Compliance
Operational Technology	Vulnerability Response for Operational Technology
Phishing Integrations	• Security Simulation and Training Integration for SecOps • KnowBe4 Integration for SecOps • Microsoft Defender for Office365 Integration for SecOps
Security Incident Response	• Performance Analytics for Security Incident Response • Security Incident Response • Major Security Incident Management
Governance, Risk, and Compliance	• GRC: Common Dashboard Elements • GRC: Risk Management Workspace • GRC: Advanced Risk • GRC: Compliance Management Workspace

Scheduled jobs for data collection

The following scheduled jobs are run to collect scores on new data automatically.

Scheduled job	Frequency	Description
Upload the benchmark scores	On Demand	Collects scores from the instance and posts to the central instance. The benchmark algorithms calculate the industry's best scores.
Download the benchmark scores	On Demand	Downloads the benchmark scores. It's available in the Benchmark Scores [sn_bm_client_score_list] table.

Opt-in for benchmark scores

Get benchmark scores by registering your instance to the ServiceNow central instance. The latter maintains information of multiple industries to provide the benchmark score.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
For more information on Benchmarking, see Benchmarks overview.

Procedure
1. To register your instance with the central instance, follow these steps:
   a. Navigate to **All** > **System Properties** > **All Properties**.
   b. Select *sn_bm_client.central_instance_url* system property.
   c. In the **Value** field, enter the benchmark central instance URL.
      Note: If the instance is provisioned, your details are pushed to the central instance automatically.
   d. Select **Opt-in** from the widget to validate and establish a connection with the central instance.
2. To upload your score to the central instance, follow these steps:
   a. Navigate to **All** > **System Scheduler** > **Scheduled Jobs**
   b. Select the *Upload the benchmark scores* scheduled job.
   c. Select **Update**.
      The scores are uploaded to the central instance. However, the scheduled jobs by the central instance run once a month to update the scores on the dashboard widgets.
3. To download the score from the central instance, follow these steps:
   a. Navigate to **All** > **System Scheduler** > **Scheduled Jobs**
   b. Select the *Download the benchmark scores* scheduled job.
   c. Select **Execute Now**.
      The scores are available in the Benchmark Scores [sn_bm_client_score_list] table, which is reflected in the dashboard widgets.

Set targets

Set targets in days to remediate the vulnerabilities, security incidents, and misconfigurations.

Before you begin
Role required: admin

Procedure
1. Select **Targets** on the widget or select the **Targets** icon on the KPI Details page.
2. Select the **For everyone** button.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In the **New value** field, enter the number of days in which you want to achieve the target.
4. Select the target start date.
5. Select the target review date.
6. Select **Update**.

Security Simulation and Training Integration for Security Operations

Strengthen your organization's defense against prominent cybersecurity threats by incorporating phishing integrations with the Cybersecurity Executive Dashboard. The Phishing Integrations enhance the Cybersecurity Executive Dashboard by seamlessly incorporating data from third-party phishing simulation tools such as KnowBe4 and Microsoft Defender for Office 365.

The following integrations elevate the Cybersecurity Executive Dashboard's capabilities, providing a unified perspective on your organization's security posture, employee readiness, and susceptibility to phishing attacks:

- KnowBe4 integration
- Microsoft Defender for Office 365 integration

Configure Knowbe4 integration

Gain immediate insights into your staff's vulnerability to phishing attacks by integrating with KnowBe4, a leading cybersecurity awareness training platform. Through KnowBe4 integration, identify trends and areas of improvement in your cybersecurity training programs, monitor overall phishing resilience and proactively strengthen your organization's security measures.

Before you begin

Role required: sn_sec_phish.admin and sn_sec_phish_kb4.kb4_admin

Procedure

1. Navigate to **All** > **KnowBe4 Integration** > **KnowBe4 Configurations**.
2. Select **New**.
3. On the form, fill in the details:

KnowBe4 Configuration form

Field	Description
Integration Instance	Name of the integration instance. Select the integration instance using the Lookup icon.
Base URL	URL to integrate with KnowBe4.
API Key	API key acquired from KnowBe4 account.
Page	Page number from where simulations should be fetched.
Page Size	Number of simulations that should be included.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select **New** if no integration instance is available.

b. On the form, fill in the details:

Integration Instance form

Field	Description
Name	Name for the integration instance.
Application	Name of the application (KnowBe4 Integration for SecOps).
Integration	KnowBe4 is the default.
Active	Default is activated (selected). If cleared, the instance isn't active.
Description	Short description of the integration instance.

4. Select **Submit**.
5. Navigate to **All** > **Security Simulation and Training** > **Integrations**.
6. Select Knowbe4 integration.
7. Select **Execute Now** to execute and collect data from KnowBe4.

Configure Microsoft Defender for Office 365 integration

Gain valuable insights into phishing simulation metrics directly within the Cybersecurity Executive Dashboard through seamless integration with Microsoft Defender for Office 365.

Before you begin

Role required: sn_sec_phish_msatk.ms_admin

About this task

To learn more about simulating a phishing attack and setting up a tenant, see:

- Simulate a phishing attack with Attack simulation training
- Getting started using Attack simulation training
- Set up a tenant

Procedure

1. Navigate to **All** > **Microsoft Attack Integration** > **Microsoft Attack Configurations**.
2. Select **New**.
3. On the form, fill in the details:

Microsoft Attack Configuration form

Field	Description
Integration Instance	Name of the integration instance. Select the integration instance using the Lookup icon.
Tenant ID	Tenant ID of the application created on the Microsoft Azure portal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Client ID	Client ID of the application created on the Microsoft Azure portal.
Client Secret	Client secret of the application created on the Microsoft Azure portal.
Bookmark	Date from which the simulations must be fetched.
Token Url	Base URL from where the token is created to access the Microsoft Simulations API.
All Simulation Url	Base URL of the Microsoft Simulations API.

a. Select **New** if no integration instance is available.

b. On the form, fill in the details:

Integration Instance form

Field	Description
Name	Name of the integration instance.
Application	Name of the application (Microsoft Defender for Office 365).
Integration	Third-party integration reference (Microsoft Attack Integration).
Active	Default is activated (selected). If cleared, the instance isn't active.
Description	Short description of the integration instance.

4. Select **Submit**.
5. Navigate to **All** > **Security Simulation and Training** > **Integrations**.
6. Select Microsoft Attack integration.
7. Select **Execute Now** to execute and collect data from Microsoft.

Risk and compliance dashboard for GRC: Metrics

The Risk and compliance dashboard gives the compliance and risk users a comprehensive overview of risk and compliance information in a single dashboard that aids in their key decisions.

You can navigate to the Risk and compliance dashboard from the single unified Cybersecurity Executive Dashboard to view the risk and compliance metrics of Governance, Risk, and Compliance applications.

The dashboard provides features such as:

- Compliance overview
- Risk overview
- Privacy overview
- Business continuity overview

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Third-party risk
- Audit overview

Pre-requisites to access the Risk and compliance dashboard

Important: You must have primary access to the Cybersecurity Executive Dashboard to activate the Cybersecurity and risk functional plugin with which you can access the Risk and compliance dashboard.

A new functional domain is introduced to segregate Cybersecurity and Risk related data. You can activate the cybersecurity and risk plugin by selecting the **Activate** UI action button. By default, this functional domain is inactive.

Required ServiceNow AI Platform roles

The main GRC user role is the sn_grc_dashboards.grc_ciso_user who can view the reports on the Risk and compliance dashboard. This role contains:

- sn_compliance.reader
- sn_risk.reader

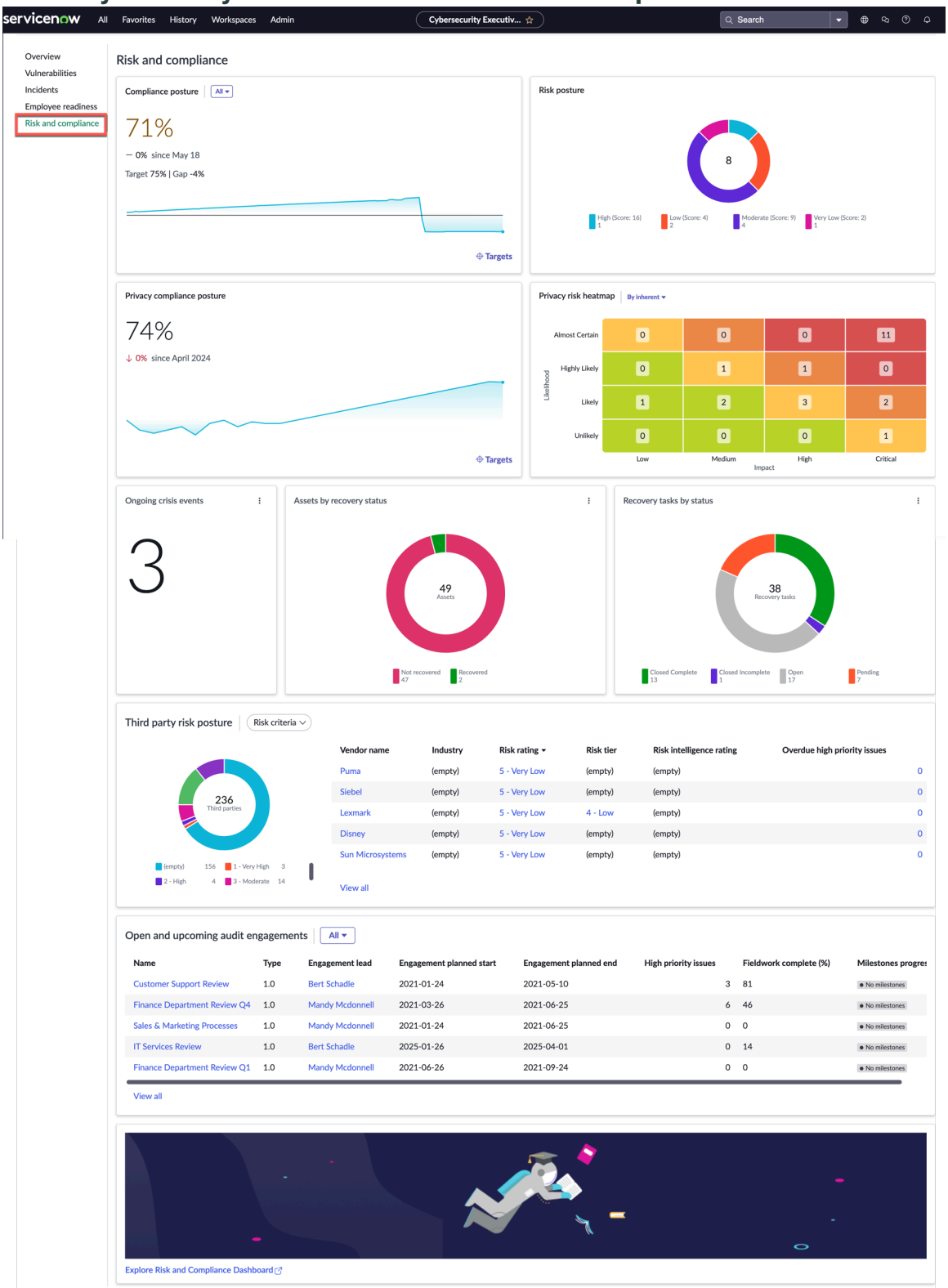
Note: However, you must have the sn_bod.ciso role to log in, view and share the Cybersecurity Executive Dashboard from which you can navigate to the Risk and compliance dashboard.

Access the Risk and compliance dashboard

1. To access the Risk and compliance dashboard, navigate to **All** > **Cybersecurity Executive Dashboard** > **Cybersecurity Executive Dashboard**.
2. Select **Risk and compliance** label from the list on the left of the dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Cybersecurity Executive Dashboard for risk and compliance metrics



3. To visualize your data, and to view the reports and solutions available on the dashboard that is designed for the user, select the Explore Risk and Compliance Dashboard label.

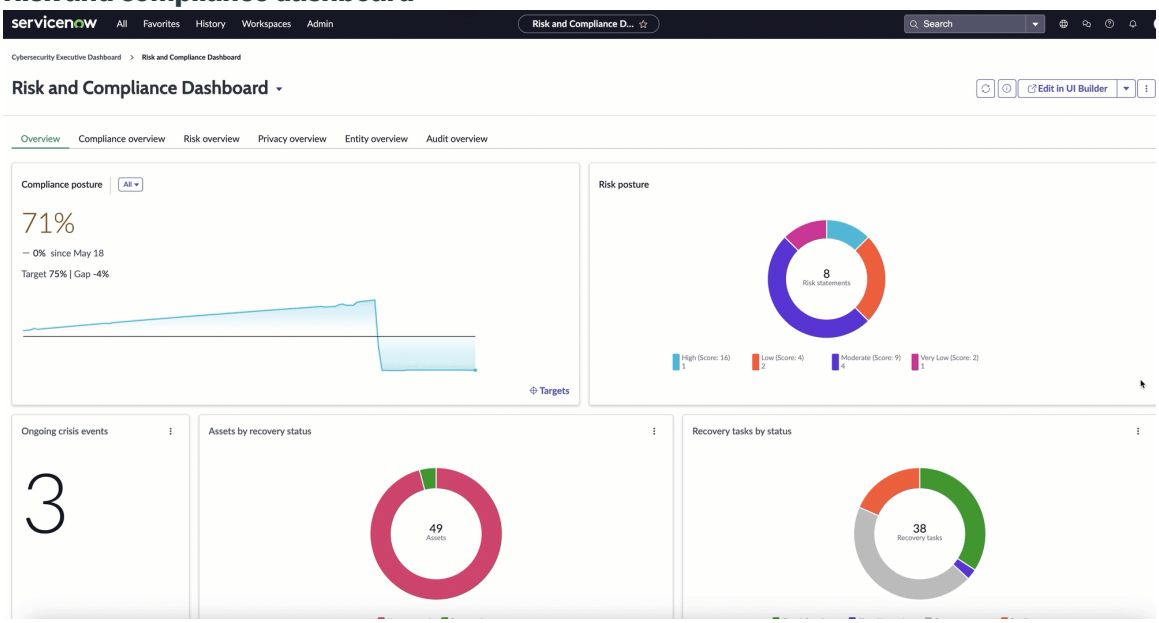
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk and Compliance Dashboard reports and solutions

The Risk and Compliance dashboard is a unified dashboard that provides a comprehensive analytical data of reports available from the major GRC applications for the chief information security officer to understand the compliance and risk posture of the organization. The dashboard consolidates data from various products within the ServiceNow GRC suite of applications.

Note: All reports are available only when the corresponding workspaces are installed.

Risk and compliance dashboard



Required ServiceNow AI Platform roles

For Compliance related reports

User must have sn_grc_dashboards.grc_ciso_user role and sn_bod.ciso role.

For Risk related reports

User must have sn_grc_dashboards.grc_ciso_user role and sn_bod.ciso role.

For Business Continuity Management related reports

User must have sn_bcm.viewer role and sn_bod.ciso role.

For Third-party risk related reports

User must have sn_vdr_risk_asmt.vendor_assessment_reviewer role and sn_bod.ciso role.

For Privacy related reports

User must have sn_privacy.analyst role and sn_bod.ciso role.

For Audit related reports

User must have sn_audit_ws.auditor role and sn_bod.ciso role.

Access the Risk and Compliance Dashboard

To open the dashboard, navigate to **All** > **Cybersecurity Executive Dashboard** > **Cybersecurity Executive Dashboard**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Indicators

Compliance posture

- Compliance percentage: Formula indicator that depicts compliance posture.
- All Controls: Automated indicator that supports the formula indicator.
- Compliant Controls: Automated indicator that supports the formula indicator.

Privacy compliance posture

PA indicator: Processing activity compliance score percentage.

Breakdowns

Functional Domain.

Reports

Note: All reports are available only when the corresponding workspaces are installed.

Overview tab

Title	Type	Source table	Description
Compliance posture	Line chart	Control [sn_compliance_control]	Provides cybersecurity and risk, and IT risk and compliance posture based on data analysis to the compliance managers.
Risk posture	Donut chart	The source tables are as follows: • Risk [sn_risk_risk] • Detailed aggregated risk [sn_risk_advanced_risk_assessment_result] (When the Advanced Risk application is installed and Advanced Risk Assessment is enabled	Provides the risk count based on the risk ratings.
Ongoing crisis events	Single Score	Recovery event [sn_recovery_event] where event type is actual	Displays the total number of ongoing crisis events that are neither approved nor closed.
Assets by recovery status	Donut chart	Assets [sn_recovery_event_asset]	Provides the total number of assets for ongoing crisis

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tab (continued)

Title	Type	Source table	Description
			events grouped by their recovery status, including assets that have been recovered and those that have not.
Recovery tasks by status	Donut chart	Recovery tasks [sn_recovery_event_task]	Provides the status of recovery tasks in various states for ongoing crisis events.

Compliance overview tab

Title	Type	Source table	Description
Authority documents	Donut chart	Authority Document [sn_compliance_authority_document]	Provides data of compliant and non-compliant authority documents in the chart. The list provides details of the authority documents, their individual compliance score in percentage, count of high priority issues and high risk exceptions on the authority documents, and the count of compliant cases.
Policies	Donut chart	Policy [sn_compliance_policy]	Provides the count of compliant and non-compliant policies in the chart. The list provides details of the policies, their individual compliance score in percentage, count of high priority issues and risk exceptions raised on each policy, and the count of compliant cases.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk overview tab

Title	Type	Source table	Description
Risk posture	Donut chart 	The source tables are as follows: • Risk [sn_risk_risk] • Detailed aggregated risk [sn_risk_advanced_risk_assessment_result] (When the Advanced Risk application is installed and Advanced Risk Assessment is enabled)	Provides the risk count based on the risk ratings.
Risk posture	List 	GRC Content Status [sn_grc_content_reports]	Provides the risk rating for each organizational risk to understand the overall risk assessment results. These ratings help organizations understand the potential impact and likelihood of various risks, enabling them to prioritize and manage these risks. The Risk posture card also highlights the following information for each risk: • **Risk appetite**: Risk appetite value defined. • **High priority issues**: The number of issues with priority is defined as High. • **Overdue risk response tasks**: Number of overdue risk response tasks. • **KRI Breach %**: Percentage of Key Risk Indicators (KRIs) that have

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk overview tab (continued)

Title	Type	Source table	Description
			exceeded their predefined thresholds or limits.
Third-party risk posture	Donut chart	Third-party risks [sn_grc_dashboards_third_party_risk]	Provides the risk rating for each third party. The risk rating is the overall assessment rating that considers the scores and ratings from all assessments conducted for a third party or vendor. The Third-party risk posture card also highlights the following information for each third party or vendor: • **Risk criteria**: Group of risk domains (sometimes called risk areas in other platform features) that applies to a particular type of third party. • **Risk tier**: Value determined based on the responses collected after an inherent risk assessment (IRQ) is completed. • **Risk intelligence rating**: Aggregate of all the scores collected from Risk intelligence providers. • **Overdue risk response tasks**: Number of overdue risk response tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Privacy overview tab

Title	Type	Source table	Description
Privacy compliance posture	Line	PA indicator: Processing activity compliance score percentage [pa_indicators]	Provides the compliance posture by month and is plotted by referring to the overall compliance score across all the processing activities.
Overdue high priority issues	Single score	Issues [sn_grc_issue]	Provides a focused overview of all overdue high-priority privacy-related issues, enabling quick identification and resolution of critical tasks to ensure compliance and data protection.
Privacy risk heatmap	Heatmap	Risk assessment methodology [sn_risk_advanced_risk_assessment_methodology]	Provides the privacy risk assessment data in the form of a heatmap. Privacy risk assessments are detailed assessments that are conducted if the criticality score is high. Assess each risk that is associated with the processing activity and know the aggregated risk score on the processing activity. After you assess the privacy risks, you can view the privacy risk posture on the risk heatmap.

Entity overview tab

Title	Type	Source table	Description
Entities	List	Entity compliance status [sn_compliance_entity_score]	Provides the summary of risks directly associated with the entity that contribute to the overall risk rating of the entity. The list also displays the compliance score of entities, and high

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Entity overview tab (continued)

Title	Type	Source table	Description
			priority issues and risk exceptions that are raised as a result of the non-compliant controls associated with the entity.

Audit overview tab

Title	Type	Source table	Description
Open and upcoming audit engagements	List 	Engagement [sn_audit_engagement]	Provides a list of open and upcoming audit engagements. The list also provides details of the engagement lead for each authority document, each engagement's planned start and end dates, high-priority issues, percentage of fieldwork that is completed, and the milestones in progress.

Filters

Name	Type	Description
Risk criteria	Report	Depending on which risk criterias you select, the donut chart and list shows the third parties or vendors that are in those risk areas.

Threat Intelligence Security Center

The Threat Intelligence Security Center (TISC) platform provides technology solution for aggregation, management and operationalization of threat intelligence.

Get started

Click on a tile to get started.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Explore  Learn how Threat Intelligence Security Center can help you with its key features and benefits.	Configure  Set up and configure Threat Intelligence Security Center to meet your specific needs.	Integrate  Integrate with Threat Intelligence Security Center
Administer  Manage and customize your Threat Intelligence Security Center.	Use  Manage your Threat Intelligence Security Center Library and objects.	Report Templates  Manage and customize your Case Management Reports.
MITRE ATT&CK Repository  Manage MITRE ATT&CK Repository Data.	TISC Data Archival  Understand TISC Data archival and rules	Reference  Get additional information about Threat Intelligence Security Center.

Request apps on Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Installing Threat Intelligence Security Center (sn_sec_tisc) will auto install all the dependent applications from ServiceNow Store.

More resources

Visit the Security Incident Response forum on the ServiceNow Community.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Troubleshoot and get help

- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Explore

Threat Intelligence Security Center (TISC) enables you to collaborate with the threat intelligence teams and has multiple capabilities to collect and process various threat intelligence feeds and a workspace to analyze, collaborate, action, and share the necessary information.

Watch an overview about the Threat Intelligence Security Center application.

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

Threat Intelligence Security Center is enhanced with capabilities to manage data collection, data processing such as DE-duplication, normalization and aggregation, analysis of threat intelligence, dissemination of threat intelligence, and also workspace that provides the administration tasks.

Key features

The following are the Threat Intelligence Security Center (TISC) key features that are explained in detail in the further sections:

- **Curated Catalog of OSINT Threat Feeds**: Provides access to a broad selection of popular open-source threat intelligence feeds, confirming wide coverage.
- **Premium Feed Integration**: Enhances the quality of threat intelligence by integrating premium feeds.
- **Automated Observable Extraction**: Automatically identifies and extracts the commonly used observable types from uploaded files, streamlining the threat data ingestion process.
- **Diverse Data Aggregation**: Supports multiple data formats including STIX, MISP, JSON, and others, enabling seamless feed consolidation.
- **Enrichment Capabilities & Validation**: Provides enrichment and validation capabilities by removing false positives, assigning confidence scores, validating indicators, and adding contextual information to improve data quality.

  The TISC integration capabilities:

  - Enrichment integrations includes Threat Lookup, Sighting Search and Observable Enrichment.
  -
    - Enriches observables with threat intelligence, performs sighting searches and threat look ups to determine maliciousness of an observable.
    - Supports CrowdStrike Falcon EDR with continuous monitoring and real-time alerting.
  - Security Tool integrations for orchestration such as SIEMs, EDR and Firewalls.
- **Correlation Rules Engine**: Automatically establishes relationships between intelligence records, enabling deeper insight into threat patterns.
- **Customizable Threat Scoring**: Enables fine-tuning of threat scores for more nuanced and accurate threat assessment.
- **Internal Intelligence integration**: Enables integration of internal intelligence sources, including Vulnerability Response (VR), Security Incident Response (SIR), and Configuration Management Database (CMDB).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **User-Specific Dashboards**: Tailors visualizations and data views according to Threat Intelligence personas, improving user experience and relevance.
- **Graphical Visualization Tools**: Facilitates understanding of complex threat intelligence data through intuitive graphical visualizations such as relationship graphs and interactive investigation canvases to simplify threat intelligence analysis.
- **Dedicated Analyst Workspace**: Provides a dedicated, streamlined Threat Intelligence Analyst workspace that enables threat intelligence analysts to focus on investigation and analysis with minimal distractions.
- **Threat Case Management**: Supports investigative workflows with task tracking and case handling.
- **MITRE ATT&CK Integration**: Enables users to link case records with MITRE ATT&CK framework data for enhanced kill chain analysis.
- **Seamless SIR Integration**: Ensures smooth data migration and interoperability between Security Incident Response and Threat Intelligence Security Center applications.
- **Notification & Alert Rules**: Establishes trigger alerts to notify teams based on evolving threat intelligence.
- **Data Retention & Cleanup Policies**: Enables organizations to define data management rules to maintain application performance and compliance.
- **Reporting & Collaboration**: Generates comprehensive status reports and investigation summaries using rich-text editors and customizable templates.
- **Domain Separation for MSSPs**: Supports multitenant environments, enabling Managed Security Service Providers (MSSPs) to segregate customer data securely.
- **Extensive API integration**: Offers TISC API for seamless connectivity with other security tools and platforms.

Threat Intelligence Security Center users

User	Description
Administrator	Administers and configures the initial setup and ongoing maintenance of the Threat Intelligence Security Center, including configuring data sources and managing intelligence settings.
Analyst	Threat Intelligence Analysts are responsible for conducting analysis and research tasks requested by the team. They can import ad hoc intelligence to support their work and use the system's tools for analysis, collaboration, and managing the intelligence library.

TISC Key terminology

The terms defined below are used throughout the Threat Intelligence Security Center (TISC).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Terminology Definitions

Terminology	Definition
Data Processing	A Threat Intelligence Platform (TIP) is a technology solution that collects, aggregates, and organizes threat intelligence data from various sources and patterns. Threat intelligence is the data that is collected, processed, and analyzed to understand a threat actors targets and attack behaviors.
Observables	Observables represent stateful properties (such as the MD5 hash of a file or the value of a registry key) or measurable events (such as the creation of a registry key or the deletion of a file) that are pertinent to the operation of computers and networks. For more information, see Observables.
Indicators	Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity. For example, an Indicator may be used to represent a set of malicious domains and use the STIX Patterning Language to specify these domains. The Indicator SDO contains a simple textual description, the Kill Chain Phases that it detects behavior in, a time window for when the Indicator is valid or useful, and a required **pattern** property to capture a structured detection pattern. For more information, see Indicators.
Objects	Defines the set of STIX Domain Objects (SDOs), each of which corresponds to a unique concept commonly represented in Cyber Threat Intelligence (CTI). Using SDOs and STIX Relationship Objects (SROs) as building blocks, individuals can create and share broad and comprehensive cyber threat intelligence. For more information, see TISC Library Repository.
Relationships	A relationship is a link between two observables or two SDOs or Observable and SDO that describes the way in which the objects are related. Relationships can be represented using an external STIX Relationship Object (SRO) or, in some cases, through certain properties which store an identifier reference that comprises an embedded relationship. For more information, see Relationships Objects.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Home page in TISC Workspace

The TISC home page serves the landing page and provides a summary of **Feeds Overview**, **Trending Threats**, and **Intelligence Sharing** enabling visualization of threat intelligence data.

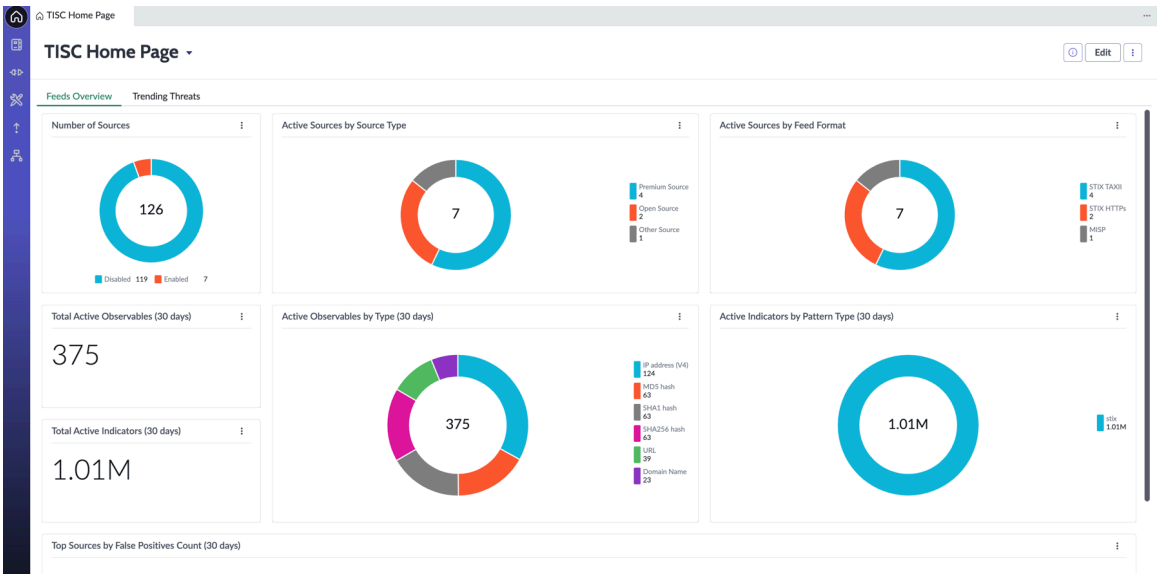
Before you begin

Role required: sn_sec_tisc.analyst

On the Home page, you can perform the following procedure to visualize the threat intelligence data.

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Security Center**.
   The TISC Home page is displayed.



2. View the TISC home page with different widgets data.
   The home page view consists of three different tabs: **Feeds Overview**, **Trending Threats**, and **Intelligence Sharing**. The content on the home page comes from various sources such as observables, indicators, and data feeds.

   a. **Feeds Overview**: This tab provides a high level overview of different sources that the data is ingested and sources that are configured for the data ingestion.

Feeds Overview

Widget Name	Description	Action
Number of Sources	Displays the number of sources by status such as draft, enabled, and disabled in the system.	When this widget is clicked, the list page is opened with the filtered records.
Active Sources by Source Type	Displays the distribution of active sources by source type.	When this widget is clicked, the list page is opened with the filtered records.
Active Sources by Feed Format	Displays the number of enabled sources by Feed Type.	When this widget is clicked, the list page is opened with the filtered records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Widget Name	Description	Action
Total Active Observables (30 days)	Displays the top 10 sources by volume of intelligence records that were created in the last 30 days.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Active Observables by Type	Displays the top total volume of observable aggregates that were created in the last 30 days.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Active Indicators by Pattern Type	Displays the total volume of Indicator aggregates by pattern type that were created in the last 30 days.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Total Active Indicators (30 days)	Displays the total volume of indicator aggregates that were created in the last 30 days.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Top Sources by False Positives Count (30 days)	Displays the total volume by of False Positive observables that were created in the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.

b. **Trending Threats**: This tab provides a high level overview of the trending threats.

Trending Threats

Widget Name	Description	Action
Latest Reports (Top 10)	Displays the list of reports and links - Top 10 order by published date.	Selecting a record from this list view opens it in a new tab on the home page.
Latest RSS Feeds (Top 10)	Displays the list of RSS feeds and links - Top 10 order by published date.	Selecting a record from this list view opens it in a new tab on the home page.
Active Observables by Threat Score Range (30 days)	Displays the observables count that were created in the last 30 days distributed by Threat Score ranges.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Active Observables by Reputation (30 days)	Displays the observables count that were created in the last 30 days distributed by Reputation.	When this widget is clicked, the KPI details page of the widget for the selected filter is opened in a new tab.
Top tags (30 Days)	Displays the top tags on the records created in the last 30 days based on the frequency of usage.	Select a tag from the chart and this opens the list view filtered by the selected tag.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Widget Name	Description	Action
		▪ A horizontal bar chart displaying the most frequently used tags. ▪ Indicates which tags are commonly applied to observables or feeds. ▪ Helps identify trending classifications or recurring patterns in threat data.
Most Targeted Sectors (30 days)	Displays the top 10 sectors ranked by activities reported that were created in the last 30 days.	Select a sector in the chart and this opens the list view filtered by the selected sector. ▪ A bar chart highlighting sectors (such as Commercial, Government, Aerospace, and so on) most targeted by threats. ▪ Shows the frequency of targeting per sector. ▪ Useful for understanding industry-specific threat trends and prioritization.

c. **Intelligence Sharing**: This tab provides a high level overview of the intelligence sharing.

Intelligence Sharing

Widget Name	Description	Action
Inbound Intel - Record Count (30 days)	Displays the number of inbound intel records received in the last 30 days, categorized by type (Observable, Object, Indicator).	When this widget is clicked, the list page is opened with the filtered records.
Outbound Intel - Record Count (30 days)	Displays the number of outbound intel records shared in the last 30 days, categorized by type (Observable, Object, Indicator).	When this widget is clicked, the list page is opened with the filtered records.
Inbound Intel - Distribution by Status (30 days)	Displays the distribution of inbound intelligence records by status over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Outbound Intel - Distribution by Status (30 days)	Displays the distribution of outbound intelligence	When this widget is clicked, the list page is opened with the filtered records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Widget Name	Description	Action
	records by status over the last 30 days.	
Inbound Intel - Top Sharing Profile (30 days)	Displays the top profiles based on inbound intel received over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Outbound Intel - Top Shared Profile (30 days)	Displays the top profiles based on outbound intel shared over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Inbound Intel - Most Shared Types (30 days)	Displays the most frequently received intel types (Object, Indicator, Observable) over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Outbound Intel - Most Shared Types (30 days)	Displays the most frequently shared intel types (Object, Indicator, Observable) over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Inbound Intel - Distribution by Format (30 days)	Displays the format distribution (e.g., MISP, STIX) of inbound intel over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.
Outbound Intel - Distribution by Format (30 days)	Displays the format distribution (e.g., MISP, STIX) of outbound intel over the last 30 days.	When this widget is clicked, the list page is opened with the filtered records.

Configuring Threat Intelligence Security Center

Set up the features, components, and integrations that you need to provide service and support to your customers.

Download TISC application from ServiceNow Store

Before you run the Threat Intelligence Security Center application in your instance, you must download it from the ServiceNow® Store and install it.

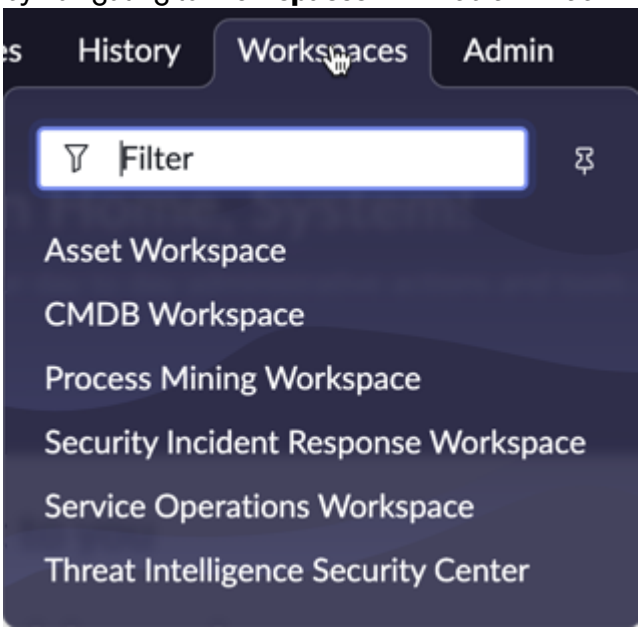
Before you begin

Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Follow the instructions for downloading an application from the ServiceNow Store and install the **Threat Intelligence Security Center Security Operations** application.
2. After installation is complete, you can open the Threat Intelligence Security Center Workspace by navigating to **Workspaces** > *Threat Intelligence Security Center*



What to do next

After you successfully downloaded the application, verify that you've completed all the tasks mentioned here in this section, Set up Threat Intelligence Security Center for a smooth integration.

Set up Threat Intelligence Security Center

Before you use the Threat Intelligence Security Center, you must download it from the ServiceNow Store.

Roles installed

Review the following information and verify that you've completed all the tasks for a smooth integration. Below is the list of different user persona defined to access and work with the application:

- Threat Intelligence Analyst (sn_sec_tisc.analyst)
- Threat Intelligence Administrator (sn_sec_tisc.admin)

Entitlements applicable for TISC Roles

Setup	Description
Assign and verify the required ServiceNow AI Platform and Threat Intelligence Security Center roles.	The following roles are required for configuration and verification of the expected results:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Entitlements applicable for TISC Roles (continued)

Setup	Description

	• As an admin, you must install the TISC application from the ServiceNow Store and assign the role as sn_sec_tisc.admin.
	• This sn_sec_tisc.admin role performs the following tasks:
	  ○ Configures the Data Sources to ingest the data. For more information, see Threat Intelligence Feeds.
	  ○ Configured the integrations required for Enriching Observable data in TISC. For more information, see TISC Enrichment Integrations.
	  ○ Configures Data Import Approval Roles for importing data using Import Assistant. For more information, see Working with Data Imports.
	  ○ Configures Threat Score Calculator using required criteria for automatic calculation of Threat Score of observables. For more information, see Define Threat Score Calculator.
	  ○ Configures required Taxonomies and Taxonomy Values. For more information, see Creating Taxonomies.
	  ○ Configure the MITRE ATT&CK repository relevant to your organization. For more information, see MITRE-ATT&CK Repository.
	Note: As a sn_sec_tisc.admin, you can also assign the sn_sec_tisc.analyst role.
	• The sn_sec_tisc.analyst role performs the following tasks:
	  ○ Views the overview of data in the system using Product Homepage. For more information, see Home page in TISC Workspace.
	  ○ Import data into system using Import Intelligence button in Threat Library Page. For more information, see Threat Intelligence Security Center Library.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Entitlements applicable for TISC Roles (continued)

Setup	Description
	○ ▪ Search across the data present in the application using search provided in Threat Library page. ▪ Manages the data ingested from various sources in Threat Library. ▪ Performs various Enrichment actions on Observables. ▪ Creates and Manages Cases. For more information, see Creating cases using Threat Analyst Workbench.

Dependency Plugins

Plugin	Description
This following applications are required for installation of this application: • Security Case Management common workspace components [com.snc.escm.ws_commons]. • Threat Intelligence Support Common [com.snc.threat]. • Column Level Encryption (com.glide.encryption) • Large JSON and XML Payload Builder API (com.glide.streaming_builder) • Security Support Core (com.snc.security_support.core) • Node map Experience Component (sn_node_map) • Reporting UI Component for Workspace(sn_sec_reporting) • Rich Text Editor Component for Security Operations(sn_escm_rte) • Security Integration Framework(sn_sec_int) • Security Support Common(sn_sec_cmn) • Security Support Orchestration(sn_sec_cmn_orch)	Verify that the ServiceNow core applications that are required to support the integration are installed and activated before you configure this integration.

Integrate

Use this section to understand the Threat Intelligence Security Center integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Integrations** section includes the following modules.

Integrations

Module Name	Description
Catalog	View all available threat intelligence feeds and enrichment integrations as tiles. You cannot create feeds or integrations from this section.
Intel Feeds	View details about threat intelligence feeds and configure new feeds. The available feeds are: • All Feeds: Shows all configured threat intelligence feeds. • STIX TAXII: Supports configuration of feeds using the STIX/TAXII protocol. • STIX HTTPS: Ingests STIX formatted data over HTTPS. • MISP: Integrates feeds from MISP (Malware Information Sharing Platform). • Text: Supports ingestion of plain text-based threat data. • CSV: Import threat intelligence data in CSV format. • JSON: Supports ingestion of structured data in JSON format. • RSS: Configure RSS feeds for automated ingestion of updates. • Custom: Configure custom feed types such as MISP, CrowdStrike.

Threat Intelligence Security Center Catalog

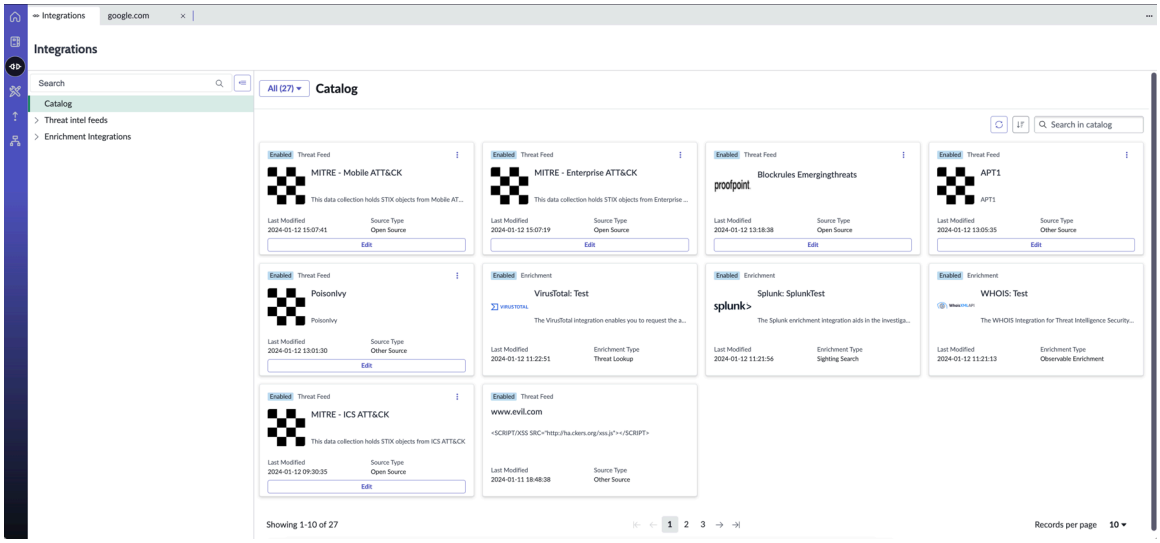
The Threat Intelligence Security Center Catalog is a curated list of Threat Intelligence feeds and enrichment integrations available in the application for you to enable them after adding the required information, and schedule the feed to automatically ingest Threat Intelligence data on a set frequency.

As a sn_sec_tisc.admin, you can also search and edit the existing source configurations, enable or disable, and delete the configurations from the Catalog. Any new data source is added to the Catalog, that will appear as a new configuration card on the Catalog.

Role required:

- sn_sec_tisc.admin (create/update)
- sn_sec_tisc.analyst (read)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: The cards on the catalog are differentiated by its label which is present at the top of the card Threat Feed/Enrichment.

Actions on the Catalog view

The Catalog view enables you to perform the following actions.

Actions on the Catalog view

Action	Description
All	Use this dropdown menu to filter feeds and integrations based on their current state. You can filter based on the following states: • **All**: Displays all the feeds and integrations on the page. This is the default option. • **Enabled**: Displays all the feeds and integrations that are in an enabled state. • **Disabled**: Displays all the feeds and integrations that are in a disabled state. • **Draft**: Displays all the feeds and integrations that are in a draft state.
	Use this action to refresh the Catalog.
	Use this action to sort all the feeds and integrations based on the following: • **Last Modified (recent)** • **Last Modified (oldest)** • **Name (A-Z)** • **Name (Z-A)**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Actions on the Catalog view (continued)

Action	Description
Search in catalog	Use this action to search for feeds/ integrations based on the name and description within the catalog.

Threat Intelligence Feeds

Use Threat Intelligence Feeds to add, edit, or remove Threat Intelligence feed data source.

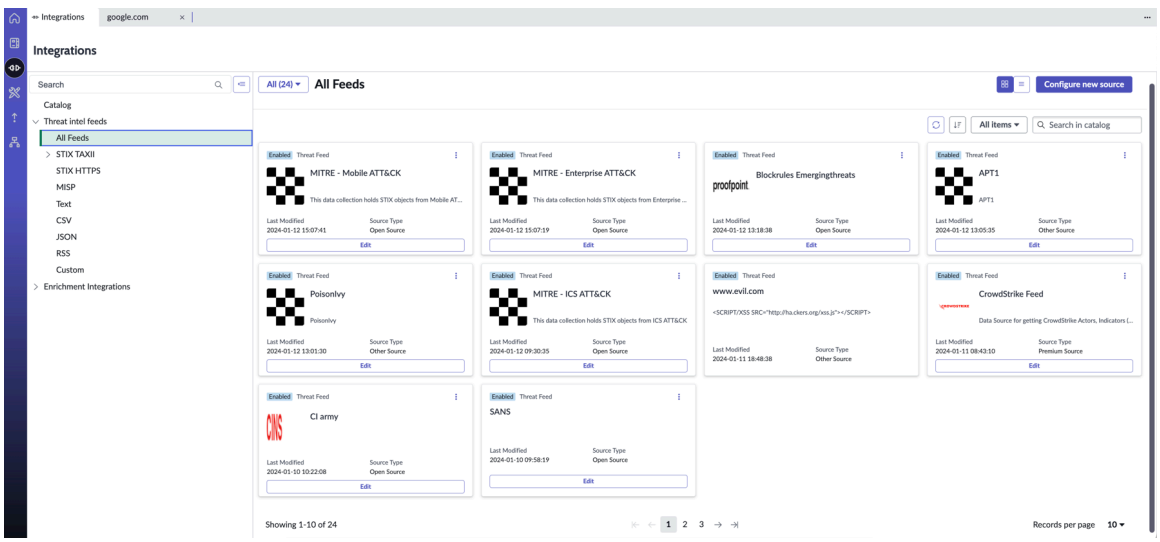
The data source feeds are available from the Threat Intel Catalog under Integrations section.

The catalog for threat intelligence feeds is built to show the available feed data sources in the form of tiles and has the ability to filter, search, and navigate to the details of the source configuration and perform various actions.

All Feeds

The base system includes a series of cards for each of the feeds that you can enable and use.

The Feeds can be viewed by navigating to **Workspaces** > **Threat Intelligence Security Center** > **Integrations** > **Threat Intel Feeds** > **All Feeds**.



Actions on the All Feeds view

The All Feeds section enables you to perform the following actions.

Actions on All Integrations view

Action	Description
All	Use this drop-down menu to filter feeds based on their current state. You can filter based on the following states:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Actions on All Integrations view (continued)

Action	Description
	• **All**: Displays all the feeds on the page. This is the default option. • **Enabled**: Displays all the feeds that are in an enabled state. • **Disabled**: Displays all the feeds that are in a disabled state. • **Draft**: Displays all the feeds that are in a draft state.
	Use this action to view all the feeds in the form of cards.
	Use this action to view all the feeds in the form of a list view.
	Use this action to refresh the page.
	Use this action to sort all the integrations based on the following: • **Last Modified (recent)** • **Last Modified (oldest)** • **Name (A-Z)** • **Name (Z-A)**
All items	Use this action to filter and list the threat intelligence feed tiles by source type or feed type. **Source Type**: • Open Source • Other Source • Premium Source **Feed Type**: • CSV • Custom Feed • JSON • MISP • RSS • STIX HTTPs • Text
Search in catalog	Use this action to search for feeds based on the name and description within the catalog.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Types of Threat Intel Feeds

The following are the types of threat intelligence feeds which can be configured and enabled:

Threat Intelligence Feeds

Type	Description
TAXII Feeds	Feeds that are available as STIX/TAXII Collections format.
STIX HTTPS	Threat Intelligence feeds in STIX format that can be accessed through REST APIs on HTTPS protocol.
MISP	Feeds that are in the MISP Format Feeds.
Text	Feeds that are available as hosted files in text format. **Note:** Only URLs, domains, file names, hashes, and IP addresses are extracted.
CSV	Feeds that are available as hosted files in CSV format. **Note:** Only URLs, domains, file names, hashes, and IP addresses are extracted.
JSON	Feeds that are available as hosted files in JSON format. **Note:** Only URLs, domains, file names, hashes, and IP addresses are extracted.
RSS	Feeds that are available in RSS format. The application will store the data as RSS Feed Records.
Custom	Feeds that are configured using custom parsers. **Note:** Only URLs, domains, file names, hashes, and IP addresses are extracted.

For the next steps in the procedure, refer to the respective section for configuring a each specific feed type. Threat Intelligence Feeds.

Configure a new threat intelligence feed

Configure new threat intelligence feed data source.

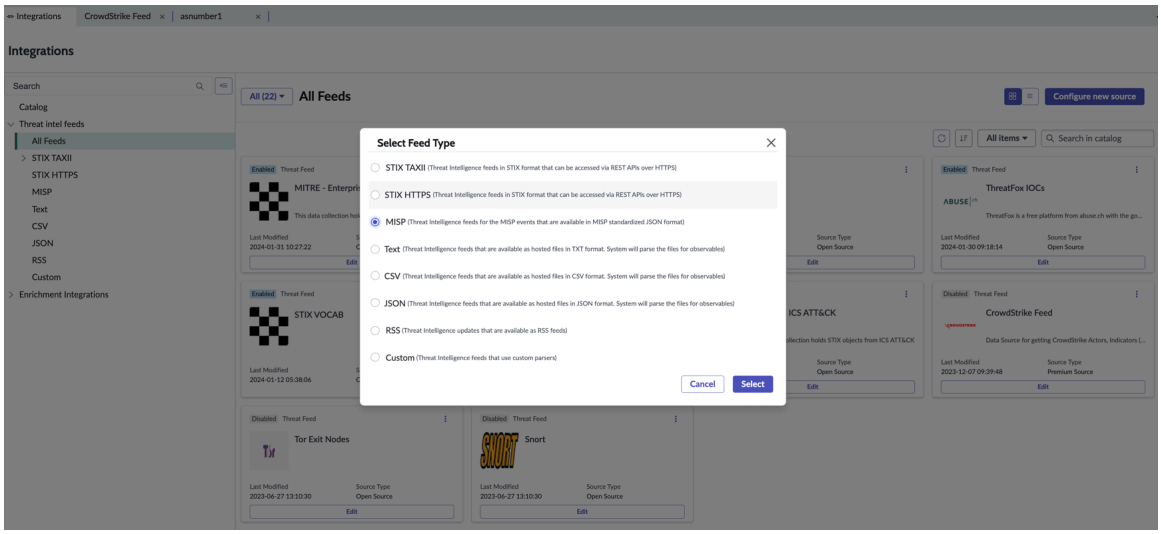
Before you begin
Role required: sn_sec_tisc.admin

To configure a new threat intelligence feed, follow the procedure:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **Threat Intel Feeds** > **All Feeds**.
4. Click **Configure new source**.
   The various feed types are displayed.



5. Select the respective feed type.
6. On the form, fill in the fields.

Configure new source

Field	Description
Name	Enter a name for the feed.
Description	Description of the feed.
Feed Type	The feed type. For example, MISP. By default, this value is displayed based on the type of feed that you selected from the Catalog.
Logo	Attach the logo of the source feed. **Note:** The size should be 72px/72px.
Industry	Select the industry category such as Aerospace, Agriculture, and so on for which the feed is applicable to.
Source Type	Select the type of source from the list of available source types. List of available sources are: ○ Government ○ ISACs ○ Open Source

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Premium Source ○ Other Source

7. Click **Select**.
8. Fill in the fields in the Configuration section, as appropriate.

Configuration

Field	Description
Expiry period (days)	Enter the expiry period for the feed in days. For example, 180 days. **Note:** Whatever the data that is ingested from the source will be expired 180 days after the ingestion.
Use REST Message	Select **Use REST Message** check box if you need to use REST Message/REST Method functionality that is provided by ServiceNow AI Platform. If this check box is not selected, then the application uses the endpoint provided in **REST Endpoint URL** to fetch the data from the feed. For more information, see Outbound REST web service on ServiceNow AI Platform documentation. **Note:** The REST message and REST method fields are mandatory when you select the REST message.
REST Message	Select the REST Message record from the list of REST message records which are already configured in the instance. For more information, see Outbound REST web service on the ServiceNow AI Platform documentation. **Note:** Select this value when you need to view specific headers, and define the REST related records using the REST message option.
REST Method	Select REST Method from the list of available REST Methods configured for the selected REST Message. For more information, see Outbound REST web service on the ServiceNow AI Platform documentation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Confidence	Set the confidence for all the applicable records that are ingested through this specific feed. **Note:** Set the confidence between 0-100 for this source.
Data Parsing Mechanism	Select the appropriate data parsing mechanism option. The available options are: ○ **Automated IoC Extraction**: This option is selected by default when configuring Text, CSV, or JSON feeds. ○ **Custom Field Mapping**: Select this option if you want to define how the specific fields in your feed data should be mapped to the observable attributes. Once selected, you can configure the mappings in the **Field Mapping** section. For more detailed information on the custom field mapping, see Configure Custom Field Mapping. **Note:** The data parsing mechanism option is only available for Text, CSV, and JSON feeds, where the feeds **Report Processor** is set to `SimpleFeedDatasourceResponseProcessor`.
REST endpoint URL	Enter the REST endpoint URL where the data is hosted by the threat intelligence feed. **Note:** For MISP feed types, the REST endpoint URLs that end with `/manifest.json` are supported.
Authentication Required	Select this check box if authentication is required for your new threat intelligence feed. **Note:** This is only applicable when REST Endpoint URL is being used to retrieve the data.
Authentication Type	The authentication type for the source feed. Following are the authentication types that are configured and provisioned within the base system for the users: ○ API ID / API Key ○ API ID / API Secret ○ API Key ○ API Key / API Secret

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ API Username / API Password / API Key ○ Basic Authentication
Headers to be passed with request	Any headers to be passed with the requests can be provided in Request Header Mapping. ○ Header should be provided in key-value pair separated by colon(':'). ○ Each header key value pair should be provided in a new line. ○ For providing authentication parameters as header values, enclose the required Authentication Label with '${' and '}$'. For example, x-api-key:${API Key}$.
Advanced	Select this check box to define custom integration script and report processor script. **Note:** When you select this check box, the **Integration script** and **Report Processor** fields will be appeared for you to select the custom scripts.
Integration script	Integration script invokes a call to the REST Endpoint URL using the authentication parameters and the headers as configured in the feed, and then the script fetches the data that is available from the specific feed. Within the base system following are the custom scripts includes available, which are provisioned within the application for the integrations scripts: ○ FeedDatasourceIntegrationBase ○ MITRESourceIntegration ○ RSSFeedDatasourceIntegration ○ SimpleFeedDatasourceIntegration ○ SimpleMISPFeedDatasourceIntegration The default integration script is based on the feed type that you select. For example, if you select MISP feed type which is a standard format to process and fetch the data then the integrations script is **SimpleMISPFeedDatasourceIntegration**. **Note:** For the Custom integration scripts, you can create a script include by extending **FeedDatasourceIntegrationBase** and override the required methods.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Report processor	The report processor script processes data fetched from the feed using the integration script. The base system includes the following custom scripts, which are provisioned within the application to support report processor script: ○ AtomFeedDatasourceResponseProcessor ○ FeedDatasourceResponseProcessorBase ○ MITRECollectionDataProcessor ○ RSSFeedDatasourceResponseProcessor ○ SimpleDataplaneFeedResponseProcessor ○ SimpleFeedDatasourceResponseProcessor ○ SimpleFeodotrackerFeedResponseProcessor ○ SimpleMISPFeedDatasourceResponseProcessor ○ TAXIIV2CollectionDataProcessor The default report processor for STIX HTTPS feeds is `SimpleMISPFeedDatasourceResponseProcessor`. This processor is preconfigured by the application and cannot be modified or replaced.

9. Fill in the fields in the Scheduling section, as appropriate.

Scheduling

Field	Description
Run	Set the frequency at which you want to ingest the records. The feed will run and execute based on the scheduling job interval. The available job intervals are: ○ Daily ○ Weekly ○ Monthly ○ Periodically ○ Once ○ On Demand ○ Business Calendar: Entry Start ○ Business Calendar: Entry End **Note:** By default, the frequency is set to On Demand.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For more information, see Scheduled Jobs and how to Automatically run a script of your choosing.
Fetch Data From	The start date from when the data needed to be fetched. This field should be set with the time from when the data needs to be ingested from the corresponding source. Once this field is set, the next ingestion run would fetch the data from the configured time and consecutive ingestion runs would fetch incremental Data. For example, Source is scheduled to ingest the data every hour. The user sets **Fetch Data From** to Jan 12 6:00AM on Jan 12 9:30AM, the ingestion triggering on Jan 12 10:00AM would fetch the data from Jan 12 6:00AM to Jan 12 10:00AM. The next ingestion that triggers at 11:00AM would fetch only the incremental data from Jan 12 10:00AM to Jan 12 11:00AM. **Note:** This means the scheduled runs will fetch data incrementally starting from the specified date onwards. **Important:** Also, this is not applicable for Text, CSV, and JSON feeds.

Tags

Field	Description
Select Tags	Use the tags to annotate or ear mark records that are ingested into the system from this source. Start entering the tag name in the **Search** bar to choose the available tags in the application or enter new tag name and click **Add** to assign it to the source.

10. Click the **Save** action to store and create the feed.
    The provided details are validated, and by default the feeds status is disabled.
11. **Optional:** Click the **Save as Draft** action to only store the feed configurations as draft.
    Users cannot enable a feed when it is saved in draft. If you're not sure about the configuration details, you can use the **Save as Draft** option. After you get the configuration details, you can fill the remaining information in the draft version and create it.
12. Click **Enable** to enable the record.

    Once the threat intelligence feed record is enabled, you can execute the record to run the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The threat intelligence feed record is labeled and indicated as **enabled**. Similarly, you can disable the threat intelligence feed by clicking **Disable** button.
- You can also enable, disable, or delete a particular feed by using the **Actions** menu of the required feed tile on the **Catalog** or **Threat Intel Feeds** page.

13. Click **Delete** to delete the threat intelligence feed record.
14. Select **Integrations Run** section to verify the run details.

Note: The above threat intelligence feed configuration procedure is same for all other threat intelligence feed types, except for STIX TAXII. For more information on how STIX TAXII is configured, see Configure a new TAXII Feed.

Configure Custom Field Mapping

Field Mapping allows you to configure how each field in a data feed such as Text, CSV or JSON is interpreted and assigned to the corresponding observable.

Before you begin

Role required: sn_sec_tisc.admin

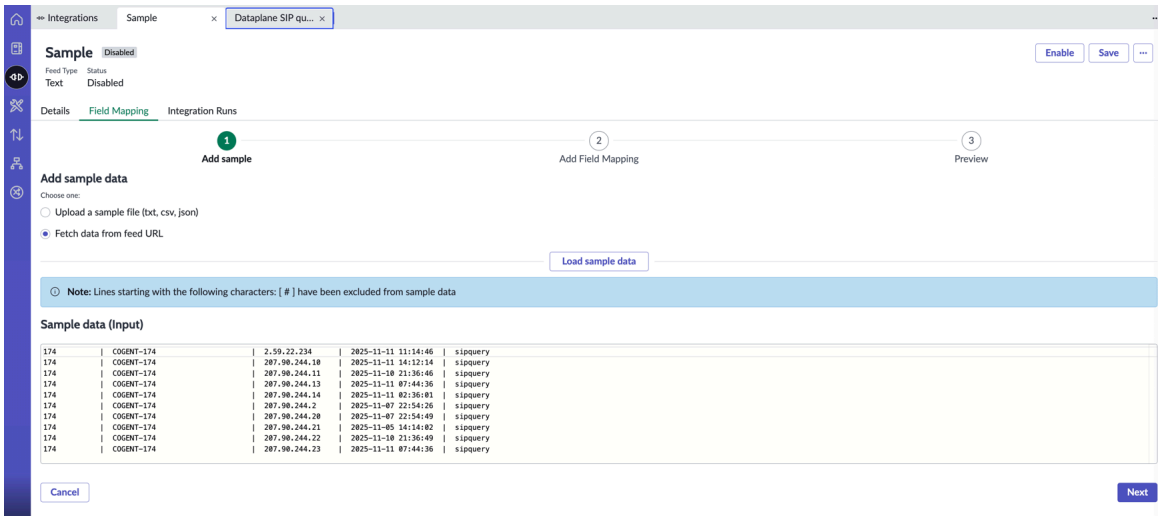
Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. Select **Threat Intel Feeds** > **All Feeds** > **Text**.
3. Select **Configure new source**.
4. Fill in the text feed form details as required.
   For more information see, Configure a new threat intelligence feed.
5. On the new form view, drill down to **Data Parsing Mechanism** field under the **Configuration** section.
   For more information on Data Parsing Mechanism, see Configure a new threat intelligence feed.
6. Select **Custom Field Mapping** option.
7. Navigate to the **Field Mapping** section.
8. Select **Configure** to add the field mapping for the new data source.
   This section involves three steps such as adding sample data, field mapping, and previewing the mapped sample records.
9. To add the sample data, select **Load Sample Data**.
   This displays the sample data from the selected option, the application displays only the relevant data rows and lines that begin with `#` are excluded from the sample data. The comment identifiers can be modified with the system property: `sn_sec_tisc.feed_comment_identifiers`.

   The application will fetch a sample of the incoming data either from a sample file (such as .txt, .csv, or .json) or directly from the configured feed URL (the feed URL and credentials entered in the **Details** section). This allows you to preview the structure and contents of the data before defining field mappings.
10. Select either **Upload a sample file** or **Feed data from feed URL**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This sample data will fetch the first ten records by default, this total number of records to be retrieved can be modified with the system property `sn_sec_tisc.feed_field_mapping_sample_count`.



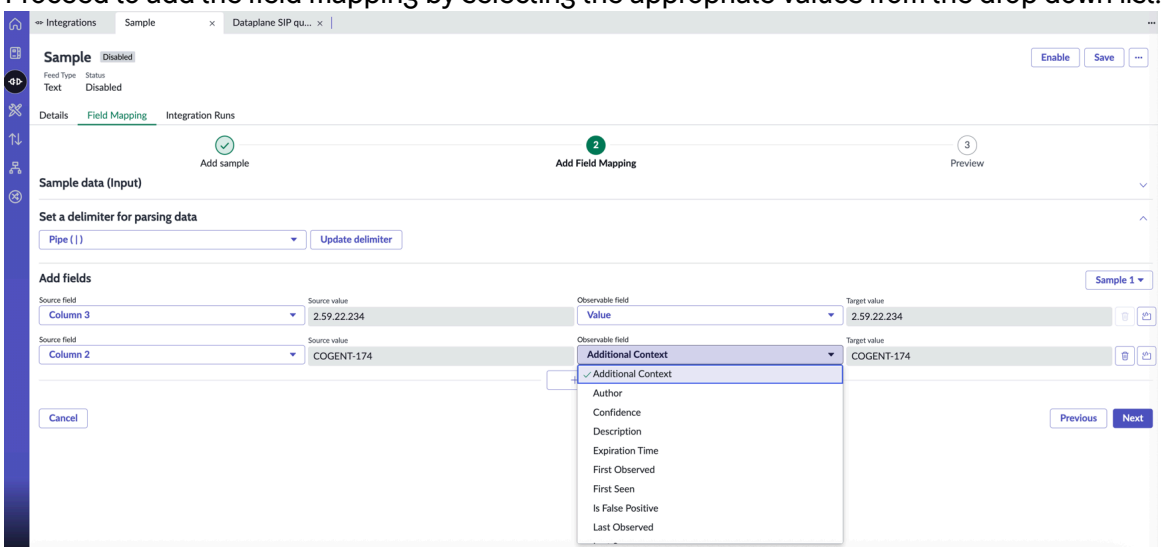
11. Select **Next** to configure the field mapping.
12. Select **Set a delimiter for parsing data** option from the drop down list.
    When working with Text feeds, the delimiter is essential for correctly parsing the data into individual fields.

    In this scenario, the text feed uses the pipe operator (|) as the delimiter which separates each value in the sample text data into distinct columns. Correctly identifying and applying this delimiter is essential to ensure accurate field mapping and successful data ingestion.

    Regular expressions(RegEx) are also supported as delimiters for the text feed, providing additional flexibility when parsing complex feed data and not support for the JSON and CSV feeds.

    > **Note:** For CSV feeds comma (,) is the default delimiter and JSON feeds doesn't require any delimiter.

13. Select **Update delimiter**.
    The options to add fields for field mapping are displayed.
14. Proceed to add the field mapping by selecting the appropriate values from the drop down list.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

15. Use the **Transform Script** to transform and normalize the input values before mapping them to observables.
You can map the same source column (for example, column 2) multiple times such as to the **Additional Context** field using a dedicated script handler.

> **Important:**
> - Multiple source field mapped with the same target observable fields of type *string*. For a reference list of string-type fields, see the `sn_sec_tisc_observable_source` table.
> - The **Observable fields** type such as **Additional Context**, **Author**, and **Description** allow multiple field mappings. Review and update the mappings as needed.
> - The same source field can be mapped to multiple target fields without any limitations.

Transform scripts can be applied to customize how data is processed and enriched during mapping.

a. Select **Enable/disable transform script** icon to configure the script.
The Configure script for source field dialogue box is displayed.

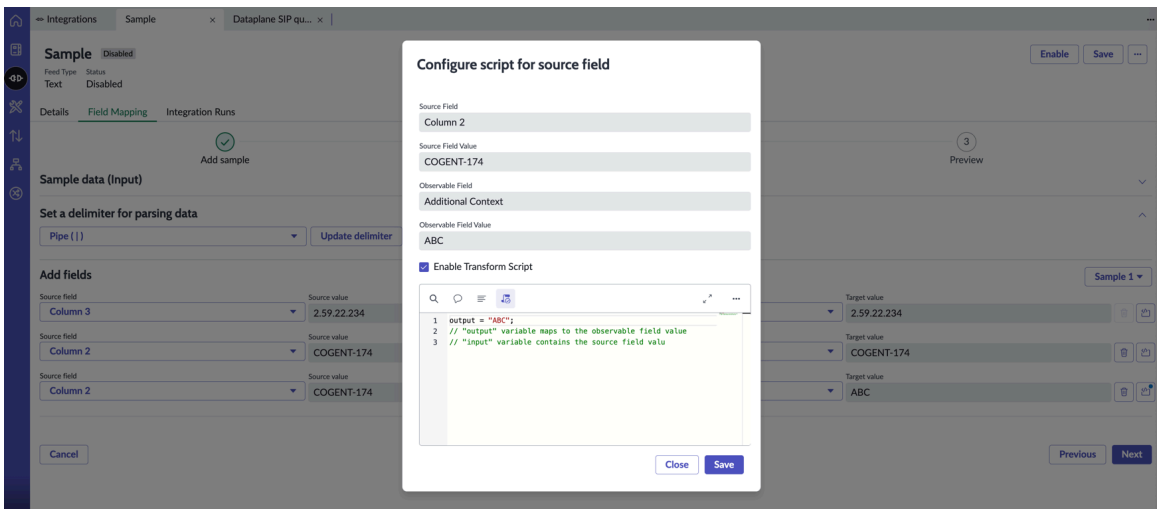
b. Select **Enable Transform Script** check box on the **Configure script for source field** dialogue box.

c. Add or modify the script.

For example, if your input field contains values such as low, medium, or high and you want to map these values to numerical confidence levels (between 0–100), then you can use **Transform Script** to convert the input value and map it to the **Confidence** field of the observable.

For example, if your input field contains a string value and you want to map these values to a string type as **Additional Context (observable type)**, then you can either use the **Transform Script** to input the value or without the **Transform Script** to map it to the **Additional Context** field of the observable.

> **Note:** Each individual mapping record supports its own script, allowing users to define custom transformation logic for every mapping.

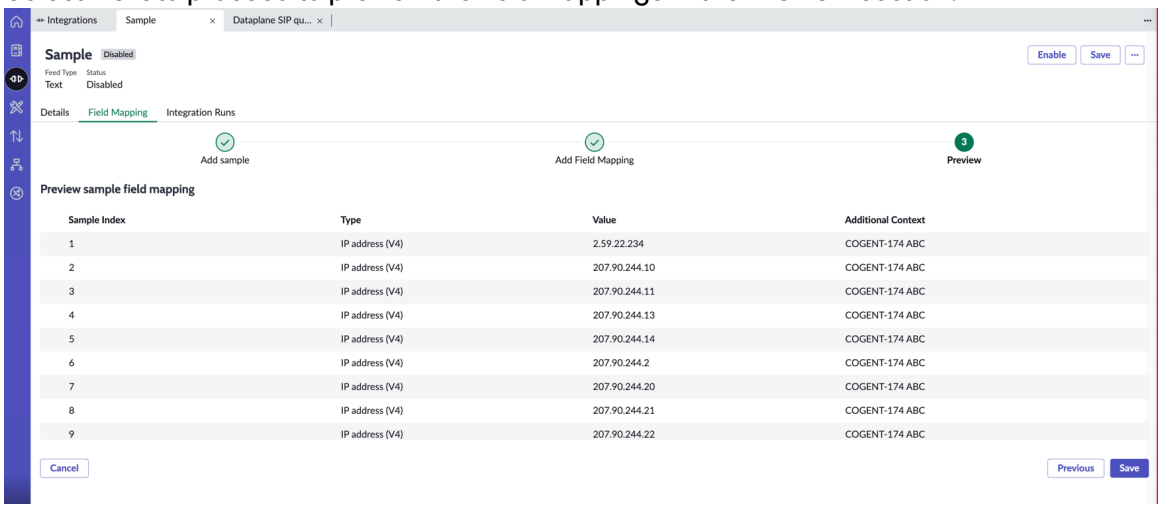


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Select **Save** to save the script to get the updated target value.

e. Close **Configure script for source field** dialogue box and proceed with the next step.

16. Select **Next** to proceed to preview the field mappings in the **Preview** section.



17. Preview the sample field mapping and select **Save**.
A confirmation message is displayed indicating that the field mapping is saved successfully.

As part of sample field mapping, the application automatically identifies the observable type (such as IP address v4 and so on) that the user has mapped from the sample data. This mechanism streamlines the mapping process and ensures the appropriate observable types are assigned based on the input.

If multiple source fields are mapped to the same **Observable field** such as **Additional Context**, then after feed ingestion the values will appear in the respective mapped field (which is the **Additional Context**), each separated by a new line. The following is the sample screen shot of the observable column displayed in the new line.

Important: Field Mapping Integration Run: Any integration run performed for this feed type will use the saved field mapping configuration. This ensures that incoming data is consistently parsed and mapped to the correct observable attributes based on the structure defined during the configuration.

Note: Select **Edit Field Mapping** to edit and make any necessary changes to the field mapping if required. An alert message is displayed to confirm if you want to proceed with editing. Acknowledge the prompt and select **Yes** to continue. Make the necessary changes to the field mappings using the updated sample data and save the changes.

Any edits made to the field mapping will be applied to the future integration runs for this feed.

Always verify the sample data after changes to ensure correct parsing before running the integration.

View Threat Intel Feeds

This section provides you the threat intel feeds that are configured in the base system.

View STIX TAXII Feeds

View the configured STIX TAXII feeds in the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_sec_tisc.admin

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **STIX TAXII**.
   The MISP feeds within the base system are described in the following table.

Threat Feed	Description	URL
Cyware TAXII	The Cyware Threat Intelligence eXchange (CTIX) is a platform designed to facilitate the sharing of cyber threat intelligence among organizations.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedFuture TAXII	Recorded Future is an independent threat intelligence cloud platform which enables organizations to identify and mitigate threats across cyber, supply-chain, physical and fraud domains.	https://api.recordedfuture.com/taxii2
Pulsedive TAXII	Pulsedive is a threat intelligence platform that provides a wide range of cyber threat intelligence services and tools to organizations.	https://pulsedive.com/taxii2/api/

4. Click **Edit** to edit the feed.

View STIX HTTPs Feeds

View the configured STIX HTTPs feeds in the base system.

Before you begin
Role required: sn_sec_tisc.admin

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **STIX HTTPs**.
   The following table describes the STIX HTTPs feeds within the base system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ThreatFeed	Description	URL
MITRE - Mobile ATT&CK	This data collection holds STIX objects from Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	This data collection holds STIX objects from ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE - Enterprise ATT&CK	This data collection holds STIX objects from Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Click **Edit** to edit the feed and make necessary updates.

View MISP Feeds

View the MISP Feeds that are configured in the base system.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **MISP**.
   The MISP feeds within the base system are described in the following table.

Threat Feed	Description	URL
DigitalSide Threat Intel OSINT Feed	Data source to fetch Open Source Cyber Threat Intelligence information from DigitalSide Threat-Intel OSINT feed, which is mostly based on malware analysis and compromised URLs, IPs and domains.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLhaus IOCs	URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
Malware Bazaar	MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community,	https://bazaar.abuse.ch/downloads/misp/manifest.json

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
	AV vendors and threat intelligence providers.	
ThreatFox IOCs	ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers.	https://threatfox.abuse.ch/downloads/misp/manifest.json

4. Click **Edit** to edit the feed.

View Text Feeds

View the text Feeds that are configured in the base system.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **Text** option.
   The following lists the configured text feeds within the base system.

Threat Feed	Description	URL
Haley's Brute Force IPs	Provides a list of attacking machine IP addresses during the last 2 years sorted by IP address	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Blockrules Emergingthreats	Emerging Threat (ET) Intelligence provides actionable threat intel feeds to identify IPs involved in suspicious and malicious activity.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper Web	List of hosts that have tried and failed to log on to the pop3 service at bsdly.net.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Tor Exit Nodes	Tor Exit Nodes can be used to detect traffic coming from the TOR network.	https://www.dan.me.uk/torlist/?exit
Talos Intelligence IP Blacklist	Talos was formed by combining SourceFire's Vulnerability Research Team, the Cisco Threat Research and Communications group, and the Cisco Secure	https://www.talosintelligence.com/documents/ip-blacklist

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
	Applications Group. The combined expertise is backed by a sophisticated infrastructure, and Cisco's unrivaled telemetry of data that spans across networks, endpoints, cloud environments, virtual systems, and daily web and email traffic.	
SANS	ISC provides a free analysis and warning service to thousands of Internet users and organizations.	https://isc.sans.edu/feeds/topips.txt
Snort	Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity.	https://snort.org/downloads/ip-block-list
CI army	The CINS Army list is a subset of the CINS Active Threat Intelligence ruleset, and consists of IP addresses that meet one of two basic criteria: 1) The IP's recent Rogue Packet score factor is very poor, or 2) The IP has tripped a designated number of 'trusted' alerts across a given number of their Sentinels deployed around the world.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	Raw IPs for the firewall block lists. These come from: Spam nets identified by Spamhaus (www.spamhaus.org), Top Attackers listed by DShield (www.dshield.org) and Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
Blocklist Greensnow	GreenSnow is a team consisting of the best specialists in computer security, GreenSnow harvests a large number of IPs from different computers located around the world.GreenSnow is comparable with SpamHaus.org for attacks of any kind except for spam.	https://blocklist.greensnow.co/greensnow.txt
CI army	The CINS Army list is a subset of the CINS Active Threat	https://cinsscore.com/list/ci-badguys.txt

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
	Intelligence ruleset, and consists of IP addresses that meet one of two basic criteria: 1) The IP's recent Rogue Packet score factor is very poor, or 2) The IP has tripped a designated number of 'trusted' alerts across a given number of their Sentinels deployed around the world.	
Blocklist	www.blocklist.de is a free and voluntary service provided by a Fraud/Abuse-specialist, whose servers are often attacked via SSH-, Mail-Login-, FTP-, Webserver- and other services.	https://lists.blocklist.de/lists/all.txt
Tor Exit Nodes	Tor Exit Nodes can be used to detect traffic coming from the TOR network.	https://www.dan.me.uk/torlist/?exit
Botscout BOT IPs	BotScout helps prevent automated web scripts, known as "bots", from registering on forums, polluting databases, spreading spam, and abusing forms on web sites.	http://botscout.com/last_caught_cache.txt
Dataplane VNC RFB	IP addresses identified as initiating VNC remote frame buffer sessions.	https://dataplane.org/signals/vncrfb.txt
Dataplane TELNET login	IP addresses identified as attempting login via TELNET password authentication.	https://dataplane.org/signals/telnetlogin.txt
Dataplane SSH password authentication	IP addresses identified as attempting login via SSH password authentication.	https://dataplane.org/signals/sshpwauth.txt
Dataplane SSH client connection	IP addresses identified as performing SSH client protocol negotiations.	https://dataplane.org/signals/sshclient.txt
Blockrules Emergingthreats	Emerging Threat (ET) Intelligence provides actionable threat intel feeds to identify IPs involved in suspicious and malicious activity.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Dataplane SMTP greeting	IP addresses identified as SMTP clients issuing unsolicited HELO or EHLO commands.	https://dataplane.org/signals/smtpgreet.txt

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
Dataplane SIP query	IP addresses identified as sending SIP OPTIONS queries.	https://dataplane.org/signals/sipquery.txt
Dataplane IP protocol 41	IP addresses identified as open IPv4 protocol 41 relay (i.e. IPv6 over IPv4).	https://dataplane.org/signals/proto41.txt
Dataplane SIP invitation	IP addresses identified as sending SIP INVITE operations.	https://dataplane.org/signals/sipinvitation.txt
Dataplane DNS CH TXT version.bind	IP addresses identified as sending DNS CH TXT VERSION.BIND queries.	https://dataplane.org/signals/dnsversion.txt
Dataplane DNS TCP	IP addresses identified as sending DNS over TCP port 53 queries.	https://dataplane.org/signals/dnstcp.txt
Dataplane DNS recursion desired IN ANY	IP addresses identified as sending recursive DNS IN ANY queries.	https://dataplane.org/signals/dnsrdany.txt
Dataplane DNS recursion desired	IP addresses identified as sending recursive DNS queries.	https://dataplane.org/signals/dnsrd.txt
Phishing Database from GitHub Active Phishing Links	Data source for fetching Active Phishing Links from Phishing Database available on Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Phishing Database from GitHub Active Domains	Data source for fetching Active Domains from Phishing Database available on Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Phishing Database from GitHub Active IPs	Data source for fetching Active IPs from Phishing Database available on Github.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Blocklist Bots	All IP addresses which have been reported within the last 48 hours as having run attacks attacks on the RFI-Attacks, REG-Bots, IRC-Bots or BadBots.	https://lists.blocklist.de/lists/bots.txt
Blocklist Apache Attacks	All IP addresses which have been reported within the last 48 hours as having run attacks on the service	https://lists.blocklist.de/lists/apache.txt

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
	Apache, Apache-DDOS, RFI-Attacks.	
Voip Blacklist By Scopserv	Retrieve list of blocklisted ips from the Voip Blacklist.	http://voipbl.org/update/?dm=bl
Threatview Domain Blocklist	Malicious Domains identified for phishing/serving malware/command and control.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Threatview MD5 Hash Blocklist	MD5 hashes of malicious files or associated with - malware, ransomware, hack tools, bots etc.	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Threatview URL Blocklist	Malicious URL's serving malware, phishing, botnets and C2.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Threatview SHA File Hash Blocklist	SHA hashes of files known or linked with malware execution.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Threatview IP Blocklist	Malicious IP Blocklist for known Bad IP addresses.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Threatview C2 Hunt Feed	Infrastructure hosting Command and Control Servers found during Proactive Hunt by Threatview.io	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
Threatview OSINT Threat Feed	Malicious indicators of compromise gathered from OSINT Source - Twitter and Pastebin.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Click **Edit** to edit the feed.

View CSV Feeds

View the CSV Feeds that are configured in the base system.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **CSV**.
   The CSV feeds within the base system are explained in the following table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ThreatFeed	Description	URL
PhishStats	Phishing URLs from the past 30 days from PhishStats.	https://phishstats.info/phish_score.csv
Abuse.ch SSL Certificate Blacklist	The SSL Certificate Blacklist (CSV) is a CSV that contains SHA1 Fingerprint of all SSL certificates blacklisted on SSLBL.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Botnet C2 IP Blacklist	An SSL certificate can be associated with one or more servers (IP address:port combination). SSLBL collects IP addresses that are running with an SSL certificate blacklisted on SSLBL. These are usually botnet Command&Control servers (C&C). SSLBL hence publishes a blacklist containing these IPs which can be used to detect botnet C2 traffic from infected machines towards the internet, leaving your network.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Phishtank online	NA	https://data.phishtank.com/data/online-valid.csv

4. Click **Edit** to edit the feed.

View JSON Feeds

Before you begin
Role required: sn_sec_tisc.admin

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **RSS** option.
   The following lists the configured JSON feeds within the base system.

Threat Feed	Description	URL
Feodotracker C&C Hosts	Data source to fetch Botnet C2 IP Blocklist from Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
Feodotracker	Data source to fetch Botnet C2 IP Blocklist from Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist.json

4. Click **Edit** to edit the feed.

View RSS Feeds

View the RSS feeds configured in the base system.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **RSS** option.
   The following lists the configured RSS feeds within the base system.

Threat Feed	Description	URL
CISO2CISO.COM RSS Feed	RSS Feed data from CISO2CISO.com	https://ciso2ciso.com/feed/
Google Project Zero	Google Project Zero	https://rssmock.free.beeceptor.com/getGoogleProjectFeed
Schneier on Security RSS Feed	RSS Feed data from Schneier on Security	https://www.schneier.com/feed/atom/
Krebs on Security RSS Feed	RSS Feed data from KerbsonSecurity	https://krebsonsecurity.com/feed/
We Live Security RSS Feed	RSS Feed data from welivesecurity	http://feeds.feedburner.com/eset/blog
JISA Softech RSS Feed	RSS Feed data from JISA	https://www.jisasoftech.com/feed/
Cisco Newsroom Security RSS feed	Latest Security News from cisco.	https://newsroom.cisco.com/c/services/i/servlets/newsroom/rssfeed.json?feed=security
HelpNet Security	Information security news with a focus on enterprise security.	https://www.helpnetsecurity.com/feed/
Security Affairs	Information on the digital forensics from top-tier media.	https://securityaffairs.com/feed
Volexity RSS Feed	RSS Feed data of information security blogs from Volexity.	https://www.volexity.com/blog/feed/
Hackers News RSS Feed	RSS Feed data from "The Hacker News	https://feeds.feedburner.com/

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Feed	Description	URL
		TheHackersNews?format=xml
Graham Cluley RSS Feed	RSS feed data from Graham Cluley	https://grahamcluley.com/feed/

4. Click **Edit** to edit the feed.

View Custom Feed

View the custom feed that are shipped within the base system.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **Custom**.
   The following table list out of the box Custom feed.

ThreatFeed	Description	URL
CrowdStrike Feed	Source for getting CrowdStrike Actor, Observable and Reports data.	https://api.crowdstrike.com

4. Click **Edit** to edit the feed.

Configure custom CrowdStrike feed

The CrowdStrike feed enables users to ingest indicators, actors, reports, and their associated context from the CrowdStrike Falcon Intelligence feed into TISC.

Before you begin

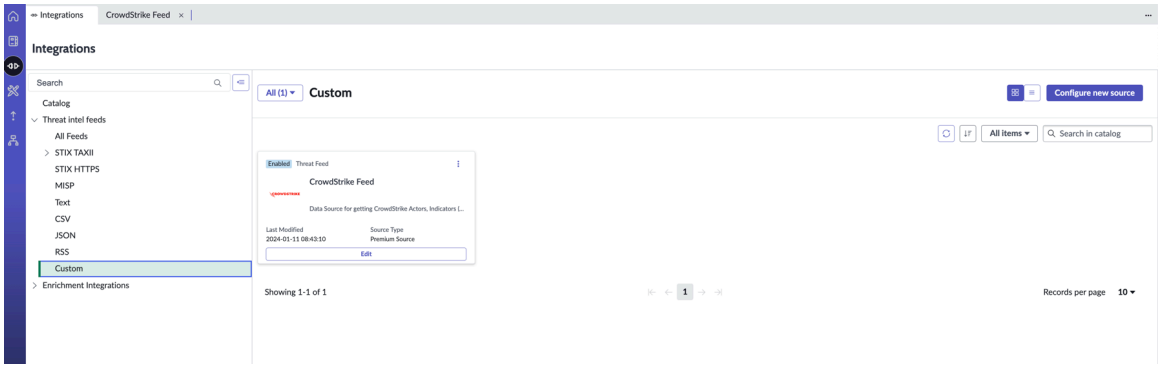
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. Select **Custom**.
3. Click on the **Edit** button from the *CrowdStrike* **Feed** form page.

> **Note:** By default, the CrowdStrike feed is disabled, you must edit the configurations to enable the feed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Drill down to the **Configuration Details** section.
5. Enter the **Client ID**, and **Client Secret**.

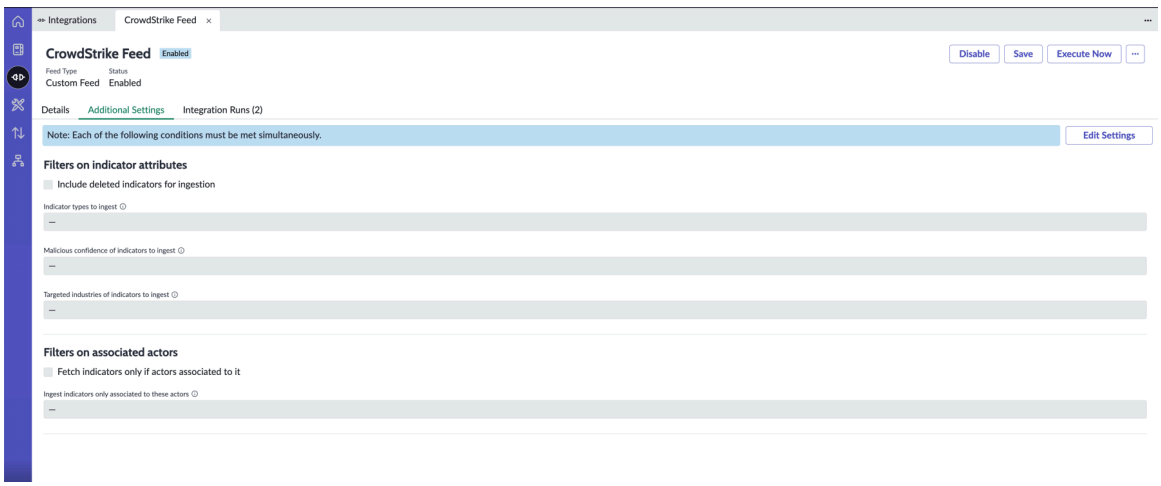
Note:

a. You must generate your Client ID and Client Secret in case if you don't have it. For more information on the Client ID and Client Secret, see Defining your first API Client section.

b. Get Client ID and Client Secret from *`CrowdStrike`* for required scopes. Below are the scopes that are required for the Client ID and Client Secret from *`CrowdStrike`*:

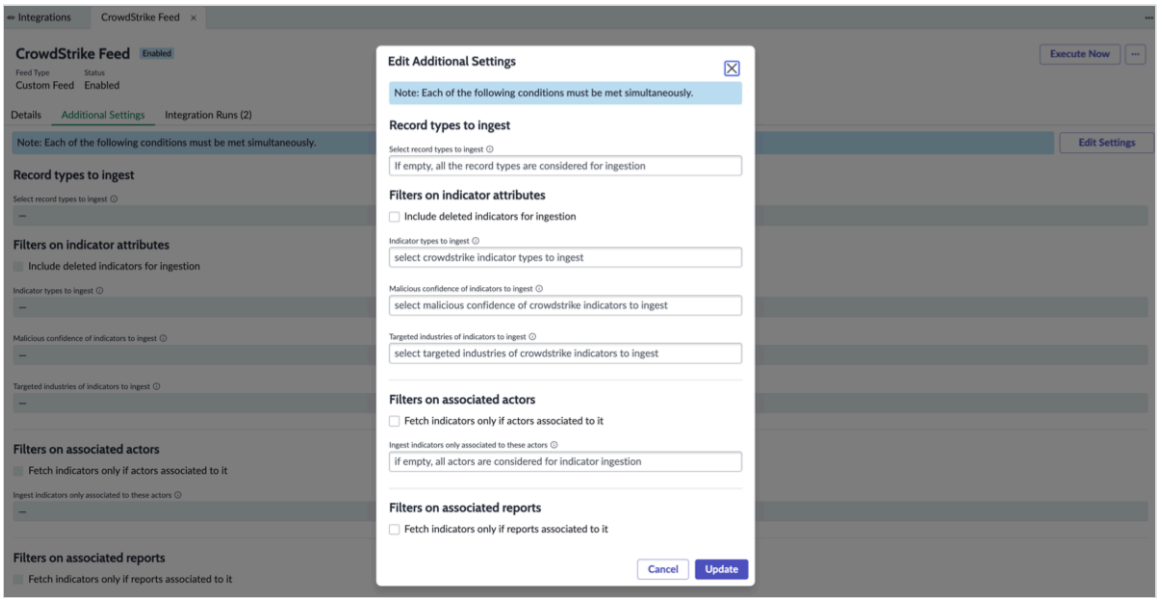
- Indicators (Falcon intelligence)
- Actors (Falcon Intelligence)
- Reports (Falcon Intelligence)

6. Navigate to **Additional Settings** to configure the filters that will be applied while ingesting indicators from CrowdStrike.



7. Click **Edit Settings**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. Select the required filters.

> **Note:** All the filters configured will be applied in conjunction while ingesting indicators from CrowdStrike.

9. Select the required values from the below available filters.

Filters on indicator attributes

Field	Description
Include deleted indicators for ingestion	Select this check box to allow the ingestion of indicators that have been deleted. **Note:** Deleted indicators will be created as observables only if they were previously ingested. A **Deleted in CrowdStrike** tag is added to indicators that are removed from CrowdStrike.
Indicator types to ingest	Select the specific CrowdStrike indicator types you want to ingest. If none are selected, then all the available indicators will be retrieved by default.
Malicious confidence of indicators to ingest	Select the malicious confidence level of CrowdStrike indicators to ingest. If left blank, all indicators will be fetched from CrowdStrike regardless of their malicious confidence.
Targeted industries of indicators to ingest	Select the targeted industries associated with CrowdStrike indicators to ingest. If none is selected, all the indicators will be fetched from CrowdStrike regardless of targeted industry.
Filters on associated actors	
Fetch indicators only if actors associated to it	Select this check box to fetch indicators only if they are associated with actors.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Ingest indicators only associated to these actors	Specify comma-separated actor names related to the indicators for ingestion. If not provided, all the indicators will be fetched from CrowdStrike regardless of associated actors.
Filters on associated reports	
Fetch indicators only if reports associated to it	Select this check box to fetch indicators only if they are associated with reports.
Ingest indicators only associated to these reports	Enter comma-separated report names associated with the indicators for ingestion. If left blank, all the reports will be included in the ingestion process. If not provided, all the indicators will be fetched from CrowdStrike regardless of associated reports.
Filters on associated malware families	
Fetch indicators only if malware families associated to it	Select this check box to fetch indicators only if they are associated with malware families.
Ingest indicators only associated to these malware families	Enter comma-separated malware family names associated with the indicators for ingestion. If left blank, all malware families will be included in the ingestion process. If not provided, all the indicators will be fetched from CrowdStrike regardless of malware families.
Mapping of Indicator Malicious confidence to TISC confidence **Note:** The High, Medium, and Low values are the source value or malicious confidence received from CrowdStrike.	
High	Enter a confidence value (0–100) for indicators with high malicious confidence. **Note:** If a matching malicious confidence mapping is found in the **Additional Settings**, it will override the value provided in the **Details** section even if a confidence value is manually entered.
Medium	Enter a confidence value (0–100) for indicators with medium malicious confidence.
Low	Enter a confidence value (0–100) for indicators with low malicious confidence.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Unverified	Enter a confidence value (0–100) for indicators with unverified malicious confidence.

10. Click **Update** on the **Additional Settings** dialog box to save the modified additional settings.
11. Click **Enable** to enable CrowdStrike Feed for ingestion.

> **Note:** The premium feed is same as other feeds except the response that is parsed during the configuration. A specific response is parsed to CrowdStrike by adding the Client ID and Client Secret.

What type of data is fetched from *CrowdStrike*:

a. Indicators from CrowdStrike that are updated after the configured ingestion time and matching the filters configured as part of additional settings. These indicators from CrowdStrike will then be mapped to observables in TISC. Below are the indicator types that are ingested in TISC:
   - SHA256 Hash
   - MD5 Hash
   - SHA1 Hash
   - URL
   - Domain
   - IP Address
   - Mutex Name
   - File Name
   - Email Address
   - Username
   - IP Address Block

b. Threat Actors from CrowdStrike that are updated after the configured ingestion time will be mapped to Threat Actors in TISC.

c. Reports from CrowdStrike that are updated after the configured ingestion time will be mapped to threat reports in TISC based on the matching attributes.

d. In addition to the entities mentioned above, the following related data is also fetched:
   i. Threat actors, reports, and indicators related to the previously ingested indicators.
   ii. Threat actors and indicators associated with all reports ingested during the current ingestion process.

> **Note:** Filters configured in **Additional Settings** will also be applied when ingesting the indicators associated with the previously ingested indicators, reports, or actors.

12. **Optional:** Click **Duplicate** to duplicate the feed.
For more information, see Duplicate threat intelligence feeds.

System Properties for CrowdStrike

The following details the system properties for CrowdStrike.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. sn_sec_tisc.crowdstrike_actor_batch_size: Denotes the number of actors to be pulled in a single API call. Note: applicable only when the integration doesn't find the necessary present in the system.
   - Type: Integer
   - Value: 250
2. sn_sec_tisc.crowdstrike_api_limit: Number of records to fetch at a time from CrowdStrike. Higher the number, more the memory would consumed for processing the payload.
   - Type: Integer
   - Value: 1000
3. sn_sec_tisc.crowdstrike_indicator_batch_size: Denotes the number of indicators to be pulled in a single API call. Note: applicable only when the integration doesn't find the necessary present in the system.
   - Type: Integer
   - Value: 150
4. sn_sec_tisc.crowdstrike_offset_limit_total: The allowed total of offset and limit from CrowdStrike API.
   - Type: Integer
   - Value: 50000
5. sn_sec_tisc.crowdstrike_report_batch_size: Denotes the number of reports to be pulled in a single API call. Note: applicable only when the integration doesn't find the necessary present in the system.
   - Type: Integer
   - Value: 50

Configure custom MISP feed

The Malware Information Sharing Platform (MISP) API feed enables you to import events from the MISP server, along with their associated attributes and objects, into the TISC library.

Before you begin

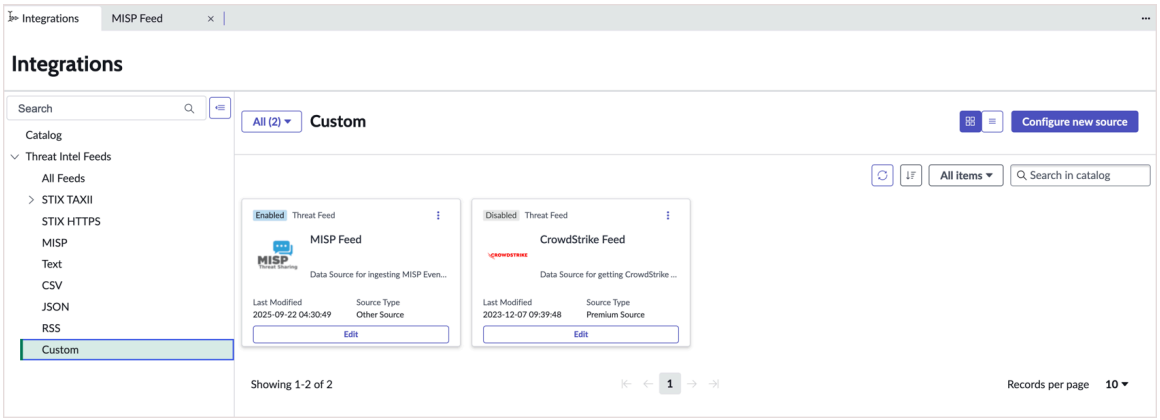
Role required: sn_sec_tisc.admin

Procedure

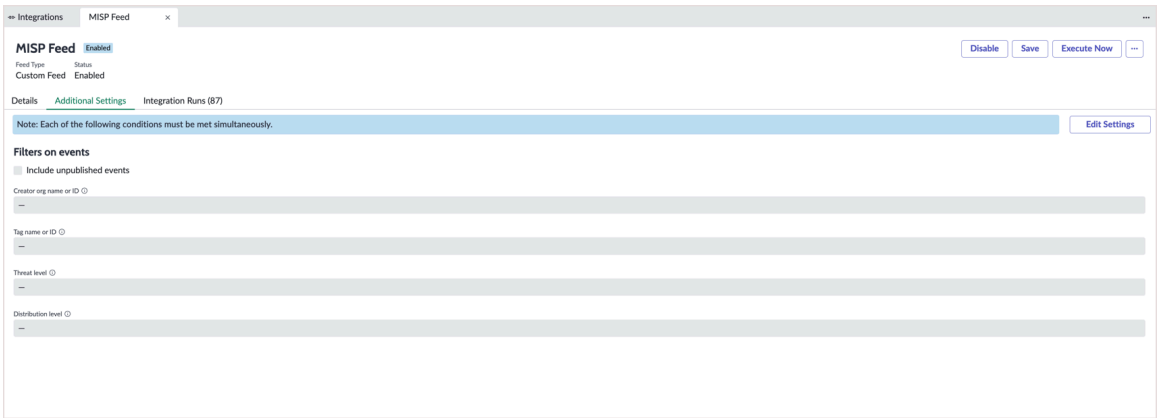
1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. Select **Custom**.

> **Note:** By default, the MISP feed is disabled, you must edit the configuration to enable the feed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

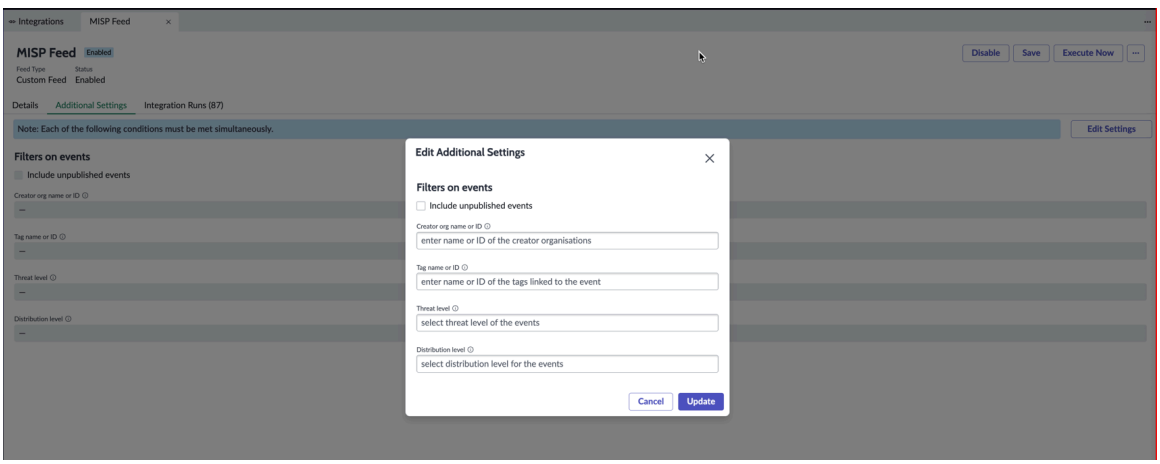


3. Select the **Edit** button on the **MISP Feed** card.
4. Drill down to the **Configuration Details** section.
5. Update the **REST endpoint URL** field.
6. Add the required authentication details for the MISP server (if any).
7. Navigate to **Additional Settings** to configure the filters to fetch the data from MISP.



The **Additional Settings** tab is used to set up filters that determine which MISP events are ingested.

8. Select **Edit Settings**.



9. Select the required filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: All the filters configured will be applied in conjunction while ingesting the events.

The following section provides a detailed explanation of each available option. Review each option in the following table to understand how the filters can be applied to optimize which MISP events are ingested into the TISC library.

10. Select the required values from the following available filters.

Edit Additional Settings

Field	Description
Filters on events	
Include unpublished events	Select this check box if you want to include unpublished events.
Creator org name or ID	Enter a comma-separated list of organization names and/or IDs associated with the event. **Note:** If the organization name contains leading or trailing spaces, enclose the name in double quotes to ensure proper processing.
Tag name or ID	Enter a comma-separated list of tag names and/or tag IDs associated with the event.
Threat level	Select a threat level to filter incoming events. Leaving this field empty includes events of all threat levels.
Distribution level	Select a distribution level to limit events. Leaving this field empty includes events of all distribution levels.

Note:

Once you've defined the **Additional Settings** following the instructions above, you can duplicate the feed when creating another. For more information, see Step 13.

11. Select **Update** on the **Additional Settings** dialog box to save the modified additional settings.
12. Select **Enable** to enable the MISP feed for including the MISP events.

The TISC application uses the date configured in the **Fetch data from** field as the baseline for retrieving events and associated attributes.

The **Fetch data from** date determines which events and associated attributes are retrieved. TISC compares this date with specific timestamps based on the event status:

- **Published events**: Compared against the **Published timestamp**.
- **Unpublished events**: Compared against the **Last updated timestamp**.

An event is retrieved only if its relevant timestamp is later than the configured **Fetch data from** date.

Using the appropriate timestamp for each event status ensures accurate retrieval of both newly published events and recently updated unpublished events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

13. **Optional:** Select **Duplicate** to duplicate the feed.
    For more information, see Duplicate threat intelligence feeds.

Note:

- Each MISP event imported into the TISC library, whether as a **Threat Report** or **Threat Event**, includes an associated **External Reference** record.
- This record is accessible via the **Related Records** tab and provides a direct URL link to the corresponding MISP event on the MISP server. This also enables a quick access to the original event data.
- For details on how MISP events, along with their associated attributes and objects, are mapped to TISC entities, refer to KB2197697.
- Entity types that aren't included in the mapping described in the KB article aren't ingested into the TISC Library.

Understanding STIX TAXII

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI). Trusted Automated Exchange of Intelligence Information (TAXII) is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS.

With STIX, all aspects of suspicion, compromise, and attribution are represented as objects and descriptive relationships. STIX information can be visually represented for an analyst or stored as JSON to be quickly machine readable.

Cyber Threat Intelligence (CTI) was chartered to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. The CTI is primarily focused on development and standardization of Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII).

Configure a new TAXII Feed

You can maintain TAXII feeds for sharing STIX-formatted information. Each TAXII feed contains one or more TAXII collections.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **Threat Intel Feeds** > **STIX TAXII** > **TAXII Feeds**.

Note: Configure TAXII feed to serve as a profile for all the TAXII Collections within.

4. Click **Configure new source**.
   The Configure new TAXII Feed page is displayed.
5. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create New Data Source

Field	Description
Name	Enter a name for the feed.
Description	Description of the feed.
Source Type	The type of source such as Open Source, Premium Source, and so on provided for the feed. The available source types are: ○ Government ○ ISACs ○ Open Source ○ Premium Source ○ Other Source
Logo	Attach the logo of the source feed.
Industry	Select the industry category such as Aerospace, Agriculture, and so on for which the feed data source is applicable to.

Fill in the fields in the Configuration section, as appropriate.

Configuration

Field	Description
TAXII Version	Select the TAXII Version of the TAXII server that needs to be configured. Supported versions are 2.0 and 2.1.
Configuration Type	Provide a configuration type to fetch TAXII collections. Available values are: ○ **Discovery Service URL**: Choose Discovery Service URL to fetch collections from all available API roots within the discovery service of the TAXII server. ○ **API Root URL**: Choose API Root URL to fetch collections from the specific API root of the TAXII server.
Authentication	Select the required option from the drop down list if the authentication is required. The available options are: ○ **None**: Select this option if there is no authentication required. ○ **Basic**: Select this option to provide username and password. ○ **API Key**: Select this option to provide an API key.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Choose a REST message**: Select this option for any other type of authentication. The REST message options are: ▪ **Use REST Message**: Select this box if you need a REST message to build a pre-build REST Message. If you don't select then this will use the value in endpoint field. Click the lookup icon, and select the REST message from the list. ▪ **REST Method**: Select this box if you need a REST method. Click the lookup icon, and select the REST method from the list. **Note:** The REST message and REST method fields become available when the REST message option is selected.
URL	Enter either the TAXII Server Discovery Service URL or specific API Root URL based on the selected configuration type.
Advanced section	
Advanced	Select the check box to choose a different Integration script and Report Processor. Make sure the chosen scripts are compatible with the selected TAXII version. Based on the TAXII version and authentication, these scripts are auto populated by default.
Integration script	Invokes a call to the REST Endpoint URL API using the authentication parameters such as authentication type: User name/Password/ API Key and the headers to be passed with the request, and then the script fetches the observables or indicators STIX data that are available for the specific feed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The data that is fetched is the raw data only (no records are created) which will be attached to the integration process and can then be viewed under the **Integration Run** section. Within the base system following are the custom scripts includes, which are provisioned within the application for the integrations scripts: ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript The default integration script is based on the feed type that you select. The script includes runs a simple REST call, saves the response as an attachment, and then returns the attachment to the processor.
Report processor	The report processor invokes a call to the REST Endpoint URL. Within the base system below is the custom scripts includes, which is provisioned within the application for the integrations scripts, **TAXIIV2CollectionDataProcessor**.

Fill in the fields in the Scheduling section, as appropriate.

Scheduling

Field	Description
Run Frequency of Collections	The scheduling interval which will be applied to the TAXII collection records. Run frequency for a TAXII collection can be modified in the TAXII collection form view if required. **Note:** This setting will be applied as default to all the TAXII collections that are fetched. There is an option to override the setting in TAXII Collections if required. For more information, see Scheduled Jobs and how to Automatically run a script of your choosing.
Fetch Data From	The start date from when the data needed to be fetched. This field should be set with the time from when the data needs to be

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	ingested from the corresponding source. Once this field is set, the next ingestion run would fetch the data from the configured time and consecutive ingestion runs would fetch incremental Data. For example, Source is scheduled to ingest the data every hour. The user sets **Fetch Data From** to Jan 12 6:00AM on Jan 12 9:30AM, the ingestion triggering on Jan 12 10:00AM would fetch the data from Jan 12 6:00AM to Jan 12 10:00AM. The next ingestion that triggers at 11:00AM would fetch only the incremental data from Jan 12 10:00AM to Jan 12 11:00AM. **Note:** This means the scheduled runs will fetch data incrementally starting from the specified date onwards.

6. Click **Validate Connection**
   An information message is displayed that the TAXII Feed connection is successful. To fetch the collections proceed to the next step.
7. Click **Get TAXII Collections**.

   Note: If there are any errors, then an error message is displayed that an error occurred while fetching TAXII collections and check logs for more details.

   The TAXII Collections are displayed under the TAXII Collections section, and they are disabled by default.
8. Enable the TAXII Collections to retrieve the STIX objects available in these TAXII collections.

Duplicate threat intelligence feeds

Duplicating a threat feed allows you to create an exact copy of an existing feed, including all associated observables, indicators, actors, and so on.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select the desired integration from the **Catalog** view.
   For example, select CrowdStrike
4. Click **Edit** button for CrowdStrike feed card to open the configuration form.
5. Click the **More Actions** menu and select **Duplicate**.
   A confirmation is displayed indicating that the duplicated the current feed configuration and created a new feed with name [integrationname Feed-copy] with a link to the new duplicated feed. For example, CrowdStrike Feed-copy.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC Integrations

This section provides instructions for configuring and enabling the Threat Intelligence integrations.

TISC Enrichment Integrations

The Threat Intelligence Security Center base system does not include any pre-configured integrations. This section provides instructions for configuring both ServiceNow and third-party integrations.

Important:

Make sure that you've installed the required third-party app integrations. You can see the observables, sighting search, and threat lookup details only for the third-party apps that are installed.

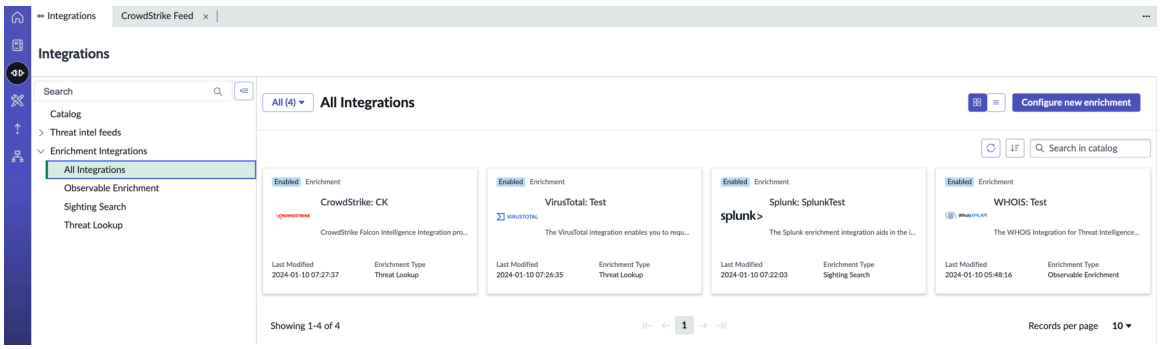
All Integration Configurations

All the integrations are separate applications that needs to be installed. TISC supports integrations with third party vendors. Any installed integrations can be configured here.

This section displays cards for each of the configured integration implementations that you can activate and use.

Each enrichment type's section would be visible only if at least one of the corresponding integration for that enrichment type is installed. For example, the **Threat Lookup** section would be visible under **Enrichment Integrations** only if at least one Threat Lookup integration is installed.

The configured integration cards can be viewed by navigating to **Workspaces** > **Threat Intelligence Security Center** > **Integrations** > **Enrichment Integrations** > **All Integrations**.



Actions on the All Integrations view

The All Integration view enables you to perform the following actions.

Actions on All Integrations view

Action	Description
All	Use this dropdown menu to filter integrations based on their current state. You can filter based on the following states:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

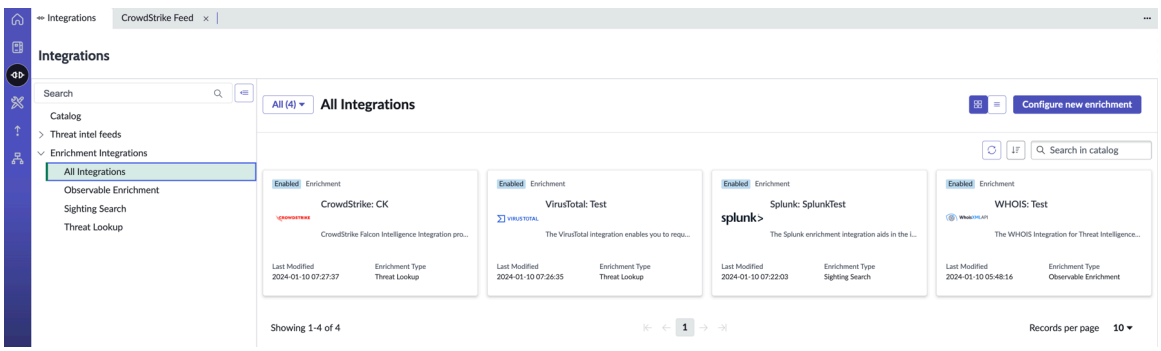
Actions on All Integrations view (continued)

Action	Description
	• **All**: Displays all the integrations on the page. This is the default option. • **Enabled**: Displays all the integrations that are in an enabled state. • **Disabled**: Displays all the integrations that are in a disabled state. • **Draft**: Displays all the integrations that are in a draft state.
	Use this action to view all the integrations in the form of cards.
	Use this action to view all the integrations in the form of lists.
	Use this action to refresh the All Integrations page.
	Use this action to sort all the integrations based on the following: • **Last Modified (recent)** • **Last Modified (oldest)** • **Name (A-Z)** • **Name (Z-A)**
Search in catalog	Use this action to search for configured integrations based on name and description within the catalog.

Configure new enrichment from All Integrations view

You can configure new enrichments from the All Integrations view or directly from the Observable Enrichment, Sighting Search, or Threat Lookup sections respectively. To configure the new enrichment from all the All Integrations view, perform the following steps.

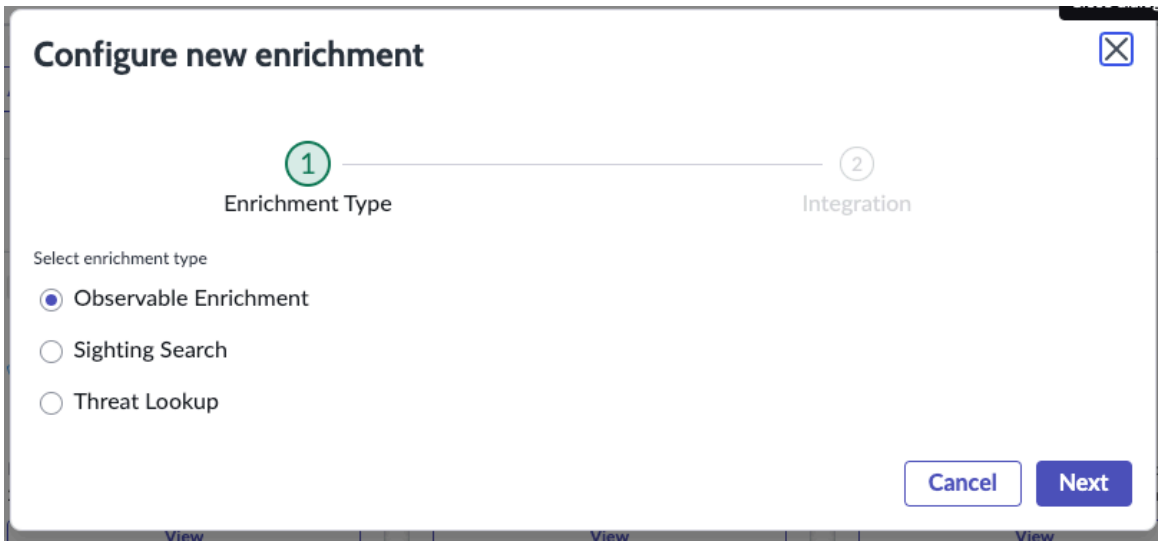
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Integrations** icon, and select the **All Integrations** section.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click the **Configure new enrichment** action.

   The Configure new enrichment pop-up appears with three enrichment types, which are Observable Enrichment, Sighting Search, or Threat Lookup. You need to choose which type of enrichment you want to configure.



4. Select an enrichment type, and click **Next**.

   This takes you to the pop-up that displays the available integrations. You need to choose the integration you want to configure.

5. Select an integration from the list of available integrations, and click **Select**.

   This takes you to the Create New Enrichment Integration page of the selected integration. This page is pre-filled with details of the selected integration by default. For example, WHOIS integration.

6. On the Create New Integration form, fill the fields.

Configure the new enrichment integration form

Field	Description
Name	Enter a name for the new enrichment integration. For example, `WHOIS1`.
Vendor Name	Name of the vendor. The details of the selected vendor are pre-filled by default. For example, `WHOIS`.
Integration Type	Type of integration that you selected. For example, Observable Enrichment. The details of the selected integration type are pre-filled by default. The following Integration Types are supported: ○ Observable Enrichment ○ Sighting Search ○ Threat Lookup

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Enter a unique description for the new enrichment integration.

7. In the Integration Configuration section, configure the integration details based on your requirements.

   The Integration Configuration section includes configuration details like API key, API Client ID or secret, username, password, and so on, which you need to fill in. These configuration details vary for different integrations.

8. Click the **Save** action to store and create the enrichment integration configuration.

   The provided details are validated, and by default the enrichment integration's status is disabled.

9. (Optional) Click the **Save as Draft** action to only store the integration configurations as draft. Users cannot enable an integration when it is saved in draft

   If you're not sure about the configuration details, you can use the **Save as Draft** option. After you get the configuration details, you can fill the remaining information in the draft version and create it.

10. To enable the enrichment integration, click **Enable**.

    The enrichment integration is enabled successfully.

11. You can also enable, disable, or delete a particular enrichment integration by using the Actions menu of the required integration tile on the Catalog page or the Enrichment Integrations page.

Configure Observable Enrichment

You can perform threat intelligence enrichment on one or more observables to determine whether they're associated with known security threats. The implementations that run depend on the ones you've activated.

Before you begin

Role required: sn_sec_tisc.admin

The Threat Intelligence Security Center supports Observable Enrichment only for the WHOIS Integration as of now. For more information, see Configure and enable Whois integration.

Note: Enrichment Integrations module is only shown if at least one of the integration supporting any of the capability is installed in the application.

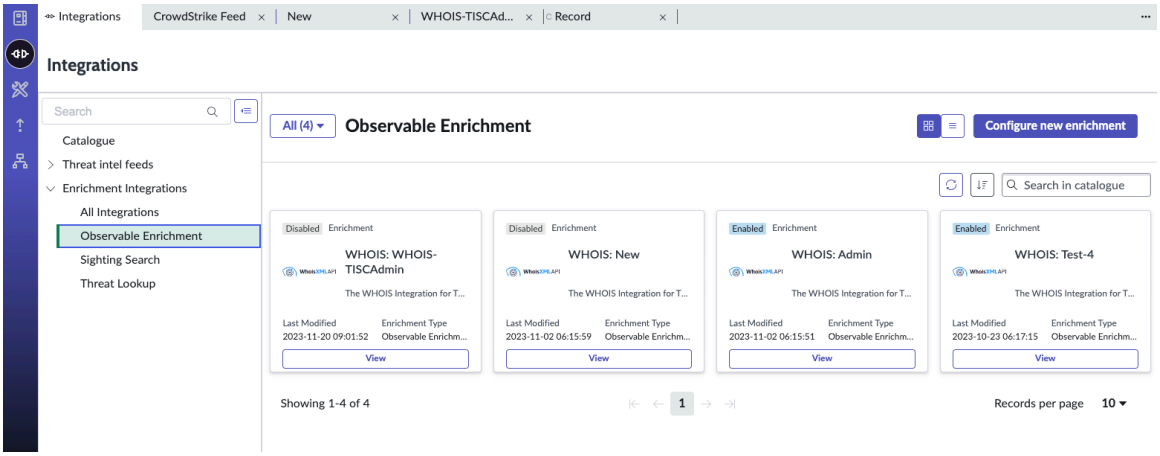
About this task

The Observable Enrichment section contains only the integrations with the integration type as observable enrichment. This section displays cards for each of the configured integration implementations that you can activate and use.

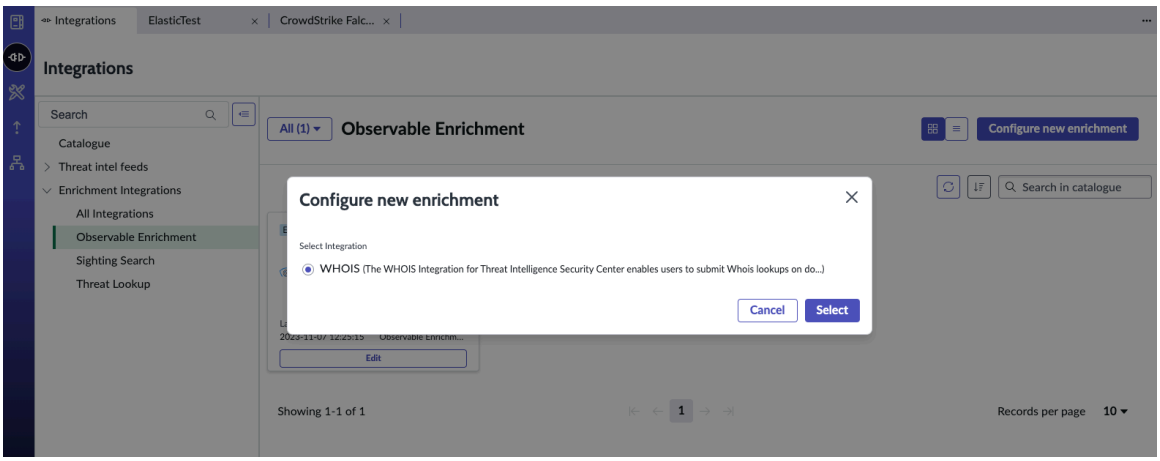
Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Integrations** icon, and select the **Observable Enrichment** section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



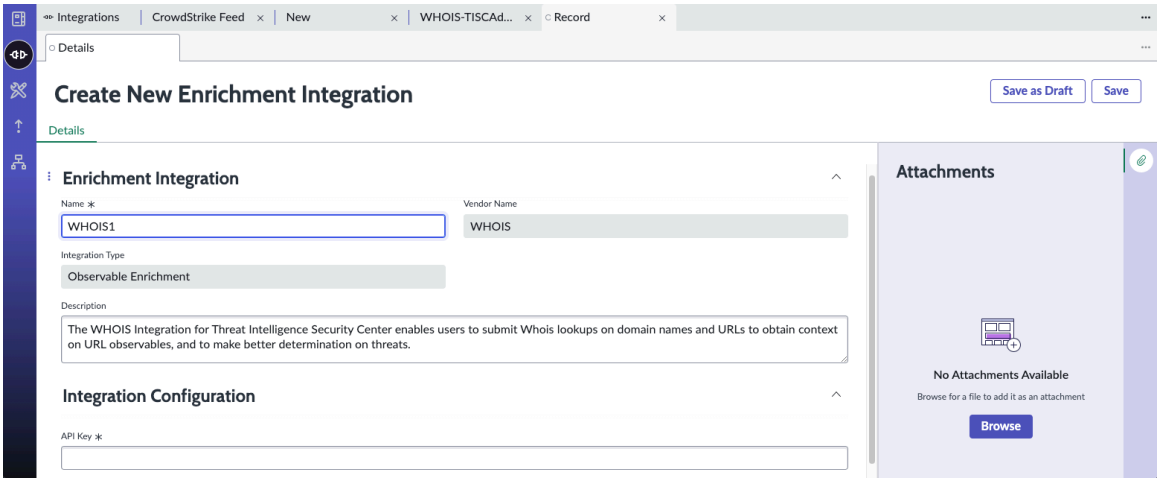
3. Click the **Configure new enrichment** action.
   This takes you to the pop-up that displays the available integrations. You need to choose the integration that you need to configure.
4. Select an integration from the list of available integrations, and click **Select**.
   This takes you to the Create New Enrichment Integration page of the selected integration. This page is pre-filled with details of the selected integration by default. For example, WHOIS integration.



5. On the Create New Integration form, fill the fields.

Field	Description
Enrichment Integration	
Name	Enter a name for the new enrichment integration. For example, `WHOIS1`.
Vendor Name	Name of the vendor. The details of the selected vendor is pre-filled by default. For example, `WHOIS`.
Integration Type	Type of integration that you selected, which is Observable Enrichment. The details of the selected integration type is pre-filled by default.
Description	Enter a unique description for the new enrichment integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. In the Integration Configuration section, configure the integration details based on your requirements.
   The Integration Configuration section includes configuration details like API key, API Client ID or secret, username, password, and so on, which you need to fill in. These configuration details vary for different apps.
7. Click the **Save** action to store and create the new enrichment integration configuration.
   After you click the **Save** or **Enable** action, the integration is validated using the provided integration configurations. By default, the enrichment integration's status is set to disabled.
8. Click **Save as Draft** action to only store the updates made to the enrichment configuration and not create it.
   If you're not sure about the configuration details, you can use the **Save as Draft** option. After you get the configuration details, you can fill the remaining information in the draft version and create it.
9. To enable the enrichment integration, click **Enable**.
   The enrichment integration is enabled successfully. You can also enable, disable, or delete a particular enrichment integration by using the Actions menu of the required integration tile on the Catalog page or the Enrichment Integrations page.

Have I Been Pwned integration

The Have I Been Pwned (HIBP) integration enables you to enrich email address and domain observables with breach data directly within the TISC.

This integration helps identify compromised credentials and assess organizational exposure to known data breaches.

During an investigation, email addresses or domains can be submitted to Have I Been Pwned for breach identification, either through the observables form or using case artifacts.

Configure and enable Have I Been Pwned integration

Configure API credentials and enrichment behavior through the dedicated Have I Been Pwned (HIBP) configuration tile in TISC integration settings.

Before you begin

Role required: sn_sec_tisc.admin

Prerequisites

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Have I Been Pwned integration depends on the Threat Intelligence Security Center (TISC) application. To enrich email and domain observables, ensure that the TISC plugin (`sn_sec_tisc`) is installed.
- Obtain a valid API key from the Have I Been Pwned portal before you begin.

About this task

The HIBP integration is an observable enrichment integration that determines whether a submitted email address or domain name has been part of a publicly known data breach.

When an analyst submits a supported observable, the integration queries the HIBP database and returns breach details, including the total number of breaches found and the type of data compromised.

The integration supports the following observable types:

- Email address
- Domain name

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Observable Enrichment**.
6. Select **Configure New Enrichment**.
7. Select the integration.
   For example, Have I Been Pwned to configure the HIBP integration.
8. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Enrichment Integration	
Name	Enter a name for the new enrichment integration. For example, Have I Been Pwned.
Integration Category	Indicates the integration category that you selected.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, Have I Been Pwned.
Integration Type	Type of integration that you selected.
Description	Enter the description for the new enrichment integration.
Integration Configuration	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
API Key	Indicates the API key that you obtained from the Have I Been Pwned site.

9. Drill down to the **Integration Configuration** section.
10. Enter (or paste) the **API Key** you acquired from the Have I Been Pwned site.
11. Click **Save**.
    The integration details are validated, and by default the Have I Been Pwned integration status is set to disabled.
12. Click **Enable** to enable the Have I Been Pwned integration.

> **Important:** Only one Have I Been Pwned integration tile can exist per instance. Attempting to create a second tile results in an error.

Result
After it is configured, Have I Been Pwned can be selected for performing enrichment on observables in Threat Intelligence Security Center.

What to do next
Run observable enrichment, see Run Have I Been Pwned enrichment integration on the detailed procedure.

Whois integration

The Whois integration enables you to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

Configure and enable Whois integration

Before you use the Whois integration, you must download it from the ServiceNow Store, and must have a valid account from Whois.

Before you begin
Role required: sn_sec_tisc.admin

The Threat Intelligence Security Center and Whois observable integration plugins are required.

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Observable Enrichment**.
6. In the **WHOIS** card, click **Configure New Enrichment** to configure **WHOIS** integration.
7. Fill in the fields on the Configure New Enrichment form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, WHOIS.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, WHOIS.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the new enrichment integration. For example, the description for WHOIS integration is, The WHOIS Integration for Threat Intelligence Security Center enables users to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

8. Drill down to **Integration Configuration** section.
9. Enter (or paste) the **API Key** you acquired from the WHOIS site.
10. Click **Save**.
    The integration details are validated, and by default the WHOIS integration's status is disabled.
11. Click **Enable** to enable the WHOIS integration.

Result
After it is configured, WHOIS can be selected for performing enrichments on observables in Threat Intelligence Security Center.

Shodan integration

Shodan is a search engine that analyzes service banner information from connected devices all around the globe.

The Shodan integration performs enrichment on the following observables:

- IP addresses
- URLs
- Domains

Configure and enable Shodan integration

Before you use Shodan integration, you must download it from the ServiceNow Store.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Observable Enrichment**.
6. In the **Shodan** card, click **Configure New Enrichment** to configure the integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, Shodan.
Vendor Name	Name of the vendor. The details of the selected vendor is auto populated and by default this field will be read only. For example, Shodan.
Integration Type	Type of integration that you selected. For example, Observable Enrichment.
Description	Enter the description for the new enrichment integration. For example, the description for Shodan integration is, Shodan helps you to analyze banner information from connected devices all around the globe.

8. Drill down to **Integration Configuration** section.
9. Enter (or paste) the **API Key** you acquired from the Shodan portal.
10. Click **Save**.
    The integration details are validated, and by default the status is disabled.
11. Click **Enable** to enable the integration.

Sighting Search

This section describes the TISC Sighting Search and Elastic Search integrations.

Configure Sighting Search

You can perform sightings search on one or multiple observables to determine the number of times the observables are sighted in your organisation logs. You can perform sighting search on observables within a selected number of days or within a date range.

Before you begin
Role required: sn_sec_tisc.admin

Note: Enrichment Integrations module is only shown if at least one of the integration supporting any of the capability is installed in the application.

The Threat Intelligence Security Center supports Sighting Search only for the following integrations:

- Splunk Search
- ElasticSearch

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

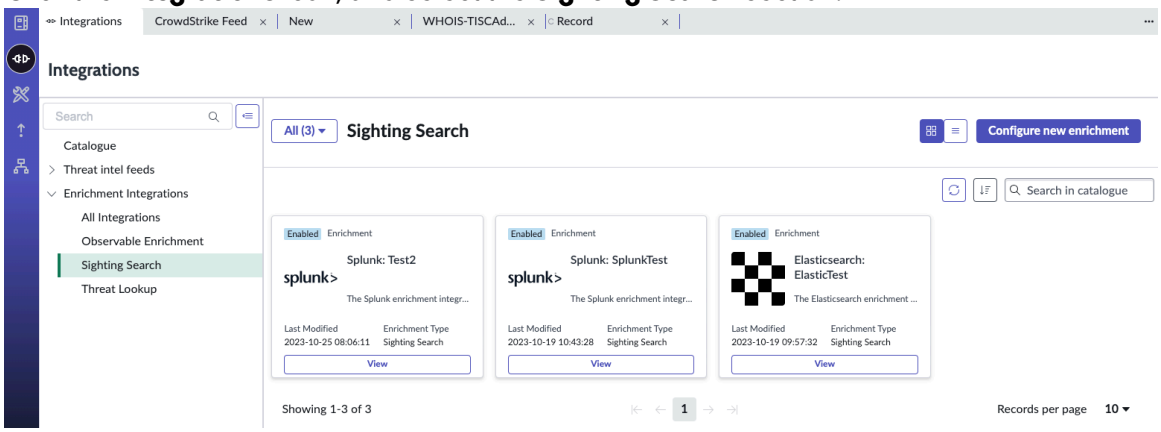
About this task

The Sightings Search section contains only the integrations with the integration type as sightings search.

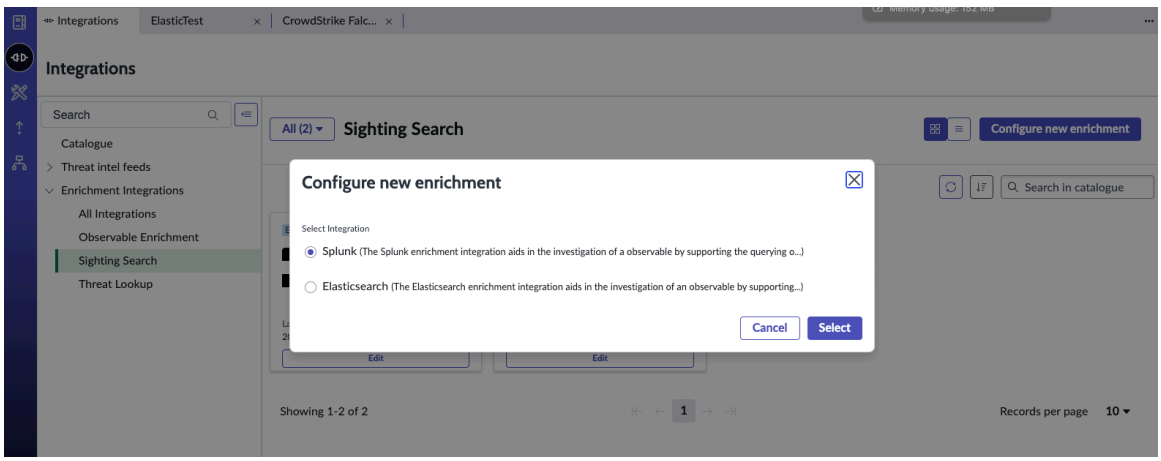
This section displays cards for each of the configured integration implementations that you can activate and use.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Integrations** icon, and select the **Sighting Search** section.



3. Click the **Configure new enrichment** action.
   This takes you to the pop-up that displays the available integrations. You need to choose the integration that you need to configure.
4. Select an integration from the list of available integrations, and click **Select**.
   This takes you to the Create New Enrichment Integration page of the selected integration. This page is pre-filled with details of the selected integration by default. For example, Splunk integration.

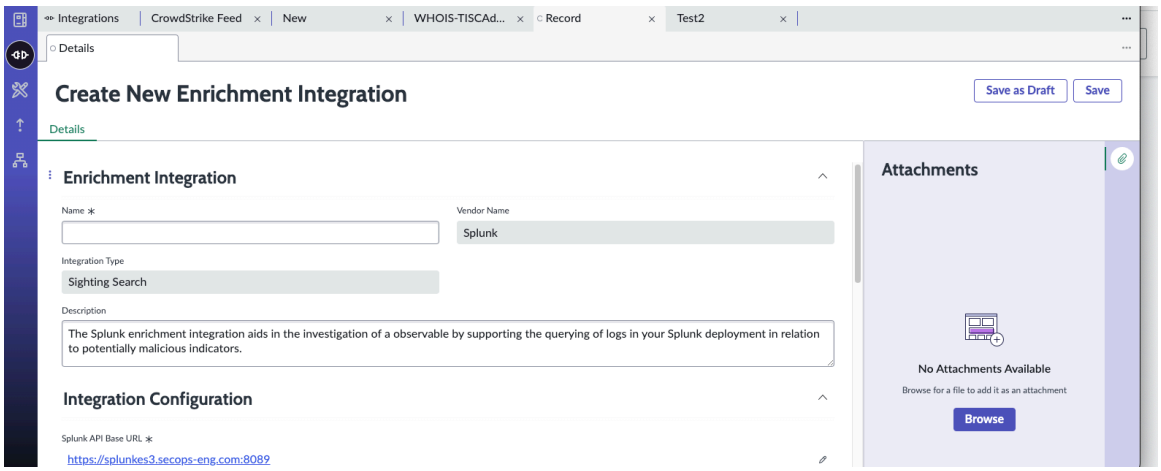


5. On the Create New Integration form, fill the fields.

Field	Description
Enrichment Integration	
Name	Enter a name for the new enrichment integration. For example, `Splunk-1`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Vendor Name	Name of the vendor. The details of the select ed vendor are pre-filled by default. For exam ple, `Splunk`.
Integration Type	Type of integration that you selected, which is Sighting Search. The details of the selected in tegration type are pre-filled by default.
Description	Enter a unique description for the new enrich ment integration.



6. In the Integration Configuration section, configure the integration details based on your requirements.
   The Integration Configuration section includes configuration details like API key, API Client ID or secret, username, password, and so on, which you need to fill in. These configuration details vary for different apps.
7. Click the **Save** action to store and create the new enrichment integration configuration.
   The provided details are validated, and by default the enrichment integration's status is disabled.
8. Click **Save as Draft** action to only store the updates made to the enrichment configuration and not create it.
   If you're not sure about the configuration details, you can use the **Save as Draft** option. After you get the configuration details, you can fill the remaining information in the draft version and create it.
9. To enable the enrichment integration, click **Enable**.
   The enrichment integration is enabled successfully. You can also enable a particular enrichment integration by using the Actions menu of the required integration tile on the Catalog page or the All Integration page.

Define queries for Sighting Search

You can use sighting search configurations for defining the queries used to find the prevalence of observables in your environment as part of observable investigation.

View queries for Sighting Search

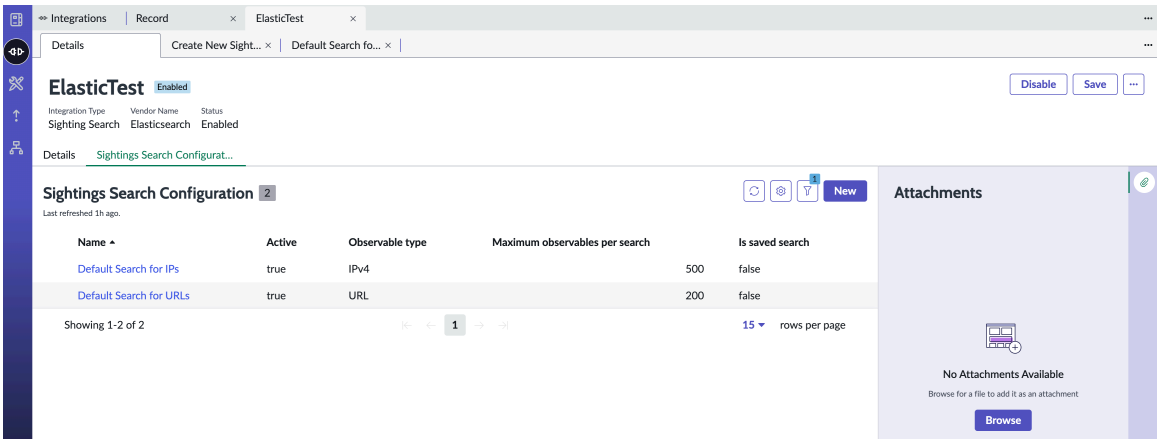
Role required: sn_sec_tisc.admin

To view the sighting search configurations, perform the following steps:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. From the Integrations page, navigate to **Enrichment Integrations** > **Sighting Search**.
3. Look for the integration for which you want to view the Sighting Search Configuration, and click **Edit**.
4. Select the **Sighting Search Configurations** tab.

   You can view the list of sighting search configurations.



5. Click on the required Sighting Search Configuration to view the details of the configuration.
6. To generate a test sighting search query, click the **Generate Test Sighting Search Query** action.

   Note: The **Generate Test Sighting Search Query** action would only work if you had configured sighting search query parameters. For more information, see Using Sighting Search Parameters.

7. In the Generate Test Sighting Search Query pop-up, enter or paste multiple observables using comma, new line, tab, or pipe separators to generate a test query.
8. Click **Generate** to generate the test sighting search query.
9. You can also perform the following actions on the Sighting Search Configurations tab:

   a. To refresh the list of sighting search configurations, click the icon.

   b. To perform a list action on the sighting search configurations, click the icon.

      You can perform the following two list actions:

      - **Edit columns**: You can use this action to add or remove existing columns and modify the order according to your requirements.
      - **Reset widths**: You can use this action to reset the widths of the columns.

   c. To filter sighting search configurations based on conditions, click the icon.

      The value 1 indicates that one condition is used for the filtering.

Create Sighing Search Configurations

Role required: sn_sec_tisc.admin

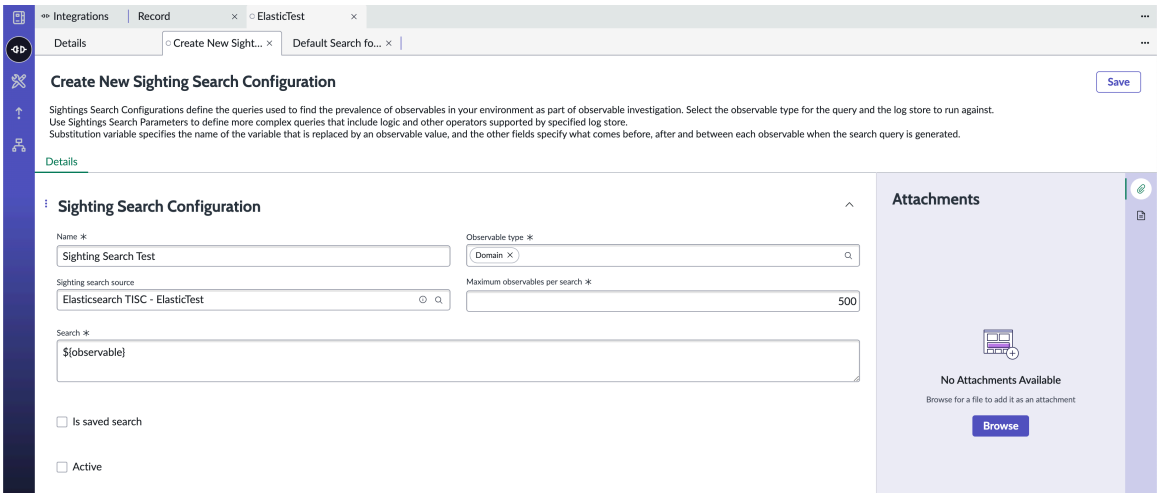
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
Maximum observables per search = "maximum number of observables
 that can be substituted in a single search query"

Search = "Search query that should be executed in sighting
 search source.
Search query can contain substitution variables that would be
 substituted with observables of specific type as configured
 in sighting search parameters when sighting search query is
 formed"
```

To create a sighting search configuration, perform the following steps:

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. From the Integrations page, navigate to **Enrichment Integrations** > **Sighting Search**.
3. Look for the integration for which you want to view the Sighting Search Configuration, and click **Edit**.
4. Select the **Sighting Search Configurations** tab.

   You can view the list of sighting search configurations.
5. To create a sighting search configuration, click **New**.



6. On the form, fill the fields.

Create a sighting search configuration

Field	Description
Name	Name for the sighting search configuration.
Observable type	Defines the type of observable category.
Sightings search source	Defines the source configured for the integration.
Maximum observables per search	The number of observables before the search query is split into multiple queries. Set this value to 500 for this integration.
Search	Add a native search string to form a query. For example, `${observable}`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Is saved search	Runs a saved search, that is, the Name field should match the name of the saved search.
Active	Query runs only if it active option is selected.

7. Click **Save**.

Using Sighting Search Parameters

You can use sighting search parameters that define more complex queries, which include logic and other operators supported by the specified log store.

View Sighting Search Parameters

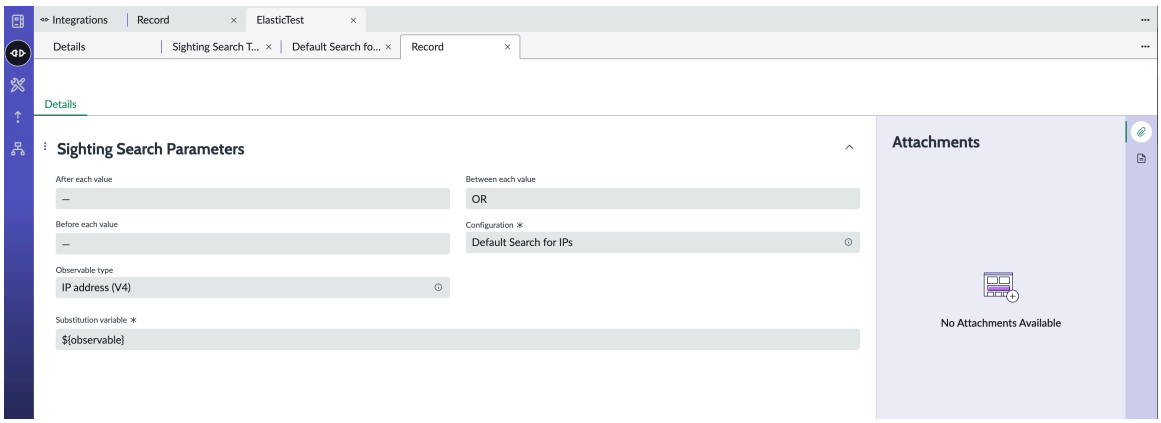
Role required: sn_sec_tisc.admin

To view the sighting search parameters, perform the following steps:

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. From the Integrations page, navigate to **Enrichment Integrations** > **Sighting Search**.
3. Look for the integration for which you want to view the Sighting Search Configuration, and click **Edit**.
4. Select the **Sighting Search Configurations** tab.

   You can view the list of sighting search configurations.

5. Click on the required Sighting Search Configuration to view the details of the configuration.



6. Select the **Sighting Search Parameters** tab.

   You can view the list of sighting search parameters.

7. Click on the required Sighting Search Parameter to view the details of the parameter.
8. You can also perform the following actions on the Sighting Search Parameters tab:

   a. To refresh the list of sighting search parameters, click icon.

   b. To perform a list action on the sighting search parameters, click the icon.

      Edit columns: You can use this action to add or remove existing columns and modify the order according to your requirements.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. To filter sighting search parameters based on conditions, click the icon.

The value 1 indicates that one condition is used for the filtering.

Create Sighting Search Parameter

```
Example for query generation
```

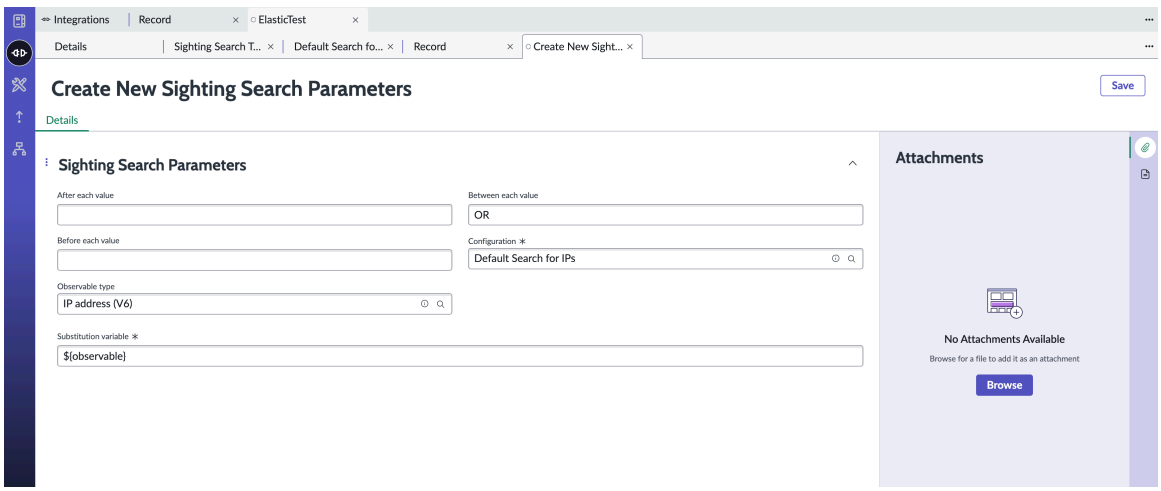
```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each
 value}{Before each Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address =
 172.32.31.41 OR ip_address = 192.168.10.12”
```

To create a sighting search parameter, perform the following steps:

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Integrations**.
2. From the Integrations page, navigate to **Enrichment Integrations** > **Sighting Search**.
3. Look for the integration for which you want to view the Sighting Search Configuration, and click **Edit**.
4. Select the **Sighting Search Configurations** tab.

   You can view the list of sighting search configurations.
5. Click on the required Sighting Search Configuration to view the details of the configuration.
6. Select the **Sighting Search Parameters** tab.

   You can view the list of sighting search parameters.
7. To create a sighting search parameter, click **New**.



8. On the form, fill the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a sighting search parameter

Field	Description
After each value	The sighting search parameter after each observable when the search query is generated.
Between each value	The sighting search parameter between each observable when the search query is generated. For example, OR.
Before each value	The sighting search parameter before each observable when the search query is generated.
Configuration	The configuration details of the search parameter.
Observable type	Defines the type of observable category.
Substitution variable	Specifies the name of the variable that is replaced by an observable value.

9. Click **Save**.

Get started with Elasticsearch integration

The Elasticsearch enrichment integration searches your logs and adds relevant sighting information to your observables.

Configure and enable Elasticsearch integration

Elasticsearch is a distributed, RESTful search and analytics engine that easily integrates with Security Operations.

Before you begin

Before you can use the Elasticsearch, you must download it from the ServiceNow Store.

Role required: sn_sec_tisc.admin

- The Threat Intelligence Security Center plugin must be installed and activated before you can use the Elasticsearch integration.
- Obtain the Elasticsearch API Base URL, Kibana Base URL, Username, and Password under your Elasticsearch profile.

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Sighting Search**

Note: The configured integrations appear as a series of cards.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. In the **Elasticsearch** card, click **Configure New Enrichment** to configure **Elasticsearch** integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the sighting search configuration.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, Elasticsearch.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the Elasticsearch integration. For example, The Elasticsearch enrichment integration aids in the investigation of an observable by supporting the querying of logs in your Elasticsearch deployment.
Integration Configuration	
Elasticsearch API Base URL	The base URL you acquired from the Elasticsearch site.
Kibana Base URL	The Kibana Base URL. [Optional] Links to a Kibana instance, when available.
Username	Your Intel Elasticsearch username.
Password	Your Intel Elasticsearch password.
Elasticsearch Index	The Elasticsearch index. These in turn will hold documents that are unique to each index. Indices are identified by lowercase names that refer to actions that are performed actions (such as searching and deleting).
Date range field	The timestamp of the configuration.
Max Rows	The maximum number of rows you want to search.
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the number of rows of raw data property in Security Incident Response properties.
MID Server	Select Any to use any active MID Server, or select a specific MID Server name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the Workflow Editor.

8. Click **Save**.
   The integration details are validated, and by default the Elasticsearch integration's status is disabled.
9. Click **Enable** to enable the Elasticsearch integration.

Result

After it is configured, Elasticsearch can be selected for performing sighting search on observables in Threat Intelligence Security Center.

Get started with Splunk Search integration

Splunk software searches, monitors, and analyzes machine-generated big data and integrates easily with Security Operations. Before you can use the Splunk Sighting Search integration, you must download it from the ServiceNow Store.

Configure and enable Splunk integration

The Splunk Enrichment integration searches your logs and adds relevant sighting information.

Before you begin

Before you can use the Splunk Search, you must download it from the ServiceNow Store.

Role required: sn_sec_tisc.admin

- The Threat Intelligence Security Center plugin must be installed and activated before you can use the Splunk Search integration.
- Obtain the Splunk and obtain the Splunk Search and obtain the API Base URL, Link URL, Username and Password from your Splunk instance.

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Sighting Search**
   The configured integrations appear as a series of cards.
6. In the **Splunk Search** card, click **Configure New Enrichment** to configure **Splunk Search** integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the sighting search configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, Splunk.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the Splunk integration. For example, The Splunk enrichment integration aids in the investigation of a observable by supporting the querying of logs in your Splunk deployment in relation to potentially malicious indicators..
Integration Configuration	
Splunk API Base URL	The base URL you acquired from the Splunk site.
Link URL	[Optional] The Link URL that links to the Splunk web interface, when available.
Username	Your Intel Elasticsearch username.
Password	Your Intel Elasticsearch password.
Max Rows	The maximum number of rows you want to search.
Earliest Result (days)	The earliest results you want to see in number of days.
Include raw data samples in search results	Select this to include samples of raw data in your sightings search results. The amount of data returned depends on your setting in the number of rows of raw data property in Security Incident Response properties.
On Premises Deployment	The On Premises Deployed environment.
MID Server	Select Any to use any active MID Server, or select a specific MID Server name.

Note: Configuring this integration activates workflows. To manage the workflows, navigate to the Workflow Editor.

8. Click **Save**.
   The integration details are validated, and by default the Splunk integration's status is disabled.
9. Click **Enable** to enable the Splunk integration.

Result

After it is configured, Splunk can be selected for performing sighting search on observables in Threat Intelligence Security Center.

TISC add-on for Splunk overview

The Threat Intelligence Security Center (TISC) for Splunk app offers integration between TISC and Splunk that enables users to seamlessly import the latest threat intelligence from TISC into

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk for monitoring and enriching alerts. Users can configure indicator collections, perform searches and utilize dashboards to analyse search matches and indicator collections effectively.

TISC integration with Splunk

The integration between the Threat Intelligence Security Center (TISC) and Splunk enables users to filter and pull in relevant threat intelligence observables data into Splunk. Within the Splunk, the users can use this data to generate security alerts.

Role required: Splunk admin

Using the TISC add-on application, you can configure the interval at which you can pull observables from ServiceNow TISC instance.

This interval determines how frequently the application can make requests to ServiceNow and retrieve the observables data. Also, you can define and apply filters to specify the observables that you want to pull from the ServiceNow TISC instance.

Once the observables are pulled from ServiceNow, the observables data is stored in Splunk's KV Store (Key-Value Store) and you can further write the correlation rules over the set of observables which were pulled in.

Creating users in ServiceNow TISC instance

You can create users in the ServiceNow TISC instance with any valid user role: sn_sec_tisc.api_obs_read_access.

Install TISC add-on app on Splunk

For more information, see Assign a role to a user.

Role required: Splunk admin.

1. Login to **Splunk**.
2. Navigate to **Apps** > **Manage Apps** or click on the **Manage** gear icon.
3. Search for the **Threat Intelligence Security Center for Splunk** app and install it.
4. Once installed, the application would be visible under the list of apps.

Configuring TISC add-on in Splunk

Follow this below procedure to configure the application.

Before you begin

Role required: Splunk admin

About this task

The below procedure describes the configuration of TISC add-on in Splunk.

Procedure

1. Search for **Threat Intelligence Security Center for Splunk** app from the left navigation.
2. Click on **Set up** under the **Actions** column.
   The **Configuration** page is displayed, and you can set up your ServiceNow TISC account.
3. Select **Add**.
4. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Add Accounts	
Name	A unique name for the account.
User Name	Provide your ServiceNow account user name. You can use the same user name that is used for the users which is created during the role creation `sn_sec_tisc.api_obs_read_access` in the above step.
Password	Provide ServiceNow account password.
Instance URL	Provide the ServiceNow instance URL address.

5. Click **Add**.
   The ServiceNow instance account is added to the Splunk.
6. Navigate to the **Inputs** page to create collections manage your data inputs for your ServiceNow account.
7. Click **Create New Input**.
   The **Add Input** dialogue box is displayed for you to add the inputs to your ServiceNow account.

   Once the input set is defined, the application sends the information to the TISC instance to retrieve a specific number of observables that meet the criteria.
8. Fill in the input details, as appropriate.

Field	Description
Name	A unique name for your input. For example, malicious IP list.
Account	Provide your ServiceNow account user name. You can use the same user name that is used for the users that is created with the role `sn_sec_tisc.api_obs_read_access` in the above step.
Interval	Set time interval in seconds to retrieve the data from TISC.
Expiry Period(in days)	Option to set the expiry period in days. **Note:** The sample expiration is set to 30 days. For example, when data is pulled on a specific date, a set of 10,000 records may be retrieved. These records will be stored in the KV (Key-Value) store within Splunk. Starting from the ingested date, the records will be retained for 30 days. On the 31st day, they will be automatically deleted from the KV store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Never Expire	Choose this option if you don't wish to expire the records ingested.
Additional Attributes	Allows you to add additional attributes from the list of recommended options to include in the KV store. Attributes must be separated by commas. A list of allowed attributes is provided in the table following the mandatory attributes table.
Filters	Define the conditions based on which data should be imported will be filtered. To set the filter conditions, you can define the criteria based on the fields such as threat score, confidence level, and type. For simple filter conditions, you can use this filtering option. However, if the filter conditions are more complex and for any advanced filtering then you can choose to add JSON filters. ○ The allowed integer operators are: "=", "!=", ">", "<", ">=", "<=" ○ The allowed string operators are: "=", "!=", "IN" **Below is an example of a simple filter**: `{Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}`
JSON	JSON based filters allows you to define more intricate conditions.

Sample advanced filter:

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation"
,"operator":"IN","field_value":"clean,suspicious,malicious"},{"
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
field_name":"threat_score","operator":">","field_value":"90"},{
"field_name":"confidence","operator":">","field_value":"90"},{"
field_name":"type","operator":"=","field_value":"ip_v4_address"
}]}
```

Note: Accounts are active by default, but inputs are inactive by default, you must activate them to start importing the data. For possible filters refer to Observable_filters section in Adds observable source records to the Threat Intelligence Security Center (TISC) application.

9. Click **Add** to add the inputs.
10. Click **Clone** or copy to copy and create a new account based on the existing account. Make sure that the input is deactivated before cloning to avoid creating duplicate entries when importing data using the same criteria.
11. Once the data is pulled in, the following information will be retrieved and stored in the KV store within Splunk along with the records pulled from TISC:

Field	Description
confidence	Indicates the confidence level associated with the accuracy of the threat score.
kvlookup_created_time	Indicates the record creation time in the key value store.
kvlookup_days_till_expiry	Indicates the number of days after which the record will be deleted from the KV store.
instance_url	Indicates the ServiceNow instance URL address.
reputation	Indicates the reputation of the entity involved.
source_reported_score	The reported source score from TISC.
sys_id	Sys ID of the record which is coming through TISC.
threat_level	Indicates the severity level of the threat.
threat_score	The score indicating the level of threat associated with a record.
threat_severity	Indicates the threat severity of the observable.
type	Indicates the observables type.
updated_by	Provides the information on who has last updated the record.
kvlookup_updated_time	Indicates the time stamp when the record was last updated in the key value store.
value	Value of the record. For example, IP, hash and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Additional Attributes

Field	Description
additional_context	Provide any additional context, as needed.
attack_phases	Indicates attack phases in a kill chain such as LM, MITRE ATT&CK.
author	Provide the author name.
comments	Add any additional comments as needed.
created	Indicates when the observable was created.
description	Provide the description.
expiration_time	Specifies the expiration time of the observable record.
extensions	Indicates the extensions of an observable.
first_observed	The first time when the data was observed.
first_seen	The first time that this record was first seen performing malicious activities.
historically_significant	Indicates if the observable is considered historically significant. This TISC system flag is used to exclude the observable from archival.
id	Unique identifier assigned to the observable by the TISC system.
is_defanged	Flag indicating whether the observable value has been defanged.
is_false_positive	A boolean flag that indicates if observable is identified as false positive.
language	Indicates the language of the text content in this object.
last_observed	The last time when the data was observed.
last_seen	The time that this object was last seen performing malicious activities.
notes	Add any additional notes for an observable record.
number	System-generated number assigned to the observable by TISC.
security_type	Specifies whether the observable belongs to the Allowlist or Denylist.
no_of_sources	Represents the number of unique sources that have contributed to the observable.
sources	Specifies the threat source from which this record is created.
status	Enter the status of the observable if active or inactive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
tisc_tags	Select the TISC tags that are associated with an observable.
taxonomies	Select the Taxonomy that is associated with an observable.
tlp	Unique value that indicates the Data sensitivity setting per TLP.
updated	Indicates when the observable record was last updated
usage_categories	Categories that the observable falls under, such as botnet or phishing.
watch_list	Flag specifying if the observable is included in the watch list.

These fields along with any others defined by your criteria will be available in Splunk and can be viewed, searched, and analyzed through the search tab.

Data storage in Splunk

This section outlines how TISC utilizes lookups during the integration within Splunk's Key-Value store for data storage. It details how these lookups are configured and retrieved within Splunk.

Lookup	Lookup Description
`threat_intel_store_lookup_test_instance_test`	Name of the KV lookup to be used for searching the incoming records.
`threat_intel_store_test_instance_test`	Name of the KV store where the data resides.
`inputlookup <lookup_name>" example : | inputlookup threat_intel_store_lookup_test_instance_test`	Query to lookup records in the KV store.

Configure Threat Lookup

You can configure the threat lookup to perform a lookup on selected observables. If the observables are of a type recognized by Threat Intelligence, the observables are scanned for malware, and the results are returned. You can perform threat lookup on one or more observables to determine maliciousness of an observable.

Before you begin
Role required: sn_sec_tisc.admin

Note: Enrichment Integrations module is only shown if at least one of the integration supporting any of the capability is installed in the application.

The Threat Intelligence Security Center supports Threat Lookup only for the following integrations:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- VirusTotal
- CrowdStrike Intelligence

For more information, see Threat Lookup.

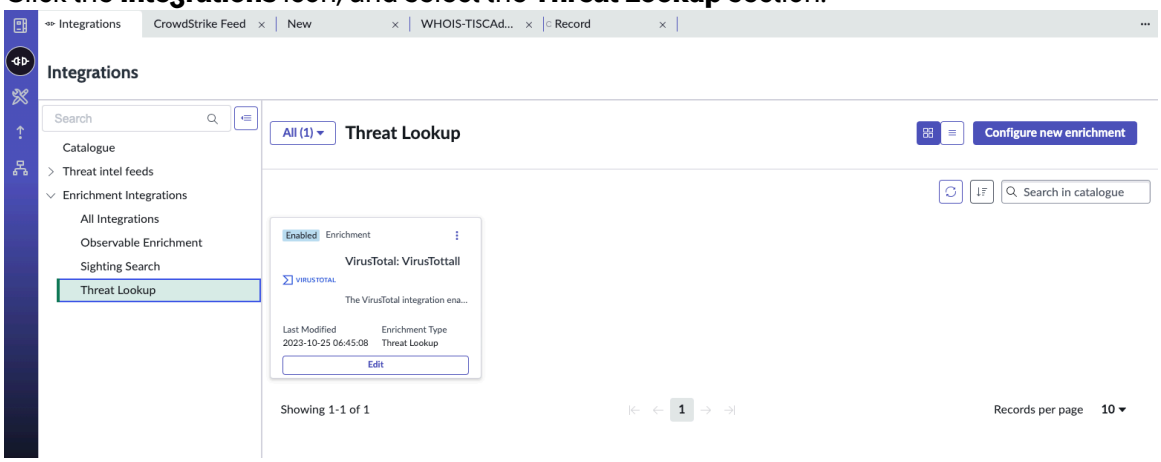
About this task

The Threat Lookup section contains only the integrations with the integration type as threat lookup.

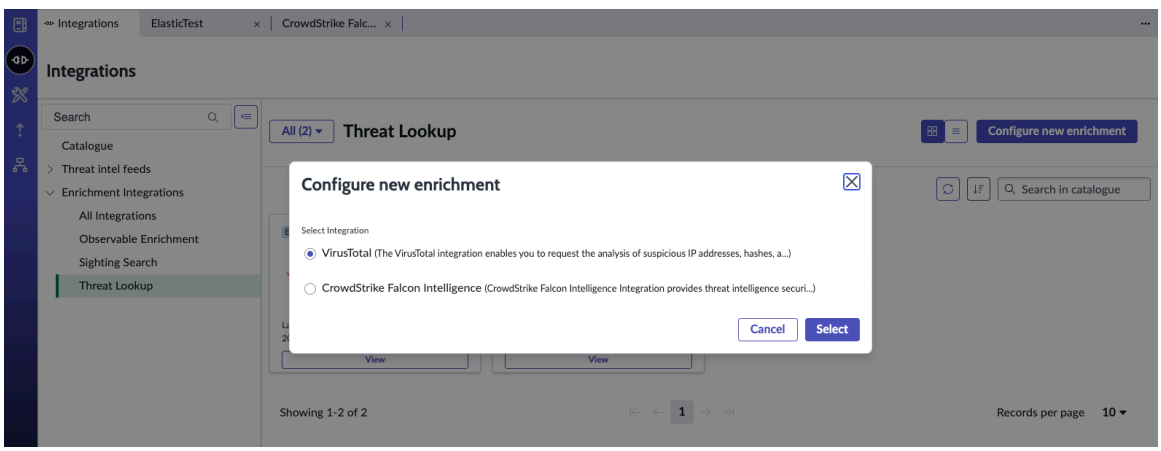
This section displays cards for each of the configured integration implementations that you can activate and use.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Integrations** icon, and select the **Threat Lookup** section.



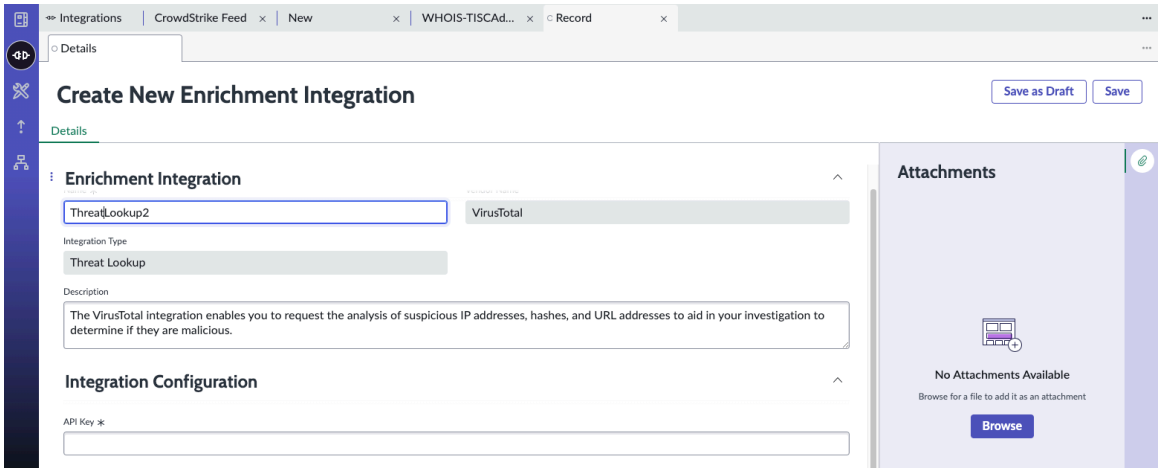
3. Click the **Configure new enrichment** action.
   This takes you to the pop-up that displays the available integrations. You need to choose the integration that you need to configure.
4. Select and integration from the list of available integrations, and click **Select**.
   This takes you to the Create New Enrichment Integration page of the selected integration. This page is pre-filled with details of the selected integration by default. For example, VirusTotal integration.



5. On the Create New Integration form, fill the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Enter a name for the new enrichment integration. For example, `VirusTotal-1`.
Vendor Name	Name of the vendor. The details of the selected vendor is pre-filled by default. For example, `VirusTotal`.
Integration Type	Type of integration that you selected, which is Threat Lookup. The details of the selected integration type is pre-filled by default.
Description	Enter a unique description for the new enrichment integration.



6. In the Integration Configuration section, configure the integration details based on your requirements.
   The Integration Configuration section includes configuration details like API key, API Client ID or secret, username, password, and so on, which you need to fill in. These configuration details vary for different apps.
7. Click the **Save** action to store and create the new enrichment integration configuration.
   The provided details are validated, and by default the enrichment integration's status is disabled.
8. Click **Save as Draft** action to only store the updates made to the enrichment configuration and not create it.
   If you're not sure about the configuration details, you can use the **Save as Draft** option. After you get the configuration details, you can fill the remaining information in the draft version and create it.
9. To enable the enrichment integration, click **Enable**.
   The enrichment integration is enabled successfully. You can also enable, disable, or delete a particular enrichment integration by using the Actions menu of the required integration tile on the Catalog page or the Enrichment Integrations page.

View Threat Lookup Reputation Calculators

You can view the Threat Lookup Finding Calculator to calculate the observable findings for your integration.

Before you begin

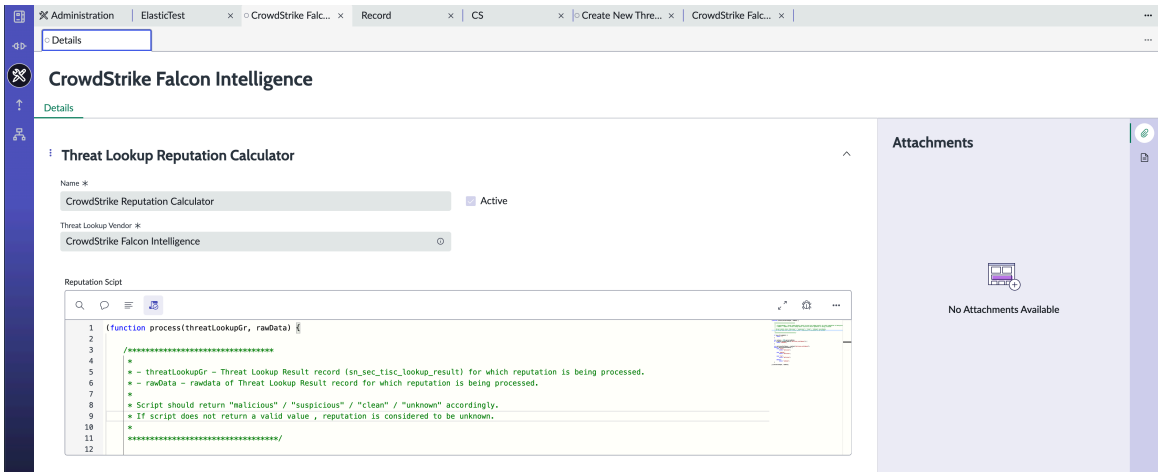
Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To learn more about the Threat Lookup Reputation Calculators, see Managing the Threat Lookup Reputation Calculator.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Select the **Threat Lookup Reputation Calculator** section.
   You can view the list of Threat Lookup Reputation Calculators.
3. Click on the required Threat Lookup Reputation Calculator to view the details of the calculator.



4. You can also perform the following actions on the Threat Lookup Reputation Calculator section:

   a. To refresh the list of Threat Lookup Reputation Calculators, click the icon.

   b. To perform a list action on the Threat Lookup Reputation Calculators, click the icon.

      You can perform the following two list actions:

      - **Edit columns**: You can use this action to add or remove existing columns and modify the order according to your requirements.
      - **Reset widths**: You can use this action to reset the widths of the columns.

   c. To filter Threat Lookup Reputation Calculators based on conditions, click the icon.

      The value 1 indicates that one condition is used for the filtering.

Threat Lookup

The Threat Lookup - VirusTotal and CrowdStrike Falcon intelligence workflow performs a lookup on selected observables. If the observables are of a type recognized by VirusTotal and as well as CrowdStrike, the observables are scanned for malware, and the results are returned.

TISC VirusTotal integration

TISC VirusTotal integration enables you to request the analysis of suspicious IP addresses, file hashes, and URL addresses to aid in your investigation to determine if they are malicious.

Configure and Enable VirusTotal Integration

Before you can use the VirusTotal integration, you must download it from the ServiceNow Store.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_sec_tisc.admin

The Threat Intelligence Security Center plugin is required in order to activate VirusTotal integration.

Procedure
1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, access VirusTotal and obtain the API Key under your VirusTotal profile.
4. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
5. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
6. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Threat Lookup**
7. Click **Configure New Enrichment** to configure **VirusTotal** integration.
8. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, VirusTotal.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, VirusTotal.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the new enrichment integration.

9. Drill down to **Integration Configuration** section.
10. Enter (or paste) the **API Key** you acquired from the VirusTotal site.
11. Click **Save**.
    The integration details are validated, and by default the VirusTotal integration's status is disabled.
12. Click **Enable** to enable the VirusTotal integration.

Result
After it is configured, VirusTotal can be selected for performing lookups on observables in Threat Intelligence Security Center.

TISC CrowdStrike Falcon Intelligence integration

CrowdStrike Falcon Intelligence provides cyber security intelligence that easily integrating with Security Operations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

The Threat Intelligence Security Center plugin is required to implement the CrowdStrike Falcon Intelligence integration.

Configure and Enable CrowdStrike Falcon Intelligence integration

Before you can use the CrowdStrike Falcon Intelligence, you must download it from the ServiceNow Store and add the appropriate Client ID and Client Secret.

Before you begin

Role required: sn_sec_tisc.admin

- Threat Intelligence Security center application must be installed and activated.
- Obtain the API Client ID and API Client Secret under your CrowdStrike Falcon Intelligence profile.
- In the CrowdStrike Falcon Intelligence portal API Scopes, enable the Read setting for Indicators (Falcon Intelligence).

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Threat Lookup**.
6. Click **Configure New Enrichment** to configure **CrowdStrike Falcon Intelligence** integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, CrowdStrike Falcon Intelligence.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, CrowdStrike Falcon Intelligence.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the new enrichment integration.
Integration Configuration	
Client ID	The client ID that you obtained from CrowdStrike.
Client Secret	The client secret key that you obtained from CrowdStrike.

8. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The integration details are validated, and by default the CrowdStrike Falcon Intelligence integration's status is disabled.

9. Click **Enable** to enable the CrowdStrike Falcon Intelligence integration.

Result

After it is configured, CrowdStrike Falcon Intelligence can be selected for performing lookups on observables in Threat Intelligence Security Center.

TISC Security Tools integrations

TISC Endpoint Detection and Response (EDR) integrations focuses on identifying and addressing security threats at an endpoint level.

EDR network solutions predicts and preempt the emerging threats and helps in enhancing overall organization’s security posture.

By integrating with other security tools such as EDR, TISC enables proactive threat monitoring on endpoints and thereby enhances the overall security posture and resilience against evolving threats.

Related topics

CrowdStrike Falcon EDR integration

CrowdStrike Falcon EDR integration

Integration with CrowdStrike Falcon EDR enables continuous monitoring and real-time alerting based on intelligence from TISC.

This integration can help streamline security operations and reduce any potential risk to the organization's business.

Configure Crowdstrike Falcon EDR integration

Before you can use the CrowdStrike Falcon EDR integration, you must download it from the ServiceNow Store Store and add the appropriate Client ID and Client Secret.

Before you begin

Role required: sn_sec_tisc.admin

- Threat Intelligence Security Center application must be installed and activated.
- Obtain the API Client ID and API Client Secret from CrowdStrike Falcon console.
- In the CrowdStrike Falcon portal API Scopes, enable the **IOC Management: read and write access**.

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. Select **Integrations** > **Security Tools** > **EDR**.
4. Click **Configure New Security Tool** to configure CrowdStrike Falcon EDR integration.
5. Select **CrowdStrike Falcon EDR** option.
6. Fill in the fields on the Configure new security tool form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create New Enrichment Integration

Field	Description
Name	Enter a name for the new security tool integration. For example, CrowdStrike Falcon EDR.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, CrowdStrike Falcon EDR.
Description	Enter the description for the new security tool integration.
Integration Type	Option that displays the integration type.
Integration Category	Option that displays the integration category.
Integration Configuration	
Base URL	The base URL is the CrowdStrike API base URL. The default value is https://api.crowdstrike.com. For more information, see https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40
Client ID	The client ID that you obtained from CrowdStrike. For more information, see https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis.
Client Secret	The client secret key that you obtained from CrowdStrike. For more information, see https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis.
Expiration period in days for any type of observables	The expiry period in days that are applied for any type of observable(s) when they are sent to CrowdStrike EDR. **Note:** This option is a fall back expiration period when the expiration time is not set for any specific observable type.
IP Observable Expiration Time	The expiry period in days that are applied for the IP type of observable when they are sent to CrowdStrike EDR.
Domain Observable Expiration Time	The expiry period in days that are applied for the domain type of observable when they are sent to CrowdStrike EDR.
Hash Observable Expiration Time	The expiry period in days that are applied for the Hash type of observable when they are sent to CrowdStrike EDR.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Click **Save**.
   The integration details are validated, and by default the CrowdStrike EDR integration's status is disabled.
8. Click **Enable** to enable the CrowdStrike EDR integration.

Note: Multiple configurations are allowed for CrowdStrike Falcon EDR integration.

Send observables to EDR

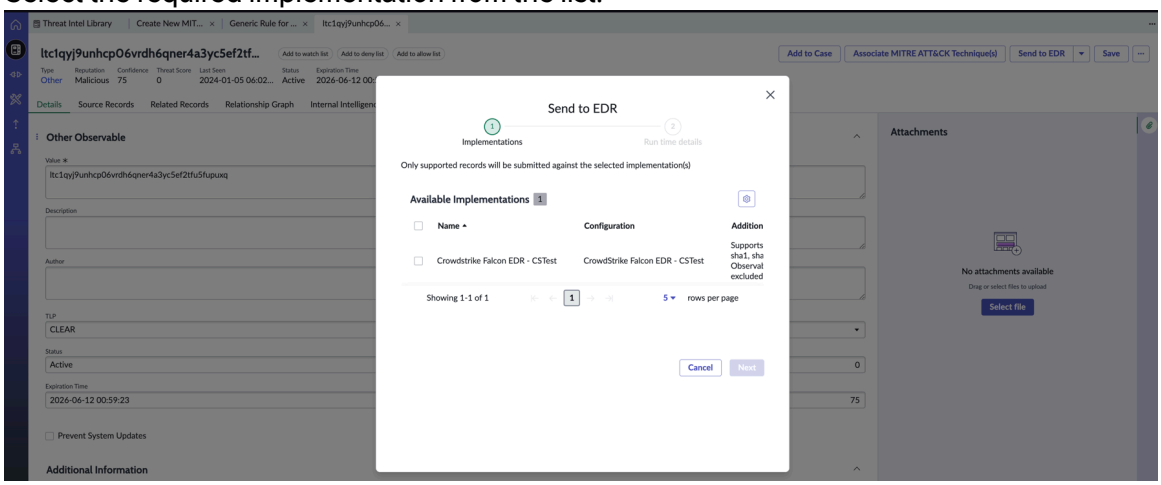
Send observables to the EDR security tool.

Before you begin

Role required: sn_sec_tisc.analyst

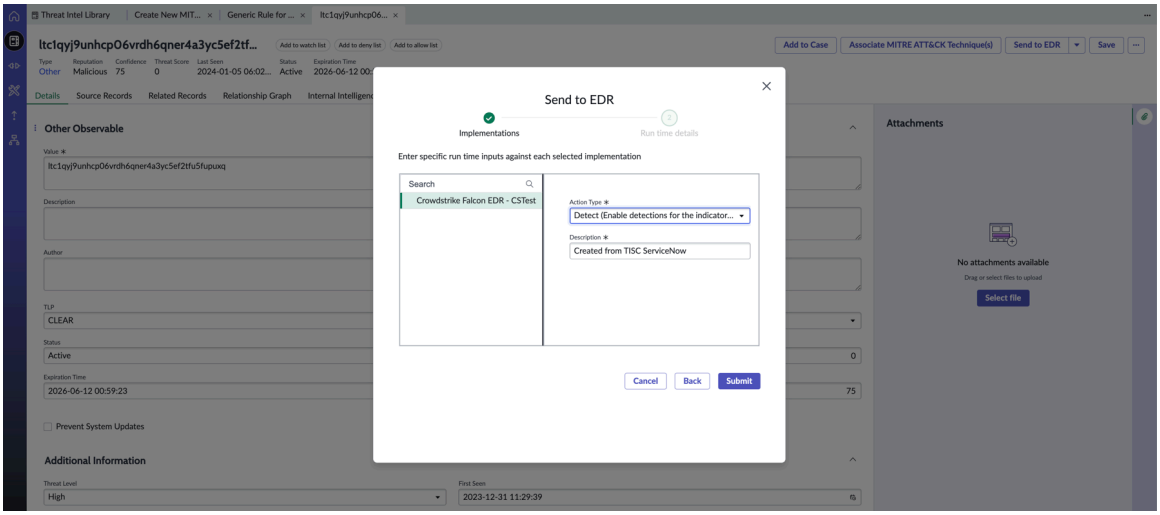
Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Intel Library** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Select **Send to EDR**.
   The Send to EDR **Implementations** modal screen is displayed.
6. Select the required implementation from the list.



7. Click **Next**.
8. Select the run time details such as the **Action Type** and **Description** of the implementation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The available options for the CrowdStrike during implementation run time details are:

- **No Action (Save the indicator for future use, but take no action)**: In the Observable form view, the threat severity of the observable is optional for CrowdStrike Falcon EDR.
- **Detect (Enable detections for the indicator at record's threat severity)**: In the Observable form view, the threat severity is mandatory for CrowdStrike Falcon EDR. The threat severity of the observable shouldn't be empty for that selected observable.

9. Click **Submit**.
   The selected action is executed and an information message is displayed that Observable Send to EDR execution has started.

Note:

- Once the execution is initiated or completed, a work notes is posted on the activity stream of the form view.
- **Send to EDR** action is also available on the observables list under **Artifacts** tab for a case record. For more information, see Add artifacts to case(s) or case task(s).

Microsoft Defender for EDR Integration

Integration with the Threat Intelligence Security Center (TISC) allows Cyber Threat Intelligence (CTI) analysts to automatically push malicious or suspicious IP addresses, domains, file hashes, and URLs to Microsoft Defender for continuous monitoring and real-time alerting.

Register and configure the Microsoft Defender in the Microsoft Azure portal

Register the Microsoft Defender EDR in the Microsoft Azure portal and grant the read and write access to the application.

Before you begin

Role required: Application developer, Tenant administrator.

Procedure

1. Log in to the Microsoft Azure portal.
2. Enter `App registrations` in the Search box, and click **Click New registration**.
3. Enter a name for your application and the redirect URI, and click **Register**.
   An example name is `Microsoft Defender for Endpoint`. The Redirect URI is used while providing admin consent for the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the **App registrations** page, select the application that you registered in Step 3.
5. Under Manage, select **Certificates & secrets**.
6. To create a client secret, select **New client secret**.
7. Copy the client secret and save it.

   In case you forgot the client secret, you can generate a new client secret.
8. Navigate to **Manage** > **API Permissions**.
9. Click **Add a permission**.
10. In the Request API permissions window, click the **APIs my organization uses** tab.
11. Search for and select **WindowsDefenderATP**.
12. In the WindowsDefenderATP permissions, select **Application permissions**.
    Enabling this permission ensures that the application runs as a background service or daemon without a signed-in user.
13. Add the following application level permission and grant admin consent for the newly added API permission.

Permission	Permission Display Name
Ti.ReadWrite.All	Read and write Indicators

Install and configure Microsoft Defender for EDR Integration

Install and configure the Microsoft Defender for EDR integration from the ServiceNow Store.

Before you begin

Role required: sn_sec_tisc.admin

- Threat Intelligence Security Center application must be installed and activated from ServiceNow store.
- Obtain the API Tenant ID, Client ID, and Client Secret from Microsoft Defender for EDR console.

Procedure

1. Download the Microsoft Defender for EDR integration from the ServiceNow Store and install it.
2. Using your instance, access **Threat Intelligence Security Center**.
3. Download the integration from the ServiceNow Store.
4. Select **Integrations** > **Security Tools** > **EDR**.
5. Click **Configure new source tool integration**.
6. Select **Microsoft Defender for EDR** option.
7. Click **Select**.
8. On the form, fill in the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure Microsoft Defender for EDR integration

Field	Description
Name	Name for the new security tool integration configuration. For example, Microsoft Defender for EDR integration.
Integration Category	Option that displays the integration category.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default.
Integration Type	Option that displays the integration type.
Description	Enter the description for the new security tool integration configuration.
Integration Configuration	
Base URL	The base URL is the Microsoft Defender for EDR API base URL. The default value is https://api.securitycenter.microsoft.com/.
Tenant ID	The tenant ID that you obtained from Microsoft Defender.
Client ID	The client ID that you obtained from Microsoft Defender.
Client Secret	The client secret key that you obtained from Microsoft Defender.
Prefilled title(used during submission)	The prefilled title defines the parameters required for submitting indicators to Microsoft Defender. These details are displayed by default, so you don't need to re-enter them each time you configure the integration.
Prefilled description(used during submission)	The prefilled description outlines the required parameters for submitting indicators to Microsoft Defender. These details are displayed by default, so you don't need to re-enter them each time you configure the integration.
Expiration period in days for any type of observables	The expiry period in days that are applied for any type of observable(s) when they are sent to Microsoft Defender EDR. **Note:** This option is a fall back expiration period when the expiration time is not set for any specific observable type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Expiration period in days for IP type of observables	The expiry period in days that are applied for the IP type of observable when they are sent to Microsoft Defender EDR.
Expiration period in days for Domain type of observables	The expiry period in days that are applied for the domain type of observable when they are sent to Microsoft Defender EDR.
Expiration period in days for Hash type of observables	The expiry period in days that are applied for the Hash type of observable when they are sent to Microsoft Defender EDR.

9. Click **Save** after complete adding the necessary configuration information.
10. Click **Enable** to enable the configuration, after you save the new Microsoft Defender EDR integration.
    A confirmation message is displayed that the enrichment integration is enabled successfully.

Result

After the integration is configured, You can select the required any type of observable that supports Microsoft Defender EDR from Threat Intel Library.

System properties for Microsoft Defender EDR

The following details the system properties for Microsoft Defender EDR.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **All** > **Glide properties catalog** > **Glide properties**.
2. Search for Microsoft Defender properties.

Property	Description
sn_tisc_defender.rate_limiter.minute	This allows the users to limit the rate of sending EDR to MS Defender on minutely basis. ○ Type: Integer ○ Value: 100
sn_tisc_defender.rate_limiter.hour	This allows users to limit the rate of sending EDR to MS Defender on an hourly basis. ○ Type: Integer ○ Value: 1500

Send observables to EDR

Send observables to the EDR security tool.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Intel Library** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Select **Send to EDR**.
   The Send to EDR **Implementations** modal screen is displayed.
6. Select the required implementation from the list.
   For example, select the implementation associated to Microsoft Defender EDR.
7. Click **Next**.
8. Select the run time details such as the **Title** and **Description** of the implementation.
9. Click **Submit**.
   The selected action is executed and an information message is displayed that Observable Send to EDR execution has started and the results of this execution will be available under the Activity Stream after the execution is complete.

> **Note:** Once the execution is initiated or completed, a work notes is posted on the activity stream of the form view and you can verify the execution progress accordingly.

TISC Security Tools - Firewall

TISC Security Tools - Firewall prevents unauthorized access to the network. Palo Alto integration with TISC helps blocking malicious IP addresses, URLs, and domains using External Dynamic List (EDL) capabilities with ServiceNow Threat Intelligence data.

Within TISC, by integrating with other security tools such as Palo Alto Networks enhances overall organization's network security.

Palo Alto Networks integration

Palo Alto Networks integration once configured enables the threat analyst to add malicious IP addresses, URLs, and domains to External Dynamic List (EDL) or remove these entries from EDL once confirmed as non-malicious or clean.

An EDL is a text file that is hosted on an external web server. For this integration, this web server is your ServiceNow AI Platform instance, which permits the Palo Alto Networks Firewall to import objects that are included in the list, IP addresses, URLs, and domains.

Create new EDL for Palo Alto Networks

Create new External Dynamic List (EDLs) for Palo Alto Networks. Once you create EDLs, you can start creating entries for those EDLs.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. After you save the newly configured Palo Alto NGFW configuration, navigate to **EDLs** section.
2. Click **New** to create new External Dynamic List (EDLs).
3. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Palo Alto Networks Firewall External Dynamic List form

Field	Description
Name	Palo Alto Networks Firewall Dynamic List name.
Observable Type	Select an observable type this EDL accepts from the choice list: IP (including CIDR), URL, or domain.
Expiry period (days)	Expiration period of the EDL. 0 (the default) indicates that the EDL entry never expires. If you change this value, this entry is active for the number of days you enter. You can enter a minimum value of 1, and there is no maximum value. For example, if you enter 30 days at 2:01 PM on Nov 1, the EDL will expire at 2:01 PM on Nov 30. All entries in this EDL then inherit this value by default unless you override the value on individual entry basis.
Create change request	This check box is selected by default to automatically create a change request and change tasks in your ServiceNow AI Platform instance, which are attached to the EDL record. The change request is used to configure the EDL list retrieval URL in the Palo Alto Networks Next-Generation Firewall server. This option is recommended if your firewall administrator is also using the ServiceNow AI Platform for firewall policy or rule changes. If you create a request, once it is closed, the EDL list is automatically activated.
Description	Description of the Palo Alto Networks Firewall Dynamic List. The name generally contains the types of sites and observables you would expect to be on this EDL, and you can use this field for more details.
Change Request	When the Create change request check box is selected, the change request number is displayed on the ServiceNow AI Platform instance once the EDL is saved. When the check box for **Create change request** is cleared, this field is not displayed.
Combine IP addresses and subnet addresses into a single entry	Option to combine both IP addresses and subnet addresses into a single entry.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	When you select this check box and if the IP of CIDR type is added then it will automatically remove the existing entries which falls in the CIDR range. For example: If there is an entry in EDL with value 192.168.1.1, and if a CIDR value of 192.168.1.0/24 is added to the same EDL, the initial IP address entry would be removed, since it falls within the CIDR range of the new entry. **Note:** This option is displayed only when you select the **Observable Type** as IP.
EDL Retrieval URL	The URL link the Palo Alto Networks firewall administrator uses for configuration in the Palo Alto Networks firewall is automatically generated and displayed.

4. Create and add more EDLs as required.
   The EDLs are displayed on the Palo Alto Networks External Dynamic Lists list.

Related topics

Palo Alto EDL Approval Rules

Palo Alto EDL Approval Rules

Approval rules allows the users to activate the approval work flow required to approve or reject the EDL entries.

Before you begin
Role required: sn_sec_tisc.admin

About this task
The TISC admin defines these approval rules to grant consent on the approval requests. As a TISC admin, you can also define multiple levels of approval from here.

Procedure

1. After you save the newly configured Palo Alto NGFW configuration, navigate to **EDL Approval Rules** section.
2. Click **New** to create a new approval rule.
   The following rules are the pre configured rules in the base system for the Palo Alto NGFW integration.

Pre configured EDL Approval Rules

Name	Description	EDL Action
Approval rule for adding to EDL	This approval rule allow the users to activate the approval work flow for adding entries to EDL.	Add to EDL

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description	EDL Action
Approval rule for removing from EDL	This approval rule allow the users to activate the approval work flow for removing entries from EDL.	Remove from EDL

3. Fill the fields in the form as appropriate.

Create New EDL Approval Rules

Field	Description
Name	Name of the approval rule.
EDL Action	Option to add or remove the EDL entry.
EDLs	Select the EDLs that requires approval. If you leave this empty then it will include all the EDLs.
Description	Enter the description for the approval rule.
Select User or Groups requiring approval	
User(s)	Select the user(s) that requires approval.
Group(s)	Select the group(s) that requires approval.
Select approver(s)	
User(s)	Select the user(s) for approval.
Group(s)	Select the group(s) for approval.
Notifications	
Notify requester on approval	Select this check box to notify the requester on approval of EDLs.
Notify requester on rejection	Select this check box to notify the requester on rejection of EDLs.

4. Click **Save** to validate and save the approval rule.
5. Click **Enable** to enable the approval rule.

Add Observables to EDL

Add observables such as IPs, domains, and hashes to External Dynamic List (EDLs).

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Add to EDL**.
   The Add to EDL modal screen is displayed.

Remove Observables from EDL

Remove observables from EDL.

Before you begin
Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Click **Remove from EDL**.
   The Remove from EDL modal screen is displayed.

Approve EDL entries for Palo Alto Networks

Approving External Dynamic List (EDL) entries is part of the pre configuration. You must approve the EDL entries before the entries are activated on EDLs for the firewall to retrieve the entry and apply the security policy.

Before you begin
Role required: sn_sec_tisc.admin

About this task
When the approval process is enabled, an EDL entry is not activated or deactivated on the EDL until it is approved.

Procedure

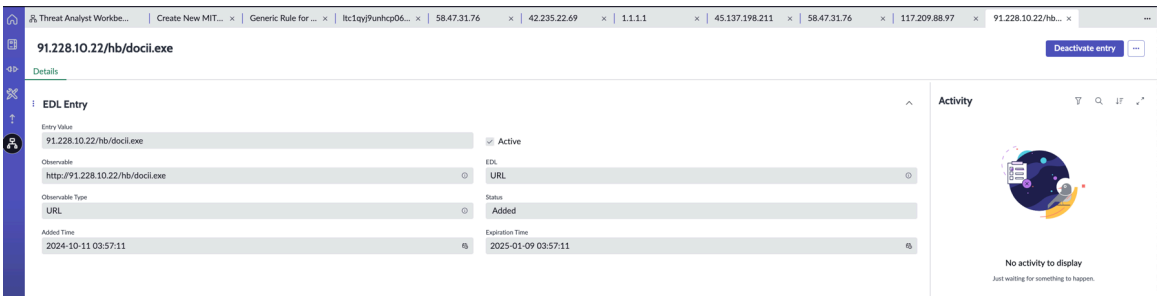
1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Analyst Workbench**.
2. Drill down to **PAN NGFW** section and select the EDL record for approval.
3. Go to **My Approvals**.
4. Select the EDL record(s) for approval.
5. Click **Approve**.
6. Under **My Approval** requests, click an item in the **State** column to open it.
7. Choose the option for approving the EDL entry.

Option	Description
Approve	On the entry record, the **Status** field changes to Added, and the **Active** check box is selected. The **Deactivate** button is displayed and active. Work notes show that the request for the EDL entry has been approved.
Reject	On the entry record, the Status field changes to **Rejected**, and the **Active** check box is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	cleared indicating the entry is not blocked on the firewall. Work notes show that the request for the EDL entry has been rejected.

After you have approved the EDL entry and it is activated, the Palo Alto Networks retrieves the EDL entry after the next retrieval interval. After the entry is retrieved, the observable is blocked from that point forward. In the following figure, note that the **Active** check box is selected, the status is Added, and the work notes indicate that the request has been approved.



TISC - Azure Sentinel integration

Threat Intelligence Security Center and Microsoft Azure Sentinel solution enables several capabilities, including importing observables from TISC to the Sentinel Workspace, enriching Sentinel incidents by fetching details of associated entities, and exporting entities associated with a Sentinel incident to TISC.

TISC playbook templates

This section describes the playbook templates that are shipped with TISC Sentinel solution.

Playbook use cases

The following table describes the various playbook use cases.

Use case	Playbook	Description
Importing Observables from TISC to Sentinel	Batch_Indicator_Uploader	Provides batching mechanism for exporting observables from TISC using Upload Indicators API provided by Microsoft Sentinel.
	Import_Observables_Batch	Enables scheduled export of observables from TISC.
Export entities from Sentinel to TISC	Export_Incident_Entities	Export all entities of a Sentinel incident.
	Export_Hash_Entity	Export file hash entities of Sentinel incident.
	Export_Domain_Entity entities	Export domain entities of Sentinel incident.
	Export_IP_Entity	Export IP entities of Sentinel incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Playbook use cases

The following table describes the various playbook use cases.

(continued)

Use case	Playbook	Description
	Export_URL_Entity	Export URL entities of Sentinel incident.
Enrich Sentinel incidents	Incident_Enrichment	Enables enrichment of Sentinel incidents by fetching details related to entities associated with it and posting information in the form of comments on the incident.

Note: All the playbooks use TISC Custom Connector internally to use TISC APIs.

Create playbooks from templates

1. Navigate to T**ISC Solution** content page from the **Content Hub in Sentinel Workspace**.
2. For each playbook shown in the contents page, do the following:
   a. Select the playbook template, a context pane is displayed in the right hand side of the screen, click **Configuration**.
   b. Read the description of the playbook template, go through the **Prerequisites** and **Post deployment** steps mentioned in the description.
   c. Click on **Deploy custom connector** (if you haven't already deployed the custom connector).

      Add the **ServiceNow instance URL** on the **Deployment Configuration** page.

   d. Click **Create Playbook**, you would be taken to the deployment configuration screen
   e. In the Create playbook configuration screen:
      - Select the appropriate resource group.
      - Modify the playbook name, or use the default name.
      - Provide the **Custom Connector nam**e (make sure this matches with name of the connector you deployed in previous step) in the Parameters section.
      - Click **Review and Create**.

Configure Import_Observables_Batch playbook

Make sure to create Batch_Indicator_Uploader playbook before the Import_Observables_Batch playbook is created.

1. Navigate to **Logic App Designer** to edit the playbook.
2. Update the Recurrence time (in hours) as required.
3. From the TISC Custom Connector component within the playbook, update the parameters that are sent to TISC API.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Parameter Name	Description
Observable Type	Following are the supported types, select one or more: ○ IP ○ File Hash ○ Domain ○ URL
Threat Score	Enter the threat score for observables. The threat score value MUST be a number in the range of 0-100.
Confidence	Enter the confidence for observables. The confidence value MUST be a number in the range of 0-100.
Reputation	Following are the supported values, select one or more: ○ Clean ○ Malicious ○ Suspicious ○ Unknown
Threat Severity	Following are the supported severity levels, select one or more: ○ Critical ○ High ○ Medium ○ Low
Threat Level	Following are the supported threat levels, select one or more: ○ High ○ Medium ○ Low
Last Updated Delta in Hours	The last updated time(in hours) for observables.

Configure Export_Incident_Entities playbook

This playbook uses TISC Add observables API. Using the Logic App Designer, you can edit the parameters that are sent to the API from the playbook. For more information see TISC API - POST /sn_sec_tisc/threat_intel_data/add_observables.

You can follow the same procedure for all the below listed playbooks which export different types of entities:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

Configure Incident_Enrichment playbook

This playbook uses TISC Observables API. Using the Logic App Designer, you can edit the parameters that are sent to the API from the playbook. For more information see TISC API - POST /sn_sec_tisc/threat_intel_data/observables.

Run playbooks

The following table describes how you can run the following playbooks.

Playbook	Action
Import_Observables_Batch	This playbook runs automatically based on the scheduled time which is mentioned in the recurrence trigger.
Export_Incident_Entities	On a Sentinel incident, select **Incident Actions** > **Run Playbook** for execution.
Export_Hash_Entity	On a Sentinel incident, select **File hash entity** > **Run Playbook** for execution.
Export_Domain_Entity	On a Sentinel incident, select **Domain entity** > **Run Playbook** for execution.
Export_IP_Entity	On a Sentinel incident, select **IP entity** > **Run Playbook** for execution.
Export_URL_Entity	On a Sentinel incident, select **URL entity** > **Run Playbook** for execution.
Incident_Enrichment	On a Sentinel incident, select **Incident Actions** > **Run Playbook** for execution.

Administer

Using the left navigation to navigate to the Administration module within Threat Intelligence Security Centre and view the following modules of TISC data administration, to further set filtering rules, approval rules, define threat score, and manage notifications.

Data Administration

Module	Description
Rules Engine	This section consists of the following rules required during the data management: 1. **Data Imports Approval Rules**: Define the approval rules and integrate the approval flow within the Import Intelligence section after submitting the data import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data Administration (continued)

Module	Description
	2. **Inbound Filtering Rules**: Create filter rules to filter the incoming source records data. 3. **Threat Scoring Rule**: Customize threat score calculator that assigns threat score to the observables.
Security Control Lists	This module help you with the security controls: **1. AllowList** **2. DenyList** **3. WatchList**
Taxonomies	This module helps you to create taxonomies for the data source records.
Notifications	This module defines how to manage email notifications.
Templates	This module briefs on how to create report templates in both design time and runtime experience.

About Rules Engine in TISC

Defining Data Imports Approval Rules

Use this section to define the approval rules and integrate the approval flow within the Import Intelligence section after submitting the data import.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Administration** icon on the workspace.
3. Go to **Rules Engine** > **Data Imports Approval Rules**.
4. Select **Approval Rule for Data Imports**.

   Within the base system, **Approval Rule for Data Imports** is the default approval rule provisioned to allow the users to activate the approval workflow.

5. Enter at least one user name or user group for each of **Select User or Groups requiring approval** and **Select approver(s)** section.
6. Click on **Enable** button to enable the approval flow for the data imports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When enabled, the data imports will be in the approval queue for the approver to approve or reject the data processing. The approver will review the changes made by the analyst and then approve or reject the data import request.

Note: An email notification is sent to the user(s) or user group(s) that the import job is processed and approved or rejected.

Defining Expiration Rules

Define expiration rules for various observables or a combination of various source objects or indicators source that are created in TISC.

Before you begin

Every source that is created in the application has an expiry period. The data feeds use the techniques such as time-based expiration period to boost the data ingestion. In TISC, the expiration rules defines the expiration time for a particular set of data sources or set of types of objects or types of observables.

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Expiration Rules**.
   The Expiration Rules page displays.
3. Click **New**.

Field	Description
Name	Enter a name for the expiration rule.
Description	Enter a description for the expiration rule.
Expiry period (days)	Specify the time duration after which the data ingested should expire or considered outdat ed. Enter the expiry period for the observable in days. For example, 100 days. **Note:** Whatever the data that is ingest ed from the source will be expired 100 days after the ingestion.
Data Sources	Indicates the expiration rule for the current da ta source. Select the list of data sources from the lookup. **Note:** Do not select this field and make sure to leave it blank if you want to se lect all the data sources. If you want to select indicator as an object you must select the object and then select the **Type of records** value as **Indicator**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: By default, a sample expiration rule sn_sec_tisc_m2m_entity_rules is provisioned for the users within the base system. For Observables, this sam ple expiration rule will be in disabled state. You must enable and activate the rule. To apply the rule on the source records, you must enable the rule.
Category	Indicates the expiration rule category type for the current data source. Select the category type from the drop-down list such as observ able or object.
Type of Records	Select the type of records.

4. Click **Enable** to enable the expiration rule after you create a new rule.
   If you don't enable the expiration rule then the rule will not be applied to the source record.

   Note:

   - Whenever you enable an expiration rule, then a duplication check happens in the background to verify if there is any duplicate rule in the system with the same combination of data sources and Type of records. If so, then the application prompts an information message that the rule already contains the same combination of data source and object category and you must modify the existing combination to enable the rule.
   - A sample expiration rule is provisioned for the users in the base system and this **Sample Expiration Rule** for observable will be in disabled state by default and you must enable and activate the rule.

5. Click **Save**.
6. Click **Delete** if you wish to delete any expiration rule.

Expiration rules for source records

Expiration rules are basically helpful to set the expiration time for the source records. The aggregate record inherits the highest expiration time from its corresponding sources records.

How the rules are applied

Example: Incoming source record type is Malware from the data source type as CrowdStrike

Rule evaluation process based on the rules provided for applying expiration times to source records:

1. **Fetch all the enabled rules:** The application starts by verifying all the rules that are currently enabled.
2. Check for specific rule combination:

   Look for a rule that specifically matches the combination of:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Data Source type**: CrowdStrike
- **Type of Records**: Malware

3. **Priority based on the matching rule combinations:**

   If there exists a rule where the data source type is **CrowdStrike** and the record type is **Malware**, this rule takes the precedence. The expiration time specified in this rule will be applied.

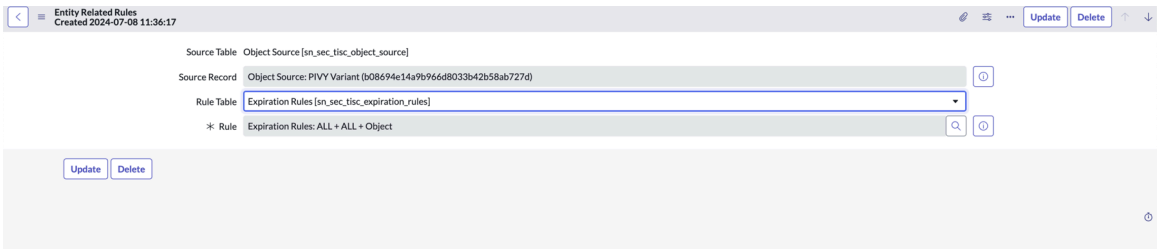
4. **Fallback rules:**

   a. If no rule matches the **CrowdStrike and Malware** combination, then the system checks for a rule where the data source type is **CrowdStrike** and the record type is **All**.

   b. If still no rule is found, it then looks for a rule where the data source type is **All** and the record type is **Malware**.

   c. Finally, if none of the above rules exist, it defaults to a rule where both data source type and record type are **All**.

5. If none of these rules exist in the system, then no expiration rule will be applied to the source records. In that case, navigate to the below table (shown in the screenshot) to check the combination of rules that were applied to the objects.



6. **Deletion of data sources:**

   Suppose, if a data source that has the expiration rules associated with it is deleted, then the deletion may be restricted or not allowed until these rules are addressed. This ensures that there are no inconsistencies in the application of expiration policies.

Create Inbound Data Exclusion Rules

Create inbound data exclusion rules in order to filter any type of data or any kind of incoming source records data.

Before you begin

The application supports the integration of multiple threat intelligence feeds, including STIX data sources. To ensure that only relevant data is ingested, customizable exclusion rules must be applied.

Role required: sn_sec_tisc.admin

About this task

Exclusion rules are created and applied on a source record to process further steps. The base system provides the **Sample Filtering Rule** for the users with a predefined rule to filter the ingested observables, indicators data, or entities/objects.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Drill down to **Rules Engine** > **Inbound Data Exclusion Rules**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **New** to define exclusion rules.
   The Create New Inbound Data Exclusion Rules page is displayed.
4. On the form, fill in the fields.

Define Exclusion Rules

Field	Description
Name	Name of the new exclusion rule.
Description	Short description of the exclusion rule.
Order	The exclusion rule priority. This field indicates the order in which the exclusion rules are executed when two or more rules share the triggering conditions. The exclusion rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, and so on. The default value is 100 for the base system exclusion rule.
Data Sources	Select the feeds for which the exclusion rule should be applied.
Table	Select the type of table that you would want to apply the filter for. For example, Observable Source, Indicator Source, and Object Source.
Filter Type (only when Table selected is Observables Source)	Filter types contains two options based on which you can apply the filter. ○ Filter based on Condition ○ Filter based on List
Filter Type (Filter based on Condition)	Filter conditions in the condition builder. These conditions are based on the source table. For example, Indicator Source and Object Source has only filter type: Filter based on Condition. To add more conditions, click **AND** or **OR**. If **AND** is selected, all conditions must be matched. If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Condition set**.
Filter Type (Filter based on List)	If the inbound observables matches against the entries in the list selected will be filtered. **Note:** These exclusion rules doesn't apply for Data Imports using the import Intelligence and the available options are Allow list, Deny list, and Watch list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The records excluded by the exclusion rule can be viewed in the following sections.

a. **Filtered Observable Records**: Filters and lists the observables records.

b. **Filtered Indicators Records**: Filters and lists the indicators records.

c. **Filtered Object Records**: Filters and lists the object records.

Note: In order to apply the exclusion rules based on tags which are added to the source records, then select *TISC* **tags** option in the Filter conditions builder.

Custom Threat Score Calculator in TISC

Custom Threat Score Calculator allows you to define and calculate a threat severity score of an observable based on the user defined criteria which provides a transparent intelligence scoring of observables. The threat score is auto calculated for observable records.

Define Threat Score Calculator

Define threat score for the observable(s) records that are generated based on the user defined parameters. The base system is provisioned with one threat scoring rule, which can be customized and enabled accordingly.

Before you begin

Role required: sn_sec_tisc.admin

Note: By default, the threat scoring rule will be inactive, you need to enable the rule to see the observables scoring.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Go to **Threat Scoring Rule**.
   The Threat Score Calculator page is displayed.

Important:

- In the application, within the base system, there is one scoring rule which is provisioned for the users to view, edit, or modify the threat score but the user cannot either create a new rule or delete the predefined threat scoring rule.
- The changes will apply for any new observables or updates to the observables from that point onwards. To restate historical scores, they should use the recalculate option.

3. On the form, the following fields contains the predefined values.

Threat Score Calculator

Field	Description
Name	Name of the threat scoring value. For example, Threat Score Calculator.
Description	Description of the threat score record. For example, Calculates threat score based on weighted sum of predefined criteria scores.
Overall weightage (Applicable to criteria builder)	This field is not editable and displays the overall weightage calculated by the system based on the weight corresponding to enabled criteria.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Scoring Critera	Indicates the scoring criteria for an observable. Following are the two available options to define the threat scoring criteria: ○ **Criteria Builder**: Use this option to add, edit, or remove, and enable and disable criteria that contributes to threat score calculation and ensure that the total aggregated weightage is 100%. ○ **Use Script (Advanced)**: The scripting feature is an advanced feature to build a custom script that should return the threat score within the range of 0-100.

Below are the available options for defining the **Scoring Criteria**:

- Criteria Builder
- Use Script (Advanced)

Following is the procedure for Criteria Builder:

Note: You can edit or modify the existing criteria or add a new criteria.

a. Select the type of criteria.
For example, Add a New Criteria.

b. Select the **Table** for which the criteria is configured.
The list of values in the drop down list are Observables, Threat Actor, Campaign, Location, Identity, Vulnerability, Threat Event, Security Incident, and Aggregates. When you select one of these options from the drop down list, a condition is applied. This condition ensures that only records related to the selected value are displayed or calculated.

Note:

- If the selected Observable, then the condition will be applied on the observable record for which the threat score will be calculated. If the selected table is not Observable, the condition will be applied only if the records are related to the Observable for which the threat score will be calculated.
- An additional Aggregates table is added to define the scores based on the number of relations that are associated to the Observables. For example, select the Table: Aggregates and the field value: Threat Actors then for an observable, if there are more than two threat actors, then, set the score and apply the conditions as applicable.
- For example, if you want to set a score for one or more threat actors associated to an observable, then, select the field as No of Threat Actors and set the desired score and apply the conditions as applicable.

c. Select the **Field** from the above selected table.

d. Enter the **Weightage** of the criteria between 0-100.
The overall weightage of all the criteria should be 100%.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Enter the name and short description of the criteria.

f. Select the **Enable scoring criteria** check box to enable the scoring criteria.

g. Define the **Conditions** and set the score for the conditions.

h. You can also add new conditions using **New Condition** button, and delete the condition using the **Delete Criteria** icon.

i. Click **Add** to add the criteria configured.

Here is an example of defining a condition to a threat score:

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Click **Re-Calculate History** button to re-caculate the threat score.
If there are changes to the threat scoring rule then you must re apply the scoring rule to the observables which has the threat score already calculated in the past, use **Re-calculate history** button to trigger the re-calculation job.

Note:

- A confirmation message is displayed for you to perform the action, `This is long running process that runs in the background. You won't be able to make changes until the process is completed. Are you sure you want to run this action?`
- For any update events that are generating for observables as part of **Re-calculate History**, the processing of webhooks is disabled and in case if you want to enable then modify this system property `webhook_ignore_threat_score_reapply`.

5. Click **Ok**.

Important: This action will trigger a long running job and the system will not allow you to make any further changes to the threat scoring rule until the job completes. For more information on how background job configuration is configured, see Vulnerability Response background job framework configuration.

The following is the **Use Script (Advanced)** script: Use this script to build a custom script that should return the threat score within the range of 0-100.

The advanced script field is auto populated with a function which takes the parameters **current** and **aggregates** and this function should return the threat score in the range of 0-100.

Here, the current parameter is the GlideRecord object of the entity (observable) for which the threat score is being calculated. For the observables, it corresponds to the GlideRecord for

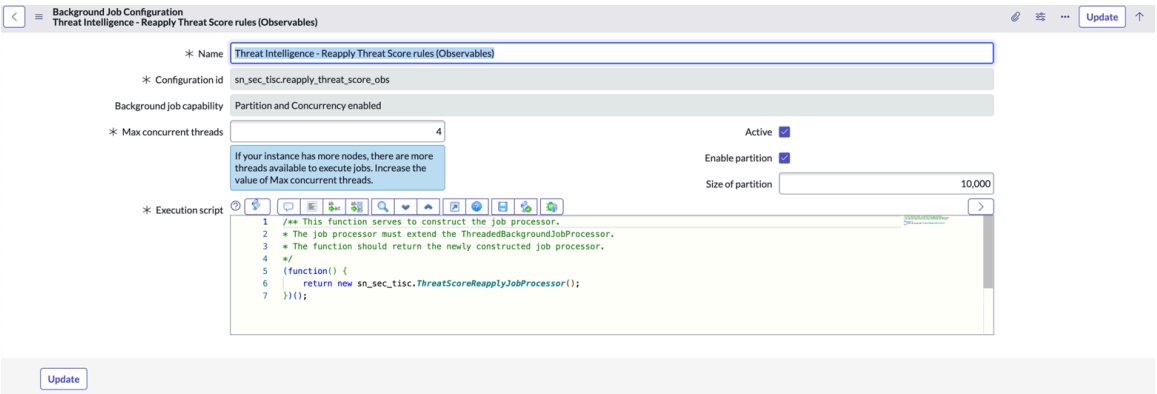
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the sn_sec_tisc_observable table. The aggregates parameter is a GlideRecord object of the sn_sec_tisc_aggregates table record which is used to access the record counts of the various associated record types (such as campaigns or identities) to the main entity (observable).

Sample example of the script in the advanced option:

```
answer = (function threatScoreCalculator(current, aggregates) {

    // return the threat score in the range of 0-100
    var threatSeverity = current.getValue("threat_severity");
    if(threatSeverity == "high")
     return 80;
    else {
        let associatedCampaigns =
 aggregates.getValue("num_of_campaigns");
        if(associatedCampaigns > 0)
            return 50;
    }
    return 0;

})(current, aggregates);
```

For your reference, below is the screenshot that shows you the threat score background job configuration process.



MITRE ATT&CK Technique Extraction Rules

Extract MITRE techniques automatically from observables or objects ingested from various data sources and also extract MITRE techniques from threat lookup results on observable record.

Before you begin

Role required: sn_sec_tisc.admin

Note: Make sure to verify that the MITRE ATT&CK repository data available in the instance that you are using. If the data is not available then the application will not perform the extraction.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Go to **Rules Engine** > **MITRE ATT&CK Technique Extraction Rules**.
   The MITRE ATT&CK Technique Extraction Rules page displays.
3. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Enter a name for the MITRE ATT&CK Tech nique Extraction rule.
Description	Enter a description for the MITRE ATT&CK Technique Extraction rule.
Integration Type	Indicates the MITRE ATT&CK Technique Ex traction rule for the Data Sources or Threat Lookup Results. Select the list of data sources from the lookup. Following are the options available for Data Sources: ○ **Data Sources - All**: which means that the rule is applicable for all the type of data sources such as Threat Intel Feeds, Import Intelligence records, API Sources (for exam ple, observables created from API), Sent from SIR (observables that are sent from SIR) and various entities that are manual ly created by the users in the Threat Intelli gence library. ○ **Data Sources - Threat Intel Feeds**: This cor responds to the extraction rules that are on ly applicable for threat intelligence feeds. ○ **Data Sources - API Sources**: This corre sponds to the extraction rules that are only applicable for API Sources. ○ **Threat Lookup integrations**: for this type of option, the extraction rule is applicable to all threat lookup integrations such as Virus total. **Note:** ▪ When you select this option, you must enter the vendor name for the threat lookup. The vendor names are automatically populated only when the threat lookup integrations are installed from ServiceNow store. ▪ For the threat intelligence data sources, the extraction rules are only supported for STIX, MISP, and Custom Feed types.
Threat Feed Type	Following are the options available for Threat Feed Type: ○ **STIX(TAXII/HTTPS)**: Option to filter the threat feeds of the STIX TAXII or HTTPS feed type and select the associated feeds from the lookup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **MISP**: Option to filter the threat feeds of the MISP feed type and select the associated feeds by searching using the lookup icon. ○ **Custom feed**: Option to filter the threat feeds of the custom feed type and select the associated feeds by searching using the lookup icon.
Feeds	Select one or more threat feed integrations for the selected feed type. **Note:** If this field is left blank then all the threat feed integrations for the se lected feed type will be automatically considered for the extraction.
Method to extract MITRE ATT&CK tactics and techniques	Option to select the extract MITRE ATT&CK tactics and techniques method. The two avail able methods are: **a.** Use Regex **b.** Use Script
Extraction Method - Use Regex	This method uses a regular expression that allows the threat analysts to define a pattern with a sequence of characters to perform ex traction method.
Tactic Regex	Option to provide regular expression for the extraction of MITRE ATT&CK tactic ID(s).
Technique Regex	Option to provide regular expression for the extraction of MITRE ATT&CK technique ID(s).
Extraction Method - Use script	This method uses a script format to perform the extraction on the observable source or object source or indicator source or threat lookup results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

	Note:
	○ This script method can be used to extract MITRE tactics and techniques from entity source record and link the tactics and techniques to the entity source record itself.
	○ This script method can be used to extract MITRE tactics and techniques from threat lookup results and link the tactics and techniques to the entity record.
	The sample script is shown below for your reference:
	`(function process(lookupResultRawData, recordGr, ruleGr, lookupResultGr) { /*********************************`
	`* - threatLookupResult: The raw data of the threat lookup result in stringified JSON format.`
	`* - recordGr: The GlideRecord of the observable record.`
	`* - ruleGr: GlideRecord of matched MITRE extraction rule`
	`* Once you extracted MITRE tactic IDs and technique IDs,`
	`* then you can use this method to link the tactics and techniques to the observable record.`
	`*********************************/`
	`var utils = new MITREExtractionUtils();`
	`var parsedRawData =JSON.parse(lookupResultRawData);`
	`var mitreDataField = parsedRawData.mitre_data;`
	`var response = utils.extractMITREDataUsingRegex(mitreDataField,'TA[0-9][0-9][0-9][0-9]','T[0-9][0-9][0-9][0-9].[0-9][0-9][0-9]');`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click **Enable** to enable the MITRE ATT&CK Technique Extraction rule after you create a new rule.
   If you don't enable the MITRE ATT&CK Technique Extraction rule then the rule will not be applied to the record.

   Note:

   a. Data sources: Whenever you enable the extraction rule, the combination of data sources and integration type should not be matching any of the existing enabled extraction rules, and if so then the application will display an error message for you to modify the existing combinations and re enable the rule.

   b. Threat Lookup: Whenever you enable the extraction rule, the vendor name should not be matching any of the existing enabled extraction rules, and if so then the application will display an error message for you to modify the vendor name and re enable the rule.

   c. A sample MITRE ATT&CK Technique Extraction rules are provisioned for the users in the base system and these rules will be in disabled state by default and you must enable and activate the rule.

Field	Description
Generic Rule for data sources ingestion	This is a generic rule for ingestion from all types of data sources including Import Intelligence and manual creation.
Generic Rule for Threat Lookup	This is a generic rule for any threat lookup integrations.

5. Click **Duplicate** to create a copy of the extraction rule.
6. Click **Disable** to disable the extraction rule.

   Note: Once it is disabled the rule will no longer be considered for the extraction of MITRE data.

7. Click **Save**.
8. Click **Delete** if you wish to delete any MITRE ATT&CK Technique Extraction rule.

MITRE ATT&CK Technique Extraction method

MITRE ATT&CK Technique Extraction method describes how the extraction methods are performed and associated techniques are verified.

1. The extraction rules for data sources (threat lookups are not applicable) are processed whenever an entity (for example, observable source or object source) source record gets created.
2. The rules are applicable for any fields within the entity source record (except date, number fields, and Usage category and Attack phases).
3. The extracted MITRE techniques are associated to the corresponding entity record and you view the records in the MITRE techniques related list in the **Related Records** tab.

   Note: The MITRE techniques are first extracted and associated to the entity source record then the techniques associations are de-duplicated and aggregated to the parent entity record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View MITRE techniques

1. Navigate to **Threat Intel Library**any entity (observable or object) record using the .
2. Click on the **Related Records** tab.
3. Select **MITRE Techniques** and view the associated techniques which are extracted.
4. Click on the MITRE technique ID to view and access the MITRE technique association record. The **Sources** column displays all the sources (also separated by a comma if there are one or more sources) which are associated to the entity source record on which the MITRE extraction is performed.

   Note: If the same tactic and technique IDs are extracted from multiple sources then only one tactic and technique association record is displayed and the **Sources** column displays all the extracted sources.

5. For troubleshooting, you can view the MITRE Extraction rule which was responsible for extraction of the tactic and technique associations by navigating to the **Technique Source Relations**.

   Note: Make sure to add the **Extraction Rule** column using the **List Actions** icon in case if you don't see the Extraction Rule column.

The extraction rules for threat lookups are processed whenever the threat lookup result record is created for any observable for which **Run threat lookup** action is triggered and the extraction is performed only on the raw data (raw_data field) payload which is available in the threat lookup result record.

Note:

- If there is no tactic ID present in the extracted entity (observable or object) source or threat lookup result for any MITRE ATT&CK technique, then the technique associations are created for all the tactics that are associated to the corresponding technique in the MITRE repository.
- If there is any tactic ID present in the extracted entity (observable or object) source or threat lookup result for any MITRE ATT&CK technique, then the technique associations is specifically created only for all that extracted tactic(s) that are associated to the corresponding technique in the MITRE repository.

Configure Tagging Rules in TISC

Use tagging rules to automatically assign tags and taxonomies to RSS feeds. Tagging rules evaluate incoming feed data based on defined criteria and apply the appropriate tags and taxonomies when a match is found.

Before you begin

Role required: sn_sec_tisc.admin

About this task

Tagging rules are available from the **Administration** module and these tagging rules are supported for RSS feeds only.

Each tagging rule consists of matching criteria that TISC evaluates against incoming feed items, and a set of tags and taxonomies that TISC applies when all criteria are satisfied. When multiple tagging rules apply, all tags and taxonomies will be aggregated accordingly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Rules Engine** > **Tagging Rules**.

The Tagging Rules list view displays all the existing tagging rules with the following fields.

Tagging Rules list view columns

Column	Description
Name	The display name of the tagging rule.
Table	The table name for the tagging rule is **RSS Feed** by default, and it is read-only.
Description	A brief summary of the rule's purpose.
Active	Indicates whether the rule is enabled or disabled. Only active rules are evaluated during feed processing. **Note:** This appears in the list view and is tagged to the tagging rule name in the form view, indicating whether it is enabled or disabled.
Method to Match	The keywords to match against the selected fields. Matching is case-insensitive by default. When defining a tagging rule, you must specify the keywords that the application will use to match against the fields you have selected. The matching process is case-insensitive by default, ensuring that matches are found regardless of letter casing. There are two available matching options for evaluating feed items: ○ **Keywords**: Allows you to specify one or more keywords that the system will search for within the selected fields. By default, the option is Keywords. ○ **Regex**: Enables you to define regular expressions for more complex matching criteria within the feed data. Choose the most appropriate matching method based on the complexity of your tagging requirements.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The following are the two base system tagging rules provisioned in the application for the RSS feeds. By default these two tagging rules are disabled, select **Enable** to enable the rules and proceed to next step.

Base system tagging rules

Field	Description	Table	Method to Match
Sample Tagging Rule	This is a sample tagging rule.	sn_sec_tisc_rss_feed	Keywords
Tag RSS Feeds with Zero Day mentions	This tagging rule is used to automatically associate the Vulnerability Intelligence: ZERODAY taxonomy with RSS feed records based on matching keywords found in the RSS feeds.	sn_sec_tisc_rss_feed	Keywords

3. Select **New** to create a tagging rule, or select an existing rule name to edit it.
   The Create New Tagging Rule form view opens. The form is divided into the following sections.
4. In the **Details** section, fill in the basic configuration fields.

Rule details fields

Field	Description
Name	A unique, descriptive name that identifies the tagging rule.
Description	Optional text that documents the purpose or scope of the rule.
Table	The table name for the tagging rule is RSS Feed by default. **Note:** As tagging rules are supported only for RSS feeds, the table name is read-only.
Fields	Select the fields that the tagging rule will match on. For example, you can choose fields such as **Description**, **Notes**, or **Title** of an RSS record. The available fields are displayed in a multi-select list that includes columns from the RSS table. Select one or more fields based on your requirements. This matching is evaluated using the defined condition across the selected fields. The rule is considered a match when a keyword is found in any of the selected field. For example, if **Notes** and **Description** are selected, then the rule triggers when a match is detected in either of the selected field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Select one or more keywords to match against the selected fields. Separate multiple keywords with commas. Each keyword is evaluated independently during matching. **Note:** ○ The application checks whether any specified keyword is present in the values of the selected fields such as the content of the **Notes** or **Description** fields of an RSS record. If a match is found, the configured TISC tags and taxonomies and taxonomy values are automatically applied to the record. ○ The matching criteria support the following field types: **String**, **HTML**, **URL**, and **JSON**.

5. Select the required Trigger Type.
Use the **Trigger type** options to define when the rule runs. These options determine when the **TISC tags** and **taxonomy** values are associated with an RSS record.

Field	Description
Run on insert	Select this check box to run the rule when a new RSS feed record is inserted.
Run on update	Select this check box to run the rule when an existing RSS feed record is updated.

Note: **Activity stream**: This section displays the changed history of the record. Auditing is enabled to track the updates to these fields for execution, review, and troubleshooting.

6. In the **Match criteria** section, define the conditions that a feed item must satisfy for the rule to apply.

Match criteria fields

Field	Description
Method to Match	Matching is case-insensitive by default. The available matching options are: ○ Keyword(s) ○ Regex Select the required option. The following section describes each matching option in detail. Refer to the descriptions as needed when configuring rules. To configure the case sensitivity, update the `sn_sec_tisc.case_sensitivity_for_tagging_rules` system property as needed.
Keyword(s)	Select one or more keywords to match against the selected fields. Separate multiple keywords with a comma.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Regex	Select this option to add the condition using a regular expression (Regex). When selected, the **Regex** field is displayed allowing you to enter a regular expression to match against the specified fields. For example, .*cve-[0-9].*
Trim padded spaces for keywords	Select this check box to trim the leading and trailing spaces from keywords. When selected, the application automatically removes spaces entered before or after each keyword. For example, if extra spaces are included around a keyword, those spaces are ignored during matching. If this check box is not selected, spaces are preserved and treated as part of the keyword. This allows you to control how precisely the match is evaluated. **Note:** Only one regular expression can be provided.

7. In the **Add TISC Tags & Taxonomies** section, select the tags and taxonomies to apply when the rule criteria are met.

Add TISC Tags & Taxonomies fields

Field	Description
Tags	Select one or more TISC tags to apply when the rule condition is met.
Taxonomies	Select one or more taxonomy values to apply when the rule condition is met. Select a taxonomy and specify the corresponding taxonomy values to apply when a match occurs.

8. Select **Save** to save the tagging rule.
9. Select **Enable** enable the tagging rule.

Note: Once you enable the rule, the tagging rules form view will be in the read-only mode. You need to disable the tagging rule to edit the form view. The tagging rule execution is asynchronous.

10. **Optional:** Select **Duplicate** to copy an existing rule.

(Optional) A confirmation message is displayed indicating that the current tagging rule has been duplicated and a new rule has been created with a unique name.

Note: When you copy an existing rule, the application creates a duplicate entry that retains all the field values from the original rule. The copied rule is created in a **disabled** state by default, allowing you to review or modify it before enabling the rule.

Trouble?

To view the result of the execution:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The application evaluates the RSS feed record against the rule conditions.
- If a match is found:
  - Configured tags and taxonomies values are automatically associated with the RSS feed record.
  - A work note entry in the activity stream is added to record the action. The work note on the activity stream includes the following details:
    - Tagging rule name
    - Applied tags
    - Applied taxonomy values

If multiple rules are triggered, each rule appears as a separate row. When multiple tags and taxonomies values are applied by a single rule, they are listed as comma-separated values with tags and taxonomies separately applied by each tagging rule. When multiple tagging rules utilize the same tags or taxonomies values, the application ensures that duplicate tags and taxonomies are automatically managed. This prevents the same tag or taxonomy from being applied more than once to an RSS Feed record.

Automated creation of zero day vulnerability

A zero day vulnerability scenario demonstrates how TISC detects and manages vulnerabilities that have not yet received CVE assignments.

Role required: sn_sec_tisc.admin

This feature enables automatic detection and processing of zero day vulnerabilities through configurable tagging rules. For more information, see Configure Tagging Rules in TISC.

Prerequisite:

Verify that the **RSS Feeds with Zero Day mentions** tagging rule is enabled. This ensures automatic association of the RSS Feeds with the **Vulnerability Intelligence: ZERODAY** taxonomy.

Zero Day Vulnerability Processing - Vulnerability Source Record Creation

Zero Day Vulnerability Processing - Vulnerability Source Record Creation.

A Vulnerability Source record is automatically created when:

- an RSS feed record is associated with a specific Zero Day taxonomy value.
- an RSS feed which is associated with the zero day taxonomy is updated and contains new entities such as CWE IDs, CVE IDs, CPEs, or Product IDs.

Record identification: Each Vulnerability Source record is uniquely identified using the RSS feed GUID, ensuring traceability to the original source.

The processing layer creates a zero day vulnerability record for the corresponding vulnerability source record, only when the vulnerability record doesn't exists.

TISC automatically populates the following fields of Vulnerability Source and Vulnerability record:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Combination of RSS feed GUID and timestamp.
Description	Indicates the record is created from the RSS feed, including the GUID reference.
Zero day flag	Set to **True**.
CVE ID	Populated when exactly one CVE is identified.
Additional Context	Includes extracted CVE IDs and Product IDs.

The following entities are extracted from RSS feeds:

- CVE IDs (vulnerabilities)
- CWE IDs (weaknesses)
- CPEs and Product IDs (affected products)

For more information about the extraction and correlation mechanism, see KB2936701 article.

About Security Control Lists in TISC

Security Control Lists (SCLs) are predefined classification list that helps the Threat Intelligence Analysts determine how observables should be treated within the application and across security tools.

Threat Intelligence Analysts can categorize the observables by adding them to specific security control lists such as allow list, deny list, or watch list.

The categorization of observables into security control lists enables automated decision-making and filtering throughout the TISC.

The following lists describes the various methods for using the SCLs categorization to filter observables:

- Applying inbound filtering rules to filter out observables based on security control lists, typically against the allow list.
- Exporting data from the observable lists of the threat intelligence library.
- Sending observables for blocking or unblocking in firewall tools that are integrated with TISC.
- Sending observables to monitor SIEM integrated applications with TISC, specifically against the watch list category.
- Using automation flows and email notifications such as not notifying the analysts during ingestion if the observable is in the deny list.
- Filtering based on these fields when using the TISC API for integration.

Defining Security Control Lists

Use this feature to add or remove observables in bulk.

Before you begin
Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Go to **Security Control Lists**.
   For example, adding observables to allow list then go to Allow list option.
3. Select **Allow List**.
4. Select the Observables type such as IP Address, File and so on to add to the allow list.
5. Click **Add**.
   The **Select Observables For Allow list** is displayed.
6. Select all those observables that are required to be added to the allow list.
7. Click **Add to Allow List**.
   The selected observables are added.
8. Similarly, select **Add to Deny list** to add the observables to the removed list.
9. Select **Add to Watch list** to add the observables to the watch list.

   Note: You can directly add the observables to allow list, deny list, or watch list directly from the Observables form view page, which are available above the form banner.

10. To verify, navigate to **Threat Intel Library**.
11. Select the observable type that was added to the allow list.
    The observable is indicated as added to allow list.

    Note: Allow list and deny list are mutually exclusive and the system will automatically ensure that an observable in allow list is not part of deny list and vice-versa.

Creating Taxonomies

Create taxonomies for the data source records.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration** > **Taxonomies**.
2. Click **New**.
3. Enter the **Name**.
4. Enable or disable the taxonomy **Status** using the form actions Enable or disable.

   Note: Disabled taxonomies will not be available for selection of any records where taxonomies are applicable.

5. Go to **Taxonomy Values** section to add taxonomy values.
6. Click **New** to open new taxonomy value form view and Enter the **Taxonomy** and **Value**.
7. Click **Save**.
8. For example, navigate to **Threat Intel Library** > **Observables** to verify the taxonomies for the observables record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Navigate to **Tags and Taxonomies** section in any observable form page and select the newly created taxonomy.

> **Note:** You can also add tags and taxonomies from the list view of the Threat Intel library.

Bulk import Taxonomies

Import the taxonomy records.

Before you begin

Role required: sn_sec_tisc.admin

About this task

You can import the taxonomies using the data from the spreadsheet. This enables you to import multiple records in bulk.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration** > **Taxonomies**.
2. Select **Import** button.
   This action opens an action to import the data file in XLSX or CSV format. you can also download the sample file to understand the format to import. The file format contains two values which includes Taxonomy and Taxonomy Value.
3. Click **Add file** link.
4. Select the file and **Upload**.
5. Click **Done**.
   A confirmation message displays that the data from the file attached are imported successfully. You can click on the link to view the import summary. By clicking on the link, the record opens in a new tab. You can view the count of taxonomies and taxonomy values created and if there are any errors that are logged it then it will be logged in the import errors section.

   > **Note:** By default, all these taxonomies and taxonomy values are created with the status as enabled. If you want to disable, then you can always do it from the list view.

6. On the **Taxonomies** page, you can click on any record, this action will show the taxonomy values as a separate tab and you can see the two taxonomy values which are imported successfully, and these taxonomy values will be in the enabled status.
7. Also, to view any of the taxonomy imports, you can always navigate to the **Imports** section, the imported taxonomies are displayed under **Taxonomy Imports** section.
8. Click **All Imports** to view all taxonomy imports created by different users in the application.
9. Click **My Imports** to see the taxonomy imports for the current logged in user.

Managing the Threat Lookup Reputation Calculator

You can use the Threat Lookup Finding Calculator to calculate the observable findings based on the responses received from threat lookup vendor.

You can create a Threat Lookup Finding Calculator for your integration and use a script to determine how you want to identify the various observable findings. The Threat Lookup Finding Calculator includes a sample script that comes with the base system, which you can use to identify the observable findings or you can modify this script according to your requirements.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For third-party integrations that provide the computed results, the Threat Lookup Finding Calculator maps the results to supported findings in the base system.

Rollup Threat Lookup Results

When you have multiple threat lookup results for an observable from the various integration vendors, then the recent threat lookup results from all the vendors are considered, and the overall observable findings are marked as follows:

Rollup Threat Lookup Findings

Latest Observable Finding	Overall Observable Finding
Malicious	If one of the integration vendors reports the observable as Malicious, then the overall observable finding is marked as Malicious.
Suspicious	If none of the integration vendors report the observable as Malicious, one of them reports it as Suspicious, and then the overall observable finding is marked as Suspicious.
Clean	If all the integration vendors report the observable as Clean, then the overall observable finding is marked as Clean.
Unknown	If none of the integration vendors report the observable as Malicious or Suspicious and one of them report it as Unknown, then the overall observable finding is marked as Unknown.

View Threat Lookup Reputation Calculators

You can view the Threat Lookup Finding Calculator to determine how reputation of observable is calculated based on response from specific threat lookup vendor.

Role required: sn_sec_tisc.admin

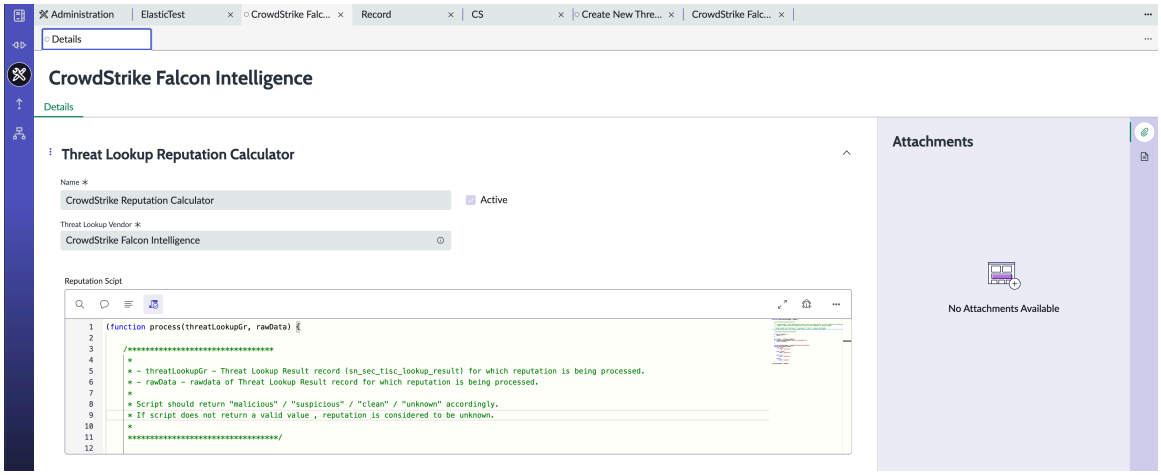
To view the Threat Lookup Reputation Calculator, perform the following steps:

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Select the **Threat Lookup Reputation Calculator** section.

   You can view the list of Threat Lookup Reputation Calculators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click on the required Threat Lookup Reputation Calculator to view the details of the calculator.



Create Threat Lookup Reputation Calculator

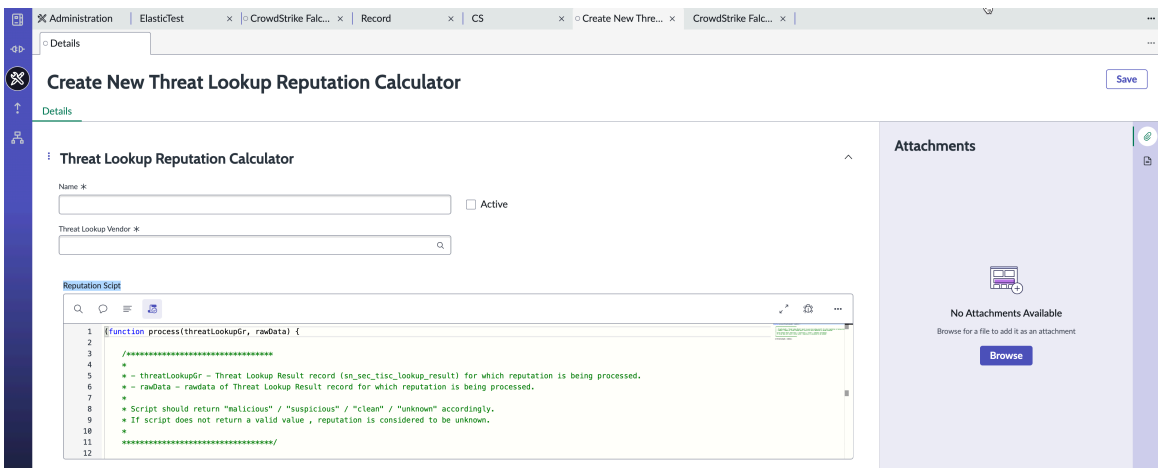
Role required: sn_sec_tisc.admin

Note: Only one threat lookup calculator can be active at any point of time per Threat lookup vendor.

To create a Threat Lookup Reputation Calculator, perform the following steps:

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Select the **Threat Lookup Reputation Calculator** section.

   You can view the list of Threat Lookup Reputation Calculators.
3. To create a Threat Lookup Reputation Calculator, click **New**.



4. On the form, fill the fields.

Create a Threat Lookup Reputation Calculator

Field	Description
Name	Name for the Threat Lookup Reputation Calculator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Active	Threat Lookup calculation runs only if Active option is selected.
Threat Lookup Vendor	Name of the Threat Lookup vendor. For example, `CrowdStrike Falcon Intelligence`.
Reputation Script	Script editor to determine how you want to identify the various observable findings. Every threat lookup integration comes with a base script for calculating threat lookup reputation.

5. Click **Save**.

Manage email Notifications

Use ServiceNow Notifications to create and manage system email notifications, and view email logs.

Email Notifications

Use email notifications to send selected users email notifications about specific tasks within the application, such as updates to observables/indicators/various other objects.

Role required: admin

Note: As a System Administrator you can view, create or edit the email notification rule details in the classic view of the application.

Threat Intelligence Security Center provides rules driven email notifications which are sent to individual email addresses or a list of email addresses. Usually, Dissemination of Threat Intel information to internal users are sent typically in the form of an email. The process involves in delivering the threat intelligence data to users according to their specified format and time lines.

Email notifications allow administrators to specify:

- When to send the notification
- Who receives the notification
- What content is in the notification

Note: If you want to make changes, then you need to configure whom the email should be sent by modifying the base system rules based on your requirements.

For more information, see Create an email notification section on ServiceNow AI Platform administration documentation.

The following table details the email notification rules that are provisioned in the base system.

Email Notifications

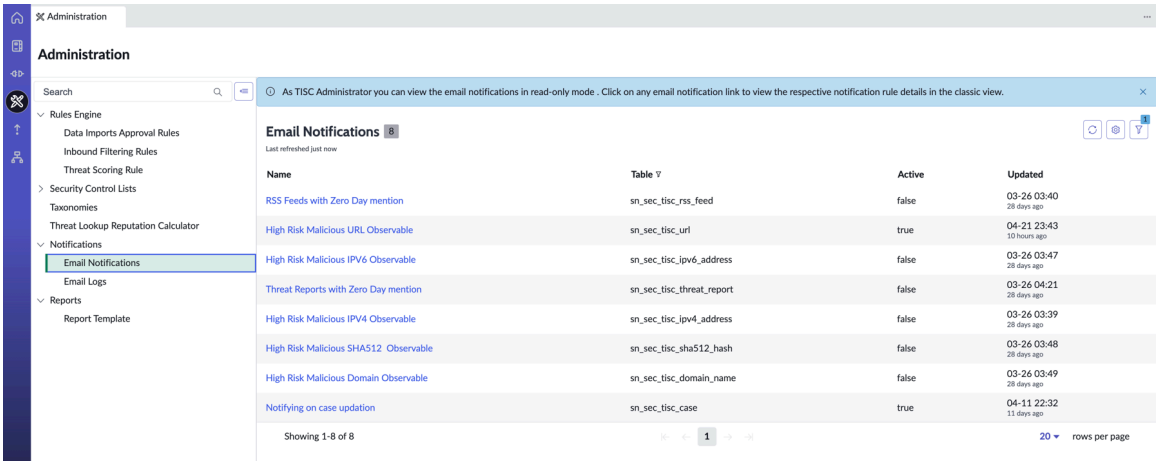
Name	Table
RSS Feeds with Zero Day mention	sn_sec_tisc_rss_feed
High Risk Malicious URL Observable	sn_sec_tisc_url

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Email Notifications (continued)

Name	Table
High Risk Malicious IPV6 Observable	sn_sec_tisc_ipv6_address
Threat Reports with Zero Day mention	sn_sec_tisc_threat_report
High Risk Malicious IPV4 Observable	sn_sec_tisc_ipv4_address
High Risk Malicious SHA512 Observable	sn_sec_tisc_sha512_hash
High Risk Malicious Domain Observable	sn_sec_tisc_domain_name
Notifying on case updation	sn_sec_tisc_case

Email Notifications



Note: Clicking on each email notification will take you to the classic UI, so that you can take necessary actions such as viewing or editing or creating the notifications.

Email logs

This section provides a clear visibility to the TISC administrators on the emails that are sent out using the configured email notification rules.

Email Notifications & Logs purview

TISC provides different purview to access, view, or modify both email notifications and logs based on different persona.

Note:

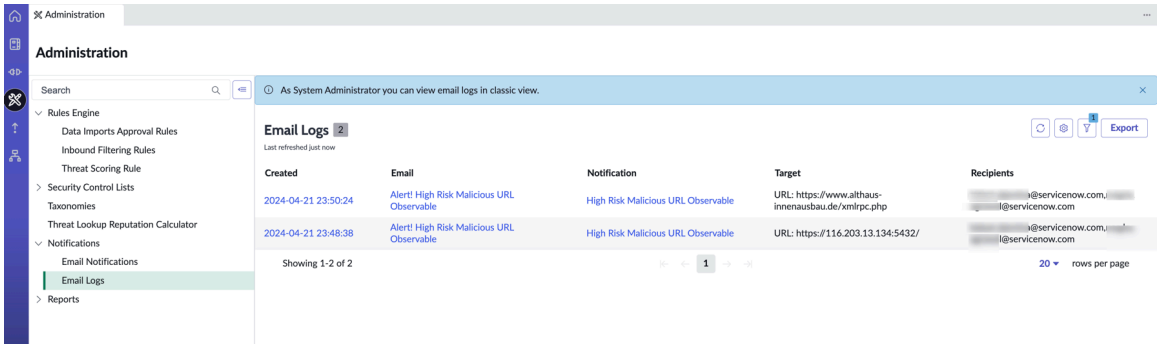
Persona	Access levels
TISC admin (sn_sec_tisc.admin)	As an sn_sec_tisc.admin, you can only view the email notifications that are configured for TISC. **Note:** Click on the email logs hyperlinks to navigate to the classic UI to view these notifications.
System administrator (admin)	As an admin, you can create, view, and edit the notifications in the classic UI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Persona	Access levels
	Note: Click on the email logs hyperlinks to navigate to the classic UI to view and create these notifications.

Note: Both TISC admin and system admin can use the filters and search for the email logs.

Email Logs



Report Templates

Defines the ability to re use the report templates that can be shared within the group of users to generate reports quickly and consistently.

Use this feature to create different types of report templates, which can be applied to case(s) that provides the status of ongoing investigation in relevance to any threat to your organization, and helps in generating reports of the same.

This section explains how to implement CTI reporting at a case level and also provides both admin (template design) and analyst (runtime) experiences.

You can add custom case task form fields or related lists to the report template that are dot-walkable. In addition, you can format and configure the report based on your requirements using various report elements.

Role required: sn_sec_tisc.admin

The following table explains a few report templates that are provisioned within the base system.

Report Template

Name	Description
Case Status Report - Threat Actor Profile	The Report is designed to provide a status about ongoing case investigation related to a threat actor trying to understand the context and relevance of the threat to the organization, adversary behaviour and potential goals, IOC enrichment, associated malware and tools, Observed TTPs, difference from existing TTPs – net new capabilities, slight modifications, and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Report Template (continued)

Name	Description
Executive Summary	The Report is designed to inform senior decision makers about a particular risk. The focus is on executive audiences and in support of strategic problems explaining why and how, rather than what and when. Any technical details and appendices in support of long-form, narrative writing will not be included in this report.
Post Investigation Summary - Threat Actor Profile	The Report is designed to provide context and relevance of the threat to the organization; adversary behaviour and potential goals; IOC enrichment; Associated malware and tools; Observed TTPs; Difference from existing TTPs – net new capabilities, slight modifications, and so on.

Note: By default, these reports are in the published state and will be in read-only mode. As the report templates will be in the read-only mode, the users can't make any edits to the templates and the analysts will not able to generate the reports as the report templates will be disabled.

Create a new Report Template

Create a new case report template according to your business needs of your organization.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Reports** > **Report Template**.
   This section displays the templates available in the base system, and also the published templates. You can pick any desired template for you to work with the reports.

   Note: From this section you can also delete the templates, if required.

3. Click **New**.
4. Enter the name and description of the template.
5. Click **Save**.
   The Template Content section displays.

   Note: Whenever you create a new report template, the template will be in the draft state which means that the template creation is work in progress and any other user will not be able to view the report template until it is complete.

6. Expand the **Template Contents** to insert the desired fields in the Template body.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- The template that you're editing allows you to define the template body and select the required variables to add to the template editor section. The templates are supported with Rich text editor (RTE) so that you can control various functions available such as indentation, font size, create tables, add images, and various other formatting capabilities.
- You can also insert images to your report templates, for that you need to copy and paste the image directly to the template. When add an image then that image is uploaded as an attachment.
- You can upload or attach an image which is up to 698 pixels, if the image is above the defined size then it will be automatically adjusted to the original size. This restriction of pixel size will help the PDF report generation to display in a proper format and the images doesn't get truncated in the report.

7. Add the required elements of the case.
8. Click **Save Content** to save the contents of your new report template.
9. Click **Preview** to preview your report format and also to see how a report is generated when you generate any case report.

Note:

- **Case Fields**: Whenever you modify your report template(s), preview the contents added to the template. For example, when you are generating a case report and you would want to add a field called Short description then you can select that field from the Case fields, then that field is added as a variable in the report template. When a report is generated for the analyst then whatever is the case short description that description will be displayed in the report.
- **Records**: Within the report template, you can also add the related records of that particular case which are displayed as the artifacts of the case. For example, if you would want to see any malicious observables in the report from the observables related lists, you can add it to your report template. These related records are displayed in the table format
- **Scripts**: Whenever you would want to see the date and time of the report then you can add the **Current Date Time** scripts to your report template, and this will add the Report Created Date and Time.
- **MITRE ATT&CK**: This displays the MITRE card associated techniques in your report.

After you add all the required Case related fields to you report template, you need publish your report template.

10. Click **Publish** to publish the template.
A confirmation message is displayed whether you want to publish the report template.

Note: When you publish a report template then this template is enabled for all the users. In case if it is outdated, and you want to restrict the report viewing for the users then you can disable the published report, which means the report template will be hidden for the users. You need to re enable the published report for the users to see and use it until then it will be hidden from viewing.

11. Click **Delete** to delete the report template in case if you don't want that report template.
If you want to rename your report template, click **Edit** and modify the desired fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Edit a Published Report Template

Use this section to edit a published report template.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Reports** > **Report Template**.
3. Select the required report template.
4. Select **Edit** button which is displayed on the Report Template.

Note:

A confirmation message indicating that you're editing a published template and must republish the template to make it available under Case Reports. Do you want to continue editing? This means that you need to republish the edited template after making the necessary changes.

5. Select **Edit** in the confirmation dialogue box.
6. Make the necessary changes by adding the required content fields or related list.
7. Select **Save Content**.
8. Select **Publish** button to publish the changes.
   Once you publish the report template, a confirmation message is displayed indicating that the report template is published successfully.

Note:

- You can also preview the report template contents before publishing the report template.
- In case if you want to delete the report template, you can select **Delete** to delete the report template.

Duplicate a Report Template

Duplicate a report template if you want to add any incremental updates, then you can create a copy of the report template.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > > **Administration**.
2. Select **Reports** > **Report Template**.
3. Select the template.
4. Click **Duplicate**.
   The contents of the selected template are duplicated and copy of that template is displayed. The template will again in the Draft state, you can customize the contents, and then rename the template as required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Edit or modify the content of the copied template.

Note: You can also delete the report templates in case if you don't need them anymore and create new templates.

System properties for Reports

The system properties for reports are explained below.

Property	Description	Value
sn_sec_reporting.max_list_columns_allowed	Limit the number of columns which can be added when rendering lists in report pdfs. This will use the columns from the beginning from the view till the allowed limit.	5
sn_sec_reporting.report_default_style_object	Use this property to control css of free form fields, left panel, report lists.	(JSON object)
sn_sec_reporting.load_all_records	Loads all the records for the lists in the report created from a template. true - Load all records and false - loads specific number of records defined by sn_sec_reporting.reporting_list_records_count property.	False
sn_sec_reporting.reporting_list_records_count	Loads specific number of records in the report editor.	20
sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	Can choose whether URLs from lists will be defanged or not.	True
sn_sec_tisc.show_all_tactics_reporting	If true, shows all tactics (including the tactics which doesn't have any techniques associated to the case) for the MITRE lists rendered in the report.	False
sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	Sys ID of the email client template for the Case (sn_sec_tisc_case) table which will be used in share report.	b55e22c54324021060eee0ea78b8f2df
sn_sec_tisc.sn_sec_tisc_case.excluded_fields	Excluded fields of the case in the report/template menu options for substituting a field.	(List of all excluded case fields
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	This property is used to get the corresponding UI message record for the case fields label in the report/ template menu options.	sn_sec_tisc_case_reporting_ctx_menu_field_h

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Working with Webhooks

A webhook is an HTTP request, triggered by an event in the source system (TISC) and sent to a destination system (where the endpoint URL is present), with a payload of event data.

These webhooks in Threat Intelligence Security Center are useful to notify the destination application whenever the events occurs.

In TISC, you can do the following:

- Configure Webhooks
- Manage Triggers
- Retry mechanism
- Perform validation
- Manage subscriptions

System properties for Webhooks

The system properties for webhooks are explained below.

Property Name	Description	Type	Value
sn_sec_tisc.webhook_ignore_threat_score_reapply	Ignore webhook events triggered by threat score recalculate history.	True/False	True
sn_sec_tisc.webhook_max_event_batch_size	Maximum batch size of events to send as part of one webhook request. The batch size will be limited to 2000 even if a higher value is set in this property.	Integer	1000
sn_sec_tisc.webhook_retry_count	Number of times a failed request should be retried before marking it as error and moving on to next batch of events. The retry count will be limited to 10 even if a higher number is set in this property.	Integer	5
sn_sec_tisc.webhook_retry_interval	Number of seconds to wait before re-attempting a failed batch. This will exponentially increase based on the retry count. For example, if retry_count is 3 and retry_interval	Integer	30

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property Name	Description	Type	Value
	is 30, retries are fired after 30, 60, and 120s. The initial retry interval will be limited to 300 seconds even if a higher value is set in this property.		

Configure webhooks

Configure a webhook to subscribe to events in Threat Intelligence Security Center.

Before you begin

Role required: sn_sec_tisc.admin

About this task

TISC webhooks provides the capability to integrate with security tools such as SIEM. Users can then subscribe to various events related to different artifacts such as observables or indicators or malware or threat actors. TISC notifies security tools (such as SIEM) when a new threat intelligence is available or any existing threat intelligence data is updated or deleted in TISC.

For example, whenever a new observable is added in threat intelligence then a payload request is sent to the webhook URL configuration. This payload request usually collects the observable information and provides it as additional information to security tools (such as SIEM).

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Webhooks Configurations** > **Webhooks**.
   The Webhooks page displays.
3. Click **New**.

Field	Description
Name	Enter a webhook name.
Description	Add the description of the webhook.
Configuration Details	
Use REST message	Select **Use REST Message** check box if you need to use REST Message/REST Method functionality that is provided by ServiceNow AI Platform. If this check box is not selected, then the ap plication uses the endpoint provided in Web hook URL to send the event information. For more information, see Outbound REST web on ServiceNow AI Platform documentation.
REST message	Select the REST Message record from the list of REST message records which are already

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	configured in the instance. For more informa tion, see [illegible] on the ServiceNow AI Platform documentation. **Note:** The REST message and REST method fields are mandatory when you select the REST message.
REST method	Select REST Method from the list of available REST Methods configured for the selected REST Message. For more information, see [illegible] on the Service Now AI Platform documentation. **Note:** Only POST Rest methods are supported for webhooks.
Webhook URL	A webhook endpoint is a URL that receives webhook event notifications.
Authentication Required	Select this check box if the authentication is required. **Note:** This is only applicable when Webhook URL is being used to retrieve the data.
Authentication Type	The authentication type for the webhook. **Note:** As of now, only Basic authentica tion type is supported.
Username	Provide a username to your authentication type.
Password	Provide a password to your authentication type.
Headers to be passed with request	Any headers to be passed with the requests can be provided in Request Header Mapping. Header should be provided in key-value pair separated by colon(':'). Each header key val ue pair should be provided in a new line. For providing authentication parameters as head er values, enclose the required Authentica tion Label with '${' and '}$'. For example, user name:${Username}$.

4. Click **Validate and Save**.
   In case if your configuration details are incorrect then the system will automatically validate the connection if configuration details are changed and then the application will prompt a warning

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

message that the validation of the webhook is failed and you need to check the configuration details and modify it accordingly.

Note:

- For the validation of webhook, empty request payload is sent to the endpoint and the user needs to ensure that the endpoint sends successful response code (200) when the empty request is passed to the configured webhook endpoint.
- By default, any webhook that is created will be in disabled state, you need to enable the webhook and activate it. A sample webhook is provisioned in the base system as a reference to the users.

Subscribe Triggers

View the list of all the subscribed webhook triggers for the current webhook.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Webhooks Configurations** > **Webhooks**.
   The Webhooks page displays.
3. Select the webhook.
   The Subscribed Triggers section is displayed.
4. Click **Subscribe** button on the Subscribed Trigger section.
   The list view shows all the enabled webhook triggers in the instance.
5. Select the desired webhook triggers and click **Subscribe** on the Webhook Triggers dialog box.
   A confirmation message is displayed that the webhook is subscribed successfully to the selected trigger(s). From here, you can also directly create a new trigger and subscribe the webhook.

Note: You can also **Unsubscribe** the webhook from the selected trigger(s).

View webhook error logs

Use this error logs section to view all the audit entries which are marked as error in the status for a particular webhook.

Before you begin

Role required: sn_sec_tisc.admin

About this task

The audit logs enables the users to further investigate, debug the execution, and identify the root cause of the execution failure.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Webhooks Configurations** > **Webhooks**.
   The Webhooks page displays.
3. Select the webhook.
4. Go to **Error Logs**.
5. View the error logs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The list view shows all the error logs from one particular webhook.

6. Go to **Batch** column.
7. Click on any **Batch ID**.

> **Note:** Each error log is associated to a batch and using the batch ID (from the Batch column) you can view the associated batch record. Click on any of the batch ID and this will open in a separate tab. Each batch ID contains the webhook batch number, error message, response status code, retry count, actual payload data, and the list of events which will be sent to the webhook.

8. Click **Retry batch** to retry the failed batches.
   When you click on this button, this sends a request payload (of that particular batch information) to the configured webhook endpoint.

> **Note:** This action is available only for the batch records which has the execution errors or completed successfully and the records those are in retry state will be automatically retried.

View webhook batches

A webhook batch record is created for each webhook execution.

Before you begin

Role required: admin

About this task

In order to reduce the number of API calls sent to the webhook endpoints, batching of events is implemented in webhooks. For each webhook, if there are multiple events triggered almost during the same time, then all these events are sent as part of the same request to the webhook endpoint.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Webhooks Configurations** > **Webhooks**.
   The Webhooks page displays.
3. Select the webhook.
4. Go to **Error Logs**.
5. View the error logs.
   The list view shows all the error logs from one particular webhook.
6. Go to **Batch** column.
7. Click on any **Batch ID**.
   The Webhook Batch page is displayed.

> **Note:** All the batches are stored in the table `sn_sec_tisc_webhook_batch`.

Below is the sample payload format that the webhook end point receives:

```
{
    "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
    "events": [
        {
            "record": "Observable",
            "record_fields": {
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
                "is_false_positive": "false",
                "reputation": "malicious",
                "sys_updated_on": "2024-07-22T14:31:26.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
                "value":
"https://urlhaus.abuse.ch/url/2578255/",
                "confidence": "89",
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
                "name": "Observable Update",
                "type": "UPDATE",
                "trigger_time": "2024-07-22T14:31:26.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        },
        {
            "record": "Observable",
            "record_fields": {
                "is_false_positive": "false",
                "reputation": "malicious",
                "sys_updated_on": "2024-07-22T14:31:19.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
                "value":
"https://urlhaus.abuse.ch/url/2578264/",
                "confidence": "89",
```


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
                "name": "Observable Update",
                "type": "UPDATE",
                "trigger_time": "2024-07-22T14:31:19.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        }
    ]
}
```


Following table lists the batch payload structure and its attributes which will be sent to the users as webhook payload:

Parameters in Batch Payload	Type	Description
batch_id	String	Specifies unique identifier for a batch.
events	Array of Objects	Contains an array of events which are triggered as part of that webhook. Each event will contain the snapshot of the field values at the time of event generation and also contains the trigger information. **Note:** For more information on viewing the parameters in the event object, see Webhook Triggers.

Note:

8. Click **Retry batch** button to retry the failed batch.

Note: You can also trigger the retry batch for the completed batches.

Webhook Triggers

Webhook triggers are used to filter the threat intelligence entities that needs to be tracked for any event changes such as Create, Update, and Delete.

Before you begin
Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Webhooks Configurations** > **Triggers**.
   The Webhooks Triggers page displays.
3. Click **New**.

Field	Description
Name	Enter a webhook trigger name.
Description	Add the description of the webhook trigger.
Table	Select the table for the webhook trigger.
Trigger Type	Defines whether the configured webhook trig ger is either create/update/delete event on the specified table. **Trigger Fields**: This is displayed when you se lect the **Trigger Type: Update**. These are the list of fields on the record for which the update event needs to be tracked. If this is empty, then the event is considered for any field change on the record. For exam ple, if the trigger fields are **Confidence** and **Reputation** for the **Observables** table, then this trigger is considered only when confi dence or reputation fields are updated. **Note:** The fields selected in the Exclu sion Fields will not be available in the se lection of Trigger Fields. **Delete**: If the **Trigger Type: Delete** then the Ex clusion Fields is not visible.
Exclusion Fields	These are the set of fields which are excluded from the webhook trigger payload.
Filter Conditions	Optional conditions that can be applied to fil ter the match records for any event trigger. For example, if threat severity is high and the Trigger Type is defined as Update on the Ob servable Table, then only those observables that are changed and where the threat severi ty is high are sent to the webhook URL.

4. Click **Save**.
   By default, the trigger is created in the disabled state.
5. Click **Enable** to enable the trigger and this trigger will be available for the webhooks to subscribe.

   Note: Click **Disable** to disable the enabled trigger and disabling will unsubscribe all the associated webhooks from this trigger.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **View Sample Payload** to select the record.
   View the sample payload of that particular webhook trigger. Based on the selected table, those records from that specified table will be populated in the **Select Record** drop down list. Select the record to view the sample payload. The sample payload is shown in the JSON format. The fields in the payload are listed below.
7. Select the type of record from the drop down list.
   The payload will be automatically changed based on the record selected.


```
{
    "record": "Observable",
    "record_fields": {
        "additional_context": "This could be a potential
 malicious IP. ",
        "attack_phases": "Lockheed Martin: Command and
 Control",
        "author": "Anomali",
        "confidence": "50",
        "description": "This could be a potential malicious IP.
 ",
        "expiration_time": "2024-12-01T00:00:00.000Z",
        "first_observed": "2024-01-01T00:00:00.000Z",
        "first_seen": "2024-01-01T00:00:00.000Z",
        "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
        "is_defanged": "false",
        "is_false_positive": "false",
        "last_observed": "2024-01-01T00:00:00.000Z",
        "last_seen": "2024-01-01T00:00:00.000Z",
        "reputation": "suspicious",
        "source_count": "1",
        "status": "active",
        "sys_created_by": "SecCommon.System",
        "sys_created_on": "2024-06-04T00:00:00.000Z",
        "sys_id": "30526b0a436a02102164e0ea78b8f210",
        "sys_updated_by": "system",
        "sys_updated_on": "2024-06-15T00:00:00.000Z",
        "tags": "critical",
        "taxonomies": "MITRE: T121",
        "threat_level": "medium",
        "threat_score": "24",
        "threat_severity": "medium",
        "tlp": "CLEAR",
        "type": "ip_v4_address",
        "usage_categories": "APT",
        "value": "116.98.170.70"
    },
    "trigger": {
        "name": "Observable Update",
        "type": "UPDATE",
        "trigger_time": "2024-07-26T07:27:29.000Z",
        "trigger_fields": [
            {
                "field_name": "confidence",
                "previous_value": "30",
                "current_value": "50"
            }
        ]
```


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
        }
}
```

List of parameters in the trigger payload

Parameter in Trigger Payload	Type	Description
record	String	Specifies the record type such as Observable or Indicator.
record_fields	Object	Specifies the record fields snapshot when the event is generated. For list of supported fields, refer to the table in the below section.
trigger	Object	Specifies the matched trigger information.
trigger.name	String	Specifies the name of the trigger
trigger.type	String	Specifies the type of the trigger. Valid values are CREATE, UPDATE, DELETE.
trigger.trigger_time	Date (in ISO format with UTC timezone)	Specifies the time of the event occurred on the record.
trigger_fields	Array of Objects	This is available only for UPDATE trigger type. It specifies the list of trigger fields which got changed as part of the event occurred. The parameters inside **trigger_fields** are: ○ **field_name**: provides the field name which got changed ○ **previous_value**: provides the previous value of the field. ○ **current_value**: provides the current value of the field.

List of supported fields for Create and Update Triggers

Table	Column Name	Column Label
Campaign	aliases	Aliases
Campaign	description	Description
Campaign	first_seen	First Seen
Campaign	last_seen	Last Seen
Campaign	name	Name

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Column Name	Column Label
Campaign	objective	Objective
Indicator	additional_context	Additional Context
Indicator	attack_phases	Attack Phases
Indicator	author	Author
Indicator	confidence	Confidence
Indicator	description	Description
Indicator	expiration_time	Expiration Time
Indicator	first_detected	First Detected
Indicator	first_observed	First Observed
Indicator	first_seen	First Seen
Indicator	id	ID
Indicator	indicator_types	Indicator Types
Indicator	ioc_classification	IOC Classification
Indicator	last_observed	Last Observed
Indicator	last_seen	Last Seen
Indicator	name	Name
Indicator	pattern	Pattern
Indicator	pattern_type	Pattern type
Indicator	pattern_version	Pattern Version
Indicator	platforms	Platforms
Indicator	revoked	Revoked
Indicator	source_count	No of Sources
Indicator	spec_version	Spec Version
Indicator	status	Status
Indicator	tags	TISC Tags
Indicator	taxonomies	Taxonomies
Indicator	threat_level	Threat Level
Indicator	threat_severity	Threat Severity
Indicator	tlp	TLP
Indicator	usage_categories	Usage Categories
Indicator	valid_from	Valid From
Indicator	valid_until	Valid Until
Malware	aliases	Aliases
Malware	attack_phases	Attack Phases
Malware	description	Description

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Column Name	Column Label
Malware	executable_process_architectures	Process Architectures
Malware	first_seen	First Seen
Malware	implementation_languages	Implementation Languages
Malware	is_family	Is Family
Malware	last_seen	Last Seen
Malware	malware_capabilities	Malware Capabilities
Malware	malware_types	Malware Types
Malware	name	Name
Object (Common Object Fields)	additional_context	Additional Context
Object (Common Object Fields)	confidence	Confidence
Object (Common Object Fields)	expiration_time	Expiration Time
Object (Common Object Fields)	id	ID
Object (Common Object Fields)	revoked	Revoked
Object (Common Object Fields)	source_count	No of Sources
Object (Common Object Fields)	spec_version	Spec Version
Object (Common Object Fields)	status	Status
Object (Common Object Fields)	tags	TISC Tags
Object (Common Object Fields)	taxonomies	Taxonomies
Object (Common Object Fields)	threat_level	Threat Level
Object (Common Object Fields)	threat_severity	Threat Severity
Object (Common Object Fields)	tlp	TLP
Observable	additional_context	Additional Context
Observable	attack_phases	Attack Phases
Observable	author	Author
Observable	confidence	Confidence
Observable	description	Description
Observable	expiration_time	Expiration Time

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Column Name	Column Label
Observable	first_observed	First Observed
Observable	first_seen	First Seen
Observable	id	ID
Observable	is_defanged	Is Defanged
Observable	is_false_positive	Is False Positive
Observable	last_observed	Last Observed
Observable	last_seen	Last Seen
Observable	reputation	Reputation
Observable	source_count	No of Sources
Observable	status	Status
Observable	tags	TISC Tags
Observable	taxonomies	Taxonomies
Observable	threat_level	Threat Level
Observable	threat_score	Threat Score
Observable	threat_severity	Threat Severity
Observable	tlp	TLP
Observable	type	Type
Observable	usage_categories	Usage Categories
Observable	value	Value
Threat Actor	aliases	Aliases
Threat Actor	description	Description
Threat Actor	first_seen	First Seen
Threat Actor	goals	Goals
Threat Actor	last_seen	Last Seen
Threat Actor	name	Name
Threat Actor	personal_motivations	Personal Motivations
Threat Actor	primary_motivation	Primary Motivation
Threat Actor	resource_level	Resource Level
Threat Actor	secondary_motivations	Secondary Motivations
Threat Actor	sophistication	Sophistication
Threat Actor	threat_actor_roles	Threat Actor Roles
Threat Actor	threat_actor_types	Threat Actor Types
Threat Report	description	Description
Threat Report	name	Name
Threat Report	published	Published

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Column Name	Column Label
Threat Report	report_types	Report Types
Vulnerability	affected_software	Affected Software
Vulnerability	description	Description
Vulnerability	exploitation_status	Exploitation Status
Vulnerability	exploit_exists	Exploit Exists
Vulnerability	name	Name
Vulnerability	published	Published
Vulnerability	record_last_modified	Record Last Modified
Vulnerability	severity	Severity

Below is the list of system fields that are applicable which are in common for every entity, and these are supported in the Webhook Trigger Payload for Create and Update triggers.

- sys_id (Sys ID)
- sys_created_on (Created)
- sys_created_by (Created By)
- sys_updated_on (Updated)
- sys_updated_by (Updated By)

Note: For the Delete, only sys_id (Sys ID) is sent to webhook endpoint URL as part of the payload and other system fields are not supported.

List of supported fields for Delete Trigger

Table	Column Name	Column Label
Observable	type	Type
Observable	value	Value
Indicator	name	Name
Indicator	pattern	Pattern
Indicator	pattern_type	Pattern type
Indicator	valid_from	Valid from
Campaign	name	Name
Malware	is_family	Is family
Malware	name	Name
Threat Actor	name	Name
Threat Report	name	Name
Threat Report	published	Published
Vulnerability	name	Name
Vulnerability	severity	Severity

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure tooltips for nodemaps

Use this section to configure tooltips for node map relationships on the investigation canvas.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration** > **Nodemap Controls** > **Tooltip Configuration**.
2. Select the desired object from the list.
   By default, the following three records are provisioned in the base system.
   a. Observables
   b. Indicators
   c. Objects
3. Select **Observable** as an example record.
4. Add one or more values to the observable record, if required.
   Similarly add values to indicators and other objects.

   Note: Each object supports a maximum of six values.

5. Select **Save** to apply the changes.
6. Go to the **Investigation Canvas** section and select **Refresh** icon.
   The same values configured on the **Tooltip Configuration** page will be displayed on each node map.

Working with automated flows

Use these defined steps to learn how you can use the automated flows in TISC and its capabilities.

Create flows that run with TISC roles. In TISC the flows are created for the following:

- Automated IOC Enrichment
- Analyze, assess and disseminate on the IoC's related to threat
- Analyze, assess the IoC's related to the threat and create incident.
- Vulnerability Management Support.
- Zero-day vulnerability tracking.

Note: All the flows are templates which are shipped in draft state for the users to customize or copy according to their own needs.

Reusable Actions

Flow action	Description
Add Tag To Entity	Adding tag to an entity which supports it (observable/indicator/object).
Remove tag from entity	Removing tag to an entity which supports it (observable/indicator/object).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Flow action	Description
Check if IP address is in CIDR range	Checking if an IP address in inside a CIDR range.
Check if IP address is in range	Checking if an IP address is in between from and to range.

Automated IOC Enrichment

Learn how to automate enrichment of IOC's using flows when they match a certain criterion.

Before you begin

Role required:

- System Administrator (view, create or edit)
- sn_sec_tisc.admin (view)

About this task

Automate enrichment of IOC's triggers only when:

- the type of the observable is a domain name, IPv4 address, or IPv6 address.
- the observable is in a processed state.
- the observable does not have the tags enriched or Skip Enrichment.

Procedure

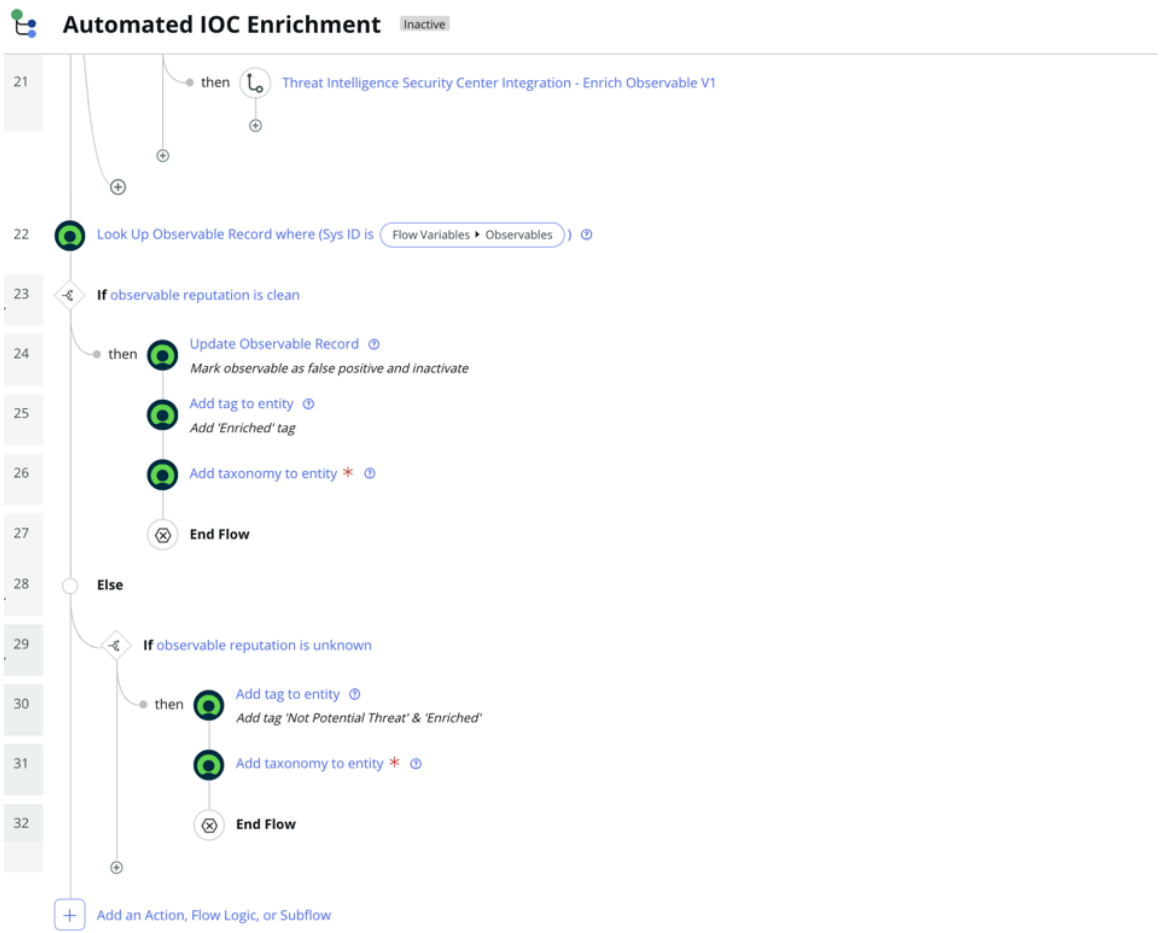
1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Automated Flows**.
3. Select **Automated IOC Enrichment** action link to view the respective rule details in the flow designer.
4. View the flow designer action for the following trigger:

```
Observable Updated where (Type is Domain Name, or Type is
 IP address (V4), or Type is IP address (V6); and Processing
 Status is Processed; and TISC Tags does not contain Enriched,
 or TISC Tags does not contain Skip Enrichment, or TISC Tags
 does not contain Potential New Threat)
```

5. **If the observable is an IPv4 or IPv6 address and it falls within an allowed CIDR range, then:**
   a. Add the observable to Allow List.
   b. Update the observables tags to Skip Enrichment.
   c. End the flow for this observable.
6. **Else, enrich the observable data with available capabilities:**
   a. Perform threat lookup and sighting search to gather additional information about the observable.
   b. Update the observable with enriched data.
   c. Add a tag **Enriched** to indicate that the IOC has been processed.
7. **Also, if the observables reputation is clean, then:**
   a. Mark observable as false positive and inactivate.
8. **Else, if observable reputation is unknown**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Add tag **Not Potential Threat & Enriched** to indicate that it is not a threat.



Analyze, assess, and disseminate observables

Learn how to analyze and disseminate observables which are related to threat.

Before you begin

Role required:

- System Administrator (view, create or edit)
- sn_sec_tisc.admin (view)

About this task

Whenever a sighting search enrichment is requested, it returns with no sightings.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Automated Flows**.
3. Select **Analyze, assess and disseminate on the IoCs related to threat** action link to view the respective rule details in the flow designer.
4. View the flow designer action for the following trigger:

```
Sighting Created where (Sighting count is 0)
```

5. **The observable has a threat score greater than 80, confidence greater than 80 and reputation is malicious:**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Add the observable to deny list.

b. End the flow for this observable.

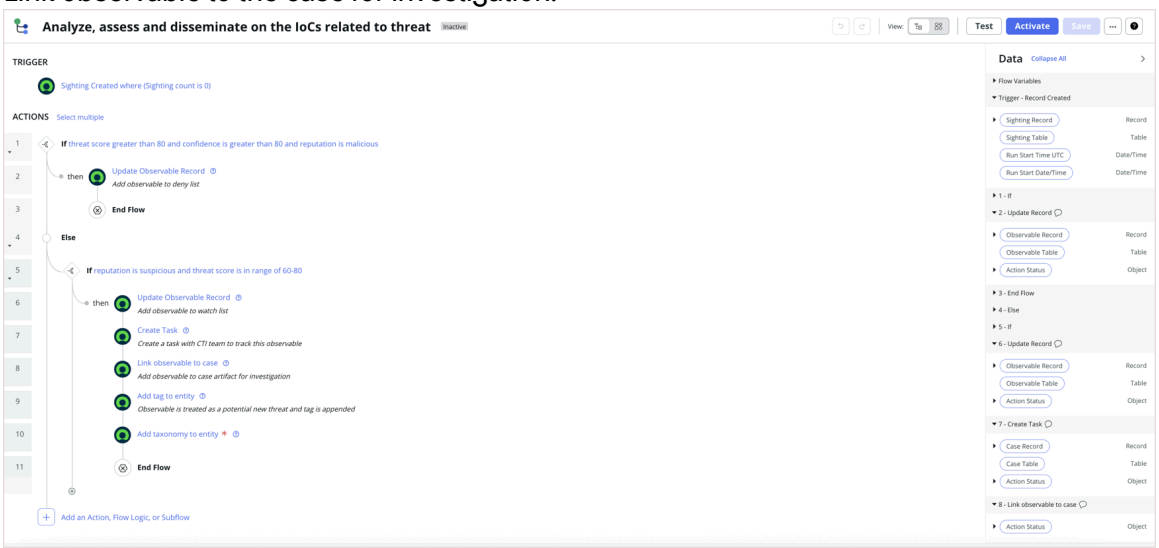
6. **Else, the observable reputation is suspicious, and the threat score is in the range of 60-80:**

a. Add a tag called Potential New Threat.

b. Add the observable to watch list.

c. Create a case task with CTI team to track this observable and analyze further.

d. Link observable to the case for investigation.



Analyze and assess threat IoC's

Learn how to analyze an IOC's which are a threat and notifying the security incident team.

Before you begin

Role required:

- System Administrator (view, create or edit)
- sn_sec_tisc.admin (view)

About this task

Whenever a sighting search enrichment is requested:

- if the observable is sighted (count > 0) and
- Observable Reputation is Malicious and
- Observable Threat score is > 80 and
- Observable Confidence > 80

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Automated Flows**.
3. Select **Analyze, assess the IoCs related to the threat and create incident** action link to view the respective rule details in the flow designer.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. View the flow designer action for the following trigger:

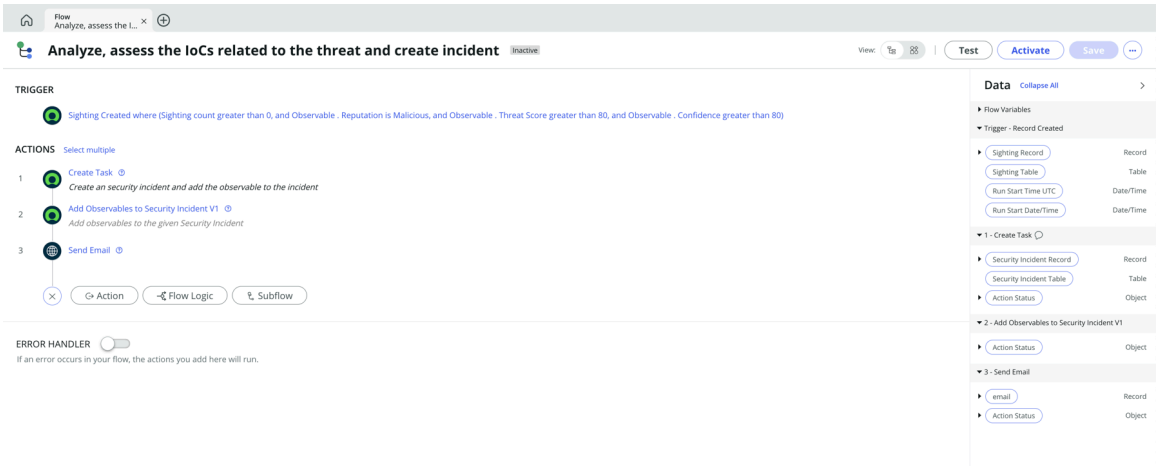
```
Sighting Created where (Sighting count greater than 0, and
 Observable. Reputation is Malicious, and Observable. Threat
 Score greater than 80, and Observable. Confidence greater than
 80)
```

5. **If Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80), then:**

   a. Create an security incident and add the observable to the incident.

   b. Add Observables to Security Incident V1.

   c. Send an email communication.



Vulnerability Management Support

Learn how a new vulnerability is created in TISC with a related vulnerability in VR.

Before you begin

Role required:

- System Administrator (view, create or edit)
- sn_sec_tisc.admin (view)

About this task

When new vulnerability is created in TISC and there is a related vulnerability in VR.

- If VR vulnerability(v2) score is > 8 OR VR vulnerability(v3) score is > 8.
- Total VI's associate to it are greater than 0.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Automated Flows**.
3. Select **Vulnerability Management Support** action link to view the respective rule details in the flow designer.
4. View the flow designer action for the following trigger:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
When new vulnerability is created in TISC and there is a
 related vulnerability in VR.
```

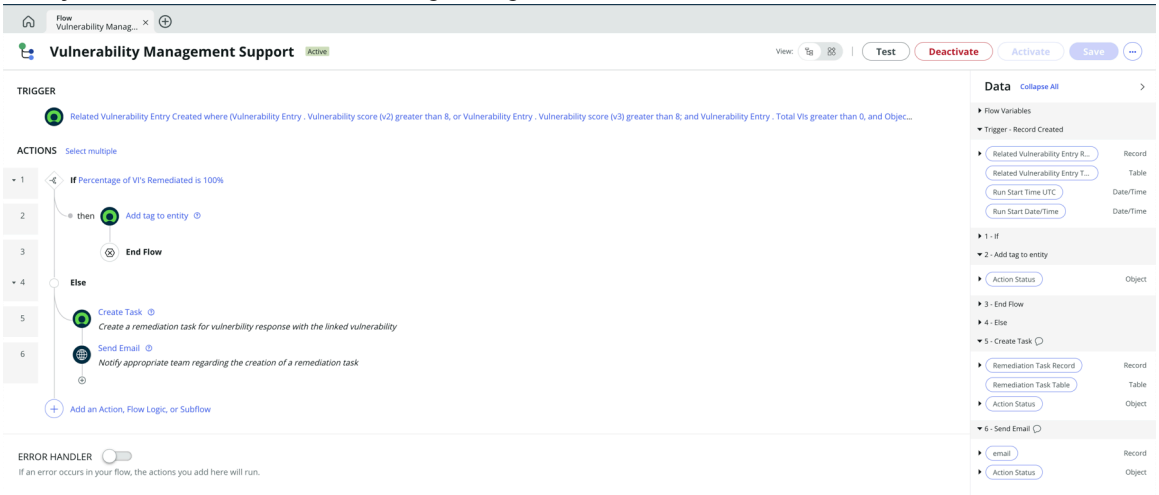
5. **If the percentage of total VI's remediated that are associated to that vulnerability is 100%, then:**

   a. Add a tag called Remediated to the observable.

6. **Else, enrich the observable data with available capabilities:**

   a. Create a remediation task for VR.

   b. Notify the concerned VR team's regarding it.



Zero-day vulnerability tracking

Learn how to analyze RSS Feeds coming into the system.

Before you begin

Role required:

- System Administrator (view, create or edit)
- sn_sec_tisc.admin (view)

About this task

Whenever a new RSS Feed is created into the system, and it has a mention of 'Zero Day' in either title or description.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Administration**.
2. Select **Automated Flows**.
3. Select **Zero-day vulnerability tracking** link to view the respective rule details in the flow designer.
4. View the flow designer action for the following trigger:

```
RSS Feed Created where (Title contains zero day, or Description
 contains zero day, or Title contains zero_day, or Description
 contains zero_day, or Title contains zero-day, or Description
 contains zero-day)
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. **If the observable is an IPv4 or IPv6 address and it falls within an allowed CIDR range, then:**
   a. Create a case for TISC Team, along with a remediation task for VR Team.
   b. Notify the concerned TISC Teams and VR Teams.

Automated flows tables

The following tables helps you to understand the relationship tables between entities and enrichment tables that are used in automated flows.

Relationship tables between entities

Table	Entity
Related Indicator Observable	sn_sec_tisc_m2m_indicator_observable
Related Indicator	sn_sec_tisc_m2m_indicator
Related Observable	sn_sec_tisc_m2m_observable
Object-Object Relationship	sn_sec_tisc_m2m_object
Related Indicator Object	sn_sec_tisc_m2m_object_indicator
Object-Observable Relationship	sn_sec_tisc_m2m_object_observable

Enrichment table

Table	Entity
Threat Lookup Results	sn_sec_tisc_lookup_result
Sightings	sn_sec_tisc_sighting
Observable Enrichment Result	sn_sec_tisc_observable_enrichment_result

Share Threat Intelligence data between TISC instances

You can share threat intelligence data between TISC instances using one of the following methods.

Sharing Methods

- **Manual sharing through the user interface (GUI)**: Manually curate and share intelligence records with a target instance through the TISC interface. For more information, see Sharing of Outbound Intelligence Records from the GUI .
- **Automated sharing using flows**: Configure flows to automatically share intelligence data to a target instance based on a defined condition. For more information, see Automated Sharing of Outbound Intelligence Records .
- **Sharing through a *TAXII* server**: Exchange threat intelligence data through TAXII collections using standardized threat intelligence sharing protocols. For more information, see .

Data transfer mechanism

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For Manual sharing via GUI and automated flow based sharing, the source TISC instance pushes the data directly to the target instance.
- For TAXII based sharing, the target TISC instance pulls data from TAXII collections configured on the source instance.

Related topics

Add to TAXII Collections from Library List View

Manual and Automated Sharing using flows

This section describes how to configure manual sharing via GUI and automated intelligence sharing between TISC instances. It outlines the setup of inbound and outbound intelligence profiles, required roles, authentication configuration, and exclusion rules in both the source and target instances.

Configuring the Target TISC Instance

Role required: sn_sec_tisc.admin

Prerequisites: Before you begin, ensure you have the appropriate roles assigned.

Role Requirements

Role Requirements

Step	Action	Required Role
Create API ingestion user	Create a dedicated user and assign required role	admin (system administrator)
Configure and manage TISC settings	Perform remaining configuration steps	sn_sec_tisc.admin
Post intelligence via API	Authenticate and submit intelligence data	sn_sec_tisc.api_post_intel (assigned to the integration user)

1. **Create a user with the role** `sn_sec_tisc.api_post_intel`:

   Create a dedicated user in the target TISC instance and assign them the `sn_sec_tisc.api_post_intel` role. This dedicated user is used to authenticate incoming intelligence data submitted to the instance.

2. **Set up an Inbound Intelligence Profile**:
3. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Administration** > **Inbound Intel Sharing**.
4. Select **Inbound Intel Sharing Profiles**.
5. Create a new profile. For more information, see .
6. In the **User for authentication** field, select the user created in the previous step.
7. Set the **Data format** to **STIX 2.1**.
8. **Save** and **enable** the profile to allow the target TISC instance to receive intelligence.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Select the **Copy Profile ID** to copy the profile ID.

> **Note:** You need the profile ID when configuring the outbound intelligence profile on the source TISC instance. For more information, see .

Configuring the Source TISC Instance

1. **Configure global sharing rules**: Ensure the following are configured and published based on your requirements:
   - Outbound Intel Data Exclusion Rules. For detailed procedure, see .
   - Outbound Intel Sharing Controls. For detailed procedure, see .
2. **Create an Outbound Intelligence Profile:**

   a. Create a new outbound profile to manage the data sharing process. For more details, see .

   b. Specify the API endpoint URL as:

   ```
   https://{instance
    name} /api/sn_sec_tisc/v1/tisc_intel_sharing_api/post_intel
   ```

   .

   c. Set the **Authentication required** to true.

   d. Enter the credentials of the user created in the target TISC instance (refer to the first step of the target setup) for the username and password.
3. **Configure Request Headers**: In the **Headers to be passed with request** field, include the following:

   Profile-GUID: {Profile ID from the target TISC instance}

   Shared-Intel-Format: STIX 2.1
4. **Obtaining the Profile ID:** The Profile ID required for the header can be found in the target TISC instance's Inbound Intelligence Profile. Use the **Copy Profile ID** button to retrieve it. For more information, see .
5. **Save** and **enable** the outbound profile.

   After configuration:
   - Save the profile.
   - Validate the connection to confirm it is functioning correctly.
   - Enable the profile to activate intelligence data sharing.

Template Configuration for Intelligence Sharing

Create and publish an outbound intelligence sharing template to define how threat intelligence is shared from the source TISC instance to the target instance.

The template determines which profiles are included, which sharing settings are applied, and which record fields are shared to the target instance. Configure and publish the global sharing rules to control what intelligence data the source instance shares outbound:

Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Create and publish an outbound intelligence sharing template with the required configuration. For more information, see .
2. Associate the published template with the outbound intelligence profile configured for the target TISC instance to begin sharing intelligence data.

Sharing intelligence using TAXII Server

You can retrieve threat intelligence from a source TISC instance into a target TISC instance using TAXII collections. This process requires configuration in both the source and target instances.

TAXII-Based Sharing

TAXII-based sharing enables structured and standardized exchange of threat intelligence between TISC instances. In this model, the source instance exposes intelligence through TAXII collections, and the target instance retrieves that data using a configured TAXII feed.

Configuring the source TISC instance

Complete the following steps in the source TISC instance before configuring the target instance.

1. **Configure global sharing rules**:

   Ensure the following are configured and published based on your requirements:

   - Outbound Intel Data Exclusion Rules
   - Outbound Intel Sharing Controls

2. **Create TAXII collections**: Set up the required TAXII collections in the source TISC instance. For instructions, see Create a TAXII collection.
3. **Create outbound intelligence sharing templates**: Create and publish an outbound intelligence sharing template with the required configuration for TAXII sharing. For instructions, see Outbound intelligence sharing templates.
4. **Add records to the TAXII collection**: You can add records using either of the following methods:
   - Ad-hoc addition via the graphical user interface (GUI). For more information, see Add records to a TAXII collection.
   - Automated addition using flows. For more information, see Automate sharing to TAXII collections.
5. **Create a TAXII API user for the target TISC instance**: Create a dedicated API user in the source TISC instance for authentication when the target instance connects to fetch intelligence data.

   Assign the role `sn_sec_tisc.taxii_server_api_user`.

Configuring the target TISC instance

After completing the source configuration, configure the target instance to pull intelligence from the source.

1. **Create a new TAXII feed**: In the target TISC instance, create a new TAXII feed. For more information, see Configure a new TAXII feed.
2. **Configure the discovery service**: Set **Configuration Type** to **Discovery Service URL** and enter the following URL:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
https://{instance_name}/api/sn_sec_tisc/taxii_server/taxii2
```

3. **Configure Authentication**:
   - Select **Basic** as the authentication method.
   - Provide the username and password of the TAXII API user created in the source instance.
4. **Save** the configuration:

   Validate the connection then click the **Get TAXII Collections** button to retrieve the enabled TAXII collections from the source instance.

5. **Enable and configure ingestion**:

   a. Navigate to the collection you want to ingest.

   b. Enable the collection.

   c. Specify the **Fetch From Time** and the desired ingestion frequency.

   All records added to the collection in the source instance after the specified time are pulled into the target instance according to the configured schedule.

Add to TAXII Collections from Library List View

Add to TAXII Collections feature enables analysts to add the selected threat intelligence including observables, indicators, and objects such as attack patterns, threat actors and so on directly to TAXII collections.

Before you begin

Role required: sn_sec_tisc.analyst

About this task

Following is the procedure that shows how to add TAXII collections to an observable.

Procedure

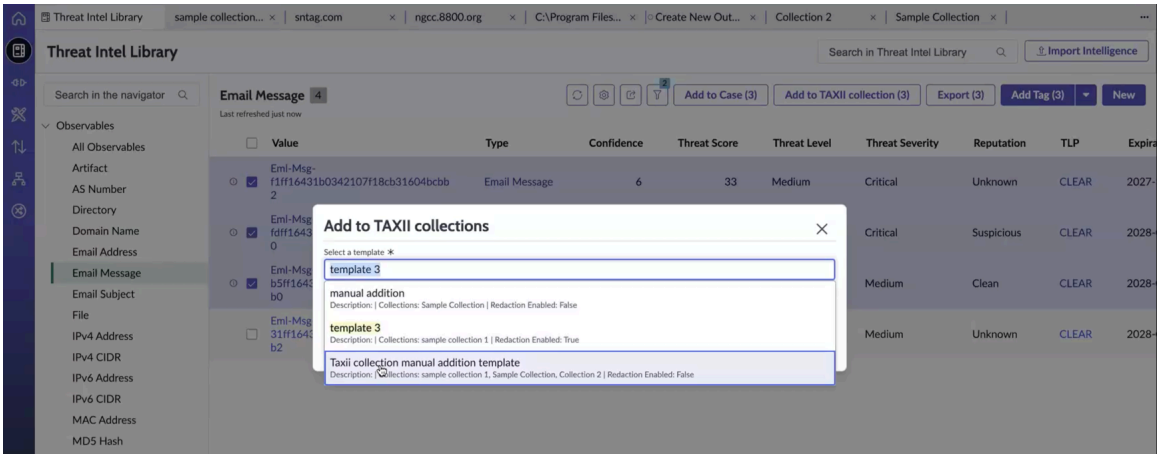
1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select the observable type.

   Note: The **Add to TAXII Collections** button is not available if you select **All Observables**. To enable this button, you must select a specific observable type, for example **Email Message**.

3. Click **Add to TAXII Collections** button.
4. Select the TAXII Collections sample template.

   All the templates configured on the Outbound Intel Sharing page appear here, allowing you to select the one you need. For more information, see .

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Select **Add**.
   You will be prompted to select a template. Any templates you've previously created will be listed here for you to select.
6. Once you have selected the template select **Add**.
   A TAXII collection addition job record is created to track the action.
7. Click on the job record to view its details.
   You will see the specific records that have been successfully added to the TAXII Collection.

   This process confirms which intelligence items were shared and provides an auditable record of the action.

   Note: A system property `sn_sec_tisc.add_to_taxii_collection_entity_threshold` defines the maximum number of entities (observable records) that can be added to a TAXII Collection in a single request. The system enforces a hard limit of 10000 entities.

8. Select the **Record** section of the job record.
9. Drill down to the **TAXII Collection Records** section.
   You will notice that the selected observable(s) are added to the TAXII collection and you will also see the exclusion rules.

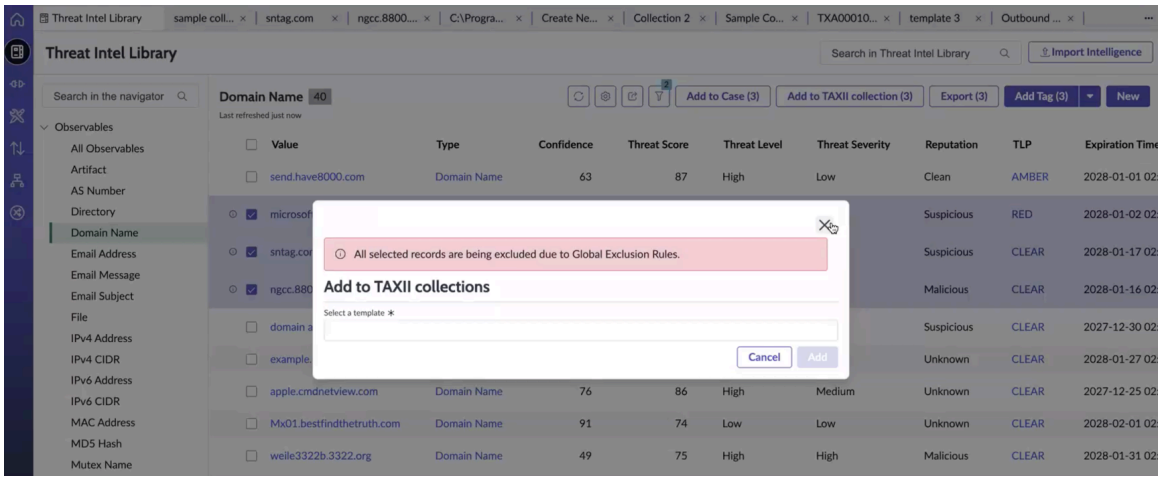
   Exclusion rules define which records or data should not be included when adding items to a TAXII Collection, ensuring that only the intended intelligence is shared. Each template comes with its own sharing template controls, which specify the attributes and information to include or exclude during sharing.

   In addition, exclusion rules also allows you to automatically prevent certain records from being added to a TAXII Collection.

   Any records that match the criteria defined in these rules are excluded and cannot be shared. For example, if a global exclusion rule is configured to block domains with a specific status, such as red or clear, any record matching that condition will be automatically excluded.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you attempt to add such records to a TAXII Collection, the application will indicate that they have been excluded (see the screenshot below), ensuring that only the intended and allowed intelligence is shared. For more information on the exclusion rules, see .



What to do next

Once you add the records to the TAXII collections, navigate to **Administration** > **TAXII Outbound Server** > **TAXII Collections** to view the added records under the **TAXII Collection Records** section. For more information, see and .

Marking Definitions for Records Added to TAXII Collections

When you add a record to a TAXII Collection, the application automatically applies marking definitions to provide additional context about the record.

For example:

If a record has a TLP (Traffic Light Protocol) classification, such as TLP White a related reference record is created to explain what that TLP level means.

This ensures that users accessing the shared intelligence are aware of the requirements of each record. When a record is added to a collection, any relevant metadata or contextual records such as TLP markings are automatically created and linked.

Managing Global Exclusion Rules in TAXII Collections

In the **Administration** section, you can view and manage all configuration-related settings, including global exclusion rules. These rules determine which records are automatically excluded from being added to a TAXII Collection.

For example, an exclusion rule might exclude domains marked with TLP Red or TLP Clear. You can customize these rules. For example, you could modify it to exclude only TLP Red records.

When you attempt to add records to a TAXII collection:

- If all selected records match the exclusion rules, the application prevents any records from being added.
- If some records from the selection are valid, then those records are added to the TAXII collection, while the excluded records are automatically filtered out.

For more information on the exclusion rules, see .

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence Security Center reference

Reference topics provide additional information about the Threat Intelligence Security Center.

Reference information	Links to topics
Domain Separation and Threat Intelligence Security Center	Domain separation and Threat Intelligence Security Center
Components installed with Threat Intelligence Security Center application	Components installed with Threat Intelligence Security Center

Domain separation and Threat Intelligence Security Center

Domain separation is supported for Threat Intelligence Security Center. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

Overview

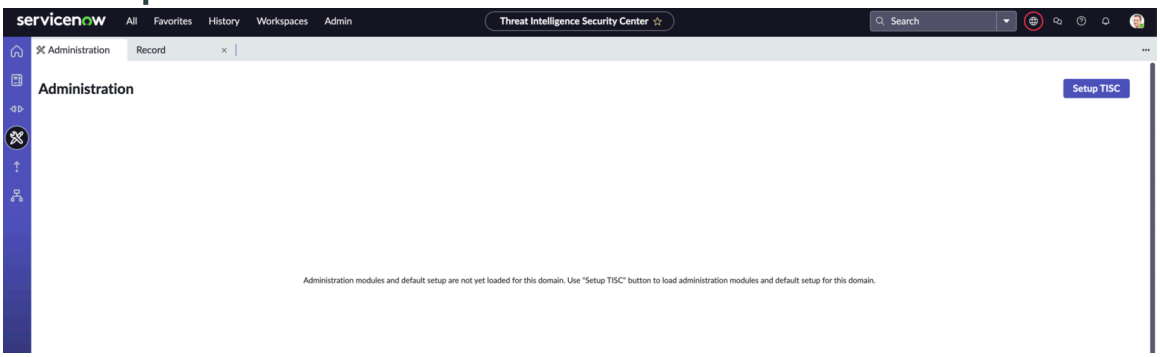
Domain separation is enabled for all the features of Threat Intelligence Security Center.

How domain separation works in Threat Intelligence Security Center

- All the configuration related records that are provisioned in the base system are shipped in the global domain. In case the instance is domain separated, users would see an explicit button **Setup TISC** under the **Administration** module of the TISC workspace. Click on this button to clone the base system provisioned global domain configurations into the respective domains.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Domain Separation



Note: Users should only enable or modify domain specific configuration records and should not enable or modify configuration records in the global domain.

- Couple of platform notification rules (sysevent_email_action) are provisioned in the base system, these notification rules should be cloned into required domains and only domain specific notification rules need to be enabled.

  Note: For more information on the rules notifications, navigat to **System Notification** > **Notifications** and filter for all the global domain notification rules defined on the tables starting with name *sn_sec_tisc* to understand how users can identify the base notification rules that are provisioned in the base system.

- All the configurations and data ingested will be specific to each domain, which means that users from one domain will not be able to access data from other domain.
- Configure a domain-separated environment with this application by installing Domain Support - Domain Extensions Installer plugin.
- There are domain columns added for all the base system application tables.
- Using the Platform provided functionality the tenant domains manage their own application data.
- The business logic and processes that can be domain-separated by instance owner is same as what Platform supports.
- The business logic and processes that can be administered by tenant domain is same as what platform supports.
- You can access the Setup page from the Administration section. Click on the link provided under the Administration section to view the domain separation view.
- To support the domain separation for the widgets using Performance Analytics (PA) indicators in the TISC Home dashboard, refer to the KB article KB1647990 for detailed procedure.

Domain Separated tables

All the tables are domain separated.

Use cases

All features of this application are domain separated.

Related topics

Domain separation for service providers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Components installed with Threat Intelligence Security Center

Several types of components are installed when you download and activate the Threat Intelligence Security Center application, including user roles and properties.

Properties installed

Role required: sn_sec_tisc.admin

Users with the Security Administrator [sn_sec_tisc.admin] role can modify them.

Property	Usage
Properties for Threat Intelligence Security Center	
This will disable all the correlation rules. If we just need to disable selected correlation rules, use "active" field on correlation rule instead. sn_sec_tisc.disable_correlation_rules	• **Type**: true | false • **Default value**: false
This property is used to enable/disable processing of aggregates in threat score calculator feature. sn_sec_tisc.aggregates_for_calculator	• **Type**: true | false • **Default value**: true
The number of rows of raw data that will be saved when a Sighting Search is performed. Range 0 - 100 sn_sec_tisc.sighting_search_raw_data_rows	• **Type**: integer • **Default value**: 50
Associate Sighting Search results with CIs in the CMDB. sn_sec_tisc.associate_ci_with_sighting_search	• **Type**: true | false • **Default value**: true
This will control whether URLs from lists will be defanged or not sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	• **Type**: true | false • **Default value**: false
This property will enable the MITRE Technique(s), to be rolled up to case(s) from the associated objects or security incidents automatically. sn_sec_tisc.auto_rollup_mitre_data	• **Type**: true | false • **Default value**: true
If true, shows all tactics (including the tactics which doesn't have any techniques associated to the case) for the MITRE lists rendered in the report. sn_sec_tisc.show_all_tactics_reporting	• **Type**: true | false • **Default value**: true
Sys ID of the email client template for the Case (sn_sec_tisc_case) table which will be used in share report. sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	• **Type**: string • **Default value**: b55e22c54324021060eee0ea78b8f2df

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
Default TLP level is applied when creating a new record. If not set manually on the form, this value will be used. sn_sec_tisc.tlp_default_value	• **Type**: choice list • **Default value**: 955c9e5543d35110baf06e434ab8f2fb
Logging level-debug,info,warn,error sn_sec_tisc.logging.verbosity	• **Type**: choice list • **Default value**: info
Properties for Threat Intelligence Feeds	
Maximum time in seconds an outbound HTTP connection waits to fetch TAXII collection data sn_sec_tisc.taxii.http.max_timeout	• **Type**: integer • **Default value**: 300
Maximum number of objects retrieved in one REST call from a TAXII server (Applicable only for TAXII versions 2.0 and 2.1) sn_sec_tisc.taxii.max_page_size	• **Type**: integer • **Default value**: 5000
Maximum number of retries for a failed TAXII2. X REST call sn_sec_tisc.taxii2.retry_count	• **Type**: integer • **Default value**: 3
Maximum number of objects retrieved in one REST call from Cyware TAXII server sn_sec_tisc.cyware_taxii.max_page_size	• **Type**: integer • **Default value**: 1000 **Note:** Specifies the page size used when fetching data from TAXII collections related to the Cyware TAXII Feed. For all other TAXII collections, the page size retrieved from the TAXII collection defaults to the value defined in the corresponding property: `sn_sec_tisc.taxii.max_page_size`.
Number of records to fetch at a time from CrowdStrike. Higher the number, more the memory would consumed for processing the payload. sn_sec_tisc.crowdstrike_api_limit	• **Type**: integer • **Default value**: 1000
Denotes the number of indicators to be pulled in a single API call. **Note:** This is applicable only when the integration doesn't find the necessary present in the system.	• **Type**: integer • **Default value**: 1000

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
sn_sec_tisc.crowdstrike_indicator_batch_size	
Denotes the number of actors to be pulled in a single API call. **Note:** This is applicable only when the integration doesn't find the necessary present in the system. sn_sec_tisc.crowdstrike_actor_batch_size	• **Type**: integer • **Default value**: 1000
Denotes the number of reports to be pulled in a single API call. **Note:** This is applicable only when the integration doesn't find the necessary present in the system. sn_sec_tisc.crowdstrike_report_batch_size	• **Type**: integer • **Default value**: 50
The allowed total of offset and limit from CrowdStrike API. sn_sec_tisc.crowdstrike_offset_limit_total	• **Type**: integer • **Default value**: 50000
Properties for Tagging Rules	
Properties for REST APIs	
Defines the maximum page size (max number of observables returned as part of the response) for Observables Fetch API. Not recommended to increase to high value as it may affect API response time. sn_sec_tisc.api_maximum_page_size_limit	• **Type**: integer • **Default value**: 1000
Defines the maximum number of observables that can be sent in the request body for Observables Add API. Not recommended to increase to high value as it may affect API response time. sn_sec_tisc.add_obs_api_max_records	• **Type**: integer • **Default value**: 100
Properties for Webhooks	
Maximum number of events to send as part of one webhook request. The batch size will be limited to 2000 even if a higher value is set in this property. sn_sec_tisc.webhook_max_event_batch_size	• **Type**: integer • **Default value**: 100
Number of times a failed request should be retried before marking it as error and moving on to next batch of events. The retry count will be limited to 10 even if a higher number is set in this property. sn_sec_tisc.webhook_retry_count	• **Type**: integer • **Default value**: 100

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
Number of seconds to wait before re-attempting a failed batch. This will exponentially increase based on the retry count. For eg, if retry_count is 3 and retry_interval is 30, retries are fired after 30, 60 and 120s. The initial retry interval will be limited to 300 seconds even if a higher value is set in this property. sn_sec_tisc.webhook_retry_interval	• **Type**: integer • **Default value**: 30
Ignore webhook events triggered by threat score re-apply sn_sec_tisc.webhook_ignore_threat_score_reapply	• **Type**: true | false • **Default value**: true
Properties for Investigation Canvas	
Setting the value to true adds new nodes to the top left corner; false adds them to the center of the canvas. sn_sec_tisc.canvas_suspend_reLayout	• **Type**: true | false • **Default value**: true
Properties for export in CTI formats	
Maximum number of rows that can be exported to a STIX 2.1 file sn_sec_tisc.stix_export_limit	• **Type**: integer • **Default value**: 10000
Include Journal type fields in export file. sn_sec_tisc.export_journal_fields	• **Type**: true | false • **Default value**: true
Properties for Threat Intelligence Sharing	
Enables or disables case sensitive for applying redaction for shared intel. (By default, the value will be false implying that the redaction will be case insensitive. Note: Changing the value of this property from false to true or true to false will DELETE all the data from redaction category as well as values table.) sn_sec_tisc.case_sensitive_for_redaction	• **Type**: true | false • **Default value**: false
Maximum number of rows allowed in the redaction upload file. sn_sec_tisc.max_redaction_rows_import	• **Type**: integer • **Default value**: 10000
Title of outbound TAXII server sn_sec_tisc.taxii_server_discovery_api_title	• **Type**: string • **Default value**: ServiceNow TAXII Server

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Usage
Description of outbound TAXII server sn_sec_tisc.taxii_server_discovery_api_description	• **Type**: string • **Default value**: Discovery endpoint for sharing cyber threat intelligence via TAXII
Title of outbound TAXII server default API root sn_sec_tisc.taxii_server_api_root_title	• **Type**: string • **Default value**: ServiceNow TAXII Server
Description of outbound TAXII server default API root sn_sec_tisc.taxii_server_api_root_description	• **Type**: string • **Default value**: SAPI root endpoint for sharing cyber threat intelligence via TAXII
Default page size of TAXII Server API response sn_sec_tisc.taxii_server_api_response_page_limit	• **Type**: integer • **Default value**: 100
Maximum number of records that can be added to a outbound TAXII server collection sn_sec_tisc.taxii_server_collection_record_limit	• **Type**: integer • **Default value**: 10000
The maximum number of entities that can be added to a TAXII collection in a single "Add to TAXII Collection" request. The system enforces a hard limit of 10,000 entities per request, regardless of any higher configured value. sn_sec_tisc.add_to_taxii_collection_entity_threshold	• **Type**: integer • **Default value**: 1000
Properties for Tagging Rules	
Enables or disables case sensitive matching of keywords or regex n tagging rules (By default this is unselected (No) meaning matches are case-sensitive). sn_sec_tisc.case_sensitive_for_tagging_rules	• **Type**: true | false • **Default value**: false

Scheduled Jobs

The following table describes the scheduled jobs:

Job	Description
Aggregate Indicator Source Records	Aggregates Indicator source records.
Aggregate Object Source Records	Aggregates Object source records.
Aggregate Observable Source Records	Aggregates Observable source records.
Cleanup of Stale Imports	Cleans up stale import job records.
Cleanup of unused new nodes of canvas	Cleans up unused new nodes of canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Job	Description
Cleanup Secure File Download Records	Cleans up secure file download records.
De-duplicate Indicator Source Records	Deduplicates Indicator source records.
De-duplicate Object Source Records	Deduplicates Object source records.
De-duplicate Observable Source Records	Deduplicates Observable source records.
Inactivate Expired Indicators	Inactivates expired indicator records.
Inactivate Expired Objects	Inactivates expired object records.
Inactivate Expired Observables	Inactivates expired observable records
Migrate Data from TI to TISC	Processes pending migration job run records
Populate aggregated records for indicator source records	Identifies parent aggregated record for newly created indicator source records
Populate aggregated records for object source records	Identifies parent aggregated record for newly created object source records.
Populate aggregated records for observable source records	Identifies parent aggregated record for newly created observable source records.
Populate TISC Reference in TI	Populates reference of TISC aggregated observable in TI observable record.
Process Approved Imports	Processes approved import jobs.
Process Imported MISP Dsm Queue Records	Processed staged MISP feed ingestion queue records.
Process Imported MISP Indicator Import Queue Records	Processes staged MISP data ingested from import intelligence
Process Imported STIX Import Queue Records	Processes staged STIX data ingested from import intelligence
Process Imported STIX Import Queue Records - Ingestion	Processes staged STIX data ingested from threat feeds.
Process Pending Case Artifacts Migration	Migrates case artifacts from Threat intelligence application to Threat Intelligence security center.
Process pending threat source ingestion Queue Records	Processes pending source ingestion queue records.
Process Queued Entities For Threat Score Calculator	processes pending threat calculator queue entries
Process Queued MISP Dsm Queue Records	Processes queued MISP data ingested from threat feed
Process Queued MISP Indicator Import Queue Records	Processes queued MISP data ingested from import intelligence
Process Queued STIX Import Queue Records - Ingestion	Processes queued STIX data ingested from threat feeds.
Process Queued STIX Indicator Import Queue Records	Processes queued STIX data ingested from import intelligence
Process Webhook Queue	Processes pending webhook queue records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Job	Description
Re-Aggregate Source Records	Re-aggregates source records for which aggregated records are deleted.
Remove filtered source record	Cleans up filtered source records
Resume CrowdStrike Integration Process Checker / Reprocess CrowdStrike Source Records	Resumes CrowdStrike feed integration runs waiting for rate limit / Reporcess source records for aggregating relationships
Sync False Positive Observables Count	Synchronizes observable false positive counts with flase positive counts per source
TISC Create Webhook Batches	Created batches for queued webhook queueu entries for processing
TISC Fire Webhooks	Executes pending webhook batches
Updating Relationship Archived Column	Updates relationship source and target records archival status

Threat Intelligence Security Center Knowledge Base articles

This section provides a curated list of key Knowledge Base (KB) articles related to Threat Intelligence Security Center (TISC). These resources include best practices, configuration guidance, compatibility information, and operational workflows to help you effectively manage threat intelligence and security within TISC.

The following knowledge base articles provide guidance on TISC concepts, configuration, integration, and best practices. The articles are maintained in the ServiceNow internal knowledge base and are referenced from the parent index article KB1778603.

TISC Knowledge Base Articles

KB ID	Title	Description
KB1778603	Knowledge base links for Threat Intelligence Security Center	A consolidated index of all knowledge base articles related to TISC. Use this article as the starting point for locating TISC documentation resources.
KB1748938	Difference Between Threat Intelligence Security Center (TISC) and Threat Intelligence Module in SIR (SIR-TI)	Explains the key architectural and functional differences between the standalone TISC product and the Threat Intelligence module available within Security Incident Response (SIR-TI).
KB1778607	How SIR/TI and TISC Integration Works	Describes the integration architecture and data flow between the SIR Threat Intelligence module and the Threat Intelligence Security Center, including synchronization behavior and supported configurations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC Knowledge Base Articles (continued)

KB ID	Title	Description
KB1706151	Migration of Data from Existing Threat Intelligence to Threat Intelligence Security Center	Provides a step-by-step guide for migrating threat intelligence data from the legacy SIR-TI module to TISC, including pre-migration checks, data mapping, and validation steps.
KB1587754	Parent Identification Logic for Various Entities in TISC	Explains the logic TISC uses to identify and assign parent entities across different threat intelligence record types such as observables, indicators, and threat groups.
KB1587756	De-duplication Logic for Various Entities in TISC	Describes how TISC identifies and resolves duplicate records across threat intelligence entities to maintain data integrity and reduce noise in the threat intelligence repository.
KB1587758	Aggregation Logic for Various Entities in TISC	Details the rules and processes TISC uses to aggregate threat intelligence data ingested from multiple sources into unified, consolidated entity records.
KB1648039	Best Practices Guide for TISC	Provides recommended practices for deploying, configuring, and maintaining the Threat Intelligence Security Center for optimal performance, data accuracy, and operational efficiency.
KB1909534	Security Control List (AllowList, DenyList, WatchList) for Threat Intelligence Security Center	Documents the configuration and usage of security control lists in TISC, including AllowList, DenyList, and WatchList. Also notes a known behavior: searches with a larger number of characters return more results compared to searches with fewer characters.
KB2148681	TISC Intelligence Exchange Use Case Guide	Covers common use cases for exchanging threat intelligence data between TISC instances and with external platforms, including configuration steps and representative scenarios.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC Knowledge Base Articles (continued)

KB ID	Title	Description
KB2332774	TISC Outbound Intelligence in MISP Format	Explains how to configure TISC to share outbound threat intelligence in MISP-compatible format so that external consumers and partner instances can ingest the data.
KB2197697	TISC MISP Processing – MISP to TISC Mapping	Provides field-level mapping details for ingesting and processing MISP threat intelligence data within TISC, including object type conversions and attribute handling.
KB2326271	TISC CrowdStrike Custom Feed – Internal Field Mapping	Documents the internal field mapping applied when TISC processes CrowdStrike custom feed data, enabling consistent normalization of CrowdStrike indicators into the TISC data model.
KB2677048	Improving Observable/ Indicator Deduplication Job Performance – Duplicate Records from Same Source Cleanup	Describes techniques and configurations to improve the performance of the TISC deduplication job, with guidance on cleaning up duplicate observable and indicator records that originate from the same source.

Related Resources

For additional information about TISC configuration and administration, see the ServiceNow product documentation for Security Operations and the TISC release notes for the current release.

TISC API References

The following table lists all the available API endpoints provided as part of TISC.

TISC APIs

API	Description	API reference documentation links
TISC API - POST	This API is designed to access observables data as well as associated threat entity information from TISC.	TISC API under REST API reference section on API implementation and reference

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC APIs (continued)

API	Description	API reference documentation links
TISC RPZ API	This API provides domains and IP addresses in RPZ format, suitable for sinkhole configurations or any systems that support RPZ policies.	TISC RPZ API
TISC TAXII Server API	The TAXII (Trusted Automated Exchange of Intelligence Information) server API allows compatible TAXII clients to access and obtain threat intelligence data from TISC TAXII Collections).	TAXII Server API
TISC Intel Exchange API	This API enables external systems to share threat intelligence data with the application in STIX 2.1, MISP format.	TISC Intel Exchange API

Using Threat Intelligence Security Center

Use Threat Intelligence Security Center to manage Threat Intelligence library records, import external threat data, and streamline case management. It helps security teams centralize intelligence data, enhance analysis, and respond more effectively to threats by integrating the relevant information into ongoing investigations.

TISC integration with SIR Workspace

TISC integration with SIR automatically attaches the context on the observables within the security Incident workspace for the Security analysts. Any new observables from SIR can be sent to TISC for further analysis by CTI team using the UI actions provides on the screens.

Additionally, any enrichment results that are produced from integrations only available in SIR can also be pushed using the UI actions provided in the workspace.

Working with Data Imports

Data imports allows you to view the all the records that are being processed for import job and also lists the import jobs that are awaiting approvals.

Viewing all imports

Use this section to view all the imported records that are displayed in the list view for all the users.

Before you begin
Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Imports**.
2. Select **Data Imports** > **All Imports**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This page displays all the records that are being processed for the import job.

3. Open any record to view the status of the import process.

> **Note:** You can also click **New Import** to create a new import record. After you click this button, the application will direct you to the **Import Intelligence** page. For more information on creating new records, see Import Threat Intelligence section and proceed further with the respective import type.

Viewing my imports

Use this section to view the import records that are created by the logged in user.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Imports**.
2. Select **Data Imports** > **My Imports**
   This page displays all the records those import records which are categorised for further process for the import job.
3. Open any record to view the status of the import process.

> **Note:** You can also click **New Import** to create a new import record. After you click this button, the application will direct you to the **Import Intelligence** page. For more information on creating new records, see Import Threat Intelligence section and proceed further with the respective import type.

4. View the summary of the import records.

> **Note:** In case if any of the import jobs are not submitted, you can **Submit** the records for further processing and send it for approval. If approval is not required for that particular import job, those records will be automatically processed.

Viewing my approvals

Use this section to review and approve the import job records.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Imports**.
2. Select **Data Imports** > **My Approvals**
   This page displays all the import records that are awaiting approval by the logged in user.
3. Open any record to approve or reject the import record.
4. Click **Approve** to approve the import job record.
   The **Approve Import** dialogue box is displayed and a confirmation message is displayed whether to approve the select imports.

> **Note:** An email notification is sent to the respective user(s) that the import job that was in process is now approved. For more information on approving rules, see Defining Data Imports Approval Rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select **Approve** from the dialogue box.
   An email notification is sent to the user who created the import job and the import job that was in process is now approved.
6. Click **Reject** to reject a record.

Note:

- You can review and resubmit the rejected import job. Make sure to add comments for rejection.
- An email notification is sent to the user who created the import job import job when the import job that was in process is rejected.
- An email notification is sent to the approvers requesting for the approval.

Import Threat Intelligence

Use this feature to add or import the threat intelligence data manually to the repository.

The following import formats are supported in the intelligence data import process:

1. Import from structured file
2. Import from standard format
3. Import from raw text
4. Import from file (unstructured)

Import data using structured file

Upload the structured data in the supported file formats such as CSV, XLSX or XLS.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
   The Threat Intel Library page is displayed.
2. Click **Import Intelligence**.
3. Click **Import from structured file** card.

Important: While importing the threat intelligence data in the supported file formats such as TXT, CSV, STIX 2.x JSON, MISP JSON, or Structured File, the file size is limited to 5 MB. The characters limit to raw text is limited to 10,000.

4. On the form, fill in the fields.

Field	Description
Choose an option	Select the required option from the drop down list such as Observables or Indicators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Observables**: Select the observables data to import. **Note:** Select this option if you are importing observables data. Also do not modify the column headers in the file. The Mandatory fields are Value and Type, and others are optional. Also, enter the date/time in YYYY-MM-DDThh:mm:ssZ format. ○ **Indicators**: Select the indicators data to import. **Note:** Select this option if you are importing indicators data. Also do not modify the column headers in the file. The mandatory fields for indicators are Pattern, Pattern Type, and Valid from and others are optional. Also, enter the date/time in YYYY-MM-DDThh:mm:ssZ format.
Preview and download sample file for Indicators	Use this link to download the sample file using the Preview link and upload the structured data in a compatible file format such as CSV, XLS, or XLSX. **Note:** The column headers must match the headers exactly. Value, Type fields are required for each observable in the file. The remaining fields are optional where as First Seen, Last Seen must be in numbers and are epoch time in milliseconds.
Upload file	Click this link to upload the file data in the recommended structure file format. **Note:** You can only upload one file at time. To add a new file you must remove the existing and add a new file.
Set definitions	
TLP	Select the Traffic Light Protocol (TLP) indicator from the drop-down list to be applied for the imported records. TLP is in TISC is labeled with different colors to ensure the sensitive data is shared with the intended users.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ CLEAR: Information can be shared without restriction. ○ RED ○ AMBER+STRICT ○ AMBER ○ GREEN
Confidence (0-100)	Set the confidence value between 0-100 for the imported records.
Expiry Period (days)	Enter the expiry period for the imported records. **Note:** This is a mandatory field.
Tags	
Add Tags	Use the tags to annotate or ear mark records ingested into the system from this source. Staart typing the tag name in the **Search** bar to choose the available tags in the system or enter new tag name and click **Add** to assign it to the source.
Taxonomy	
Select a Taxonomy	Select the taxonomy for the imported data. Using taxonomies, define dictionaries that can be used as taxonomies assigned to threat intel records. For example, CAPEC nomenclature. For more information, see Creating Taxonomies. **Note:** The taxonomy value options change based on the selected taxonomy.
Override source value	Select this check box if you wish to over ride the source values for TLP, Confidence, Expiration, Tags, and Taxonomies with the configured values. If you don't select this check box the configured values are applied if they are not empty.

5. Click **Next**.
6. Review the data before submission for processing.

Note: Reviewing of imported records is not supported for STIX option.

After you click **Next**, you can see the summary of all the information that user has provided in the above section, and the below section provides you with all the records that needs to be imported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User can perform any type of activities and the multiple users can collaborate using the comment section which is available in the right contextual menu. The list of imported records will be rendered once the entire file or raw text is processed. The import processing for large files will take more time and while it is processing you can check the status, review, and submit from the import record page as well.

Note: Any records that fail the validations are skipped from the import process and those records are not displayed on the Review & submit page for further processing.

7. Click **Update Type** and select the type to update any type of the imported records.
8. Click **Delete** to delete any type of the imported records.
9. Click **Submit**.

Note: After you submit the import record, the user will be directed to the approver to approve the corresponding import record based on the approval rules configured. If the current user who is creating the record doesn't require the approval process then the record goes through the auto approval process the import job gets auto approved while submitting request.

10. Click **View Status** to view the status of the import record or click **Done**.
    The record displays the processed status once the data is imported for processing.
11. Click **Cancel** to abort the import process.
12. Click **Go Back** to go back to the previous page and review the record, if necessary.

Import data using standard format

Upload the standard data in the supported file formats such as STIX 2.x JSON, MISP JSON.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
   Threat Intel Library page is displayed.
2. Click **Import Intelligence**.
3. Click **Import from standard file** card.

Important: While importing the threat intelligence data in the supported file formats such as TXT, CSV, STIX 2.x JSON, MISP JSON, or Structured File, the file size is limited to 5 MB. The characters limit to raw text is limited to 10,000.

4. On the form, fill in the fields.

Field	Description
File Format	Select the required option from the drop down list such as STIX 2.x JSON or MISP JSON.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **STIX 2.x JSON**: Select the format in STIX 2.x JSON to import. ○ **MISP JSON**: Select the format in MISP JSON format to import.
Upload file	Click this link to upload the data in the standard file format.
Set definitions	
TLP	Select the TLP indicator from the drop-down list to be applied for the imported records.
Confidence (0-100)	Define the confidence value.
Expiry Period (days)	Enter the expiry period for the imported records. **Note:** This is a mandatory field.
Add Tags	Use the tags to annotate or ear mark records ingested into the system from this source. Staart typing the tag name in the Search bar to choose the available tags in the system or enter new tag name and click Add to assign it to the source.
Taxonomy	
Select a Taxonomy	Select the taxonomy for the imported data. Using taxonomies, define dictionaries that can be used as taxonomies assigned to threat intel records. For example, CAPEC nomenclature. For more information, see Creating Taxonomies.
Select Taxonomy values	Indicates the taxonomy values that are associated with the Taxonomy.
Override source value	Select this check box if you wish to over ride the source values for TLP, Confidence, Expiration, Tags, and Taxonomies from the configured values. If you don't select this check box the default values are applied.

5. Click **Next**.
6. Review the data before submission for processing.

   Note: Reviewing of imported records is not supported for STIX option.

   After you click **Next**, you can see the summary of all the information that user has provided in the above section, and the below section provides you with all the records that needs to be imported.

   User can perform any type of activities and the multiple users can collaborate using the comment section which is available in the right contextual menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Any records that fail the validations are skipped from the import process and those records are not displayed on the Review & submit page for further processing.

7. Click **Update Type** and select the type to update any type of the imported records.
8. Click **Delete** to delete any type of the imported records.
9. Click **Submit**.

Note:

After you submit the import record, the user will be directed to the approver to approve the corresponding import record based on the approval rules configured. If the current user who is creating the record doesn't require the approval process then the record goes through the auto approval process the import job gets auto approved while submitting request.

10. Click **View Status** to view the status of the record or click **Done**.
    The record displays the processed status once it is processed.
11. Click **Cancel** to abort the import process.
12. Click **Go Back** to go back to the previous page and review the record, if necessary.

Import data using raw text

Import the observables data by copying and pasting raw text or entering the free text.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
   The Threat Intel Library page is displayed.
2. Click **Import Intelligence**.

Important:

- Any defanging characters will be cleaned as part of parsing and extraction of observables.
- For this pasted text option only URL, domain, file name, hashes, and IP address will be extracted and no other observable types will be extracted for the data import and in case of such type of observables such as registry, directory types, those will be skipped from importing.

3. Click **Import from raw text** card.

Important: While importing the threat intelligence data in the raw text format the characters are limited to 10,000. The raw text option can be used as a workaround to extract the observables from the PDF.

4. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Raw data text box	Enter or copy and paste the raw text here in this text box. **Note:** You can only enter or paste the raw text to 10,000 characters.
Set definitions	
TLP	Select the TLP indicator from the drop-down list to be applied for the imported records.
Confidence (0-100)	Define the confidence value.
Expiry Period (days)	Enter the expiry period for the imported records. **Note:** This is a mandatory field.
Add Tags	Use the tags to annotate or ear mark records ingested into the system from this source. Staart typing the tag name in the Search bar to choose the available tags in the system or enter new tag name and click Add to assign it to the source.
Taxonomy	
Select a Taxonomy	Select the taxonomy for the imported data. Using taxonomies, define dictionaries that can be used as taxonomies assigned to threat intel records. For example, CAPEC nomenclature. For more information, see Creating Taxonomies.

5. Click **Next**.
6. Review the data before submission for processing.

   After you click **Next**, you can see the summary of all the information that user has provided in the above section, and the below section provides you with all the records that needs to be imported.

   User can perform any type of activities and the multiple users can collaborate using the comment section which is available in the right contextual menu.

   Note: Any records that fail the validations are skipped from the import process and those records are not displayed on the Review & submit page for further processing.

7. Click **Update Type** and select the type to update any type of the imported records.
8. Click **Delete** to delete any type of the imported records.
9. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: After you submit the import record, the user will be directed to the approver to approve the corresponding import record based on the approval rules configured. If the current user who is creating the record doesn't require the approval process then the record goes through the auto approval process the import job gets auto approved while submitting request.

10. Click **View Status** to view the status of the record or click **Done**.
    The record displays the processed status once it is processed.
11. Click **Cancel** to abort the import process.
12. Click **Go Back** to go back to the previous page and review the record, if necessary.

Import data using unstructured file format

Upload the data in an unstructured format supported using the file formats such as TXT, CSV, JSON, XLS, XLSX.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
   Threat Intel Library page is displayed.
2. Click **Import Intelligence**.

Important:

- Any defanging characters will be cleaned as part of parsing and extraction of observables.
- For this unstructured file format option only URL, domain, file name, hashes, and IP address will be extracted and no other observable types will be extracted for the data import and in case of such type of observables such as registry, directory types, those will be skipped from importing.

3. Click **Import from file (unstructured)** card.

Note: While importing the threat intelligence data in the supported file formats such as TXT, CSV, STIX 2.x JSON, MISP JSON, or Structured File, the file size is limited to 5 MB.

4. On the form, fill in the fields.

Field	Description
Upload file	Click this link to upload the data in the standard file format.
Set definitions	
TLP	Select the TLP indicator from the drop-down list to be applied for the imported records.
Confidence (0-100)	Define the confidence value.
Expiry Period (days)	Enter the expiry period of the associated observables.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This is a mandatory field.
Add Tags	Use the tags to annotate or ear mark records ingested into the system from this source. Staart typing the tag name in the Search bar to choose the available tags in the system or enter new tag name and click Add to assign it to the source.
Taxonomy	
Select a Taxonomy	Select the taxonomy for the imported data. Using taxonomies, define dictionaries that can be used as taxonomies assigned to threat intel records. For example, CAPEC nomenclature. For more information, see Creating Taxonomies.

5. Review the data before submission for processing.

   After you click **Next**, you can see the summary of all the information that user has provided in the above section, and the below section provides you with all the records that needs to be imported.

   User can perform any type of activities and the multiple users can collaborate using the comment section which is available in the right contextual menu.

   Note: The supported formats to import the data are TXT, CSV, JSON, XLS and any records that fail the validations are skipped from the import process and those records are not displayed on the Review & submit page for processing.

6. Click **Update Type** and select the type to update any type of the imported records.
7. Click **Delete** to delete any type of the imported records.
8. Click **Submit**.

   Note: After you submit the import record, the user will be directed to the approver to approve the corresponding import record based on the approval rules configured. If the current user who is creating the record doesn't require the approval process then the record goes through the auto approval process the import job gets auto approved while submitting request.

9. Click **View Status** to view the status of the record or click **Done**.
   The record displays the processed status once the submission is successful.
10. Click **Cancel** to abort the import process.
11. Click **Go Back** to go back to the previous page and review the record, if necessary.

Threat Analyst Workbench

The Threat Analyst Workbench page consists of cases and case tasks that are under Threat Analysts and their team.

Use the **Case Management** feature to create and track the threat investigations and analysis activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

During the threat investigations the analysts collect the data from internal intelligence records such as observables, threat actors, campaigns, and so on.

Workbench Overview

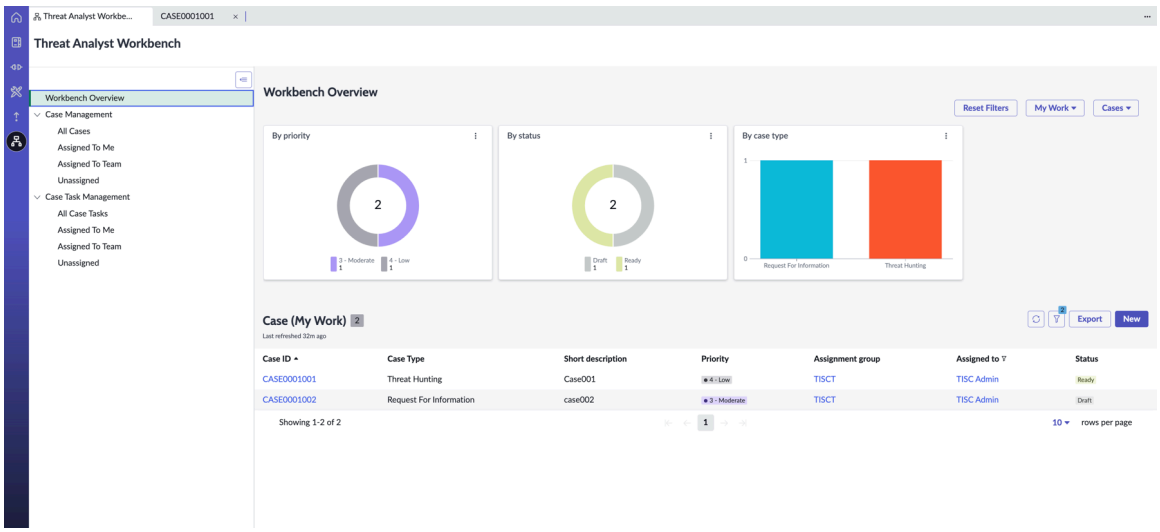
The Workbench Overview page consists of the Case Tasks and Cases that are under Threat Analysts and their team.

The overview lists all the open cases and their status which helps the analysts to manage their workload and prioritize their investigations.

Role required: sn_sec_tisc.analyst, sn_sec_tisc.admin

After the case is created, the analysts will then assign the case tasks to other analysts or teams for further investigation, and also collaborate with them to share information and insights.

There are various widgets present under each filter grouped by priority, status, and case type which are in the threat analysts' queues and threat analysts team's queue.



When filters are applied on the widgets, the bottom half of the overview page is populated with the corresponding cases or case tasks presented as list items. In order to remove the applied filters, click on **Reset Filters** to reset it to the original view.

Using this page, the threat analysts and admins can view their work, teams work, and any unassigned work. You can navigate to dropdown list. The available options are:

- My Work: Select this option to view the work assigned to you.
- My team's work: Select this option to view your team's work assigned to all the groups that you are part of.
- Unassigned work: Select this option to view the case or case task that are unassigned. To assign the case or case task, you must go to the form view and assign the user(s) or user group(s) to the case and case task(s).

You can also view cases and case tasks directly from the Workbench Overview that are assigned to you. By default, the case view is displayed, you can use the dropdown and select the case tasks if you want to view the case tasks by priority and status.

Creating cases using Threat Analyst Workbench

Cases are used to track information about a campaign or threat actor threatening your organization. After a case is created, you can add artifacts that allow you to review and analyze all related information from a single case or case task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_sec_tisc.analyst, sn_sec_tisc.admin

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Click **New**.
5. Fill in the fields as appropriate.

Create New Case

Field	Description
Case ID	A unique identifier for the case. This is system generated ID.
Short Description	Summary of the request or issue that is being investigated or a short description.
Description	A detailed description including any relevant information about the case such as background, what analysis is required, outcomes expected.
Case Type	Select the type of case being investigated. The possible options for the investigation are: ○ Threat Hunting ○ Request for Information ○ Vulnerability Management Case ○ Compliance Case ○ Incident Response Case ○ Collaboration Case ○ Others
Priority	An assessment of the severity of the request or issue.
Assignment group	The assigned group responsible for working on the case.
Status	The current status of the case.
Assigned to	The Analyst who is responsible for working on a case.
Due Date	The date and time that the task is due to be completed or closed.
Contributors	The list of assignees rolled up from tasks and should be possible to add on top of it.
TLP	Unique value that indicates the Data sensitivity setting per TLP.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Watch list	When a user is added to the watchlist, the person will receive email notifications on changes to status and priority.
Enforce Restriction	Select this check box to modify members of allowed group and allowed members. For more information, see Enforced Restrictions for case(s).

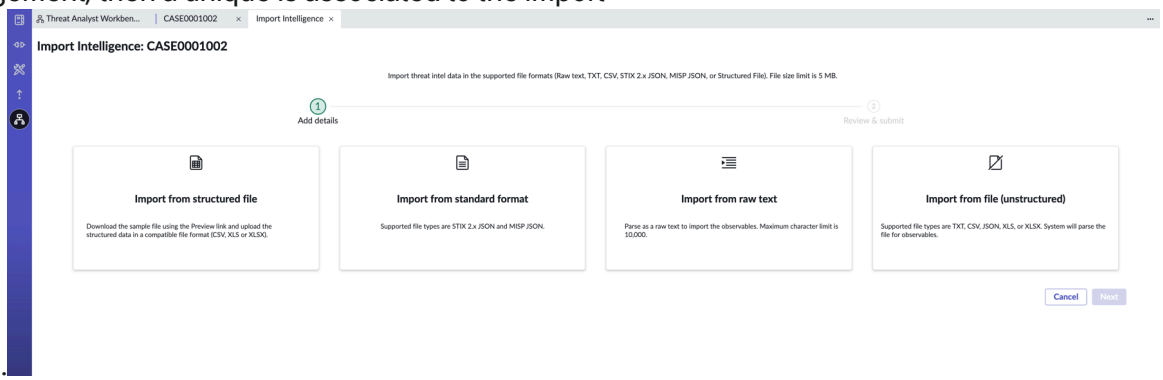
6. Fill in the fields on the Insights section, as appropriate.

Insights

Field	Description
Notes	Any additional notes related to the threat investigation.
Recommendations or Actions	Any recommendations or actions related to the threat investigation.
Analysis and Findings	Enter the analysis and findings related to the threat investigation.
Closure Summary	Add the closure summary of the findings.

7. Click **Save**.
After the record has been saved, you can click the **Import Intelligence** tab to import the threat intel data using the **Import Intelligence** feature.

Note: If you are importing and processing data from Case Management, then a unique is associated to the import record.



Enforced Restrictions for case(s)

Use this feature to restrict a case and provide list of groups and users who can access it.

Role required:

- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key considerations

1. Restrict a case and provide list of groups/users who can access it.
2. Enable Enforce restriction field on the Case form page.
3. Modify members of allowed group and allowed members.
4. Once a case is marked as restricted, only members of allowed groups, member of allowed user list and user with sn_sec_tisc.admin role can access this case.
5. Grant access to the analyst (sn_sec_tisc.restriction_access_manager) who needs to access to the Enforce restriction field.
6. Existing assigned_to analyst and analyst who marked it as restricted will also loose access if they are not added to the allowed groups or members.
7. Restriction of case within CTI team is implemented on per-case basis. Allowed members can access restricted cases if they are in allowed list. Putting them in one of the cases allowed list doesn't imply that they can access all other restricted cases.
8. If case is marked restricted and allowed members or allowed group is left empty then only sn_sec_tisc.admin can access those restricted cases.
9. Only the groups who has the analyst (sn_sec_tisc.analyst) role assigned, are allowed in the allowed members and allowed groups list.

Note: A worknote is posted if a case is marked as restricted.

Access controls for a case

Allow access controls specific to a case.

The following table describes the roles and access controls.

Role	Access	Description
sn_sec_tisc.restriction_access_manager	Read access	External Users added here will get access to view the case form but will not be able to edit any field in the case or perform any action.
	Privileged access	External Users added here will get access to edit any field in the case form but will not be allowed to run orchestrations.
sn_sec_tisc.special_access_read_manager	Read access	External Users added here will get access to view the case form but will not be able to edit any field in the case or perform any action.
sn_sec_tisc.special_access_write_manager	Privileged access	External Users added here will get access to edit any field in the case form but will not be allowed to run orchestrations.

External user access for case tasks

This section describes the external user access for case tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Case tasks assignment to external users

Case tasks are assigned to the users with the external role even though they do not have access to sn_sec_tisc.analyst role.

1. Any external user assigned with a case task can only see case task module and will have the privilege to edit the case task.
2. The external user can only see the case tasks assigned to that specific user or the group(s) the user belongs to.
3. The external user should be able to re-assign the task within the group the user belongs to.

Associate MITRE Techniques to a Case

Associate one or more MITRE technique to a case.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case.
5. Click **Associate MITRE Technique** button.
6. Click **Add Matrix** to associate the MITRE technique.
   The **Associate MITRE Technique to Case** dialogue box is displayed.
7. Select the **Matrix**.
   All the enabled matrices will be displayed for you to select the Matrix.
8. Select the tactic from the drop-down lists.
   All the tactics associated to a matrix will be displayed.

   Note: In case if you would want to add more tactics then click **Add Tactic**. The previously selected tactics will no longer be displayed in the drop-down list if you are adding a new tactic.

9. Select the **Technique**.
   All the techniques associated to your selected tactic will be displayed. In case if you are adding more tactics then you can select the associated techniques for that selected tactics.
10. Click **Save**.
    If you want to delete the entire matrix associated data then click on **Delete Matrix**, this action will only remove the associated matrix data but the matrix will remain in the MITRE ATT&CK Repository.

    The associated matrix data record is displayed under the MITRE ATT&CK Card section. In the card view:

    Note: You can toggle between multiple matrices from the Matrix drop-down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. The first row of the card view displays all the tactics associated to the current selected matrix.

b. Each tactic card shows the tactic name and number of techniques of that tactic mapped to the current case record.

c. All the associated techniques to that case are vertically showed under each tactic. You can click on any technique to view the technique form view.

11. Click **Show ID** will show the IDs for all the associated techniques.

> **Note:** Each technique card shows the technique name and technique ID only when **Show ID** is enabled.

12. Click **Refresh** to refresh the card view.
You can view the time stamp of the last refresh for the selected matrix.

> **Note:** Click pop out icon to pop out the associated matrix card to view in a new tab.

Roll up of MITRE technique associations

Roll up of MITRE technique associations from observables, indicators, objects, and security incidents which are linked or unlinked from a case record.

Before you begin

> **Note:**
>
> - Roll up of MITRE technique associations for security incidents will roll up the MITRE technique associated data from security incidents to the case management in TISC.
> - By default this property sn_sec_tisc.auto_rollup_mitre_data is enabled for the MITRE Technique(s), to be rolled up to case(s) from the associated objects or security incidents automatically.
> - If you want to perform on demand roll up of MITRE technique associations then navigate to the more actions within the **Case form view** and select **Roll Up MITRE Techniques** option. This operation will happen asynchronously and you can verify the **Activity Stream** section for the updates on the roll up activity.

Role required: sn_sec_tisc.analyst

About this task

- Whenever any entity such as an observable or indicator is linked to any case, then all the MITRE technique associations that are present for that entity are automatically rolled up to the case.
- Whenever any entity such as an observable or indicator is unlinked and removed from the case, then all the MITRE technique associations which are rolled up from the case that are present for that entity will be removed automatically and rolled up to the case.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
All the cases are displayed.
4. Open any case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Go to **Artifacts** tab.
6. Select **Observables** from the artifacts related list.
7. Select the **Link** button.
8. Select the observables that you may want to link to the case.
9. Click **Link** to link the observables.
   After you link the observables to a case then the MITRE techniques associated for that particular observable are automatically rolled up and the MITRE techniques list count under the artifacts section is automatically updated.
10. Click **Unlink** to unlink the observables from the case.
    After you unlink the observables to a case then the MITRE techniques associated for that particular observable are automatically removed and the MITRE techniques list count under the artifacts section is automatically updated.

Create case task using Threat Analyst Workbench

Create case tasks to associate with case(s).

Before you begin

Role required: sn_sec_tisc.analyst, sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Task Management** > **All Cases Tasks**.
   All the case tasks are displayed.
4. Click **New**.
5. Fill in the fields as appropriate.

Create New Case Task

Field	Description
Task ID	A unique identifier for the case task. This is system generated ID.
Short Description	Summary of the request or issue that is being investigated or a short description.
Description	A detailed description including any relevant information about the case task such as background, what analysis is required, outcomes expected.
Parent Case ID	Select the parent case ID from the lookup.
Priority	An assessment of the severity of the request or issue.
Assignment group	The assigned group responsible for working on the case task.
Status	The current status of the case task.
Assigned to	The Analyst who is responsible for working on a case task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Due Date	The date and time that the case task is due to be completed or closed.
TLP	Unique value that indicates the Data sensitivity setting per TLP.
Enforce Restriction	As an sn_sec_tisc_admin, select this check box to modify members of allowed group and allowed members. For more information, see Enforced Restrictions for case(s).

6. Fill in the fields on the Insights section, as appropriate.

Insights

Field	Description
Notes	Any additional notes related to the threat investigation.
Closure	Add the closure summary of the findings.

7. Click **Save**.
   Your case task will be associated with your case.

> **Note:** After saving the case task, you can add tags and taxonomies to the task. For more information, see Creating Taxonomies.

Working with Investigation Canvases

The Investigation Canvas is a key significant feature which provides more valuable information for the Threat Intelligence (TI) analysts. It provides a structured framework by mapping one to one or one to many relationships and visualizing information related to observables, indicators of compromise (IOCs), or entities.

By using the investigation canvas, threat analysts can effectively:

- **Map Relationships**: Visualize node connections between different entities such as observables, indicators of compromise (IOCs), threat actors, attack patterns, affected assets and so on.
- **Link cases or canvases**: Link a case or canvas to enhance the analysis and provide a more comprehensive view of the threat landscape within the case management.
  - The linking feature enables analysts dynamically add or remove nodes. This also populates the existing relationships between the nodes to the canvas.
  - Temporary Relationship graphs by saving relationships separately within the context of the Investigation Canvas.
- **MITRE technique associations**: Associate or remove MITRE techniques with nodes directly on the canvas and provide analysis on the MITRE kill chain card.

Entry Points for the investigation canvas

1. **First entry point: New Blank Canvas**: This entry point should allow the analysts to open a new and blank canvas without any nodes or links.
2. **Second Entry Point: Open Canvas in Case Investigation**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. This entry point opens an existing investigation case and allows to edit, modify, and rename the canvas.

b. A new canvas with existing artifacts as nodes.

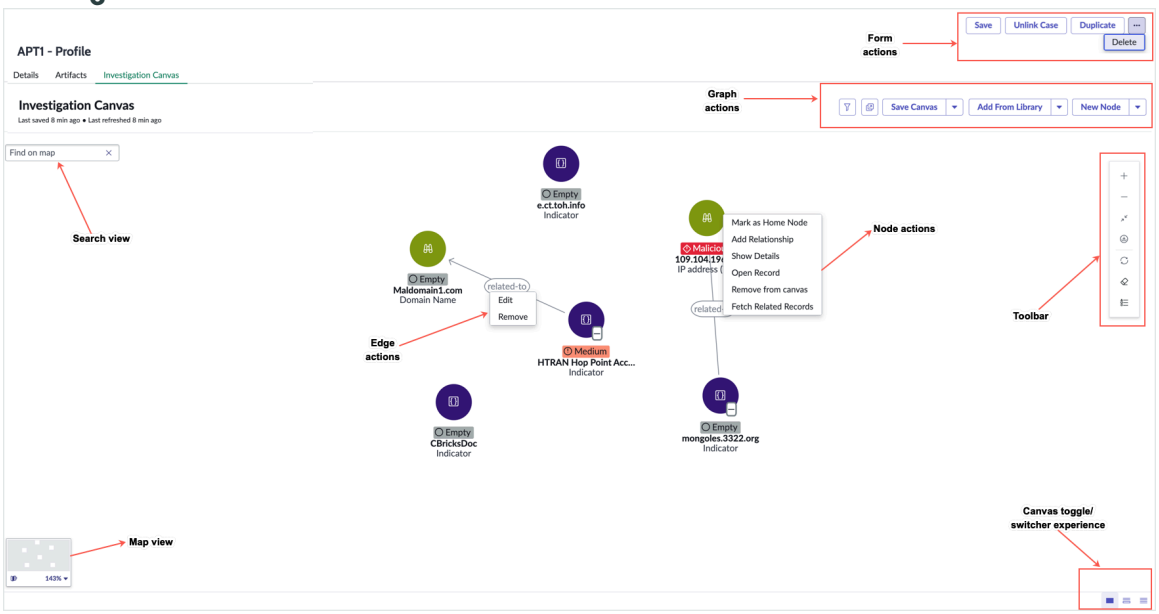
Understanding investigation canvas actions

This section describes the various actions that you can perform on the investigation canvas.

Investigation canvas includes:

1. Form actions
2. Graph actions
3. Node actions
4. Edge actions
5. Map actions

Investigation Canvas



Investigation canvas Form actions

Action	Operation
Link Case	Allows to link cases on the investigation canvas.
Unlink Case	Allows you to unlink the cases on the investigation canvas.
Duplicate	Option to duplicate the nodes on the investigation canvas.

Investigation canvas Graph actions

Action	Operation
Save Canvas	Allows you to save the investigation canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Investigation canvas Graph actions (continued)

Action	Operation
Add Data to Library	Allows you to create new relationship between two different nodes.
Add From Library	Creates new relationships and threat entities in the threat intelligence library if the newly added nodes and edges in the canvas are not already part of the library.
Add From Case Artifacts	Allows you to add data from corresponding case artifacts that is linked to the canvas.

Investigation canvas Node actions

Action	Operation
Mark as Home Node	Option to mark that specific node as a home node.
Add Relationship	Option that allows you to add various object relationships. You can add one to many or many to one or many to many node relationships.
Show Details	Option that shows details of that specific node.
Open Record	Option that allows you to open the record in a new tab.
Remove from Canvas	Option that allows you to remove the node from the canvas.
Fetch Related Records	Option that allows you to fetch the related records for that specific node.

Investigation canvas Edge actions

Action	Operation
Edit	Allows to link cases on the investigation canvas.
Remove	Allows you to unlink the cases on the investigation canvas.

Investigation canvas Map actions

Action	Operation
Zoom in	Option to zoom in the investigation canvas to easily focus on specific areas of the canvas.
Zoom out	Option to zoom out the investigation canvas to easily focus on specific areas of the canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Investigation canvas Map actions (continued)

Action	Operation
Fit to screen	Option to fit the investigation canvas to the screen size.
Export map	Option to export the investigation canvas as a PDF for better viewing.
Refresh	Option to refresh the investigation canvas data.
Switch to unified vertical layout	Option to switch the investigation canvas view to unified vertical layout to enhance the clarity between the nodes.
Switch to unified force layout	Option to switch the investigation canvas view to unified force layout to enhance the visualization of complex relationships between the nodes.

Linking an existing case from Investigation Canvas

Use this section to link an existing case from the investigation canvas.

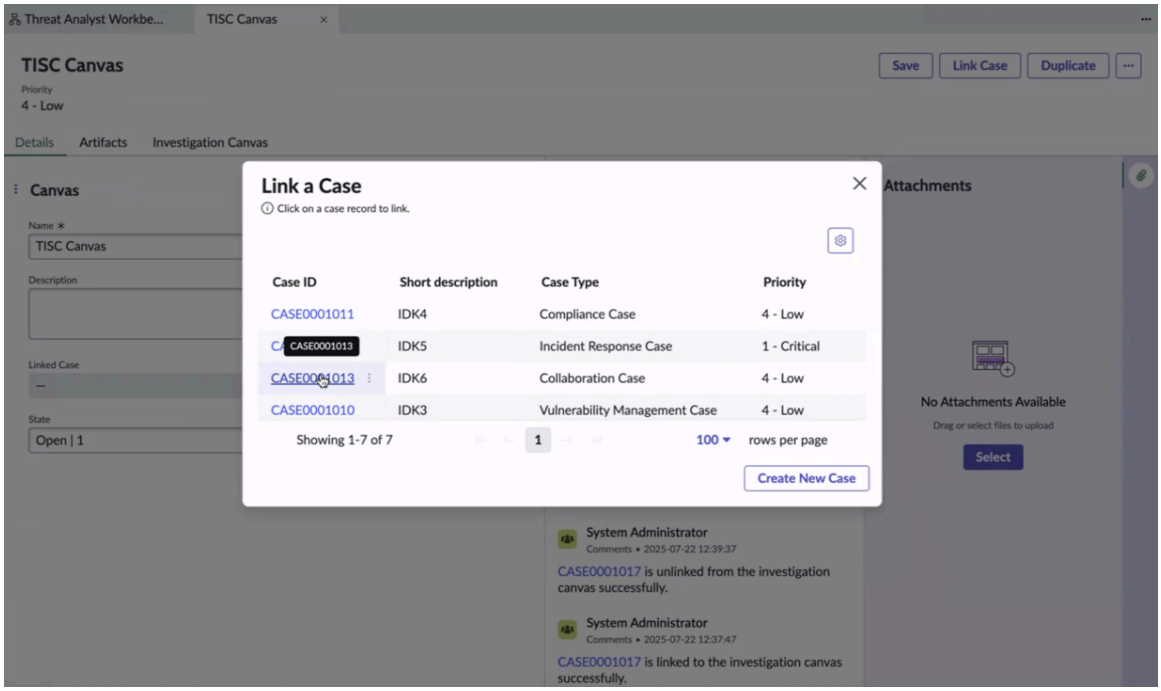
Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   This displays all the cases.
4. Select **Case Management** > **All Cases**
5. Open any case record from the list view.
6. Select **Link Case** from the **Details** section.
   The Link a Case dialogue box appears.
7. Select a case ID from the list to associate the case to an investigation canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



A confirmation message is displayed confirming that the case is linked successfully.

Note: In case if no case is available for linking to the Investigation Canvas, you can create a new case to initiate and organize your investigation context. For more information on how to create a new case, see Creating a Case and Linking from Investigation Canvas

.

8. To remove a linked case, select the **Unlink** button.

Related topics

Create an investigation canvas

Creating a Case and Linking from Investigation Canvas

Use this section to create and link a case(s) from an investigation canvas.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   This displays all the cases.
4. Open any case record from the list.
5. Select **Link Case** from the **Details** section.
   The Create and Link Case dialogue box appears.
6. Select a case from the list to associate the case to an investigation canvas.
7. Select **Create New Canvas**.
   The Create New Case dialogue box appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Fill in the form fields, as appropriate.

Field	Description
Case ID	A unique identifier for the case. This is system generated ID.
Short description	Summary of the request or issue that is being investigated or a short description.
Case Type	Select the type of case being investigated. The possible options for the investigation are: ○ Threat Hunting ○ Request for Information ○ Vulnerability Management Case ○ Compliance Case ○ Incident Response Case ○ Collaboration Case ○ Others
Priority	Indicates the priority of a case.
Assignment group	The assigned group responsible for working on the case.
Status	The current status of the case.
Assigned to	The analyst who is responsible for working on a case.

9. Select **Create and Link** to create a new case and link it directly to the investigation canvas.

   A confirmation is displayed confirming that the case is created and linked to the investigation canvas successfully.

   Note: This option is useful when no existing case is associated with the investigation canvas.

10. To remove a linked case, select the **Unlink** button.
    For more information on how to directly link an existing case to the investigation canvas, see Linking an existing case from Investigation Canvas.

Related topics

Create an investigation canvas

Linking Canvas from a Case

Use this section to link a canvas from a case.

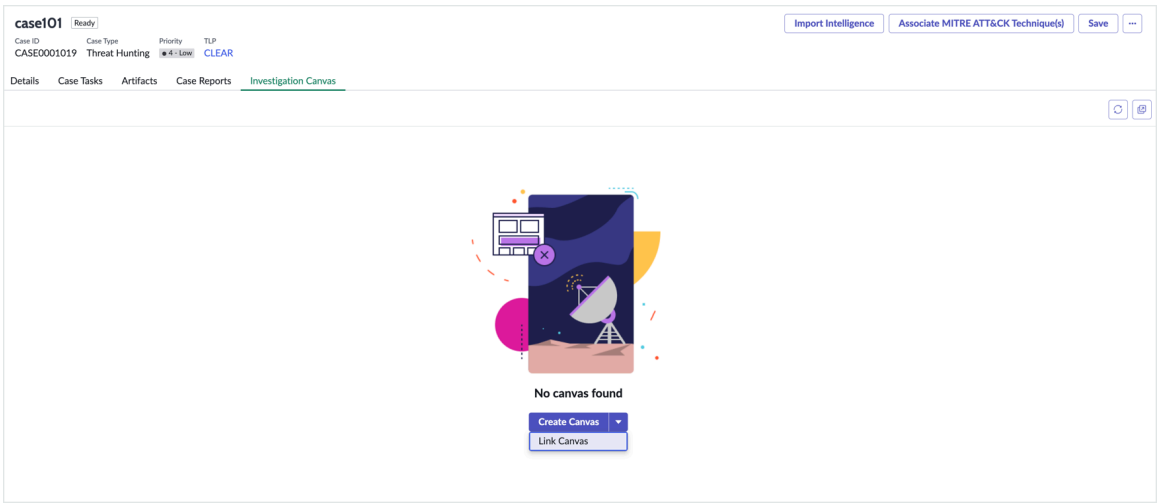
Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Investigation Canvases** > **All Canvases**.
4. From the **All Cases** list view, select a case which is not linked to the canvas.
5. Go to **Investigation Canvas** section.
6. Select **Link Case** from the drop down list on the empty canvas page (the option is shown in the following screenshot).



7. Select the canvas.
8. Select the **Link** button to link the canvas to a case.

   An information message is displayed indicating that the canvas data is refreshed successfully.

Create an investigation canvas

Create a new canvas to add observables from threat intelligence library.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Investigation Canvases** > **All Canvases**.
4. Click **New**.
5. Fill in the fields as appropriate.

Create New Canvas

Field	Description
Name	Enter the name of canvas.
Description	Add the description of the canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Linked Case	Option that displays the list of cases that do not have any canvases associated. This field value is populated based on the case that is linked to the corresponding canvas.
Priority	Select the priority of the canvas.
State	Select the state of the canvas.

6. Click **Save**
   The two new sections are displayed **Artifacts** and **Investigation Canvas**. When you create a new canvas, the canvas does not include any nodes. You must add nodes from Threat Intelligence library or artifacts through the option of add from library.
7. Go to **Investigation Canvas**.
8. Click **Add from Library**.

   Note: There are two options available to add the nodes. You can select either **Import** to import all the observables or select **Add from Library** option to add the observables from the threat intelligence library.

   The **Import node from Library** dialogue box displays.
9. Select the **Type of node** from the drop down list.
   For example, select the type as Observables if you are adding observables to the investigation canvas.
10. Select the required number of observables.
11. Click **Import**.
    After you import observables, the nodes are added to the investigation canvas. Whatever the nodes that are added to the canvas are currently added temporarily to the canvas and it will not be persisted to the canvas.
12. Select **Save Canvas**.
    If you want to process the nodes data to the canvas then you must save the data to keep it permanently.

    Note: If you do not perform the **Save Canvas** option then you may loose the data whenever you refresh the canvas.

13. Select **Add Data to Library** to create any new relationship between two different nodes.
    The relationship between the two nodes is indicated with the dotted line which means the nodes are temporary. In case, if you want to move the nodes data to the relationships, then select **Save data to library** and add data to library. After you perform this operation the dotted line will turn to a solid edge line indicating that the node is now is part of the library.
14. Use the **Filter** icon to view the type of observables and objects that are present in the canvas and you can selectively choose the type of data to be shown under the investigation canvas.
15. Also, select the pop out icon to view or perform any operation on the investigation canvas nodes on a larger space.
16. Select **Link Case** to link the case to the investigation canvas.
    a. Select the **Case ID**.
    b. Click the **Link** button.
17. Click **Duplicate** to duplicate the canvas data and nodes within the canvas.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Adding a new node to the canvas

Use this section to create and add new entities, including observables or objects, directly from the investigation canvas.

Before you begin

This feature enables quick enrichment of the canvas without having to navigate away from the current view.

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
4. Open any case record.

   Note: When creating a case, you're required to either create a canvas or link an existing one. After linking, the canvas actions including the option to add new nodes will be automatically available in the user interface.

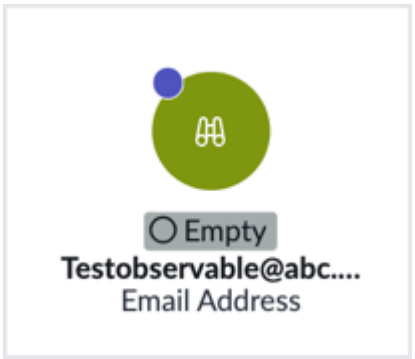
5. Select **Investigation Canvas** > **New Node**.
   - You can also view the **New Node** functionality from the drop-down list of the empty**Investigation Canvas** section of the Case.
   - Another option to view the **New Node** functionality is to view from the investigation canvas page directly.
6. To create a node, select the appropriate **Entity Category** and **Entity Type**.

Field	Description
Entity Category	Select the entity category such as Observ able, or Object.
Entity Type	Select the entity type from the available op tions based on the select category. **Note:** ○ When an entity type is selected, the corresponding object form is automati cally displayed, showing the key fields such as Name and Description along with any required fields that are need ed to identify the parent entity. ○ If you attempt to create a duplicate entity, which means if you select an entity, which is existing in the appli cation and try to create one with the same value then an error message will appear indicating that the entity al ready exists in the Threat Intelligence Library with the same value and type.

7. Fill the necessary object details such as name, description.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Select **Add** to add the new node.
   This process automatically adds the node to the investigation canvas.

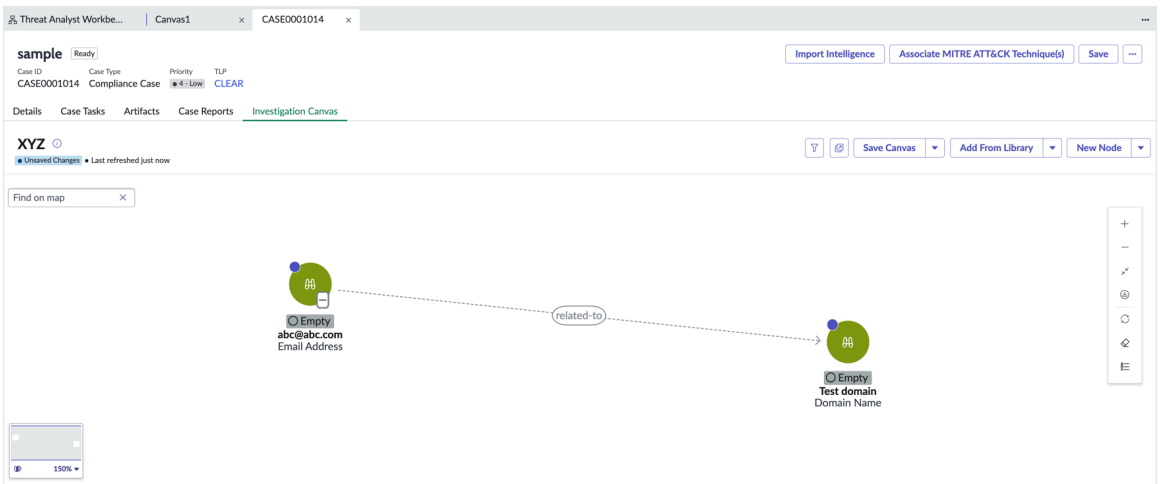


   The newly added nodes are visually differentiated with a dot on the node them from nodes that are imported through the library or case artifacts.

> **Important:** Newly added nodes are temporary and aren't saved to the threat intelligence library or canvas. If you refresh the canvas before saving, these nodes will be lost. Make sure to save the canvas after adding any new nodes to retain your changes.

9. Right click on the new node and select **Add Relationship** option to create relationships between the nodes.

> **Note:**
>
> - When creating new relationships, the edges are appeared as dotted lines, indicating they are temporary nodes and aren't saved in the Threat Intelligence Library.
> - Newly added edges are temporary and aren't saved to the threat intelligence library or canvas. If you refresh the canvas before saving, these edges will be lost. Make sure to save the canvas after adding any new edges to retain your changes.



10. Right click and select **Show Details** to view the details related to the selected entity.

> **Note:** To add data, you can either click the hyperlink within the details pane or select **Open Record** option and add the required node related data.

11. Select **Add Data to Library** option to save all the nodes and edges that were temporarily added during your investigation.
    By performing this action, the temporary records are converted to permanent aggregated records within the Threat Intelligence Library.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Investigation canvas and MITRE ATT&CK

In the investigation canvas, view the MITRE ATT&CK techniques and sub-techniques which are associated to all the nodes in the canvas.

Important: In the framework, the techniques and sub-techniques that are associated with the nodes in the canvas are highlighted.

Role required: sn_sec_tisc.analyst

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**. All the cases are displayed.
4. Select any case.
5. Go to **Investigation Canvas** tab.
6. On the investigation canvas, use the **Resizeable panels divider handle** to drag to view the MITRE ATT&CK framework.
7. Select the required MITRE ATT&CK matrix from the **Matrix** drop-down list. The MITRE ATT&CK Framework shows different levels of tactics and techniques association.
   - The top row displays all the tactics that are present in the selected **Matrix**. By default, all the tactics display the count of the total techniques and sub-techniques present for that corresponding tactics. You can use the **Refresh** icon to reload the MITRE ATT&CK framework and view the latest associations.
   - Under each tactic, the framework displays all the techniques that are present as a relationship to that corresponding tactic.
   - The framework displays the sub-techniques that are present under each technique. Expand each technique to view the sub-techniques.
8. View the MITRE ATT&CK techniques and sub-techniques related to all the nodes (entities) in the canvas.
9. Click on one or more node(s) to view the associated MITRE ATT&CK techniques and sub-techniques related to those selected node(s) in the canvas.
10. Use **View Controls** to view the associated MITRE ATT&CK techniques and sub-techniques of the selected node(s). From the controls lists:
    - Select **Show ID** to view the techniques and sub-techniques MITRE IDs.
    - Select **Show Sub Techniques** to view all the sub-techniques. When you select this option, all the techniques are shown in the expanded view. The expanded view of the technique shows all the sub-techniques that are present for that corresponding technique.
    - Select **Show Only Associated Techniques** to view only MITRE techniques that are associated to the nodes in the canvas. When you select this option, each tactic shows the total number of associated techniques and sub-techniques.
11. Click on the pop out icon to view the MITRE ATT&CK Framework in a larger space.

Important:

- Whenever you add or remove a node, the MITRE ATT&CK framework gets refreshed automatically and you can also use the refresh icon to do a manual refresh.
- Whenever you filter the specific types of nodes, even then the MITRE ATT&CK framework gets refreshed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Investigation Canvas MITRE Filters

MITRE filters enables you to create and save filters for Tactics, Techniques, and Procedures (TTPs) associated with specific adversaries and other MITRE technique attributes.

Before you begin

Role required: sn_sec_tisc.analyst

About this task

Analysts can use the filters available on the MITRE card to filter specific actor TTPs that are relevant to adversaries involved in the investigation.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
4. Open any case.
5. Go to **Investigation Canvas** tab.
6. Select **Filters** to create filters for Tactics, Techniques, and Procedures (TTPs) associated with specific adversaries and other MITRE technique attributes.
7. Fill in the necessary values in the filter panel to apply your desired filters.
   The MITRE filter panel allows you to filter and visualize MITRE ATT&CK techniques based on selected criteria such as Groups, Malware, Tools, Tags, and Priority.

Field	Description
Saved Filters	Analysts can save specific criteria as **Saved Filters** for reuse. Filters saved by an analyst are user-specific. **Note:** For example, if Analyst X saves a filter configuration, it will only be visible to Analyst X. When another analyst log in and view the filter drop down, they will not see the filters saved by others. This ensures that each user can create and manage personalized views without affecting or being affected by other users' filter preferences.
Filter Name	Name of the filter.
MITRE Group	Indicates the MITRE Group. Select one or more groups to filter techniques associated with them.
MITRE Malware	Indicates the MITRE Malware. Select one or more malware items to filter techniques associated with them.
MITRE Tools	Indicates the MITRE Tools. Select one or more tools to filter techniques associated with them.

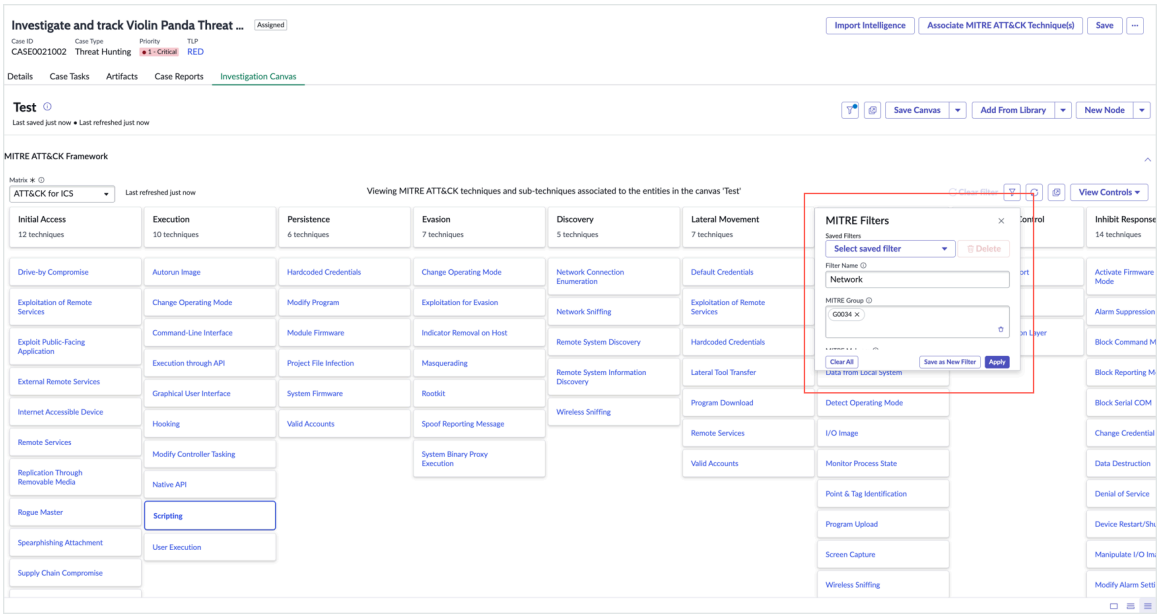
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
TISC Tags	Indicates the TISC tags. Select one or more tags to filter techniques based on their classification.
Priority of Techniques	Indicates the priority level of techniques. You can select one or more options to filter techniques based on their assigned priority.
Clear All	Allows you to clear the inputs entered in the filter panel.
Save as New Filter	Saves the criteria entered in the filter panel as a new saved filter. **Note:** Saved filter name should be unique.
Save Current Filter	Saves changes to the criteria in the currently selected saved filter. You can also rename a filter using this option. **Note:** Saved filter name should be unique.
Apply	This option allows you to apply the changes to your filters in the MITRE card.
Delete	Select this option to remove a selected saved filter. When you click the **Delete** button next to a saved filter, a confirmation message appears if you are sure you want to delete this filter. Confirming this action will permanently remove the saved filter. To remove an individual field value within the filter panel, click the **Delete (trash)** icon next to that specific field.

By applying filters using these values, the MITRE matrix is dynamically updated to display only those techniques associated with the selected attributes. This focused view enables analysts to concentrate more on the most relevant Tactics, Techniques, and Procedures (TTPs) during investigations.

In addition, analysts can further narrow down TTPs using filters for malware, tools, tags, and priority levels.

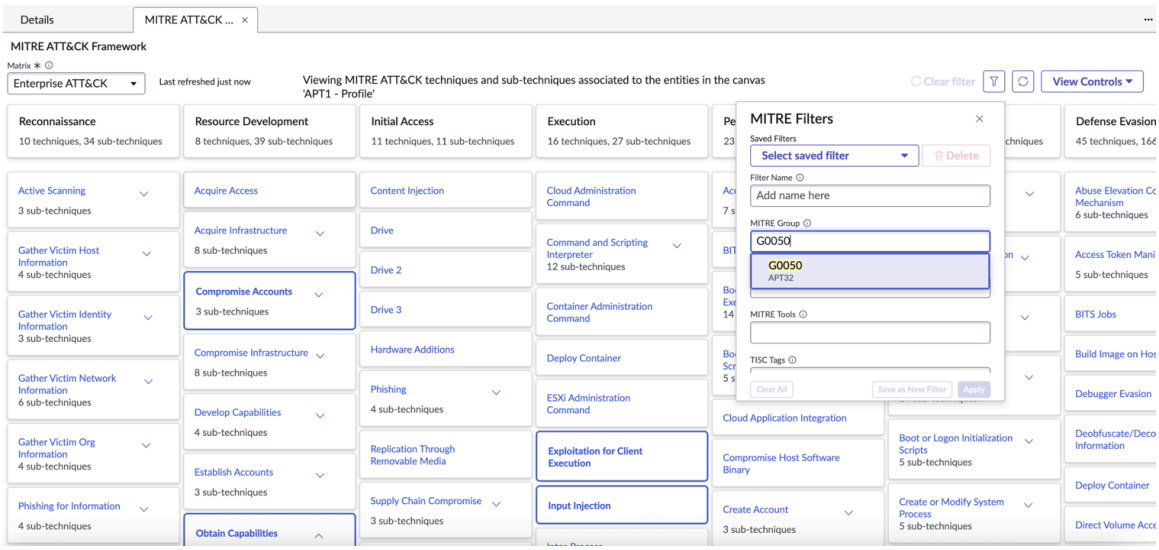
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. **Optional:** Select **Save as New Filter** to save your filter criteria.
9. Select **Apply** to apply the changes.

Example: Filtering by MITRE Group

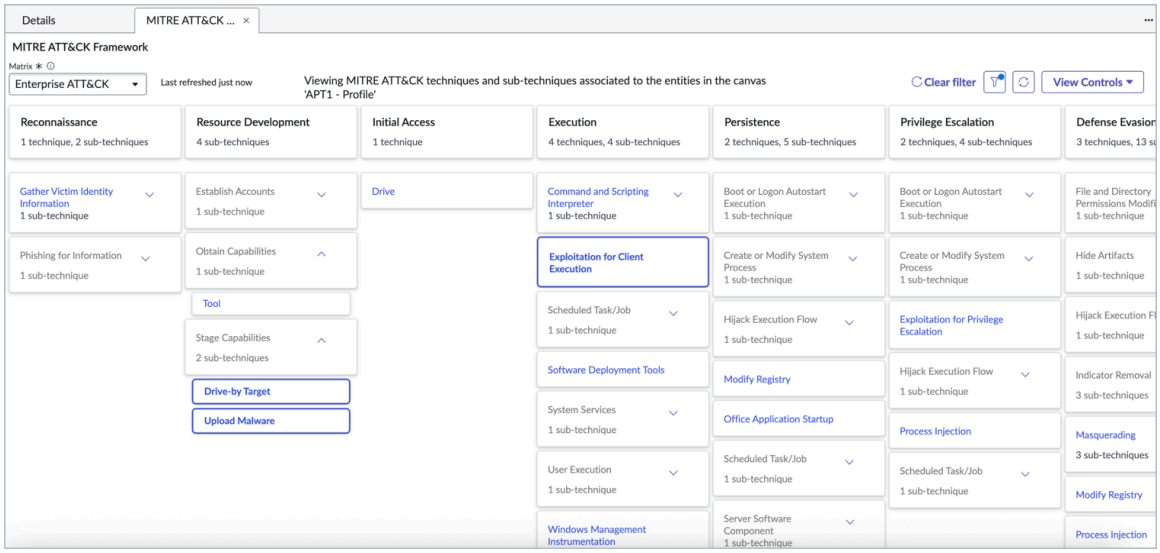
Select a MITRE group as APT32 (G1001, see the following screenshot). When you apply this filter, the MITRE matrix updates to display only those techniques that are directly linked to the selected group.



This focused view helps analysts to concentrate specifically on the Tactics, Techniques, and Procedures (TTPs) associated with the selected threat group.

When you apply the filter, a few techniques in the matrix are displayed in blue text, while other techniques appear in gray.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The visual representation on the MITRE Framework indicates how techniques and sub-techniques relate to the applied filters and investigation context.

- **Blue text:** Techniques or sub-techniques shown in blue text indicate those that match the filter criteria.
- **Blue text in bold with blue border:** Techniques or sub-techniques displayed in bold blue text with a blue border indicate those that match the filter criteria and are associated with one or more nodes on the canvas.
- **Gray card:** Parent techniques are displayed in gray when they do not directly match the filter criteria (which means they are not linked to the selected group) but are shown to represent the parental relationship to linked sub-techniques that match the filter criteria.

Add artifacts to case(s) or case task(s)

After you have created a case, you can view or add artifacts, such as security incidents, CIs, and indicators of compromise, to the case. These artifacts act as clues in solving the case.

Before you begin

Role required: admin

Note: Artifacts are available only to the existing cases. For observables and indictors, the artifacts can also be added or associated to a case from the import job using the Import Intelligence button. For more information on how to import see, Import Threat Intelligence

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case or case task.
5. Go to **Artifacts** tab.
   The associated artifacts are displayed as the related lists for that specific case or case task.
6. Link or Unlink the records from the case or case task.

Note: For more information, see Link Threat Intel Related Records

Following table lists the artifacts related lists related to the case(s) or case task(s):

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records

Related List	Description
MITRE Techniques	List the MITRE techniques related to the case(s). MITRE techniques also displays all the associated techniques in a case. For more information, see Show MITRE ATT&CK Framework for a Case(s).
Observable	List of observables related to this cases or case tasks.
Indicators	List of indicators related to this cases or case tasks.
Attack Patterns	List of attack patterns that are related to this cases or case tasks.
Campaigns	List the campaigns that are related to this cases or case tasks.
Course of Actions	List the course of actions that are related to this cases or case tasks.
Data Components	List of Data Components that are related to this cases or case tasks.
Threat Groupings	List the threat groupings that are related to this cases or case tasks.
Identities	List the identities that are related to this cases or case tasks.
Infrastructure	List the Infrastructure such as systems, software services, and any associated physical or virtual resources that are related to this cases or case tasks.
Intrusion Sets	List the intrusion sets such as a set of adversarial behaviors and resources with common properties that are related to this cases or case tasks.
Locations	List the locations records that are related to this cases or case tasks.
Malware	List the malware source records that are related to this cases or case tasks.
Marking Definitions	List the marking definitions records that are related to this cases or case tasks.
Threat Notes	List the marking definitions records that are related to this cases or case tasks.
Observed Data	List the observed data that are related to this cases or case tasks.
Threat Opinions	List the threat opinions that are related to this cases or case tasks.
Threat Reports	List the threat reports that are related to this cases or case tasks.
Sightings	List of sightings that are related to this cases or case tasks.
Threat Actors	List the threat actors that are related to this cases or case tasks.
Tools	List the tools that are related to this cases or case tasks.
Vulnerabilities	If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address that are related to this cases or case tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related List	Description
Related Cases	Lists the related cases.
Related Case Tasks	Lists the related case tasks.
Security Incidents	List the security incidents that are related to this cases or case tasks.
Affected Configuration Items	List the affected configurations items that are related to this cases or case tasks.
Affected Services	List the affected services that are related to this cases or case tasks.
Affected Assets	List the affected assets that are related to this cases or case tasks.
Vulnerability Entries	List the vulnerability entries that are related to this cases or case tasks.

Roll up of MITRE Techniques from Artifacts to Case

When intelligence records are added to a case, all associated MITRE Techniques are automatically rolled up to the case level.

Before you begin

Role required: admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case.
5. Go to **Artifacts** tab.
   The associated artifacts are displayed as the related lists for that specific case.

Show MITRE ATT&CK Framework for a Case(s)

Displays all the associated techniques of a case on the MITRE ATT&CK framework.

Before you begin

Role required: sn_sec_tisc.analyst

About this task

Select the required MITRE ATT&CK matrix from the **Matrix** drop-down list. The MITRE ATT&CK Framework shows different levels of tactics and techniques association.

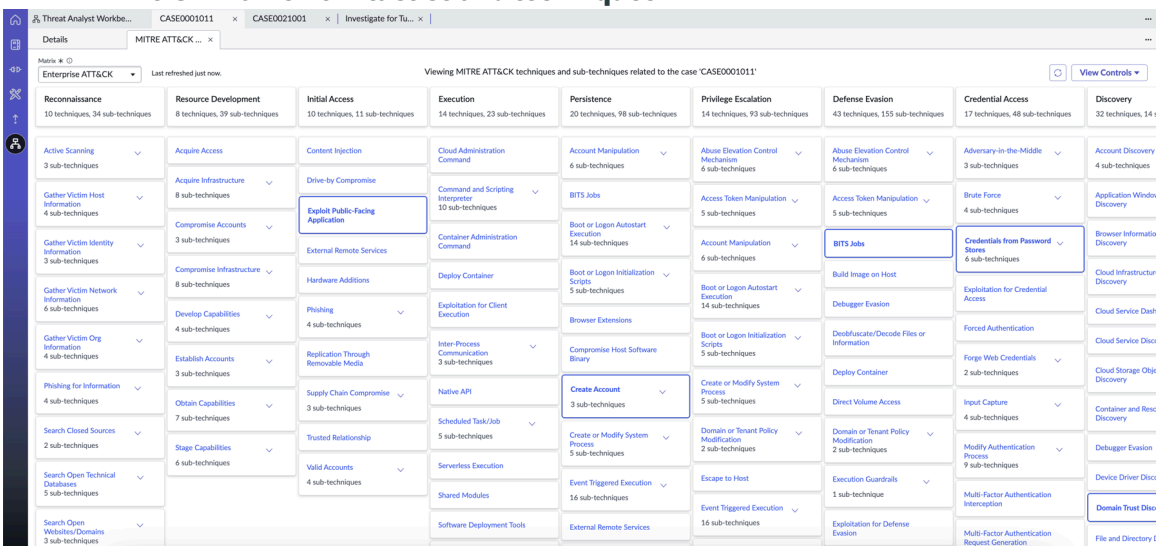
1. The top row displays all the tactics that are present in the selected **Matrix**. By default, all the tactics display the count of the total techniques and sub-techniques present for that corresponding tactics. You can use the **Refresh** icon to reload the MITRE ATT&CK framework and view the latest associations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Under each tactic, the framework displays all the techniques that are present as a relationship to that corresponding tactic.
3. The framework displays the sub-techniques that are present under each technique. Expand each technique to view the sub-techniques.

Important: In the framework, the techniques and sub-techniques that are associated with a case are highlighted.

MITRE ATT&CK Framework tactics and techniques



Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click the **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case.
5. Go to **Artifacts** tab.
   The associated artifacts are displayed as the related lists for that specific case.
6. Select **Show MITRE ATT&CK Framework** button
   When you select this button, the framework displays all the associated techniques of a case and artifacts on the MITRE ATT&CK.
7. View MITRE ATT&CK techniques and sub-techniques related to the case from the MITRE techniques that you have selected to view.
8. Select any record to view the MITRE ATT&CK techniques and sub-techniques related to the case.
9. Use **View Controls** to view the MITRE ATT&CK techniques and sub-techniques as desired.
   From the controls lists:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Select **Show ID** to view the techniques and sub-techniques MITRE IDs.
- Select **Show Sub Techniques** to view all the sub-techniques. When you select this option, all the techniques are shown in the expanded view. The expanded view of the technique shows all the sub-techniques that are present for that corresponding technique.
- Select **Show Only Associated Techniques** to view only MITRE techniques that are associated with a case. When you select this option, each tactic shows the total number of associated techniques and sub-techniques.

Run Enrichment Actions within a case

Use this section to understand how enrichments actions are performed on case(s).

Before you begin

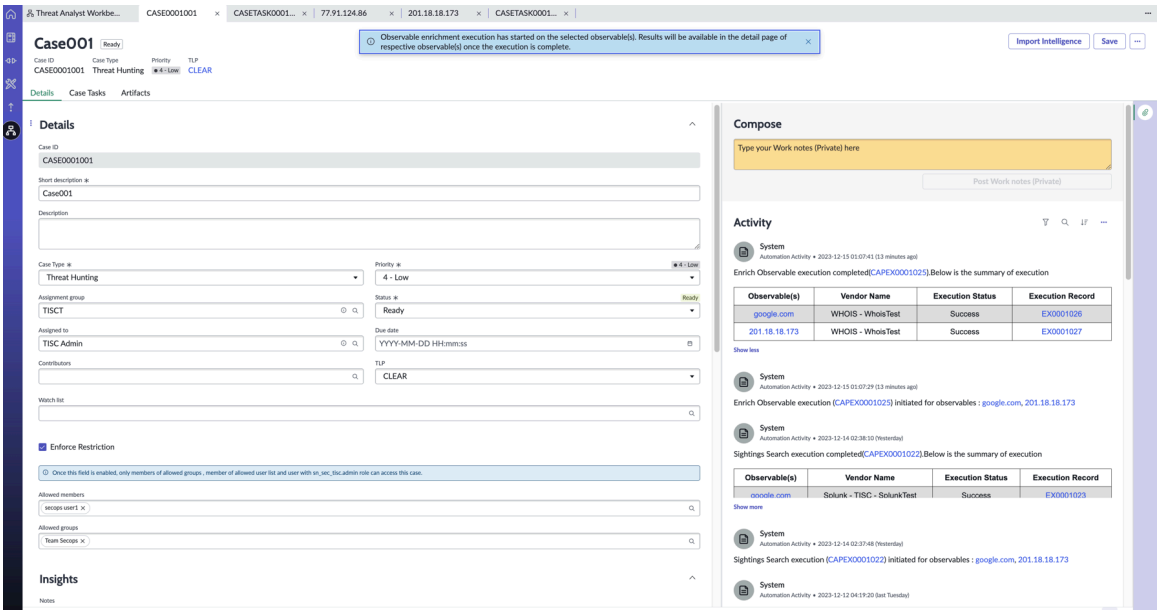
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case or case task.
5. Go to **Artifacts** tab.
6. Select the Observables related list.
7. Select one ore more Observables.
8. Click any Enrichment actions from the dropdown list.
9. Select the available implementation(s).
10. Click **Submit**.
    For example, Run Threat Lookup. The selected enrichment action will be executed and an information message is displayed that Observable enrichment execution has started on the selected observable(s). Results will be available in the detail page of respective observable(s) once the execution is complete.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Once the execution initiated or completed, a work notes is posted on the activity stream of the form view.



View Case Reports

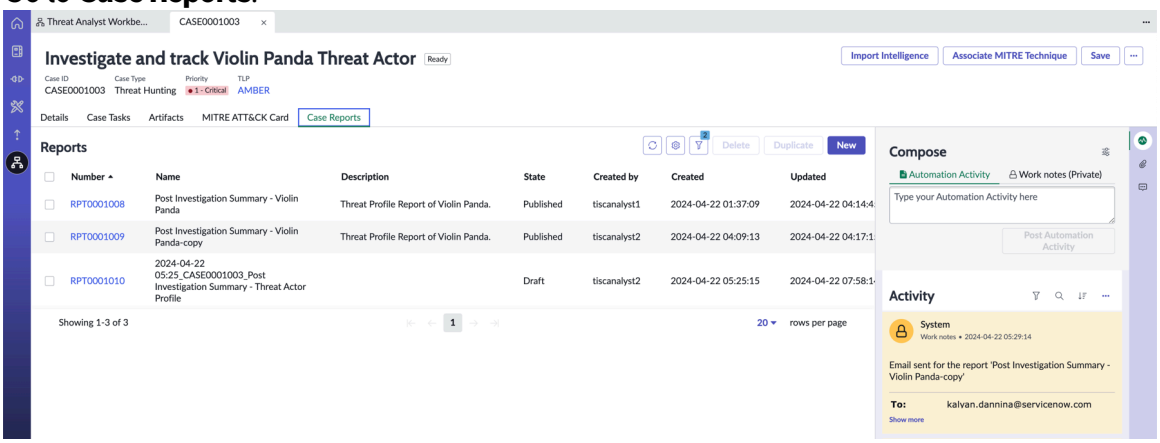
Use the case reports feature to generate reports related to the cases. These reports include post investigation report or an executive summary report.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

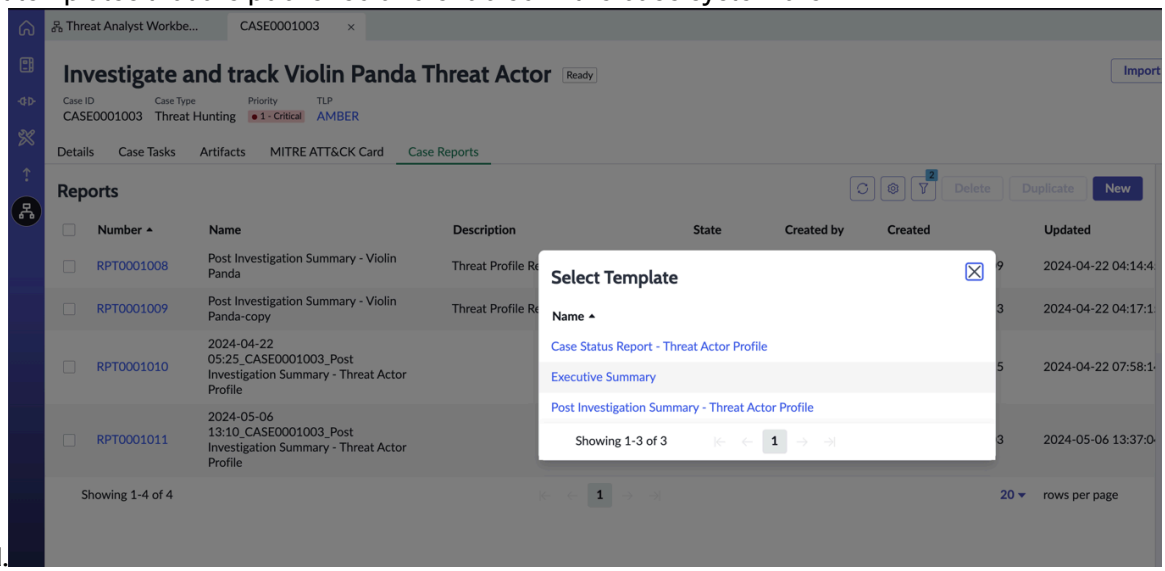
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case.
5. Go to **Case Reports**.



Note: You can delete the reports from the list, create a duplicate copy of the existing reports and customize your own report.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **New**.
   The report templates that are published and enabled in the base system are displayed.



7. Select the desired Report Template.
   The selected report template for the report type is generated. Also, here once the report is published, that means that larger group of users can view it but if the report is in a draft state then that report is hidden from the users. As an analyst you can only view the published reports but not the reports in the draft state.

   Note:

   - In case if you want to add more fields then select the fields and add it directly within your case report.
   - If you want to add related list, for example a list of observables then select Observables. All the observables associated for that particular case will be listed, select one or more observables ans click **Add**. You can also filter out the required observable and add it to your case.

8. Click **Save Content** to save the contents of your report.
9. Click **Preview** to preview the report.

   Note: You can do the following:

   - **Maximize** the report window.
   - **Download** the report using **Download** icon.
   - Pop out the report in a new tab in case if the height or size of the report to have better viewing experience.
   - **Edit** the Report Name and Report description.
   - **Publish** the report.

10. Click **Edit Content** button to republish the report.

    Note: A warning message is displayed for you to share the report:

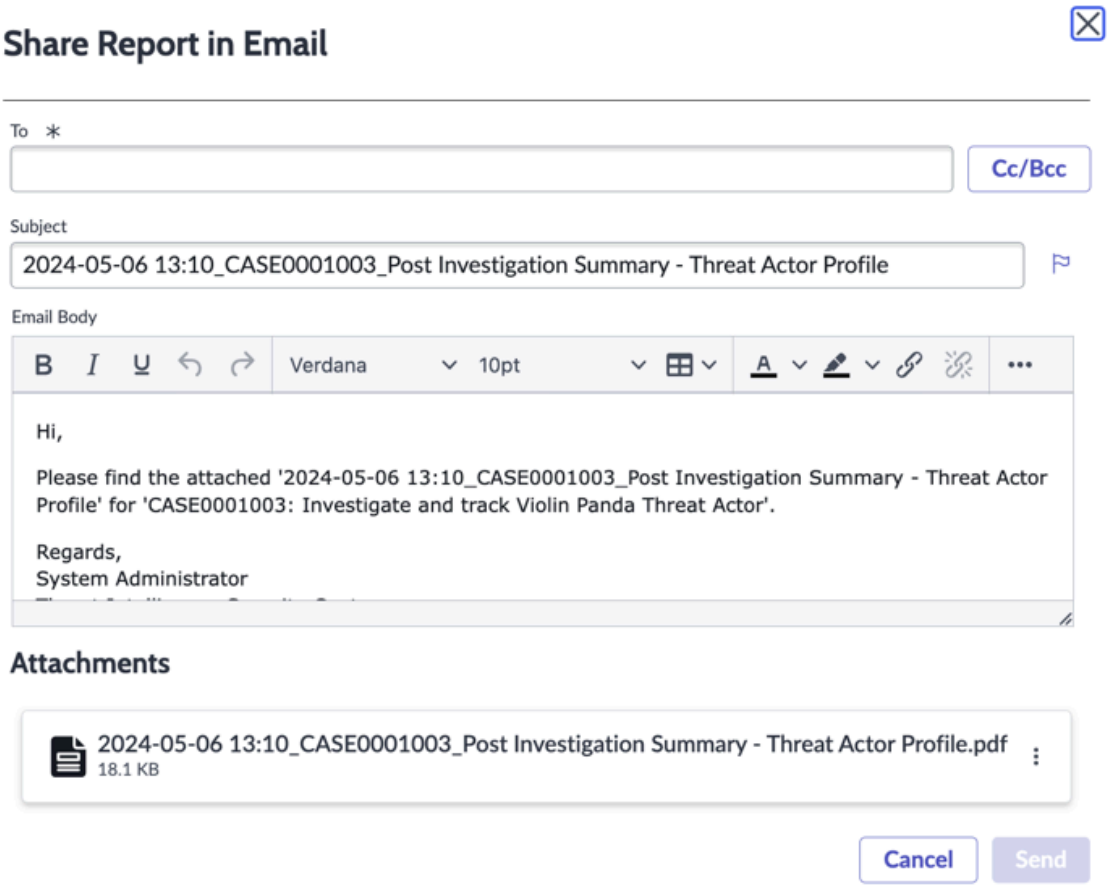
    You must republish the report after you make changes, for you to download or share the report. Do you want to still continue editing?

11. Click **Edit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you want to edit the report, then you can continue editing the report as explained or you can publish the report. Once it is published, the report will be read-only.

12. Click on **Share Report in Email** to share the report.
    While sharing the report, the PDF report that was generated is attached as an attachment to the



    Email.

13. Add the required email fields such as To (whom you want to share the report), CC, and BCC
14. Mark the email as important, if required.
15. Click **Send**.
    The report will be shared with the larger group of users.

Create a security incident from a TISC case

Create security incidents and associate observables to the security incidents from a TISC case.

Before you begin

Role required: sn_si_basic

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Open any case.
5. Click **Create Security Incident** button.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: On the **Case Management Workbench** the **Create Security Incident** button is enabled only for the open case records and disabled for the closed case records.

The Create Security Incident dialog box is displayed.

6. Fill the form with appropriate incident details:

Add details

Field	Description
Short description	Enter a short description of the security incident.
Description	Enter a description of the security incident.
Category	Defines the classification of the security incident.
Priority	Defines the priority of the security incident.
Subcategory	Defines the sub classification of the security incident based on its category.
Assignment group	Specifies the assignment group to which the security incident should be assigned.
Parent	Indicates the parent security incident, which is a TISC case from which this action is triggered.

7. Click **Next** to continue.

Note: You must enter all the mandatory fields, the **Next** button will remain disabled until you enter all the required fields.

8. Select the observables associated with the TISC case to link them to a security incident, and then click **Next** to proceed
9. Review the security incident details and observable that will be associated with the newly created security incident then click **Create** to continue and create the security incident.

Note: A confirmation message is displayed indicating that the security incident is created, with a link to the security incident, clicking the link will direct you to the security incident in the Security Incident Response Workspace.

After the security incident is created, you will be redirected to the TISC **Artifacts** tab of the case.

10. Go to **Security Incidents** section under the TISC **Artifacts** tab to view the incidents.

Note: A work notes is also posted on the TISC case activity stream indicating that the security incident (security incident number) is created with the associated with TISC observables. This work notes includes the details such as the observable type and observable value.

On the Security Incident Response Workspace, security incident form:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- A work notes is posted on the activity stream indicating that the security incident was successfully created from TISC case. This work notes also includes a link to the TISC case confirming that the selected observables have been associated with the security incident.
- In addition, you can also verify this by accessing the **Related Records** tab of the Security Incident Response Workspace and reviewing the observables entries under **Threat Intel** > **Associated Observables**. From there, you can also view the associated observables under the **TISC Context** section. You may notice that the these observables have been directly associated from TISC.

Upload Secure File Attachments

Use this section to understand on how to upload the secure file attachments to the case(s).

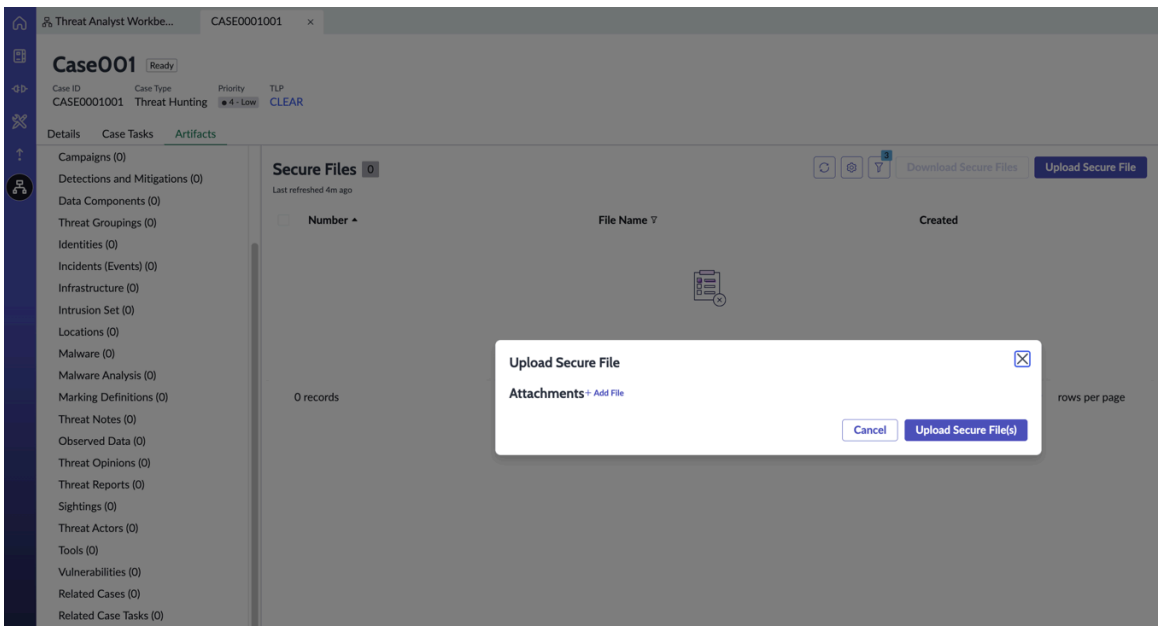
Before you begin

Role required: sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

Note: Secure Files related lists is only displayed when you have the user role, sn_sec_tisc.secure_file_access.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Case Management** > **All Cases**.
   All the cases are displayed.
4. Select any case.
5. Go to **Artifacts** > **Secure Files** related lists.
6. Click **Upload Secure File** button.
7. Click **Add File** to add the attachments.
8. Select the files and click **Upload Secure File(s)** button.
   The file attachments are uploaded.



9. Click **Download Secure Files** to download the attachments.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The attachments are available in the zip format.

10. Alternatively, you can download the file by navigating to the details page of the secure file record.

Note:

- All the secure attachments are encrypted and stored in the system using Key Management Framework (KMF). For more information, see Attachment Encryption.
- If users have subscription for *ServiceNow Integration Hub* **Professional Pack Installer**, secure files are compressed in zip format and also encrypted and stored

Threat Intelligence Security Center Library

A threat library is defined as a group of organized objects and entities that serve the organizations with structured and unstructured security threat information.

The threat information is available in the form of feeds. The feeds provides you with valuable threat data from sources such as STIX, MISP, and so on, which lists threat intelligence entities.

Threat Intelligence Security Center library explains how to browse through the data, by performing basic and advanced searches, and filtering rules, invoke import assistant, manually add threat intelligence records, take necessary actions such as adding to allow list, deny list, and watch list.

The detailed view provides the insights to the intelligence records and from list views you can perform quick actions on one or more records.

Understanding the Data Model

The data model and architecture of threat intelligence security center module is designed to support threat intelligence platform capabilities and different security views that provides detailed data for threat analysts.

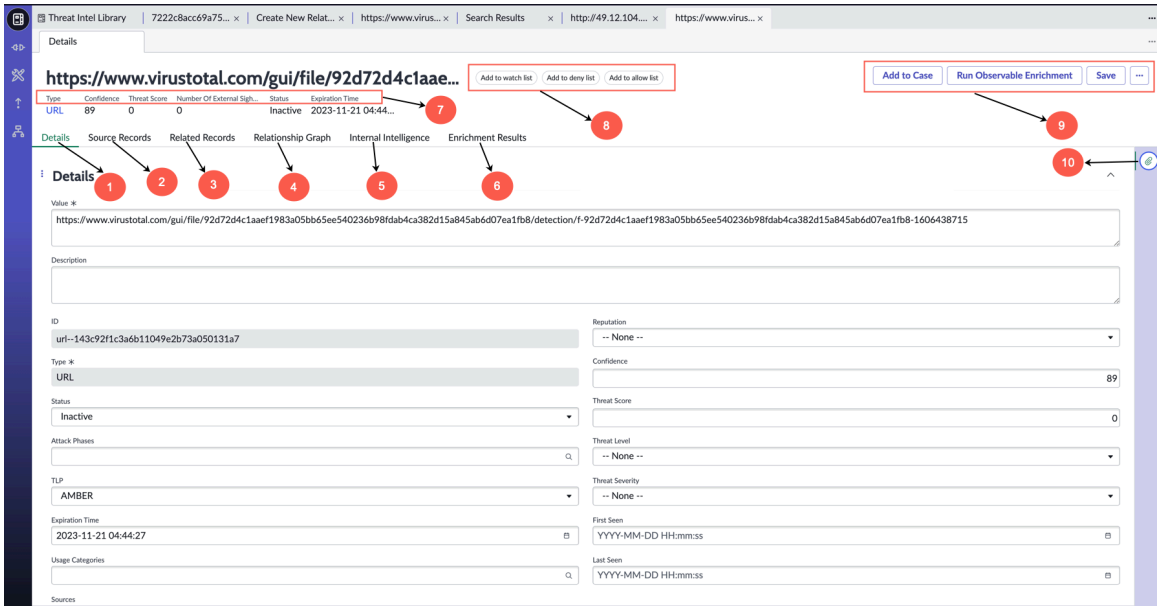
The data model has the data structures which are represented as objects in the Threat intelligence repository.

TISC Library Objects form view

The Threat Intelligence Security Center objects home page consists of the following features.

Use or navigate to these following sections and learn more about each SDOs in detail.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



TISC library objects form view

Order	Menu/Tab	Description
1	**Details** tab	Use this section to view or edit the SDOs in the form view.
2	**Source Records** tab	Source records contribute to an aggregated record as displayed in the form view. These source records are auto created from feeds or manually created by the user.
3	**Related Records** tab	Lists all the related records associated with the SDO.
4	**Relationship Graph** tab	Visual representation of the related objects.
5	**Internal Intelligence** tab	Lists the internal intelligence records of the associated objects.
6	**Enrichment Results** tab	Lists the enrichment integrations associated with the objects.
7	**Form banner**	This is read-only section, which contains the key fields such as Type, Confidence, Threat score, Number of Sightings, Status and Expiration time.
8	**Form banner UI actions**	These are the security control lists that are available for you to click if they are needed to be added to the allow list, removed from the allow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC library objects form view (continued)

Order	Menu/Tab	Description
		list (Deny list), or add it to the watch list based on the observables. Click to: • add to watch list • add to deny list • add to allow list **Note:** The Form actions are applicable only to Observables.
9	**Form UI actions**	The available form UI actions are: 1. **Add to Case**: Add the objects to the case. 2. **Run Observable Enrichment**: Run the enrichments to the selected objects. 3. **Save**: Save the record. 4. **Delete**: Delete the record.
10	**Right Contextual menu**	Provides easy access to the quick controls such as attachments, notes, and so on, based on the tasks associated with that object. This option is available across the remaining two tabs for the threat analyst to access whenever required. The contextual menu provides easy navigation to:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC library objects form view (continued)

Order	Menu/Tab	Description
		1. **Attachments**: Attach any file that are related to the objects. **Note:** Whenever you either create a new observable, indicators, or any objects or view the existing objects, the **Attachments** pane is by default displayed on the respective form view. You can either click the **Attachments** icon on the right-contextual menu or go to **Preferences** > **Workspaces** and disable the **Show the sidebar**. For more information, see Configure Next Experience Workspace preferences. 2. **Insights**: Add any additional information related to the observables or indicators which are associated with that object.
NA	**Search in Navigator**	Use this search function to search for various objects within the Threat Intel (TI) library. For example, you can search for all observables records within the TI library module.
NA	**Search in Threat Intel Library**	Use this search function to search for the source records across multiple sources based on your search criteria. The results will be displayed in a separate **Search Results** tab. For example, for an IP address 104.227.137.35, if you need to search the records, by entering 104.* then searching will narrowed down the records and displays the records that contains the IP address starting with 104 in

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

TISC library objects form view (continued)

Order	Menu/Tab	Description
		the separate **Search Results** tab. • You can also modify the existing search keywords in the Search Criteria on the same Search Results page without going back to the Threat Library page. • Similarly, you can also search based on the name and description of any particular record. • Once the records are filtered and listed, you can click on the list view which will take you to the respective record in a new tab.

TISC Library Repository

IoC repository contains STIX objects, each of these objects contain a specific piece of information.

Observables

Observables represent stateful properties (such as the MD5 hash of a file or the value of a registry key) or measurable events (such as the creation of a registry key or the deletion of a file) that are pertinent to the operation of computers and networks.

Following are the type of observables available in the application:

- Artifact
- AS Number
- Directory
- Domain Name
- Email Address
- Email Message
- Email Subject
- File
- IPv4 Address
- IPv4 CIDR
- IPv6 Address
- IPv6 CIDR
- MAC Address
- MD5 Hash

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Mutex Name
- Network
- Other Observable
- Process
- SHA1 Hash
- SHA256 Hash
- SHA512 Hash
- Software
- URL
- User Account
- Windows Registry Key
- X.509 Certificate

Define an Observable

Observables can be retrieved from scheduled feed ingestion or from the import assistant. However, you can create observables, as needed.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Click **New**.
3. Select the **Observable Type**.
   Create New Observable record form is displayed.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

4. On the form, fill in the fields.

   Note: Whenever you either create a new observable or view the existing observables, the **Attachments** pane is by default displayed on the form view. You can either click the Attachments icon on the right-contextual menu or go to **Preferences** > **Workspaces** and disable the **Show the sidebar**. For more information, see Configure Next Experience Workspace preferences.

Details section

Field	Description
Value	The value (for example, IP address or hash) associated with the observable.
Description	Description of the observable record.
Author	Enter the name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Type	The observable classification type such as an IP address, domain name, artifact, directory, file, or hash. By default, this is displayed when you selected the new record.
Status	The active or inactive status of the observable.
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
TLP	Unique value that indicates the Data sensitivity setting per TLP.
Reputation	Specifies the malicious reputation of the observable.
Status	Enter the status of the observable if active or inactive.
Threat Score	Indicates the threat score for that observable.
Expiration Time	Specifies the expiration time of the observable record.
Source	Specifies the threat source from which this record is created.
Confidence	Enter the confidence for this observable record. The confidence property identifies the confidence that the creator has in the correctness of their data. The confidence value MUST be a number in the range of 0-100.
Prevent System Updates	Setting this flag to true will prevent system from overriding values of fields on record.
Is False Positive	A boolean flag that indicates if observable is identified as false positive.

Attributes

Field	Description
Resolves To	Specifies a list of references to one or more IP addresses or domain names that the domain name resolves to.
Is FQDN	A fully qualified domain name(FQDN) is the complete address of an internet host or computer. It provides its exact location within the domain name system (DNS) by specifying the hostname, domain name and top-level domain (TLD).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Additional Information

Field	Description
Threat Level	Indicates the threat level of the observable record.
First Seen	The time that this observable record was first seen performing malicious activities.
Threat Severity	Indicates the threat severity of the observable record.
Last Seen	The time that this observable record was last seen performing malicious activities.
Usage Categories	Categories that the observable falls under, such as botnet or phishing.
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
Additional Context	Add any additional context.
Sources	Specifies the threat source from which this record is created.

Important: **Source Reported Score**: This field contains the aggregated value of threat scores reported by the sources from which the observable is ingested. To see this field on the observable record form, you must add it manually, as it is not available by default.

Attributes

Field	Description
Resolves To	Specifies a list of references to one or more IP addresses or domain names that the domain name resolves to.
Is FQDN	A fully qualified domain name(FQDN) is the complete address of an internet host or computer. It provides its exact location within the domain name system (DNS) by specifying the hostname, domain name and top-level domain (TLD).

Note: **Resolves To** and **Is FQDN** attributes are only applicable to the **Domain Name** type of observables.

Observable Type Attributes

Attribute Name	Attribute Types
Artifact	○ Decryption Key ○ Encryption Algorithm ○ MD5 Hash ○ MIME Type ○ SHA1 Hash

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute Name	Attribute Types
	○ SHA256 Hash ○ SHA512 Hash ○ URL
AS Number	○ Name ○ RIR
Directory	○ Directory Creation Time ○ Directory Last Accessed Time ○ Directory Last Modified Time ○ Encoded Path
Domain Name	○ Is FQDN ○ Resolves To
Email Address	○ Display name ○ Email Body ○ Email Recipients Bcc ○ Email Recipients Cc ○ Email Recipients To ○ Email Sender ○ Email Subject ○ Sent Date
File	○ Additional Information ○ Encoded File Name ○ File Created Time ○ File Last Accessed Time ○ File Last Modified Time ○ File Name Magic Number ○ MD5 Hash ○ MIME Type ○ SHA1 Hash ○ SHA256 Hash ○ SHA512 Hash
IPv4 Address	○ AS Number ○ MAC Address
IPv4 CIDR	○ AS Number ○ MAC Address

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute Name	Attribute Types
IPv6 Address	○ AS Number ○ MAC Address
IPv6 CIDR	○ AS Number ○ MAC Address
Network	○ Destination Bytes ○ Count Destination Packets Count ○ Destination Port ○ End Time ○ HTTP Message Body Length ○ HTTP Request Header ○ HTTP Request Method ○ HTTP Request Value ○ HTTP Request Version ○ ICMP Code Byte ○ ICMP Type Byte ○ Is Network Active ○ Is Socket Blocking ○ Is Socket Listening ○ Network Protocols ○ Socket Address Family ○ Socket Descriptor ○ Socket Handle ○ Socket Options ○ Socket Type Source Bytes Count ○ Source Packets Count ○ Source Port ○ Start Time ○ TCP Destination Flags ○ TCP Source Flags
Process	○ ASLR Enabled ○ Command Line ○ Current Working Directory (CWD) ○ DEP Enabled ○ Environment Variables ○ Is Hidden ○ Owner SID

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute Name	Attribute Types
	○ Process ID ○ Priority ○ Process Created Time ○ Service Descriptions ○ Service Display Name ○ Service Group Name ○ Service Name ○ Service Start Type ○ Service Status Service Type ○ Startup Info ○ Windows Integrity Level ○ Window Title
Software	○ Common Platform Enumeration (CPE) ○ Supported Languages ○ Software Identification (SWID) ○ Vendor Version
User Account	○ Account Created Time ○ Account Expiry Time ○ Account Login ○ Account Type ○ Additional Information ○ Can Escalate Privileges ○ Credentials Last Changed Time ○ Display Name ○ First Login Time ○ Is Account Disabled ○ Is Privileged ○ Is Service Account ○ Last Login Time ○ User ID
Windows Registry Key	○ Key Modified ○ Time Registry Value ○ Subkeys Count
X.509 Certificate	○ Additional Information ○ Authority Key Identifier ○ Basic Constraints

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute Name	Attribute Types
	○ Certificate Policies ○ CRL Distribution Points ○ Extended Key Usage ○ Inhibit Any Policy ○ Issuer ○ Issuer Alternative Name ○ Is Self Signed ○ Key Usage ○ Name Constraints ○ Policy Constraints ○ Policy Mappings ○ Private Key Usage Valid From ○ Private Key Usage Valid until ○ Signature Algorithm ○ Subject ○ Subject Alternative Name ○ Subject Directory Attributes ○ Subject Key Identifier ○ Subject Public Key Algorithm ○ Subject Public Key Exponent ○ Subject Public Key Modulus ○ Valid From ○ Valid Until ○ Version

Insights

Field	Description
Notes	Add any additional notes for an observable record.

5. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
6. Click **Continue**.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with an observable.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select the Taxonomy that is associated with an observable.
Add Taxonomy Values	Add the Taxonomy values that are associated with an observable.

Source Records

Field	Description
The source records details for an observable are displayed, if any.	

What to do next

Following table lists the related records related to the Observables:

Related Records

Related List	Description
Observable	List of observables related to this observable. **Note:** This section also contains the potential relationships between two observables. For more information, see Confirm observable-observable potential relationshipand see Define observable-observable relationships for the confirmed relationships between the two observables.
Indicators	List of indicators related to this observable.
Attack Patterns	List of attack patterns that are related to this observable.
Campaigns	List the campaigns that are related to this observable.
Infrastructure	List the Infrastructure such as systems, software services, and any associated physical or virtual resources that are related to this observable.
Intrusion Sets	List the intrusion sets such as a set of adversarial behaviors and resources with common properties that are related to this observable.
Malware	List the malware source records that are related to this observable.
Threat Actors	List the threat actors that are related to this observable.
Threat Events	List the threat events that are related to this observable.
Vulnerabilities	If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address that are related to this observable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. Also, from the **Related Records** section, you can confirm the relationships between two Observables using the **Potential Relationships** section available on the **Observables** form view. For more information on see, Confirm Potential Relationships from Related Records.
3. You can add observables to cases. For more information, see Add to Case.
4. You can also run enrichment actions to observables. For more information, see Run Enrichment Actions within a case.

Observables source records

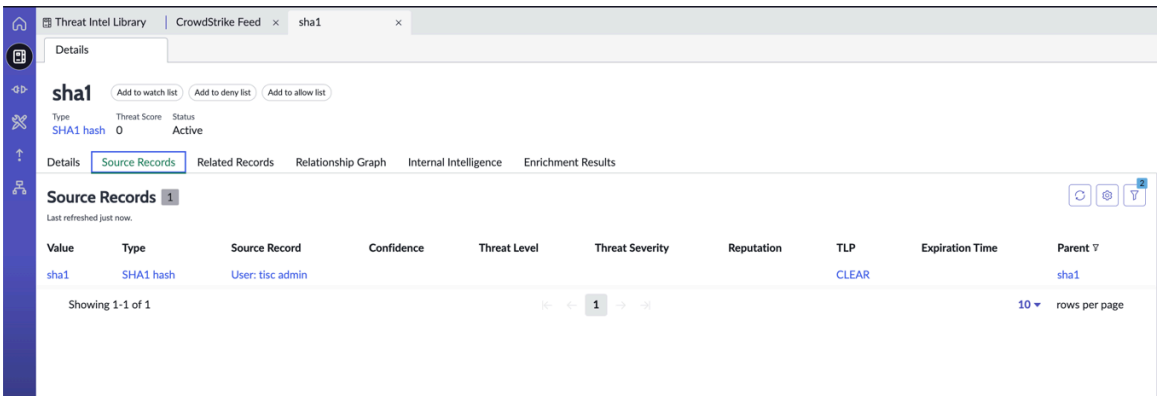
The source records contribute to an aggregated record as displayed in the form view. These source records are auto created from feeds or manually created by the user.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Select one or more observable(s).
5. Go to **Source Records**.
   The source records to an aggregated record are displayed.



6. View the records.

Link Threat Intel Related Records

Link the related records that are related to the corresponding threat intel objects.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s) record as an example.
3. Go to **Related Records** section.
4. Select any related record.
5. Click **Link**.
   The Link Objects dialogue box is displayed.
6. Select the objects from the list and click **Link** button.
   The objects associated for an observable record will be linked and displayed in the Related Records list view.
7. Click **Save**.
   Click **Unlink** button to unlink the objects

Fetch Observables Data

Fetch the observables related records data.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Observables**.
   The related observables associated with that selected object are displayed.
4. Select any observable record.
   If the given observables has any CVEs associated with it then you can fetch its vulnerable related data automatically using the button provided, and these associated records are displayed in the Business Context section of the Vulnerabilities.
5. Go to **Internal Intelligence** > **Vulnerable entries**.
   The associated CVEs records for the observables are displayed.
6. Select any CVE and click on **Fetch Vulnerability related data** button.

Note:

- An information message displays that This specific vulnerability object doesn't have any vulnerable entries associated with it. You must associate the object(s) with the vulnerable entries to fetch the data. For more information see, Fetch Vulnerability Data on how to link the records and perform the scheduled job to fetch the data. and for more information on Scheduled jobs, see Scheduled jobs.
- This button will trigger a background scheduled job, and the job initiation and execution details are displayed in the Activity Stream section. For example, when the job is triggered the activity stream displays an activity that Started fetching associated data with the vulnerable entries. The background scheduled job will continuously check for any observables that has any vulnerable entry associated with the observable and run automatically and this scheduled job will run every one hour. in case if the records are not fetched then you can manually link the records and fetch the data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

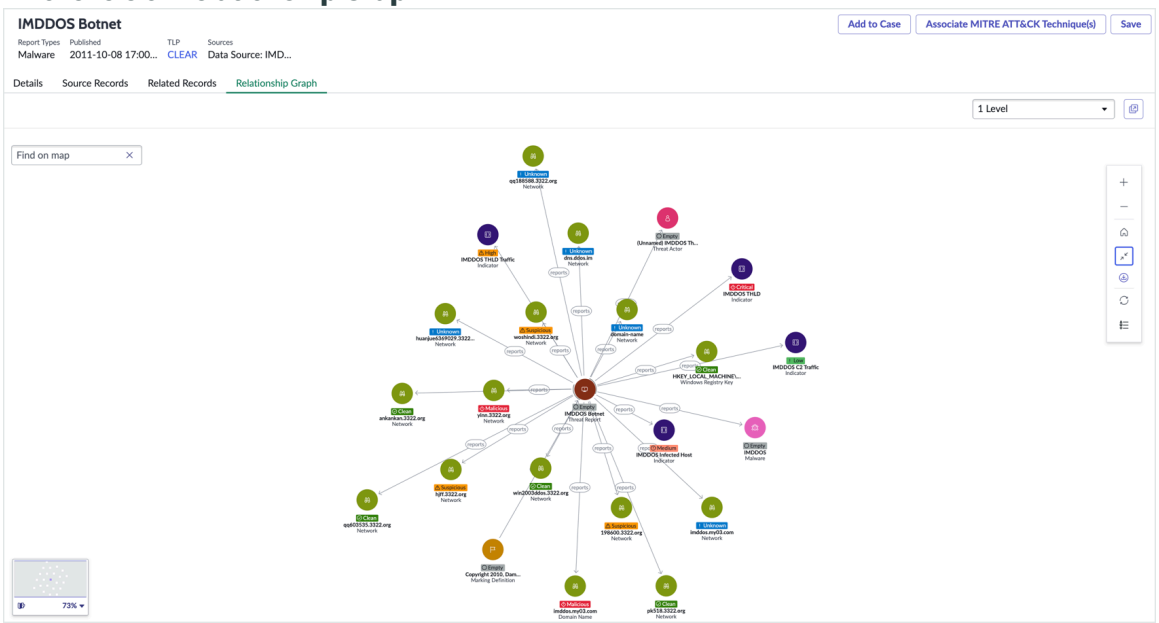
View details in Relationship Graph

Relationship Graph for observables, indicators, and various other entities in TISC has associated relationship graphs. Using the Visualizer, you can view the relationships between observables, indicators, and entities which provides context for you to further investigate. The Visualizer uses colors and icons to illustrate various information about the objects.

Role required: sn_sec_tisc.analyst

The relationship graphs displays two different levels of nodes association as part of its related records.

Two levels of Relationship Graph



You can do the following:

- Zoom into any object, fit into the screen, drag the nodes, or pin them to focus on a particular relationship.
- Click on any object to open the details pane. On the details pane, you can learn more information that is associated with the object. You can view the node properties such as Object, Object Name, Description, and Sources. By default the details section of each graph node is not displayed and you have to click on each node in the graph to view the details of the selected node.

  Note: The Visualizer is available for all the STIX Domain Objects (SDOs) except the Observed Data objects. Click **Refresh** button to refresh the visualizer.

- You can also click on the pop out icon to view the graph in a much larger window.

Link node actions in Relationship Graph

Add new related records to link the nodes.

Before you begin

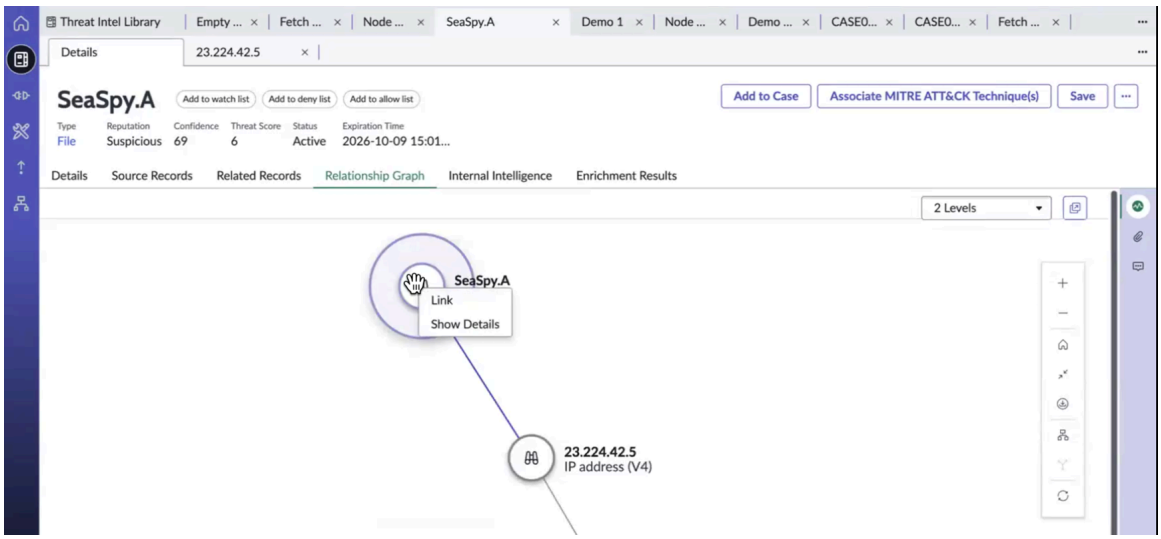
Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

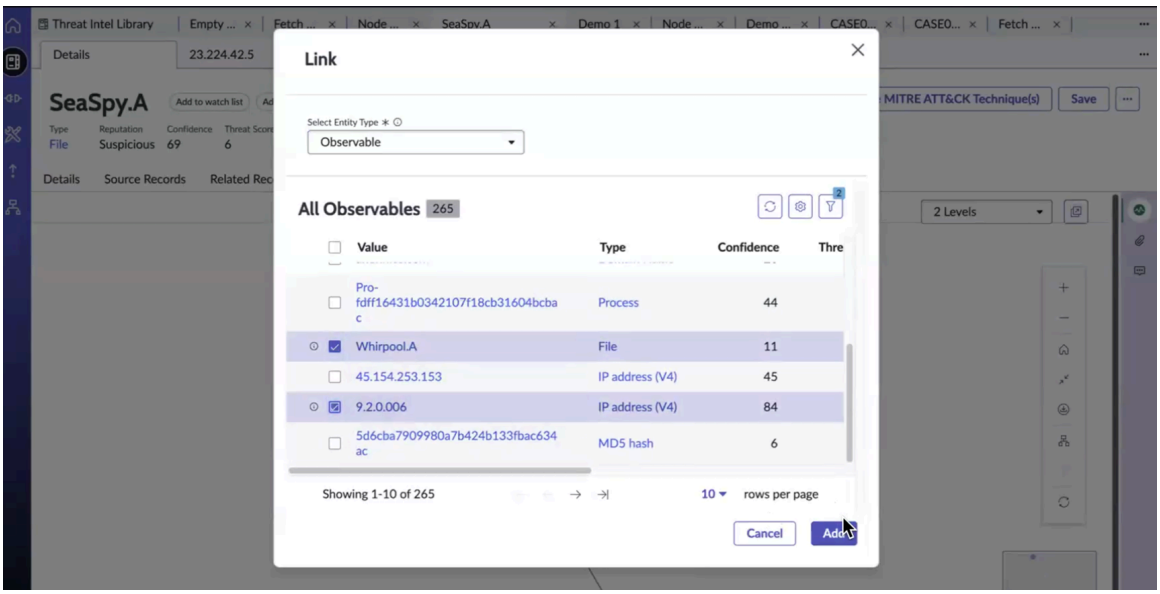
Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s) record as an example.
3. Go to **Relationship Graphs** section.
4. Click on the node.
5. Click **Link**.

Note: This action is only available at a home node level.



6. Select the entity type such as observable.
7. Select one or more observables to the parent node.
8. Click **Add**.
   The observables are added to the parent node.



9. Select **Unlink** to unlink the related records from the nodes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The related records data is unlinked but those relationships between the home node and the observable will still be there in the threat intelligence library.

10. Select **Show details** to see the associated observables data.

Working with Internal Intelligence Records

Use this feature to work with the internal intelligence data that is collected from Configuration Database Management System (CMDB) into Threat Intelligence Security Center.

View Internal Intelligence Records

View the internal intelligence records collected from CMDB, Security Incident Response (SIR), Vulnerability Response (VR) these records.

Before you begin

Internal Intelligence section provides the context from other applications on the platform such as SIR, VR and CMDB to provide broader perspective of the threat to the analysts.

Role required: sn_sec_tisc.analyst

Note: Internal intelligence tab is only visible for observables and vulnerability objects.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s) record.
3. Go to **Internal Intelligence** tab.
   The Internal intelligence section comprises of three subsections such as Security Incident Response, Business Context, Vulnerability Response.

   Note: You must have the respective applications installed on your instance for these sections to be listed within **Internal Intelligence** tab.

   a. **Security Incident Response**: Displays all the incidents that are linked with the associated observables, and vulnerability items.

      Note: The Observable(s) value must match between the SIR incident and also within the TISC only then the associated observables or indicators are listed under Security incident Response section. You can also link and unlink the records by searching the records within the source systems. For more information, see Link Threat Intel Related Records.

      - Select any record to navigate and view the details in the source system. For example, Associated Observables in Security Incident Response to fetch the associated observable records.
      - As part of the current release, following is the intelligence data that you can fetch from the source (SIR) records:
        - Associated Observables
        - Vulnerability items

   b. **Business Context**: Displays the affected users and any other configuration items. As part of the current release, following is the intelligence data that you can fetch from the source (Business Context) records:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Configuration Items
- Affected Services
- Affected Assets

c. **Vulnerability Response**: Displays the vulnerabilities intelligence data.

Vulnerability Entries: This option match the vulnerabilities and fetch the related records.

Run Enrichment Actions from Observable

Use this section to understand how enrichments actions are performed on observables and other objects.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Click any Enrichment actions from the split button.
5. Select the available implementation(s).
6. Click **Submit**.
   For example, Run Threat Lookup. The selected enrichment action will be executed and an information message is displayed that Observable enrichment execution has started on the selected observable(s). Results will be available in the detail page of respective observable(s) once the execution is complete.

   Note: Once the execution initiated or completed, a work notes is posted on the activity stream of the form view.

Add to Case

Add observables, indicators, or other objects to the case.

Before you begin

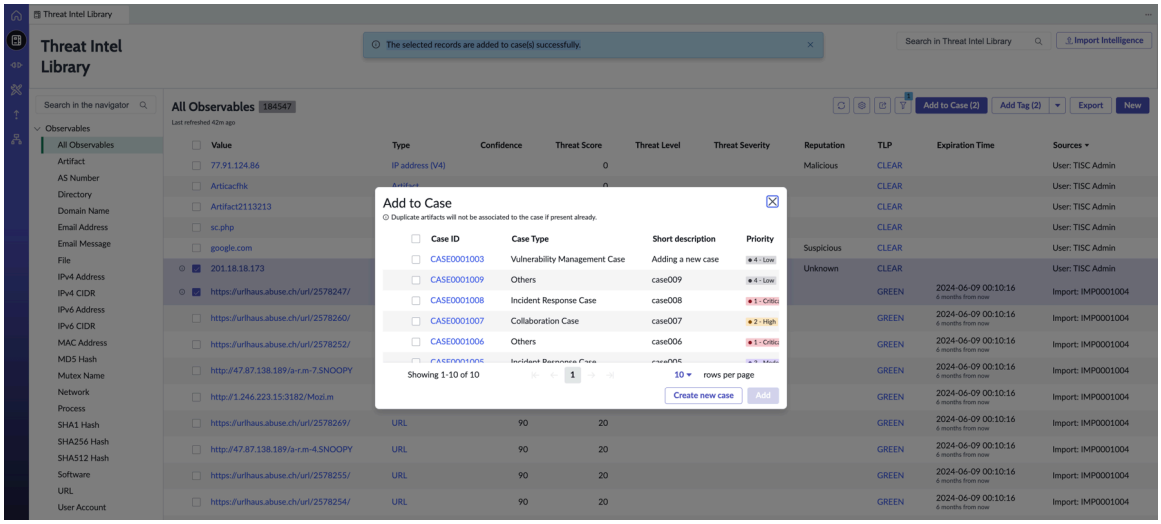
Role required: sn_sec_tisc.analyst

Following is the procedure that shows how to add a case to an observable record.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select the observable(s).
3. Click **Add to Case** button.
   This displays only the cases where the record is not already associated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Verify if you want to add the record to the existing cases and if so select the exiting case otherwise click **Create New Case**.
   Create a new case by entering the following information.

Create New Case

Field	Description
Case ID	A unique identifier for the case. This is system generated ID.
Short Description	Summary of the request or issue that is being investigated or a short description.
Case Type	Select the type of case being investigated. The possible options for the investigation are: ○ Threat Hunting ○ Request for Information ○ Vulnerability Management Case ○ Compliance Case ○ Incident Response Case ○ Collaboration Case ○ Others
Priority	An assessment of the severity of the request or issue.
Assignment Group	The assigned group responsible for working on the case.
Assigned to	The Analyst who is responsible for working on a case.

5. Click **Create** if you are creating a new case.

Note: The new case is added to the existing case list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select the newly added case(s).
7. Click **Add**.
   An information message is displayed that the selected records are added to case(s) successfully.

Run Enrichment operations in TISC

The following table below describes the interactions involved in running different enrichment operations from TISC.

TISC modal screens

Capability	UX Frameworks interactions	Integrations supported
Run Threat Look Up	On Screen 1 – Select the implementation(s) and submit. There are no common inputs or implementation specific inputs applicable for Run Threat Look Up.	• Virus Total • Crowd Strike Falcon Intelligence
Run Sighting Search	Screen 1 – Select Implementations and Screen 2 – Common Inputs are applicable. Sighting search takes date and time frequency as common inputs across multiple implementations of Splunk and other integrations.	• Elastic search • Splunk Sighting
Run Observable Enrichment	Only Screen 1 – Select Implementations. There are no common inputs or implementation specific inputs applicable for Run Observable Enrichment.	• WHOIS • Shodan

Observable Enrichment

The Enrich Observable WhoIs workflow performs enrichment on selected observables. If the observables are of a type recognized by the WhoisXML API Integration, the observables are enriched.

Note: The Threat Intelligence Security Center supports Observable Enrichment only for the WHOIS Integration.

Run Have I Been Pwned enrichment integration

Run the Have I Been Pwned (HIBP) enrichment on an email address or domain name observable to determine whether it has been involved in a known data breach.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ensure that the Have I Been Pwned integration is configured and enabled by your administrator. For more information, see Configure and enable Have I Been Pwned integration.

About this task

The integration queries the HIBP database to identify whether a submitted observable has been exposed in a publicly known data breach.

Note: The integration supports only the following observable types:

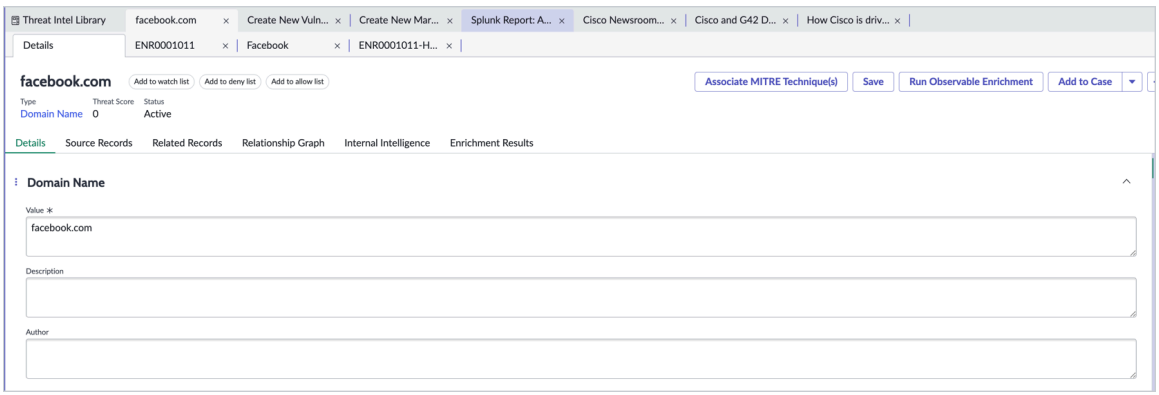
- Email address
- Domain name

Submitting an unsupported observable type such as an IP address or file hash results in the observable being excluded from enrichment with an alert message indicating that an unsupported observable type. Observables on the allow list are also excluded from submission.

You can initiate enrichment from an individual observable record or from the **Artifacts** tab of a case when working with multiple observables.

Procedure

1. Navigate to the observable record you want to enrich.
   a. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intelligence Library** and open any observable record from the Threat Intelligence Library.



   b. (Alternatively) open a case, navigate to the **Artifacts** tab, and select the **Observables** related list from Case to run observable enrichment.

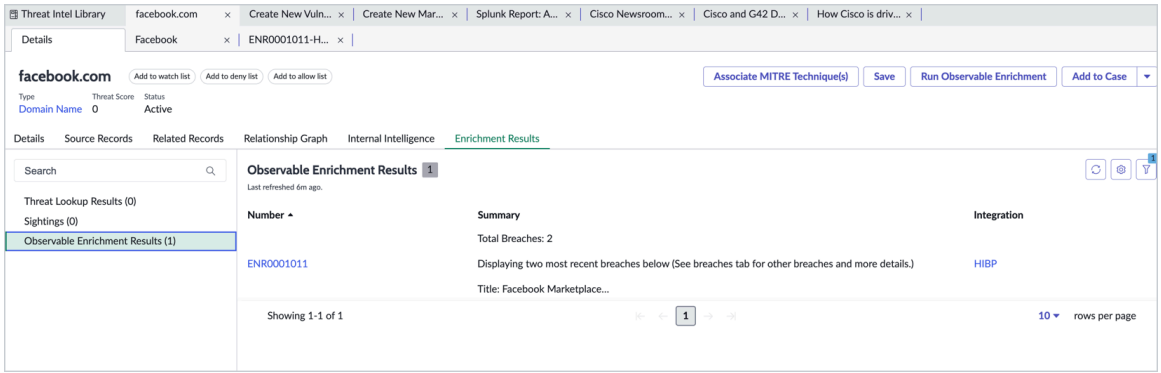
2. Select the observable or observables you want to submit for enrichment.
   When working from a case, you can select multiple observables at a time. Only observables of supported types are submitted. Unsupported types and allow listed observables are automatically filtered out.
3. Click **Run Observable Enrichment**.
4. Select **Have I Been Pwned** from the list of available integrations.
5. Click **Submit**.
   An activity stream entry is created indicating that enrichment has been initiated. After processing completes, a result record is created in the enrichment results table.

Result

To view the enrichment results:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to any observable record.
2. Go to **Enrichment Results** tab.
3. Select **Observable Enrichment Results** and open the result record.



What to do next

Viewing enrichment results

The enrichment displays the corresponding results in the following sections:

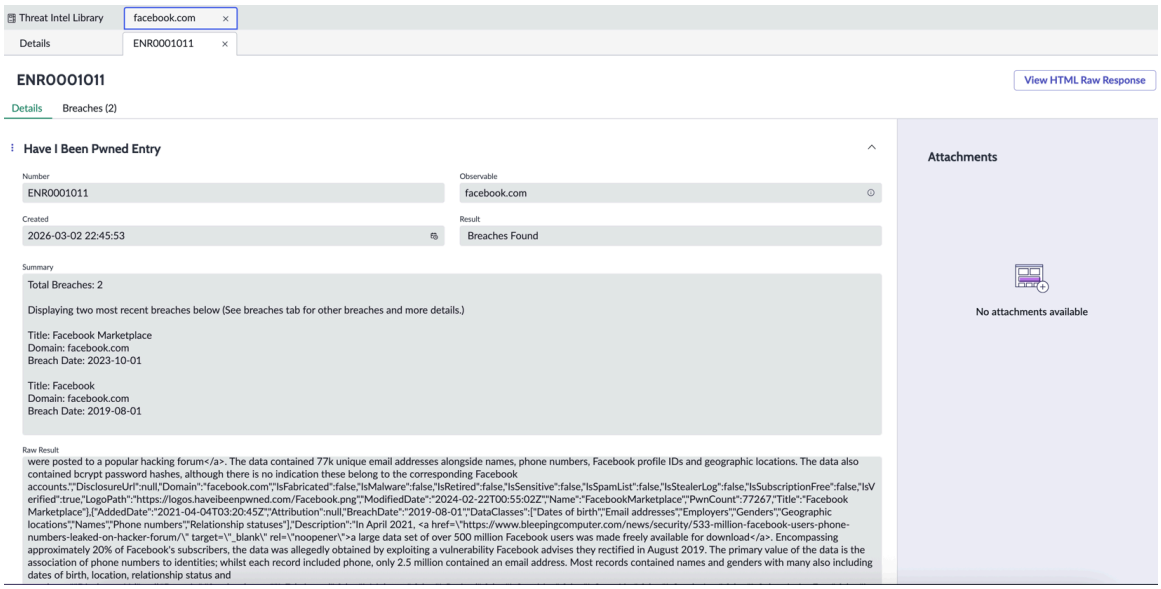
- **Details**: Provides the summary of the observable enrichment integration for the selected observable. This section includes total number of breaches identified and a concise summary of the most recent breaches. It also provides the raw response returned by the integration for reference.

View observable enrichment results details

Field	Description
Number	Unique system generated identifier for the Have I Been Pwned enrichment record.
Observable	An observable record such as email address or domain submitted for breach identification.
Created	Date and time when the observable enrichment was executed and the observable enrichment results record was created.
Result	Displays the outcome of the observable. When an observable is associated with breaches, the result will show **Breaches Found**. If no breaches are identified, the result indicates **Breaches Not Found**.
Summary	Provides an overview of observable enrichment results including: ○ total number of breaches identified. ○ the most recent breaches. ○ key details such as breach title, domain, and breach date (for a domain type of observable).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	View the summary section for a quick review of breach results.
Raw Result	Displays the response returned by the Have I Been Pwned API in JSON format. This field is intended for validation and troubleshooting purposes.



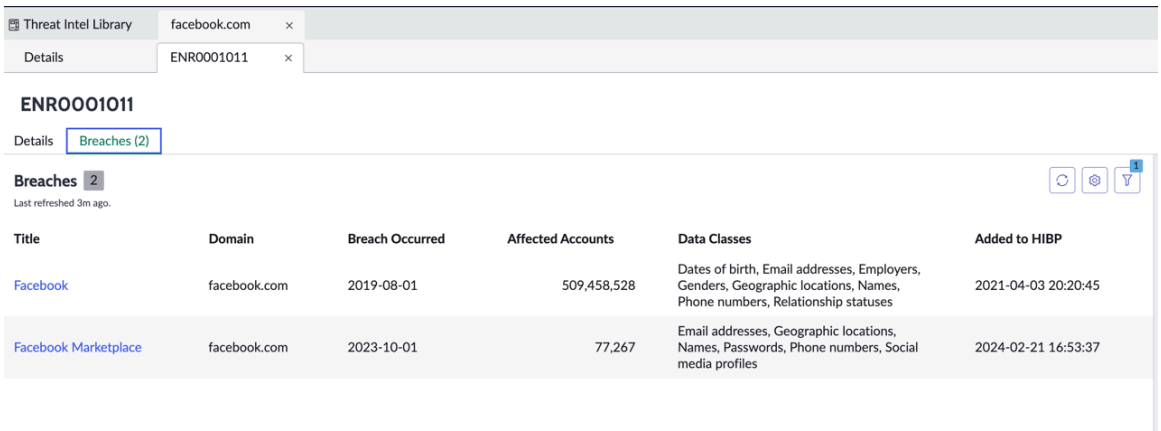
- **Breaches**: Displays breach records associated to the observable domain or email, as retrieved from the HIBP integration. Each record includes the breach title, domain, breach date, number of affected accounts, exposed data classes, and the date the breach was added to HIBP.

View Have I Been Pwned breaches

Field	Description
Have I Been Pwned Entry	Unique entry for the enrichment record.
Title	title for the breach unique across all breaches.
Domain	The domain of the primary website the breach occurred on.
Added to HIBP	The date and time (precision to the minute) the breach was added to the system in ISO 8601 format.
Breach Occurred	The date (with no time) the breach originally occurred on in ISO 8601 format (This is not always accurate).
Modified Date	The date and time (precision to the minute) the breach was modified in ISO 8601 format. This will only differ from the AddedDate attribute if other attributes represented here are changed or data in the breach itself is changed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Affected Accounts	The total number of accounts loaded into the system.
External Link	Link to the respective breach record in Have I Been Pwned.
Data Classes	Describes the nature of the data compromised in the breach.
Description	Contains an overview of the breach.
Logo Path	A URL that specifies where a logo for the breached service can be found.
Attribution	Sometimes requested by the party that provides the data to HIBP.
Disclosure URL	Hyperlink that contains public forum information such as news reported on the breach.



View HTML Response: Select this button to view the complete `html` response returned by the Have I Been Pwned integration for the selected observable. This view shows the unprocessed source data exactly as received. Use this option for validation, troubleshooting, or audit purposes to review the response payload.

You can also view the Have I Been Pwned flags, which indicate the attributes identified in the unprocessed source data, as described in the following table.

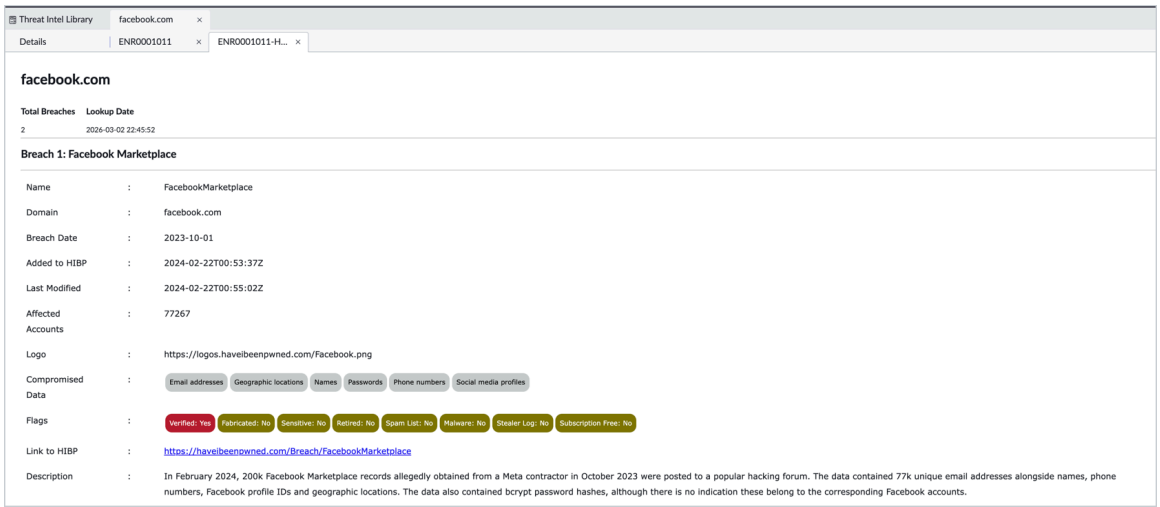
Have I Been Pwned flags

Related Record	Description
Verified	Indicates that the breach is considered unverified. An unverified breach is still loaded into HIBP when there's sufficient confidence that a significant portion of the data is legitimate.
Malware	Indicates that the data was sourced from a malware campaign rather than a security compromise of an online service.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Have I Been Pwned flags (continued)

Related Record	Description
Sensitive	Indicates that the breach is considered sensitive. The public API will not return any accounts for a breach flagged as sensitive.
Fabricated	Indicates that the breach is considered fabricated. However, it still contains legitimate email addresses.
StealerLog	Indicates if the breach is sourced from stealer logs.
Retired	Indicated that this data has been retired (permanently removed) and will not be returned by the API.
SpamList	Indicates that the data has not come as a result of a security compromise (or is a spam list).
Subscription Free	Indicates if the breach is subscription-free.



Note: The HIBP integration provides breach awareness only. It does not support actions to remediate or resolve breaches, as the breaches originate from external third-party systems.

Related topics

- Configure Observable Enrichment
- Configure and enable Have I Been Pwned integration

Whois integration

The Whois integration enables you to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

Configure and enable Whois integration

Before you use the Whois integration, you must download it from the ServiceNow Store, and must have a valid account from Whois.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.admin

The Threat Intelligence Security Center and Whois observable integration plugins are required.

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Observable Enrichment**.
6. In the **WHOIS** card, click **Configure New Enrichment** to configure **WHOIS** integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, WHOIS.
Vendor Name	Name of the vendor. The details of the selected vendor is populated by default. For example, WHOIS.
Integration Type	Type of integration that you selected. For example, Threat Lookup.
Description	Enter the description for the new enrichment integration. For example, the description for WHOIS integration is, The WHOIS Integration for Threat Intelligence Security Center enables users to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats.

8. Drill down to **Integration Configuration** section.
9. Enter (or paste) the **API Key** you acquired from the WHOIS site.
10. Click **Save**.
    The integration details are validated, and by default the WHOIS integration's status is disabled.
11. Click **Enable** to enable the WHOIS integration.

Result

After it is configured, WHOIS can be selected for performing enrichments on observables in Threat Intelligence Security Center.

Shodan integration

Shodan is a search engine that analyzes service banner information from connected devices all around the globe.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Shodan integration performs enrichment on the following observables:

- IP addresses
- URLs
- Domains

Configure and enable Shodan integration

Before you use Shodan integration, you must download it from the ServiceNow Store.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Using your instance, access **Threat Intelligence Security Center**.
2. Download the integration from the ServiceNow Store.
3. When the installation is complete, navigate to **Workspaces** > **Threat Intelligence Security Center**.
4. Select **Integrations** > **Enrichment Integrations** > **All Integrations**.
5. Alternatively, you can navigate to **Integrations** > **Enrichment Integrations** > **All Integrations** > **Observable Enrichment**.
6. In the **Shodan** card, click **Configure New Enrichment** to configure the integration.
7. Fill in the fields on the Configure New Enrichment form.

Enrichment Integration

Field	Description
Name	Enter a name for the new enrichment integration. For example, Shodan.
Vendor Name	Name of the vendor. The details of the selected vendor is auto populated and by default this field will be read only. For example, Shodan.
Integration Type	Type of integration that you selected. For example, Observable Enrichment.
Description	Enter the description for the new enrichment integration. For example, the description for Shodan integration is, Shodan helps you to analyze banner information from connected devices all around the globe.

8. Drill down to **Integration Configuration** section.
9. Enter (or paste) the **API Key** you acquired from the Shodan portal.
10. Click **Save**.
    The integration details are validated, and by default the status is disabled.
11. Click **Enable** to enable the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run Threat Lookup

Select one or more implementations as applicable to run threat lookup on observables.

Before you begin

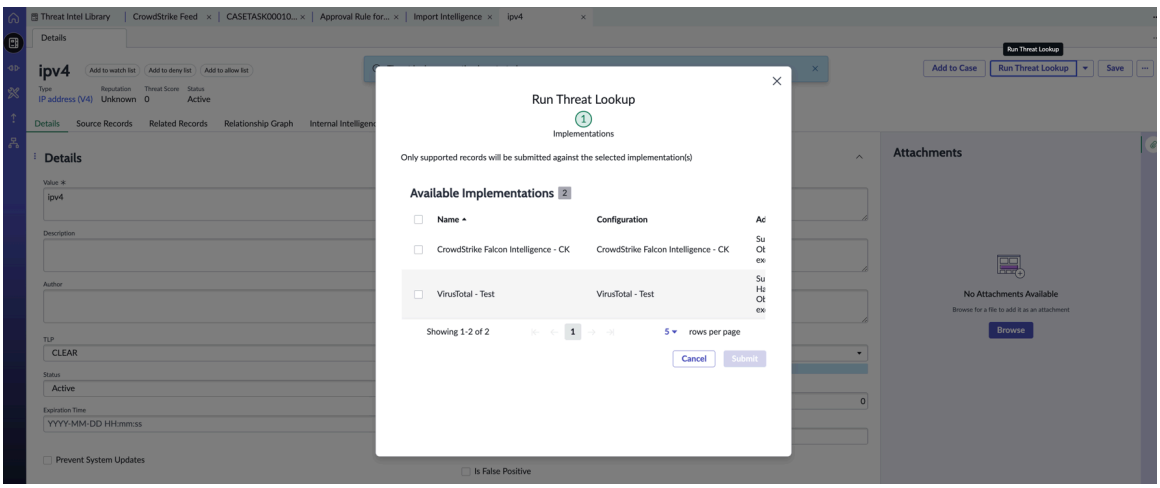
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Click **Run Threat Lookup**.
   The Run Threat Lookup **Select Implementations** modal screen is displayed.

   Note: The Run Threat Lookup performs the threat intelligence lookups to determine whether the observables are associated with any known threats.

6. Select the required implementation(s) from the list.



7. Click **Submit**.
   The selected enrichment action will be executed and an information message is displayed that Threat lookup execution has started.

   Note:

   - Once the execution initiated or completed, a work notes is posted on the activity stream of the form view.
   - The enrichment results pushed from SIR workspace can be found in the **Enrichment Results** tab of that corresponding Observables details page in TISC Workspace.
   - The enrichment results pushed from SIR workspace can be identified using **Source** field of the enrichment result table.

Run Sighting Search

Perform Run Sighting Search related integration.

Before you begin

Role required: sn_sec_tisc.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

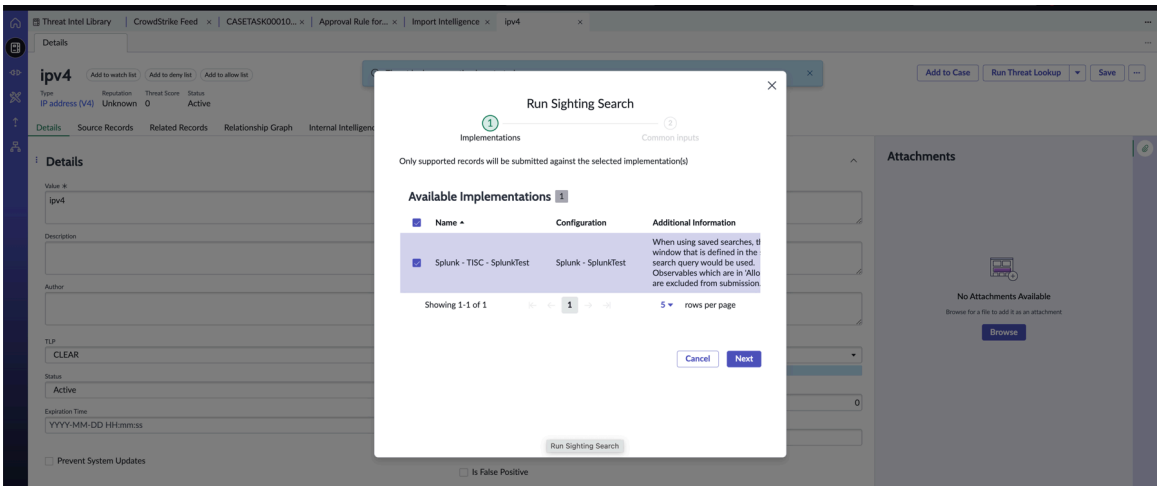
To perform this action select the implementation and add common run time inputs that apply for all the selected implementations as applicable.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.
3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Click **Run Sighting Search**.
   The Run Sighting Search **Select Implementations** modal screen is displayed.

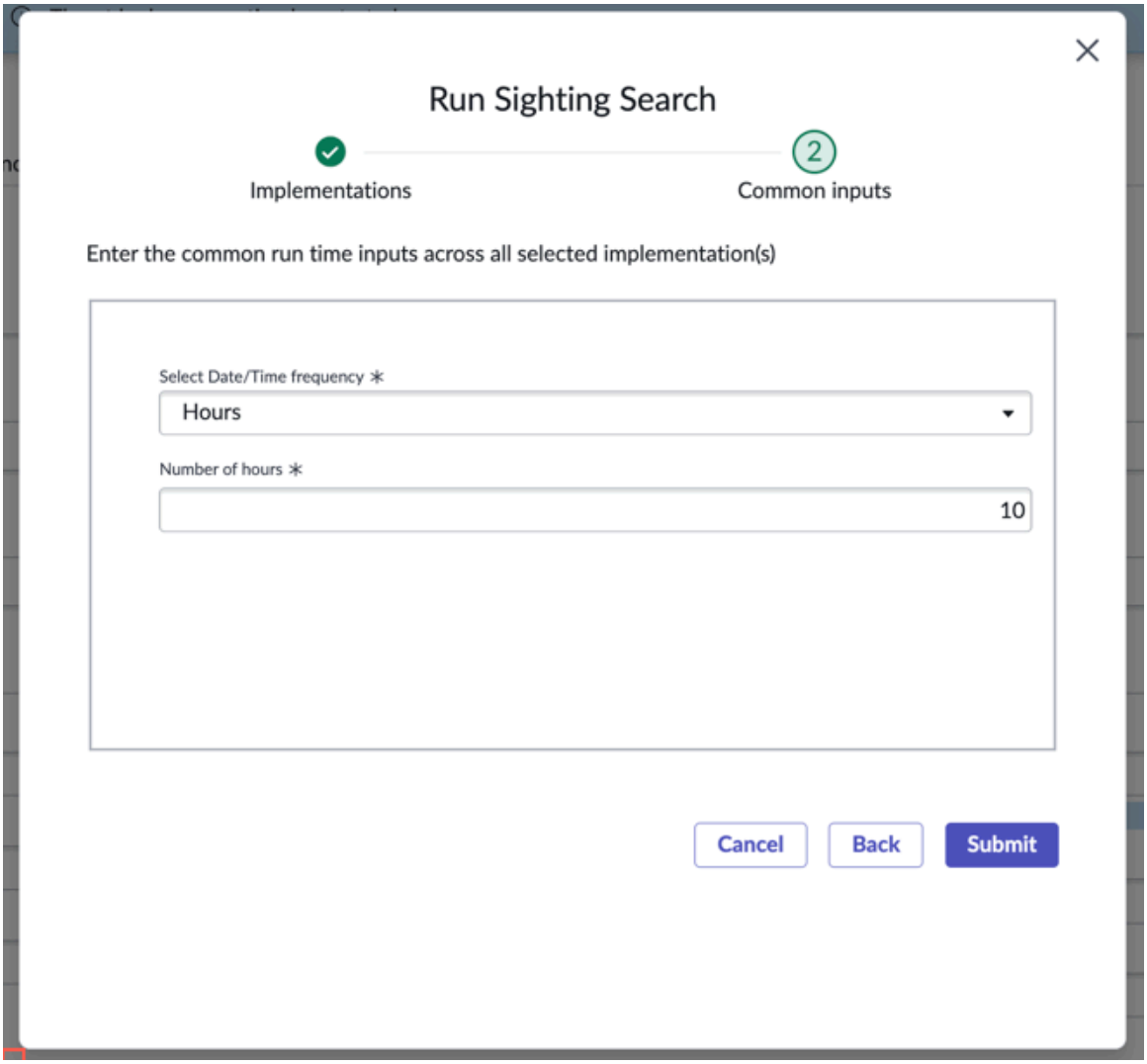
   Note: The Run Sighting Search performs the threat intelligence lookups to determine whether the observables are associated with any known threats.

6. Select the required implementation(s) from the list.



7. Click **Next**.
8. Select the common run time input value such as Select Date/Time frequency and Number of hours.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Click **Submit**.
   The selected enrichment action will be executed and an information message is displayed that Run Sighting Search execution has started.

Note:

- Once the execution initiated or completed, a work notes is posted on the activity stream of the form view.
- The enrichment results pushed from SIR workspace can be found in the **Enrichment Results** tab of that corresponding Observables details page in TISC Workspace.
- The enrichment results pushed from SIR workspace can be identified using **Source** field of the enrichment result table.

Run Observable Enrichment

Select one or more implementations as applicable to run threat lookup on observables.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

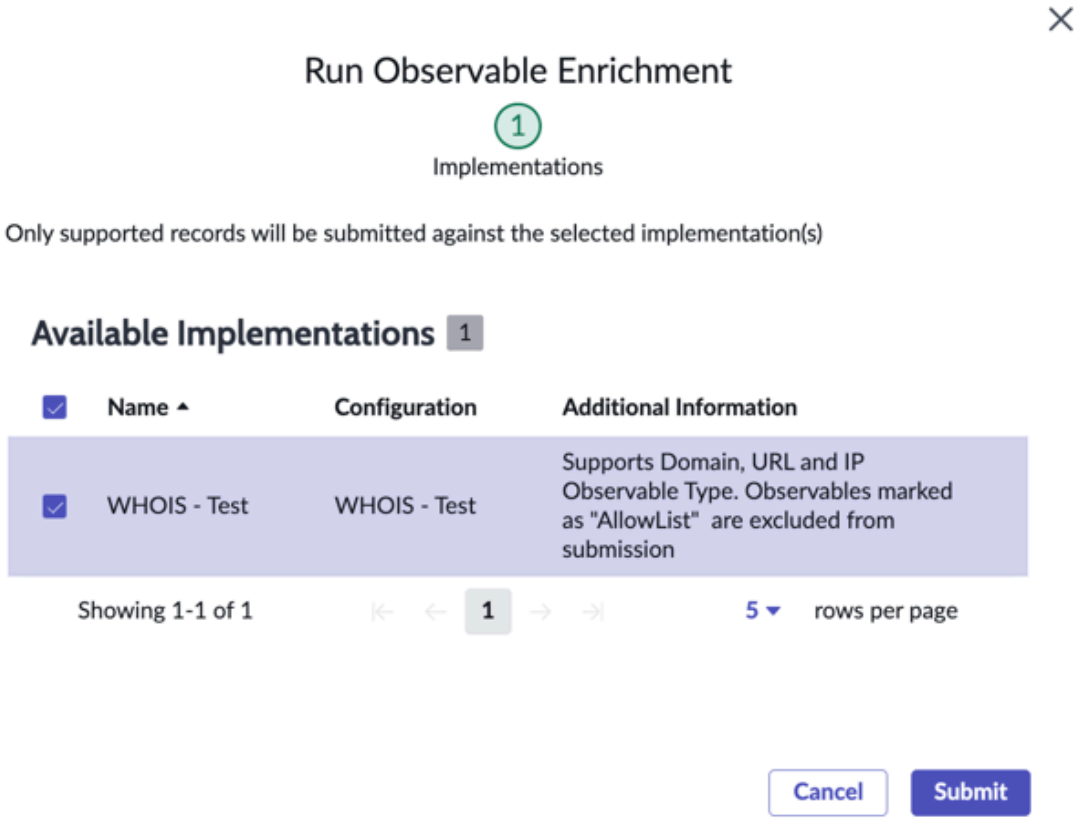
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Analyst Workbench** icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Go to **Observables** > **All Observables**.
4. Open any observable record.
5. Click **Run Observable Enrichment**.
   The Run Observable Enrichment **Select Implementations** modal screen is displayed.

   Note: Only supported records will be submitted against the selected implementation(s)

6. Select the required implementation(s) (for example, WHOIS) from the list.



7. Click **Submit**.
   The selected enrichment action will be executed and an information message is displayed that Threat lookup execution has started.

   Note:

   - Once the execution initiated or completed, a work notes is posted on the activity stream of the form view.
   - The enrichment results pushed from SIR workspace can be found in the **Enrichment Results** tab of that corresponding Observables details page in TISC Workspace.
   - The enrichment results pushed from SIR workspace can be identified using **Source** field of the enrichment result table.

View Enrichment Results

View observables, indicators, and various objects enrichment results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s) record.
3. Go to **Enrichment Results** tab.
   The Enrichment Results displays the TISC integrations enrichment results.

Enrichment Name	Description
Threat Lookup Results	Lists all the associated threat lookup results for an observable.
Sightings	Lists all the associated sightings for an observable.
Observable Enrichment Results	Lists all the associated observable enrichment results for an observable.

Indicators

Indicators are artifacts observed on a network or operating system that are likely to indicate an intrusion. Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs, or domain names.

Define an Indicator

Define an Indicator.

Before you begin
Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Indicators**.
2. Select **Indicator**.
3. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

4. On the form, fill in the fields.

Details section

Field	Description
ID	Unique ID of the indicator.
Description	Description of the indicator.
Name	Name of the indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Pattern	The detection pattern for this Indicator may be expressed as a STIX Pattern.
Pattern Type	The pattern language used in this indicator.
Pattern Version	The version of the pattern language that is used for the data in the pattern property which must match the type of pattern data included in the pattern property.
Valid From	The time from which this Indicator is considered a valid indicator of the behaviors it is related or represents.
Valid Until	The time after which this Indicator should no longer be considered a valid indicator of the behaviors it is related to or represents.
IOC Classification	The IOC classification of the indicators.
Indicator Types	Indicates the various categories of the indicator.
Status	Indicates the status of the indicators.
Platforms	Defines the platforms for which this indicator is applicable for.
TLP	Unique value that indicates the Data sensitivity setting per TLP.
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
Confidence	Enter the confidence for this indicator record. The confidence property identifies the confidence that the creator has in the correctness of their data. The confidence value MUST be a number in the range of 0-100.
Threat Level	Indicates the threat level of the indicator record.
Expiration Time	Specifies the expiration time of the indicator record.
Threat Severity	Indicates the threat severity of the indicator record.
Usage Categories	Categories that the observable falls under, such as botnet or phishing.
First Seen	The time that this indicator record was first seen performing malicious activities.
Last Seen	The time that this indicator record was last seen performing malicious activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source	Specifies the threat source from which this record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for an indicator.

Additional Information

Field	Description
Additional Context	Add any additional context for this indicator.
Spec Version	The version of the STIX specification used to represent the indicator. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created	Specifies the time when the indicator is created in system.
Updated	Specifies the time when the indicator is updated in system.
Extensions	Indicates the extensions of indicator.
Processing Status	Represents the processing status of this indicator.

5. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
6. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with an indicator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select the Taxonomy that is associated with an indicator.
Add Taxonomy Values	Add the Taxonomy values that are associated with an indicator.

Source Records

Field	Description
The source records details for an indicator are displayed, if any.	

What to do next

You can now click any of the following related lists to view additional information about objects associated with the indicators.

Related Records

Related List	Description
MITRE Techniques	Lists the MITRE techniques related to this indicator.
Attack Patterns	Lists the Attack Patterns source that describe the methods that adversaries attempt to compromise targets that are related to this indicator.
Campaigns	Lists the Campaigns Source that describe a set of malicious activities or attacks that occur over time against a specific set of targets that are related to this indicator.
Courses of Action	Lists the courses of action related to this indicator.
Data Sources	Lists the data sources related to this indicator.
Data Components	Lists the data components related to this indicator.
Identities	Lists the identities that are related to this indicator.
Indicators	Lists the indicators that are related to this indicator. **Note:** This section also contains the potential relationships between two indicators. For more information, see Confirm indicator-indicator potential relationshipsand see Define indicator-indicator relationships for the confirmed relationships between the two observables.
Infrastructure	Lists the Infrastructure Source that describe any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack that are related to this indicator.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties that are related to this indicator.
Locations	Lists the geographical locations associated with the object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Related List	Description
Malware	Lists malware source records that are related to this indicator.
Marking Definitions	Lists the marking definitions associated with this object.
Malware Analysis	Lists the metadata and results of a particular static or dynamic analysis performed on a malware instance associated to this indicator.
Observables	Lists the related observable records that are related to this indicator.
Observed Data	Lists the observed data that are cyber security related entities such as files, systems, and networks and associated with this indicator.
Sightings	Lists sightings source records associated with this object.
Threat Actors	Lists changes associated with the observable.
Threat Events	Lists the event or situation that has the potential for causing undesirable consequences or impact that are associated with the indicator.
Threat Groupings	Lists the threat groupings as objects that have a shared context.
Threat Notes	Lists the threat notes that convey information to provide further context or analysis that are associated with the indicator.
Threat Opinions	Lists the threat opinions as an assessment of the accuracy of the information that are associated with the indicator.
Threat Reports	Lists the threat reports associated with this indicator.
Tools	Lists the tool associated with this object.
Vulnerabilities	If the observable is an IP address, this list shows any resources (configuration items) that have a matching IP address.
Related Cases	Lists the related cases that are associated with this indicator.
Related Case Tasks	Lists the related case tasks that are associated with this indicator.
Related Canvases	Lists the related canvases that are associated with this indicator.
Indicators References	List of external references that describes this indicator.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. Also, from the **Related Records** section, you can confirm the relationships between two Observables using the **Potential Relationships** section available on the **Indicators** form view. For more information on see, Confirm Potential Relationships from Related Records.
3. You can add indicators to cases. For more information, see Add to Case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Entities

The Threat Entities module provides structured records used to manage threat intelligence objects in the TISC. These records align with STIX domain object concepts and help standardize how threat activity is documented and analyzed.

Use this module to create and manage entities such as:

- **Attack Patterns** to document adversary tactics and techniques.
- **Campaigns** to track coordinated threat activity over time.
- **Courses of Action** to define recommended remediation steps.
- **Identities** to represent individuals, groups, or organizations.
- **Infrastructure** to record systems and services used in operations.
- **Intrusion Sets** to group related threat activity.
- **Malware** and **Malware Analysis** records for malicious tools and findings.
- **Threat Actors** to represent adversaries.
- **Threat Events**, **Threat Reports**, **Threat Notes**, and **Threat Opinion** to capture contextual intelligence.
- **Marking Definitions** to apply data handling classifications.

Related topics

Observables

Indicators

Attack Patterns

Attack patterns are a type of Tactics, Techniques, and Procedures (TTPs) that describe the methods that adversaries attempt to compromise targets.

Attack patterns are used to help categorize attacks. They generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.

For example, spear phishing is a common type of attack where an attacker sends a carefully crafted email message to a party with the intent of getting them to click a link or open an attachment to deliver malware. Attack Patterns are more specific, such as spear phishing by a particular threat actor (example - that the target won a contest) can also be an Attack pattern.

Define an attack pattern

Define an attack pattern to help threat analysts categorize the attacks.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Attack Pattern**.
4. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Attack Pattern Details view

Field	Description
ID	Unique ID for an attack pattern.
Name	Enter a name for this attack pattern.
Description	Enter a description for an attack pattern.
Aliases	Alternative names to identify this attack pattern. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
Attack Phase	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
Permissions Required	Select the required permissions for this attack pattern.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this attack pattern mode. The confidence property identifies the confidence that the creator has in the correctness of their data. The confidence value MUST be a number in the range of 0-100.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.
Prevent System Updates	Setting this flag to true will prevent system from overriding values of fields on record.

Important: After you create a new object record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Insights

Field	Description
Notes	Add any additional notes for an attack pattern.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object, attack pattern. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created	Specifies the time when the record is created in the system.
Updated	Specifies the time when the record is modified in the system.
Extensions	Indicates the extensions of attack pattern.
Processing Status	Represents the processing status of this object, attack pattern.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with an observable.
Add Tags	Add new tags.
Taxonomies	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Select Taxonomy	Select a Taxonomy that is associated with an attack pattern.
Add Taxonomy Values	Add Taxonomy values that are associated with an attack pattern.

What to do next

You can now click any of the following related lists to view additional information about objects associated with the attack pattern.

Related Records

Field	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists campaigns associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Campaign

Campaign is defined as grouping of adversarial behaviors that describes a set of malicious activities or attacks, sometimes called waves that occur over a period of time against a specific set of targets.

Define Campaign

Define a campaign to group adversarial behaviors.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Campaign** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Campaign view

Field	Description
ID	Unique ID for an adversarial behavior.
Name	Enter a name for an adversarial behavior.
Description	Enter a description for this campaign.
Objective	The campaign's primary goal, objective, desired outcome, or intended effect. What the threat actor or intrusion set hopes to accomplish with this campaign.
Aliases	Alternative names to identify for this campaign.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
TLP	Traffic Light Protocol (TLP) indicates the sensitive information shared with the correct audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity for this attack pattern.
Confidence	Enter the confidence for this campaign.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for an campaign.

Additional Information

Field	Description
Additional Context	Add any additional context for this campaign.
First Seen	The time that this object first seen performing adversarial behavior.
Last Seen	The time that this object was last seen performing adversarial behavior.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created	Specifies the date and time when the object was created in the source.
Extensions	Indicates the extensions of attack pattern.
Updated	Specifies the date and time when the object was updated in the source.
Processing Status	Represents the processing status of this object, campaign.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with an campaign.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with an campaign.
Add Taxonomy Values	Add Taxonomy values that are associated with campaign.

What to do next

You can now click any of the following related lists to view additional information about objects associated with campaign.

Related Records

Field	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Set	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Malware	Lists malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Courses of Action

Courses of action is an action taken either to prevent an attack or to respond to an attack that is in progress.

Courses of action describes technical or automated responses such as applying patches, reconfiguring firewalls. It can also describe higher-level actions like employee training or policy changes.

For example, courses of action to mitigate a vulnerability could describe applying the patch that fixes it.

Define Courses of Action

Define courses of action to prevent an attack or to respond to an attack that is in progress.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Courses of Action** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Courses of Action Details view

Field	Description
ID	Unique ID for a courses of action to prevent an attack.
Name	Enter a descriptive name for this courses of action.
Description	A description that provides more details and context about the courses of action, potentially including its purpose and its key characteristics.
Action	To capture structured or automated courses of action.
TLP	Traffic Light Protocol (TLP) indicates the sensitive information shared with the correct audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity for this attack pattern.
Confidence	Enter the confidence for this courses of action.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for a courses of action.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, courses of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with an observable.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with an attack pattern.
Add Taxonomy Values	Add Taxonomy values that are associated with an attack pattern.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Click any of the following related lists to view additional information about objects associated with the courses of action.

Related Records

Field	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Malware	Lists malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Observables	Lists the observables associated with this object.
Sightings	Lists the sightings associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Identity

Identities represent actual individuals, organizations or groups, and classes of individuals, systems, or groups. Identities apply for STIX 2.x.

An Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity represents targets of attacks, information sources, object creators, and threat actor identities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define identities

Define identities who represent actual individuals, organizations, or groups.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Identity** object.
4. Click **New**.

> **Note:** Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Identity Details view

Field	Description
ID	Unique ID for an identity.
Name	Enter a descriptive name for this identity. When referring to a specific entity (an individual or organization), this property must contain the canonical name of the specific entity.
Description	A description that provides more details and context about the course of action, potentially including its purpose and its key characteristics.
Roles	The list of roles that this Identity performs.
Identity Class	The type of entity that this identity describes. For example, individual or organization.
Sectors	The list of industry sectors that this Identity belongs to.
Contact information	The contact information such as email and phone number for this Identity.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience.It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this identity.
Source	Specifies the threat source from which this object record is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for the identity.

Additional Information

Field	Description
Additional Context	Add any additional context related to this identity.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the identity.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with the identity.
Add Taxonomy Values	Add Taxonomy values that are associated with the identity.

What to do next

Click any of the following related lists to view additional information about objects associated the identity.

Related Records

Field	Description
External References	Lists external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware	Lists malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Threat Actors	Lists individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Infrastructure

The Infrastructure SDO represents a type of Tactics, Techniques, and Procedures (TTPs). They describe any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack. Infrastructure applies for STIX 2.x.

The elements of an attack are represented by other SDOs or SCOs. However, the Infrastructure SDO represents a named group of data that constitutes the infrastructure.

Examples of infrastructure include, C2 servers used in an attack, a device, or a server that is part of a defense, or database servers targeted by an attack.

Define infrastructure

Define an Infrastructure that is any systems, software services, and any associated physical or virtual resources intended to support some purpose of an attack.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Infrastructure** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Infrastructure Details view

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Name	Enter a descriptive name for this course of action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	When referring to a specific entity (an individual or organization), this property must contain the canonical name of the specific entity.
Description	A description that provides more details and context about the Infrastructure, potentially including its purpose, how it is being used, how it relates to other intelligence activities captured in related objects, and its key characteristics.
Infrastructure Types	Describes the categorisation of infrastructure.
Aliases	Alternative names to identify this infrastructure. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
First Seen	The time that this infrastructure was first seen performing malicious activities.
Last Seen	The time that this infrastructure was last seen performing malicious activities.
Confidence	Enter the confidence for this course of action.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this infrastructure.

Additional Information

Field	Description
Additional Context	Add any additional context for this infrastructure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the time when the record is created in the source.
Updated	Specifies the time when the record is modified in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the infrastructure.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this infrastructure.
Add Taxonomy Values	Add Taxonomy values that are associated with this infrastructure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Click any of the following related lists to view additional information about objects associated the identity.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Intrusion Set

An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties. An Intrusion Set usually involves a single organization. Intrusion set applies for STIX 2.x.

An Intrusion Set may capture multiple Campaigns or other activities. These activities share attributes indicating a commonly known or unknown Threat Actor.

New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.

An Intrusion Set is the entire attack package and may be used over a long period in multiple Campaigns to achieve potentially multiple purposes.

Define Intrusion Set

Define an intrusion set that is a grouped set of adversarial behaviors and resources with common properties.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Intrusion Set**.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Intrusion Set Details view

Field	Description
ID	Unique ID for an intrusion set.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Enter a descriptive name for this intrusion set. When referring to a specific entity (an individual or organization), this property must contain the canonical name of the specific entity.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.
Aliases	Alternative names to identify this intrusion set. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
Goals	The high-level goals of this Intrusion Set, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer.
First Seen	The time that this intrusion set was first seen performing malicious activities.
Last Seen	The time that this intrusion set was last seen performing malicious activities.
Primary Motivation	The primary reason, motivation, or purpose behind this Intrusion Set. The motivation is why the Intrusion Set wishes to achieve the goal (what they are trying to achieve).
Secondary Motivations	The secondary reasons, motivations, or purposes behind this Intrusion Set. These motivations can exist as an equal or near-equal cause to the primary motivation. However, it does not replace or necessarily magnify the primary motivation, but it might indicate additional context. The position in the list has no significance.
Resource Level	This property specifies the organizational level at which this Intrusion Set typically works, which in turn determines the resources available to this Intrusion Set for use in an attack.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this intrusion set.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this intrusion set.

Additional Information

Field	Description
Additional Context	Add any additional context for this intrusion set.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time when the record is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the time when the record is created in the source.
Updated	Specifies the time when the record is modified in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the intrusion set.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this intrusion set.
Add Taxonomy Values	Add Taxonomy values that are associated with this intrusion set.

What to do next

Click any of the following related lists to view additional information about objects associated with the intrusion set.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists the campaigns associated with this object.
Identities	List of identities associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Location

A Location represents a geographic location. Locations are primarily used to give context to other SDOs. Locations apply for STIX 2.x.

The location may contain, some or all of the following: region (North America), civic address (New York, US), latitude, and longitude.

The Location SDO may relate to an Identity or Intrusion Set to indicate that the identity or intrusion set is in that location. It can also relate to a malware or attack pattern to indicate that the target victim is in a particular location.

For example, a Location could be used in a relationship to describe that the Bourgeois Swallow intrusion set originates from Eastern Europe.

At least one of the following properties or sets of properties must be provided:

- region
- country
- latitude and longitude

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define Location

Define a geographic location to provide more context to other Suspicious Domain Objects (SDO).

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Location** object.
4. Click **New**.

> **Note:** Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields

Identity Details view

Field	Description
ID	Unique ID for the location.
Name	Enter a descriptive name to identify the location.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.
Latitude	The latitude of the Location in decimal degrees. Positive numbers describe latitudes north of the equator, and negative numbers describe latitudes south of the equator. The value of this property must be from -90.0 through 90.0 respectively.
Longitude	The longitude of the location in decimal degrees. Positive numbers describe longitudes east of the prime meridian and negative numbers describe longitudes west of the prime meridian. The value of this property must be from -180.0 through 180.0, inclusive.
Precision	Defines the precision of the coordinates specified by the latitude and longitude properties. This is measured in meters. The actual location may be anywhere up to precision meters from the defined point.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	If this property is not present, then the precision is unspecified. If this property is present, the latitude and longitude properties must be present.
Region	The region that this location is in.
Country	The country that this location is in.
Administrative Area	The state, province, or other sub-national administrative area that this location is in.
City	The city that this location is in.
Street Address	The street address that this location describes. This property includes all aspects or parts of the street address.
Postal Code	The postal code that this location is in.
Confidence	Enter the confidence for this course of action.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this location.

Additional Information

Field	Description
Additional Context	Add any additional context for this location.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Extensions	Indicates the extensions for this location.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the time when the record is created in the source.
Updated	Specifies the time when the record is modified in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the location.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this location.
Add Taxonomy Values	Add Taxonomy values that are associated with this location.

What to do next

Click any of the following related lists to view additional information about objects associated with the location.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists the campaigns associated with this object.
Identities	List of identities associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Observables	Lists the observables associated with this object.
Sightings	Lists the sightings associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Malware

Malware is a type of TTP that represents malicious code. It refers to a program that is covertly inserted into a system. Malware applies for STIX 2.x.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The intent of a malware is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS).

The Malware SDO characterizes, identifies, and categorizes malware instances and families from data that is derived from analysis. This SDO captures detailed information about how the malware works and what it does.

Define Malware

Define a malware that represents malicious code.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Malware** Threat Intel object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Malware Details view

Field	Description
ID	Unique ID to identify the Malware instance.
Name	Enter a name to identify the malware instance or family, as specified by the producer of the SDO. For a malware family, the name must be defined.
Description	A description that provides more details and context about the malware instance or family, potentially including its purpose and its key characteristics.
Malware Types	Indicates the various categories of the malware.
Is Family	Select this check box to specify if the object represents a malware family or a malware instance.
Aliases	The alternative names used to identify this malware or malware family. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.
First Seen	The time that this malware instance or family was first seen performing malicious activities.
Last Seen	The time that this malware instance or family was last seen performing malicious activities
Process Architectures	Indicates the process architectures for this malware.
Implementation Languages	Indicates the implementation languages for this malware.
Malware Capabilities	The capabilities that may be exhibited by a malware instance or family.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this malware.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for the malware record.

Additional Information

Field	Description
Additional Context	Add any additional context for this malware record.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, malware.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the malware.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with the malware.
Add Taxonomy Values	Add Taxonomy values that are associated with the malware.

What to do next

Click any of the following related lists to view additional information about objects associated with the malware.

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Campaigns	Lists the campaigns associated with this object.
Detections and Mitigations	Lists the detections and mitigations that are related to this malware.
Identities	List of identities associated with this object.
Indicators	Lists related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists locations that provide geographic context to this object.
Malware Analysis	Lists malware analysis records associated with this object.
Malware	Lists malware records associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Observables	Lists the observables associated with this object.
Sightings	Lists the sightings associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Malware Analysis

Malware Analysis captures the metadata and results of a malware. Malware analysis applies for STIX 2.x.

Malware Analysis includes static or dynamic analysis performed on a malware instance or family.

Define Malware Analysis

Define malware analysis that captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Malware Analysis** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Malware Analysis Details view

Field	Description
ID	Unique ID to identify the malware analysis.
Product	The name of the analysis engine or product that was used. Product names SHOULD be all lowercase with words separated by a dash "-". For cases where the name of a product cannot be specified, a value of anonymized must be used.
Version	The version of the analysis product that was used to perform the analysis.
Host VM	A description of the virtual machine environment used to host the guest operating system, if applicable that was used for the dynamic analysis of the malware instance or family. If this value is not included in conjunction with the operating_system_ref property, this means that the dynamic analysis may have been performed on bare metal (i.e. without virtualization) or the information was redacted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The value of this property MUST be the identifier for a SCO software object.
Operating System	The operating system used for the dynamic analysis of the malware instance or family. This applies to virtualized operating systems as well as those running on bare metal. The value of this property MUST be the identifier for a SCO software object.
Configuration Version	The alternative names used to identify this malware or malware family.
Modules	The specific analysis modules that were used and configured in the product during this analysis run.
Analysis Engine Version	The version of the analysis engine or product (including AV engines) that was used to perform the analysis.
Analysis Definition Version	The version of the analysis definitions used by the analysis tool including AV tools.
Analysis Started	The date and time that the malware analysis was initiated.
Analysis Ended	The date and time that the malware analysis was ended.
Result	The classification result as determined by the scanner or tool analysis process.
Result Name	The classification result or name assigned to the malware instance by the scanner tool.
Submitted	The date and time that the malware was first submitted for scanning or analysis. This value will stay constant while the scanned date can change. For example, when Malware was submitted to a virus analysis tool.
Analysed Observable	Select the observable that was analysed.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this malware analysis.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Insights

Field	Description
Notes	Add any additional notes for the malware family record.

Additional Information

Field	Description
Additional Context	Add any additional context for this malware record.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, malware.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the malware.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with the malware.
Add Taxonomy Values	Add Taxonomy values that are associated with the malware.

What to do next

Click any of the following related lists to view additional information about objects associated with the malware.

Relatd Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Malware	Lists malware records associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Observables	Lists the observables associated with this object.
Sightings	Lists the sightings associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Marking Definition

The marking-definition object represents a specific marking. Data markings typically represent handling or sharing requirements for data.

Define Marking Definition

Define marking definitions to handle and share the requirements for the data.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Marking Definition** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Marking Definition Source Details view

Field	Description
ID	Unique ID to identify a Marking Definition.
Name	A name used to identify the Marking Definition.
Definition Type	The type property identifies the type of object. The definition_type property identifies the type of Marking Definition.
Definition	The definition property contains the marking object itself, for example TLP.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this object. The confidence property identifies the confidence that the creator has in the correctness of their data. The confidence value MUST be a number in the range of 0-100.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Insights

Field	Description
Notes	Add any additional notes for this Marking Definition.

Additional Information

Field	Description
Additional Context	Add any additional context for this Marking Definition.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the vulnerability.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this vulnerability.
Add Taxonomy Values	Add Taxonomy values that are associated with this vulnerability.

What to do next

Click any of the following related lists to view additional information about objects associated with the vulnerability.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns associated with this object.
Campaigns	Lists the campaigns associated with this object.
Detections and Mitigations	Lists the detections and mitigations associated with this object.
Identities	Lists the identities associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Malware Analysis	Lists the malicious analysis associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Threat Events	Lists the Threat Events associated with this object.
Threat Groupings	Lists the Threat Groupings associated with this object.
Threat Notes	Lists the Threat Notes associated with this object.
Threat Opinions	Lists the Threat Opinions associated with this object.
Tools	Lists the Tools associated with this object.
Vulnerabilities	Lists the Vulnerabilities associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Object Sighting

Sightings denote that an object was seen. Objects may be a malware, tool, threat actor, and so on.

Sightings track who and what is the target, how attacks are carried out, and to track trends in attack behavior.

The Sighting relationship object contains extra properties not present in the generic relationship objects. These extra properties represent data specific to sighting relationships.

Define Object Sighting

Define object sighting that describes that an object (malware, tool, threat actor, and so on) was seen.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Object Sighting** object.
4. Click **New**.

> **Note:** Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Choose Entity&Value

Field	Description
Entity	Select the entity object sighting record. **Note:** During any new object sighting record creation, an associated relationship record is required for aggregation.
Sighting of	Indicates the that a particular entity or indicator was observed in an environment which can be an indication to a potential threat. **Note:** Select the sighting related record which is associated to the object selected in the Entity field so that related records can now be created and aggregate the sighting records.

Object Sighting Details view

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Description	A description that provides more details and context about the Sighting.
First Seen	The beginning of the time window during which the SDO referenced by which the property was sighted.
Last Seen	The end of the time window during which the SDO referenced by which the property was sighted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Count	If present, this must be an integer between 0 and 999,999,999 inclusive and represents the number of times the SDO referenced by which the property was sighted.
Is Summary	Indicates whether the Sighting should be considered the summary data. Summary data is an aggregation of previous Sightings reports and should not be considered primary source data.
Is Internal	Indicates whether the Sighting is internal.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this course of action.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this intrusion set.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the identity.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this infrastructure.
Add Taxonomy Values	Add Taxonomy values that are associated with this infrastructure.

What to do next

Click any of the following related lists to view additional information about objects associated with the object sighting.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Objects	Lists the objects associated with the sightings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Observed Data

Observed Data conveys information about cyber security-related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs). Observed data applies for STIX 2.x.

Observed Data captures both a single observation of a single entity (file, network connection) as well as the aggregation of multiple observations of an entity.

You can use Observed Data by itself (without relationships) to convey raw data collected from any source. Sources include analyst reports, sandboxes, and network and host-based detection tools.

For example, Observed Data can capture information about an IP address, a network connection, a file, or a registry key. Observed Data is not an intelligence assertion, it is simply the raw information without any context for what it means.

Define Observed Data

Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Observed Data** object.
4. Click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Observed Data Details view

Field	Description
ID	Unique ID to identify the observed data.
First Observed	The initial time when the data was seen.
Last observed	The last time when the data was seen.
Observed Count	The number of times that each Cyber-observable object was seen. The value must be an integer from 1 through 999,999,999.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for the observed data
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this observed data.

Additional Information

Field	Description
Additional Context	Add any additional context for this observed data.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created	Specifies the date and time when the object is created in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Extensions	Indicates the extensions of attack pattern.
Updated	Specifies the date and time when the object was updated in the source.
Processing Status	Represents the processing status of this object, course of action.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the observed data.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this observed data.
Add Taxonomy Values	Add Taxonomy values that are associated with this observed data.

What to do next

Click any of the following related lists to view additional information about objects associated with the observed data.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Threat Actor

Threat Actors are individuals, groups, or organizations who act with malicious intent. Threat actors applies for STIX 2.x.

A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.

Threat Actors use their resources, and the resources of an Intrusion Set, to conduct attacks, and run Campaigns against targets.

You can identify Threat Actors by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

Define Threat Actor

Define threat actors who are individuals, groups, or organizations who act with malicious intent.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Actor** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Actor Details view

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Name	Enter a descriptive name to identify the location.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.
Aliases	A list of other names to identify this threat actor. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
Goals	The high-level goals of this threat actor, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers.
Threat Actor Types	The type(s) of this threat actor.
Threat Actor Roles	The various threat actor role(s) for this object.
First Seen	The time that this Threat Actor was first seen. This property is a summary property of data from sightings and other data that may or may not be available in STIX. If new sightings are received that are earlier than the first seen timestamp, the object may be updated to account for the new data.
Last Seen	The time that this Threat Actor was last seen.
Primary Motivation	The primary reason, motivation, or purpose behind this Threat Actor. The motivation is why the Threat Actor wishes to achieve the goal (what they are trying to achieve). For example, a Threat Actor with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.
Sophistication	The skill, specific knowledge, special training, or expertise a Threat Actor must have to perform the attack.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Secondary Motivations	This property specifies the secondary reasons, motivations, or purposes behind this Threat Actor. These motivations can exist as an equal or near-equal cause to the primary motivation. However, it does not replace or necessarily magnify the primary motivation, but it might indicate additional context. The position in the list has no significance.
Resource Level	The organizational level at which this Threat Actor typically works, which in turn determines the resources available to this Threat Actor for use in an attack. This attribute is linked to the sophistication property — a specific resource level implies that the Threat Actor has access to at least a specific sophistication level.
Confidence	Enter the confidence for this course of action.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this threat actor.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat actor.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat actor.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat actor.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat actor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Attack Patterns	Lists the attack patterns that help categorize attacks that are associated with this object.
Campaigns	Lists the campaigns associated with this object.
Identities	List of identities associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	List of locations associated with this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Observables	Lists the observables associated with this object.
Sightings	Lists the sightings associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Threat Event

An event or situation that has the potential for causing undesirable consequences or impact.

A hacker attacking a website is a threat event. If the hackers manage to damage any website or steal information, that would be defined as a threat event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Define Threat Event

Define a threat event when an event that results in unauthorized access to and acquisition of nonpublic information or the disruption or misuse of any information system.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Event** object.
4. Click **New**.

> **Note:** Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Threat Actor Details view

Field	Description
ID	Unique ID for a course of action to prevent a threat event.
Name	Enter a descriptive name to identify the threat event.
Description	A description that provides more details and context about the threat event, potentially including its purpose and its key characteristics.
Confidence	Enter the confidence for this course of action.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this threat actor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat event.
Add Tags	Add new tags.
Taxonomies	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Select Taxonomy	Select a Taxonomy that is associated with this threat event.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat event.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat event.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Threat Grouping

A Threat Groupings object explicitly asserts that the referenced STIX Objects have a shared context. Threat groupings applies for STIX 2.x.

A Threat Groupings object represents a set of data that, given sufficient analysis, matures to convey an incident or threat report as a STIX Report object. For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident.

A Threat Groupings object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process. For example, a threat analyst may collaborate with others in their trust community to examine a series of Campaigns and Indicators.

The Threat Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.

Define Threat Grouping

Define threat groupings as objects that have a shared context.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Grouping** object.
4. Click **New**.

Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. On the form, fill in the fields.

Threat Grouping Details view

Field	Description
ID	Unique ID for a course of action to prevent a Threat Group type of attack to happen.
Name	Enter a descriptive name to identify the threat group.
Description	A description that provides more details and context about the threat event, potentially including its purpose and its key characteristics.
Confidence	Enter the confidence for this course of action.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this threat grouping.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat grouping.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat grouping.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat grouping.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat grouping.

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Threat Events	Lists the threat events associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Note

A Threat Note conveys informative text to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to. Threat notes applies for STIX 2.x.

For example, an analyst may add a Note to a Campaign object created by another organization. The note may indicate that they've seen posts related to that Campaign on a hacker forum.

Notes are usually created by human analysts and are composed of human-oriented text, they contain an extra property to capture the author that created the Note.

Define Threat Note

Define threat notes that convey information to provide further context or analysis that is not available in existing objects.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Note**.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Threat Note Details view

Field	Description
ID	Unique ID for a threat note.
Abstract	Specify a brief summary of the note content.
Content	Specifies the content of the note.
Authors	Specifies the name of the author (example, an analyst).
Confidence	Enter the confidence for this course of action.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Insights

Field	Description
Notes	Add any additional notes for this threat note.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat grouping.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat grouping.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat grouping.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat note.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Threat Events	Lists the threat events associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Threat Opinion

An Opinion is an assessment of the accuracy of the information in a STIX Object produced by a different entity. Threat opinions apply for STIX 2.x.

The opinion property captures the level of agreement or disagreement using a fixed scale. The fixed scale also supports a numeric mapping to enable consistent statistical operations across opinions.

For example, an analyst from a consuming organization might say that they "strongly disagree" with a Campaign object and provide an explanation about why.

Opinions are subjective, and the specification does not address how best to interpret them.

Human analysts create Opinions and are composed of human-oriented text, they contain an extra property to capture the author that created the Opinion.

Define Threat Opinion

Define threat opinions as an assessment of the accuracy of the information in a STIX object.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Opinion** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Threat Opinion Details view

Field	Description
ID	Unique ID for a threat opinion.
Opinion	The producer's opinion about the STIX object.
Explanation	Specifies the content of the opinion.
Authors	Specifies the name of the author (example, an analyst).
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Confidence	Enter the confidence for this course of action.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this threat opinion.

Additional Information

Field	Description
Additional Context	Add any additional context for this threat opinion.
Spec Version	The version of the STIX specification used to represent this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the time when the record is created in the source.
Updated	Specifies the time when the record is modified in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat opinion.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat opinion.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat opinion.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat opinion.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Threat Events	Lists the threat events associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Threat Report

Threat Reports are collections of threat intelligence focused on one or more topics. Threat reports apply for STIX 2.x.

Threat reports include description of a threat actor, malware, attack technique, including context and related details. They are used to group-related threat intelligence together so that it can be published as a comprehensive cyber threat story.

The Threat Report SDO contains a list of references to STIX Objects along with a textual description and the name of the report.

Define Threat Report

Define threat reports that describe a threat actor, malware, attack technique, including context and related details.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Threat Report** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Threat Report Details view

Field	Description
ID	Specify a name to identify the threat report.
Name	Specify a brief summary of the note content.
Description	A description that provides additional insight and context about the report.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Report Types	Specifies the name of the author (example, an analyst).
Published	The date that this report has been officially published by the report author.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this threat note.

Additional Information

Field	Description
Additional Context	Add any additional context for this attack pattern.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat grouping.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat grouping.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat grouping.

What to do next

Click any of the following related lists to view additional information about objects associated with the threat reports.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Threat Events	Lists the threat events associated with this object.
Threat Groupings	Lists the threat groupings associated with this object.
Threat Reports	Lists the threat reports associated with this object.
Tools	Lists legitimate software that is used by threat actors to perform attacks associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tool

Tools are legitimate software that are used by threat actors to perform attacks. Tools apply for STIX 2.x.

Tools enable you to know how and when threat actors use them for executing campaigns. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, administrators, network administrators, or even normal users.

For example, remote access tools (RDP) and network scanning tools (Nmap) are tools that a threat actor uses during an attack.

Define Tools

Define tools as legitimate software that is used to perform attacks.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Tool** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Tools Details view

Field	Description
ID	Unique ID to identify a tool.
Name	Enter a descriptive name to identify the tool.
Description	A description that provides more details and context about the tool, potentially including its purpose and its key characteristics.
Tool Types	The kind(s) of tool(s) being described.
Aliases	An alternative names used to identify this Tool. **Note:** To add new alias which is not existing in the application click on the **Add New Aliases** icon which is available within the Alias field itself.
Tool Version	The version identifier associated with the Tool.
Attack Phases	Represents attack phase in a kill chain such as LM, MITRE ATT&CK.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this tool.

Additional Information

Field	Description
Additional Context	Add any additional context for this tool.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: After you create a new observable record, **Prevent System Updates** check box is displayed.

Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the threat grouping.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this threat grouping.
Add Taxonomy Values	Add Taxonomy values that are associated with this threat grouping.

What to do next

Click any of the following related lists to view additional information about objects associated with the tools.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Detections and Mitigations	Lists the detections and mitigations associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records (continued)

Field	Description
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Other Objects

Define and manage data classifications within TISC.

Data Sources represent broad categories of security telemetry. Data Components provide a more granular breakdown of the specific type of data collected within a source.

These records support consistent documentation of detection coverage and analytical context. You can associate data sources and components with relevant threat entities to identify required telemetry, assess monitoring gaps, and support detection engineering and threat analysis activities.

Data Component

Data components are used to identify specific properties or values of a data source.

Define Data Component

Define a data component to identify the properties or values of a data source

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Data Component** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Data Component Details view

Field	Description
ID	Unique ID to identify a Data Component.
Name	A name used to identify the Data Component.
Description	A description that provides more details and context about the vulnerability, potentially including its purpose and its key characteristics.
Data Source	Indicates the normalized degree of severity of this vulnerability
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Confidence	Indicates the confidence for this object. The confidence must be between 0-100.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this Data Component.

Additional Information

Field	Description
Additional Context	Add any additional context for this Data Component.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of Data Component.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the vulnerability.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this vulnerability.
Add Taxonomy Values	Add Taxonomy values that are associated with this vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
Click any of the following related lists to view additional information about objects associated with the Data Component.

Related Records

Field	Description
Attack Patterns	Lists the attack patterns associated with this object.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Data Sources

Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source.

Define Data Sources

Define a data source to represent the various subjects or topics of information.

Before you begin
Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Data Sources** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Vulnerabilities Details view

Field	Description
ID	Unique ID to identify the data source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	A name used to identify the data source.
Description	A description that provides more details and context about the data source, potentially including its purpose and its key characteristics.
Collection Layers	Indicates the description of where the data source may be physically collected such as Host, Network, Cloud Control Plane, and so on.
Platforms	Indicates the system an adversary is operating within could be an operating system or application.
Contributors	Indicates the contributors for this data source.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this data source.

Additional Information

Field	Description
Additional Context	Add any additional context for this data source.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.
Extensions	Indicates the extensions of attack pattern.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the data source.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this data source.
Add Taxonomy Values	Add Taxonomy values that are associated with this data source.

What to do next

Click any of the following related lists to view additional information about objects associated with the data source.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Vulnerability

A Vulnerability is a weakness or defect in a software or hardware component that attackers exploit. Vulnerabilities apply for STIX 2.x.

The weakness or defect is in the requirements, designs, or implementations of the code found in a software or hardware component. This weakness is directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

CVE is a list of information security vulnerabilities and exposures that provides common names for publicly known problems [CVE].

For example, if a piece of malware exploits CVE-2015-12345, a Malware object could be linked to a Vulnerability object that references CVE-2015-12345.

Define Vulnerability

Define vulnerability as a weakness or defect in a software or hardware component that attackers exploit.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Vulnerability** object.
4. Click **New**.

   Note: Whenever you create new object records for observables, indicators, entities or objects a source record is created and a prompt message is displayed that the new object record is created and then the user is redirected to the aggregated record.

5. On the form, fill in the fields.

Vulnerabilities Details view

Field	Description
ID	Unique ID to identify a Vulnerability.
Name	A name used to identify the Vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	A description that provides more details and context about the vulnerability, potentially including its purpose and its key characteristics.
Severity	Indicates the normalized degree of severity of this vulnerability
CVSS3.0	Indicates the CVSS v3 for this vulnerability.
CVSS2.0	Indicates the CVSS v2 for this vulnerability.
Exploitation Status	Indicates the exploit status that is associated with this vulnerability
Published	Indicates when the vulnerability is published.
Record Last Modified	Indicates when the record when last modified.
Affected Software	Lists the affected software associated with the vulnerability.
TLP	TLP is used to ensure that sensitive information is shared with the appropriate audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity.
Source	Specifies the threat source from which this object record is created.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.

Insights

Field	Description
Notes	Add any additional notes for this vulnerability.

Additional Information

Field	Description
Additional Context	Add any additional context for this vulnerability.
Spec Version	The version of the STIX specification used to represent this object. The value of this property must be 2.1 for STIX Objects defined according to this specification.
Lang	This property identifies the language of the text content in this object.
Created Time In Source	Specifies the time the object is created in the source.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Extensions	Indicates the extensions of attack pattern.
Modified Time in Source	Specifies the time the object is modified in the source.
Processing Status	Represents the processing status of this object, course of action.
Created	Specifies the date and time when the object is created in the source.
Updated	Specifies the date and time when the object was updated in the source.
Created By Ref	This property specifies that the identity object that describes the entity had created this object.

6. Click **Save**.
   After you save, a prompt message is displayed indicating that A new observable record is created. Click **Continue** to edit the record and create new relationships.
7. Click **Continue**.

> **Important:** After you create a new observable record, **Prevent System Updates** check box is displayed.
>
> Select this check box to prevent any updates from the system after the observable or indicator or STIX objects records are created.

Tags&Taxonomies

Field	Description
Tags	
Select Tags	Select the tags that are associated with the vulnerability.
Add Tags	Add new tags.
Taxonomies	
Select Taxonomy	Select a Taxonomy that is associated with this vulnerability.
Add Taxonomy Values	Add Taxonomy values that are associated with this vulnerability.

What to do next

Click any of the following related lists to view additional information about objects associated with the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related Records

Field	Description
External References	Lists the external references which refer to non-STIX information. This property is used to provide one or more external object identifiers.
Campaigns	Lists the campaigns associated with this object.
Detections and Mitigations	Lists the detections and mitigations associated with this object.
Indicators	Lists the related Indicators of Compromise (IoC) that have been identified by the threat source associated with this object.
Infrastructure	Lists systems, software services, and any associated physical or virtual resources that are associated with this object.
Intrusion Sets	Lists a set of adversarial behaviors and resources with common properties associated with this object.
Locations	Lists the locations that provide geographic context to this object.
Malware	Lists the malicious code associated with this object.
Marketing Definitions	Lists the marketing definitions associated with this object.
Sightings	Lists the sightings associated with this object.
Observables	Lists the observables associated with this object.
Observed Data	Lists the observed data associated with this object.
Threat Actors	Lists the individuals, groups, or organizations who act with malicious intent associated with this object.
Vulnerabilities	Lists a weakness or defect in a software or hardware that attackers exploit which is associated with this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

1. You can link and unlink the related records associated with this object. For more information, see Link Threat Intel Related Records.
2. The various SDOs within the TI library also contains the potential relationships. To establish a relationships between any two objects, you use the **Potential Relationships** link from the **Threat Intel Library** to confirm the relationships between the objects. For more information, see Confirm object-object potential relationships.
3. Also, use the **Related Records** section from the objects form view to confirm the relationships between two Objects using the **Potential Relationships** section available on the form view. For more information on see, Confirm Potential Relationships from Related Records.
4. You can add objects to cases. For more information, see Add to Case.

Create a CWE record

Create a Common Weakness Enumeration (CWE) record to represent a weakness identified in a system or product, and link it to relevant vulnerabilities.

Before you begin

Role required: sn_sec_tisc.analyst

You must have the appropriate role to create records in the threat intelligence library.

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Library** > **Vulnerability Artifacts** > **CWEs**.
2. Click **New**.
3. Fill in the fields appropriately.

CWE Weakness

Field	Description
ID	Enter a unique identifier for the CWE. **Note:** The ID is pre-populated with the CWE# prefix. Append a unique numeric or alphanumeric value. The system validates uniqueness on save and prevents duplicate IDs.
Name	Name of the CWE weakness.
Description	Enter the description.
Type	Select a **Type**: **Primary** or **Secondary**. **Note:** The type indicates whether this CWE is a primary or secondary weakness as defined by the NVD schema.

4. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. **Optional:** To link vulnerabilities to this CWE, scroll to the **Vulnerabilities** related list and click **Link**.
6. **Optional:** To link related CWEs, scroll to the **Related Records** > **CWEs** related list and click **Link**.

Create a Product

Create New Product feature allows you to record the product's version, vendor, and classification details, to ensure products are accurately linked to vulnerabilities and related records.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **All** > **Workspaces** > **Threat Intelligence Library** > **Vulnerability Artifacts** > **Product**.
2. Select **New**.
3. Fill in the fields appropriately.

Vendor

Field	Description
ID	Unique identifier for the product record.
Name	Name of the product.
Product Version	Specific version of the product.
Product Version Range	Range of product versions to which the record applies.
Product Family	Parent product or product line to which this product belongs.
Is Product Group	Indicates whether the record represents a product group instead of a single product.
CPE	Common Platform Enumeration (CPE) string that standardizes product identification.
Vendor	Organization that develops or publishes the product.
Architecture	System architecture supported by the product, such as x86 or ARM.
Language	Language associated with the product or release.
Host Name	Host system name associated with the product, if applicable.
Patch Level	Patch level applied to the product version.
Service Pack	Service pack applied to the product version.
Specification	Additional specifications or details relevant to the product.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created in Source	Date when the product record was originally created in the source system.
Last Modified in Source	Date when the product record was last updated in the source system.
Status	Current state of the product record, such as Active or Inactive.

4. Click **Save**.
5. Go to the **Related Records** section.
6. Scroll to the **Product Identifiers** related list and click **Add**.
   Clicking **Add** opens the **Product Identifier** form in a new tab. The parent context (product) is automatically populated in the corresponding field. Enter the required form details.
   You can use the same process to add **Related Products**, **Product Vulnerabilities**, and **Product Vulnerability Remediations** records.
7. Click **Save**.

Result
The product identifier record is created and appears in the **Product Identifiers** related records of the **Product**.

Related topics

Create a CWE record

Create a Vendor to a Vulnerability

Create Remediations

Create a Vendor to a Vulnerability

Use this feature to create a vendor. Once created, you can associate the vendor to a product or link them to a vendor comment.

Before you begin
Role required: sn_sec_tisc.analyst

Procedure
1. Navigate to **All** > **Workspaces** > **Threat Intelligence Library** > **Vulnerability Artifacts** > **Vendor**.
2. Select **New**.
3. Fill in the fields appropriately.

Vendor

Field	Description
Name	The name of the vendor or supplying organization.
Organization	The full legal or organizational name associated with the vendor.
Description	A brief summary describing the vendor, their products, or their role in the context of the vulnerability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Website URL	The official website address of the vendor or organization.
Contact Details	Contact information for the vendor, such as an email address, phone number, or support portal URL.

4. Click **Save**.
5. To also add **Vendor Comments**, navigate to **Threat Intel Library** > **Vulnerability Artifacts** and open any vendor record to which you want to add a comment.
6. Go to the **Related Records** section.
7. Scroll to the **Vendor Comments** related list and click **Add**.
   Clicking **Add** opens the Vulnerability Vendor Comment form in a new tab. The parent context (vendor) is automatically populated in the corresponding field. Enter the required form details as explained in the previous steps.
8. Scroll to the **Vulnerability Vendor Comments** related list and click **Add**.
   The **Vendor** field is automatically populated with the current vendor record.
9. Select the **Vulnerability** to which the comment applies.
10. Enter the vendor **Comment**.
11. **Optional:** Modify the **Comment Date**.
    The field defaults to current date.
12. Click **Save**.

Result
The vendor comment is created and appears in the **Vulnerability Vendor Comments** related list of the vendor record.

Create Remediations

Create a remediation record to document a fix or workaround for a vulnerability affecting a specific product.

Before you begin
Role required: sn_sec_tisc.analyst

About this task
At least one vulnerability record and one product record must exist in the system before creating a remediation. Remediations are always created in the context of a vulnerability and product combination.

Procedure
1. Navigate to **All** > **Workspaces** > **Threat Intelligence Library** > **Vulnerability Artifacts** > **Remediations**.
2. Select **New**.
3. Fill in the fields appropriately.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Remediation

Field	Description
Remediation Id	A unique identifier for the remediation record.
Products	The product or products to which this remediation applies.
Vulnerability	The vulnerability that this remediation addresses.
Type	The category of remediation being documented. ○ **Mitigation**: a workaround or partial fix. ○ **Workaround**: a temporary measure. ○ **Vendor Fix**: an official fix from the vendor. ○ **First Fix**: the initial fix available for the vulnerability. ○ **None Available**: no remediation is currently available. ○ **No Fix Planned**: the vendor does not plan to fix the vulnerability.
Description	Description of the remediation, including what it addresses and how it should be applied.
Remediation Published Date	The date on which this remediation was officially published.
Restart category	Indicates what category of restart is required by this remediation to become effective. Select one of the following values, as required: ○ **Connected**: a connected dependency requires a restart. ○ **Dependencies**: dependent services or components must be restarted. ○ **Machine**: the entire machine requires a restart. ○ **Service**: a specific service must be restarted. ○ **System**: the full system requires a restart. ○ **None**: no restart is required.
Action Link	A URL pointing to the remediation resource, advisory, or vendor patch page. Enter a fully qualified URL (for example, `https://vendor.com/advisory/CVE-2024-1234`). Use this field to direct

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	users to external remediation guidance or download locations.
Prerequisites	Lists the conditions that must be met for the vulnerability remediation to apply to this product. Use this field to document preparatory actions such as backing up data, stopping services, or verifying system compatibility. All prerequisite values are entered manually.

4. Click **Save**.
5. To also add **Remediations**, navigate to **Threat Intel Library** > **Vulnerability Artifacts** and open any vulnerability record or product record to which you want to add a remediation.
6. Go to the **Related Records** section.
7. Scroll to the **Remediations** related list and click **Add**.
   Clicking **Add** opens the remediation form in a new tab. The parent context (vulnerability or product) is automatically populated in the corresponding field. Enter the required form details as explained in the previous steps.
8. Click **Save**.

Result

The remediation record is created and appears in the **Remediations** related list of the associated vulnerability and product records. The **Remediated Records Count** field on the vulnerability record is automatically incremented.

Access the Vulnerability Entities

The Vulnerability Intelligence Center (VIC) uses the following entities to store and organize vulnerability, product, and vendor intelligence data.

Product

The Product entity stores information about software and hardware products that may be affected by vulnerabilities from the table `sn_sec_tisc_intel_product`.

Label	Description
ID	Indicates the Product ID, which must be unique.
Name	Indicates the name of the product. The value should be the product's full canonical name, including version number.
Vendor	Indicates the corresponding vendor for the product. References the Vendor table (`sn_sec_tisc_vendor`). Vendors can be created in the Threat Intelligence Library.
Product Family	Indicates the product family that the product falls into.
Architecture	Specifies the architecture for which the product is intended, such as x86, ARM, or x64.
Host Name	Specifies the host name or system name where the product is installed or running.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Language	Specifies the language or locale of the product.
Patch Level	Indicates the patch level or update level of the product.
Service Pack	Indicates the service pack level applied to the product.
Specification	Provides additional specification details about the product.
Product Group	Indicates the parent product group this product belongs to. References the product table itself, as product groups are also stored in the product table.
Last Modified in Source	Timestamp indicating when the product information was last modified in the source system.
Created in Source	Timestamp indicating when the product was first created in the source system.
Replaced By Product	Reference to a product that replaces this product. Used when a product has been superseded or replaced by a newer version or alternative.
Product Version(s)	Specifies the version or versions of the product as comma-separated values. Indicates specific version numbers for product identification.
Product Version Range	Specifies a range of product versions affected. Used in vulnerability contexts to indicate version ranges using operators or specific version bounds.
Is Product Group	Boolean flag indicating whether this entry represents a product group rather than an individual product.
CPE	The Common Platform Enumeration (CPE) attribute that provides standardized product identification using CPE 2.3 or CPE 2.2 format.
Status	Indicates the current lifecycle status of the product. Valid values: • **Active**: Product is currently active and supported. • **Legacy (End of Product)**: Product has reached end-of-life but may still be in use. • **Deprecated By Vendor**: Product has been officially deprecated by the vendor and is no longer supported.

Remediation

The Remediation entity stores information about available fixes, mitigations, and workarounds for vulnerabilities from the table `sn_sec_tisc_vulnerability_remediation`.

Label	Description
Remediation Id	Auto-generated unique identifier for the remediation record. Used for internal tracking and reference purposes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Description	Contains a thorough human-readable discussion of the remediation, including detailed steps and guidance for addressing the vulnerability.
Prerequisites	Lists the conditions that must be met for the vulnerability remediation to apply. Contains any vendor-defined constraints or requirements for obtaining and applying the fix.
Action Link	Contains the URL where the remediation can be obtained.
Type	Specifies the category of the remediation. The following are the valid values for this type: • **Workaround**: A temporary solution that mitigates the vulnerability without fixing the root cause. • **Mitigation**: Actions that reduce the severity or impact of the vulnerability. • **Vendor fix**: An official patch or update provided by the vendor that resolves the vulnerability. • **First fixed**: The first version where the vulnerability has been fixed. • **None available**: No remediation is currently available. • **Will not fix**: The vendor has decided not to fix this vulnerability. • **No fix planned**: There are no plans to fix this vulnerability in the future.
Restart Category	Indicates whether a restart is necessary after remediation and, if so, this specifies the required type of restart. The following are the valid values for this category: • **Connected**: Restart of connected systems or services is required. • **Dependencies**: Restart of dependent components or services is required. • **Machine**: Full machine or system restart is required. • **Parent**: Restart of the parent process or service is required. • **Service**: Restart of the specific service is required. • **System**: System level restart is required. • **Vulnerable component**: Only the vulnerable component needs to be restarted. • **Zone**: Restart of the security zone or container is required.
Remediation Published Date	Contains the date from which the remediation is available.
Vulnerability	Reference to the vulnerability being remediated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Products	Specifies a list of products to give context to the remediation. Contains references to products affected by or related to this remediation.

Vendor

The Vendor entity stores information about organizations that develop or distribute products from the table `sn_sec_tisc_intel_vendor`.

Label	Description
Name	Indicates the name of the vendor.
Contact Details	Provides contact information for the vendor, such as email addresses and phone numbers.
Organization	Specifies organizational context for the vendor, such as department, division, or organizational unit.
Description	Provides a detailed description of the vendor's role, scope, and relevant background information.
Website URL	Contains the vendor's official website URL.

CWE Weakness

The CWE Weakness entity stores Common Weakness Enumeration records that describe categories of software weaknesses from the table `sn_sec_tisc_cwe_weakness`.

Label	Description
ID	Indicates the unique CWE identifier, such as CWE-79 or CWE-89, that standardizes the identification of software weaknesses.
Name	Indicates the name of the CWE weakness as defined in the CWE catalog.
Description	Provides a detailed description of the weakness, its characteristics, and potential security implications.
Type	Specifies the type classification of the CWE weakness. The following are the valid values for this type: • **Primary**: The initial, underlying weakness that directly enables a subsequent weakness to occur. • **Secondary**: The weakness that is triggered or made possible by the occurrence of the primary weakness.

Vulnerability Product Mapping

The Vulnerability Product Mapping entity defines the relationship between vulnerabilities and affected products from the table `sn_sec_tisc_m2m_vulnerability_product`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Vulnerability	Reference to the vulnerability record that affects the associated product.
Product	Reference to the product record that is affected by the associated vulnerability.
Status	Indicates the relationship status between the vulnerability and product. Valid values: • **Known affected**: Product version is confirmed to be affected by the vulnerability. • **Known not affected**: Product version is confirmed to not be affected by the vulnerability. • **First affected**: First version of the product affected by the vulnerability. • **First fixed**: First version where the vulnerability has been fixed. • **Fixed**: Product version has been fixed and is no longer vulnerable. • **Last affected**: Last version of the product affected by the vulnerability. • **Recommended**: Recommended version to use to avoid the vulnerability. • **Under investigation**: Product version is currently being investigated by the vendor; it is not yet known whether this version is affected.

Related Vulnerability CWE

The Related Vulnerability CWE entity maps vulnerabilities to their associated CWE weaknesses from the table `sn_sec_tisc_m2m_vulnerability_cwe`.

Label	Description
Vulnerability	Reference to the vulnerability record associated with the CWE weakness.
CWE	Reference to the CWE weakness record.

CWE Weakness Relationship

The CWE Weakness Relationship entity defines hierarchical and associative relationships between CWE weakness records from the table `sn_sec_tisc_m2m_cwe`.

Label	Description
Source CWE	Reference to the source CWE weakness record in the relationship.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Target CWE	Reference to the target CWE weakness record in the relationship.
Relationship Type	Specifies the type of relationship between the source and target CWE weaknesses. Valid values: • **Parent/Child**: Hierarchical relationship where one CWE is a parent or child of another. • **Peer**: Peer relationship where CWEs are at the same level or category. • **Requires/Can Precede**: One CWE requires or can precede another in an attack chain. • **Can Also Be**: One CWE can also be classified or manifested as another.

Attribute

The Attribute entity defines metadata attributes that can be assigned to vulnerabilities from the table `sn_sec_tisc_intel_attribute`.

Label	Description
Name	Indicates the name used to identify the attribute in the system.
Description	Provides a detailed description of the attribute's purpose, usage, and meaning.
Active	Boolean flag indicating whether the attribute is currently active and available for use.
Internal Identifier	Contains the internal system identifier for the attribute. Used for programmatic reference and integration purposes.
Attribute Type	Specifies the category or type of the attribute. The following are the valid values for this type: • **Score attribute**: Attribute related to scoring metrics. • **Threat attribute**: Attribute related to threat characteristics or properties. • **Other attribute**: General purpose attribute not fitting other categories. • **Score value**: Attribute representing a specific score or numerical value.

Vulnerability Attribute Value

The Vulnerability Attribute Value entity stores attribute values assigned to specific vulnerabilities from the table `sn_sec_tisc_m2m_vulnerability_attribute_value`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Vulnerability	Reference to the vulnerability record that has this attribute value assigned.
Attribute	Reference to the attribute definition being assigned to the vulnerability.
Qualitative Value	Contains the qualitative or text-based value for the attribute, such as "High" or "Critical". Used when the attribute value is descriptive rather than numeric.
Quantitative Value	Contains the quantitative or numeric value for the attribute, such as CVSS scores or probability values. Used when the attribute value is a number or decimal.

Vulnerability Identifier

The Vulnerability Identifier entity stores alternative or supplementary identifiers for vulnerabilities from the table `sn_sec_tisc_vulnerability_identifier`.

Label	Description
Vulnerability	Reference to the vulnerability record that this identifier represents.
Identifier	Contains the unique identifier value for the vulnerability. This can be a vendor-specific ID or standardized identifier such as GHSA-xxxx-xxxx-xxxx or OSV-xxxx-xxxx.
Identifier Assigned By	Indicates the organization or authority that assigned the identifier, such as MITRE, NVD, or GitHub.

Vulnerability Vendor Comment

The Vulnerability Vendor Comment entity stores vendor-provided statements and comments about specific vulnerabilities from the table `sn_sec_tisc_m2m_vulnerability_vendor_comment`.

Label	Description
Vulnerability	Reference to the vulnerability record that the vendor is commenting on.
Vendor	Reference to the vendor providing the comment.
Comment	Contains the vendor's comment or statement about the vulnerability, including vendor-specific clarifications or additional context.
Comment Date	Timestamp indicating when the vendor comment was published or last updated.

Product Identifier

The Product Identifier entity stores alternative identifiers associated with products from the table `sn_sec_tisc_intel_product_identifier`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Label	Description
Product	Reference to the product record that this identifier belongs to.
Identifier Type	Specifies the type of identifier used for product identification. The following are the valid values for this category: • **Hashes**: Cryptographic hash values for verifying product integrity, such as SHA-256 or MD5. • **Model Numbers**: Manufacturer's model numbers or part numbers. • **PURL**: Package URL, a standardized way to identify software packages. • **SBOM URLs**: URLs pointing to Software Bill of Materials documents. • **Serial Numbers**: Unique serial numbers assigned to product instances. • **SKUs**: Stock Keeping Units for product identification. • **Generic URIs**: Generic Uniform Resource Identifiers for product references.
Identifier	Contains the actual identifier value, such as a hash value, model number, PURL string, or serial number.
Additional Information	Provides supplementary information about the identifier, including additional context or notes that clarify or qualify it.

Related Product

The Related Product entity defines relationships between products from the table `sn_sec_tisc_m2m_product`.

Label	Description
Source Product	Reference to the source product in the relationship.
Target Product	Reference to the target product in the relationship.

Vulnerability Class

The vulnerability class options are configured in the `sn_sec_tisc_vulnerability_class` table, enabling you to define and manage vulnerability class selections on the **Vulnerabilities** page.

Field	Description
Name	Name of the vulnerability class.
Description	A brief description of the vulnerability class.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Fetch Vulnerability Data

Fetch vulnerability related data such as configuration items, vulnerable entries, and business context.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Vulnerability** object.
   The related vulnerabilities associated with this object are displayed.
4. Select the respective vulnerability record.
   If there any CVEs associated with it then you can fetch its vulnerable related data automatically using the button provided, and these associated records are displayed in the Business Context section of the Vulnerabilities.
5. Go to **Internal Intelligence** > **Vulnerable entries**.
   The associated CVEs records are displayed.
6. Select any CVE and click on **Fetch Vulnerability related data** button.

   Note:

   - This link will automatically associate the records and fetch that particular business context of records.
   - In case if there are no records associated then an information message is displayed that This specific vulnerability object doesn't have any vulnerable entries associated with it. You must manually associate the object(s) with the vulnerable entries to fetch the data.
   - This button will trigger a background scheduled job, and the job initiation and execution details are displayed in the **Activity Stream** section. For example, when the job is triggered the activity stream displays an activity that Started fetching associated data with the vulnerable entries. For more information on how the scheduled jobs are run to fetch the data, see Scheduled jobs.

7. Click **Link** to manually link the objects.
8. Select the records to be linked and fetch the vulnerability related data using the **Fetch Vulnerability related data** button.
   Once when you click this button, the background job will be triggered and the data will be automatically fetched to its respective section. A message displays that Job to fetch data associated with the vulnerable entries has started. You can track the status in the activity stream and refresh the list once the job is complete to check the results. For example, if the data is related to the configurations items then you check the results in the Configuration items section. For more information on adding CVEs, see Add CVEs to third-party entries.

   Note: Similarly, you can fetch the observables records data. For more information, see Fetch Vulnerability Data.

Define RSS Feeds

A threat intelligence feed is a real time, continuous data stream that gathers information related to cyber risks or threats. RSS Feeds provides an easy way to stay up to date with your favorite websites, such as blogs or latest cyber security news.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **RSS Feeds** object.

   Note: The ingested feeds can be browsed using this section but you cannot create new records.

4. On the form, following fields are auto-populated.

RSS Feeds Details view

Field	Description
Title	Title of the RSS Feed.
Description	A description that provides more details and context about the RSS feeds, potentially including its purpose and its key characteristics.
Link	Indicates the link added to the RSS feeds.
Source	Specifies the RSS feed source from which this object record is created.
Published Date	Indicates when the RSS feed is published.
Author	Indicates the author for the RSS feed.

5. Click **Save**.

Insights

Field	Description
Notes	Add any additional notes for this feed.

Additional Information

Field	Description
Media URL	Indicates the media URL.
Feedback Comments	Any additional feedback comments on the feedback.

Working with Reports in TISC

The Reports module in the Threat Intelligence Library section enables you to create, manage, and publish reports that use any intelligence available in the Threat Intelligence Library.

Reports in the threat intelligence library are categorized into case reports and intelligence reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

They support key capabilities such as previewing, publishing, sharing via email, and downloading. These reports provide analysts with a structured and shareable format for threat intelligence reporting.

Case Reports

Case Reports contain information specific to an individual case. Using the case designated templates, analysts can generate reports that automatically pull data from the fields, related records, and intelligence within the selected case.

Access to the Case Reports is strictly controlled. Only users or groups with permission to access the case can view or interact with its reports. Without the appropriate permissions, the report and its contents are not accessible.

Case Reports follow the same structure and capabilities as the existing CTI case reporting. For more information, see Report Templates. These case reports appear in **All Reports** and **Case Reports** views of the threat intelligence library **Reports** module providing a structured and secure result for case level investigations.

Intelligence Reports

Intelligence Reports provide a flexible way to generate structured reports using any available threat intelligence from the Threat Intelligence Library. Using templates of the **Intelligence Report** category, analysts can create reports that incorporate data from library lists and specific intelligence objects without depending on a case.

Unlike Case Reports, Intelligence Reports do not display case-specific fields or records. Instead, analysts can use record selection tools, slash commands, and table insertion options to customize the content of the report.

Slash commands in the threat intelligence report allow you to quickly insert dynamic content such as record counts, specific records, or system users into a report.

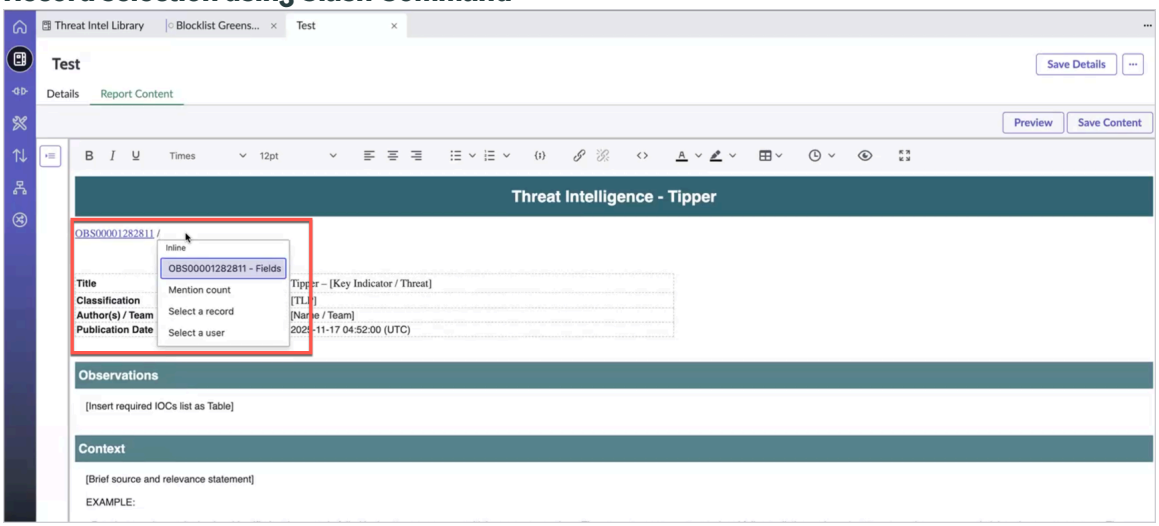
The following describes the usage of slash commands available within the Intelligence Report Editor.

Slash Command	Usage	Wokflow	Supported Tables
Mention Count	When you select this option, you can choose a table from the **Supported Tables** list to add the total record count to the report.	**1.** Select **Mention Count** from the slash command menu. **2.** Choose a table from the supported table list. **3.** The application inserts the total records count for the selected table into the report.	• Observable • Indicator • Attack Pattern • Campaign • Course of Action • Identity • Infrastructure • Intrusion Set • Location • Malware
Select a Record When you navigate to an observable	You can select a table from the provided **Supported Tables** list, and once selected,	**1.** Select **Mention Count** from the slash command menu.	• Malware Analysis • Marking Definition • Object Sighting

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Slash Command	Usage	Wokflow	Supported Tables
and type "/", an option to select a corresponding fields appears. This allows you to browse and search the available fields for that record. Selecting a field automatically inserts its value into your input. The following is the screen shot that illustrates the navigation of selecting a record(s) using slash command.	a drop down menu will display all the available records in that table, allowing you to choose the desired record.	**2.** Choose a table from the supported table list. **3.** The application inserts the total record count for the selected table into the report.	• Observed Data • Threat Actor • Threat Event • Threat Grouping • Threat Note • Threat Opinion • Threat Report • Tool • Vulnerability • Data Component • Data Source
Select a User	By selecting this option, you can choose any individual from the list of system users to include in the report.	**1.** Select **Select a User** from the slash command menu. **2.** Choose a user from the system user list. **3.** The selected user is inserted into the report.	NA

Record selection using Slash Command



Reports include pre-defined templates, tables offering a comprehensive view of relevant intelligence.

Intelligence Reports appear in the **All Reports** and **Intelligence Reports** views of the threat intelligence library **Reports** module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View All Reports

Use this section to view all the list of reports.

Before you begin
Role required: sn_sec_tisc_analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library**.
2. Select **Reports** > **All Reports**
   This page displays the list of reports.
3. Open any report.
4. Select **Download** to download the report.
5. Select **Share** to share the report in email format.
6. Enter the recipient and select **Send**.

> **Note:** You can also preview the report before sharing.

View Case Reports

View Case Reports.

Before you begin
Role required: sn_sec_tisc_analyst

About this task
Case Reports provide a structured way to document and present intelligence tied to a specific case. Using templates designated with a Case report context, analysts can generate reports that automatically draw from the fields, related records, and data within a selected case.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library**.
2. Select **Reports** > **Case Reports**
   This page displays the list of case reports.
3. Select any report.
4. Select **Download** to download the report.
5. Select **Share** to share the report in email format.
6. Enter the recipient and select **Send**.

> **Note:** You can also preview the report before sharing.

View Intelligence Reports

View intelligence reports.

Before you begin
Role required: sn_sec_tisc_analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library**.
2. Select **Reports** > **Intelligence Reports**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This page displays the list of intelligence reports.

3. Select any report.
4. Select **Download** to download the report.
5. Select **Share** to share the report in email format.
6. Enter the recipient and select **Send**.

Note: You can also preview the report before sharing.

View my reports

View the reports that you created.

Before you begin

Role required: sn_sec_tisc_analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library**.
2. Select **Reports** > **My Reports**
   This page displays the list of reports.
3. Select any report.
4. Select **Download** to download the report.
5. Select **Share** to share the report in email format.
6. Enter the recipient and select **Send**.

Note: You can also preview the report before sharing.

MITRE-ATT&CK™ Repository

The MITRE-ATT&CK repository is available under the Intelligence Library where the data from the MITRE sources are ingested.

The MITRE data that is coming to the repository is stored in a separate MITRE repository from Threat Intel Library data, where MITRE data isn't rolled up for aggregation or de-duplication flow and is independent.

The available data sources within the application are:

1. MITRE - Enterprise ATT&CK
2. MITRE - Mobile ATT&CK
3. MITRE - ICS ATT&CK

The data for these sources are stored in a separate MITRE repository under TI library in the base system. In case, if you want to create a new MITRE source then configure a custom source. For more information, see View Custom Feed and in the form view click **Advanced** check box and select the **Report Processor** as: **MITRECollectionDataProcessor**.

Manage Matrices

Manage the matrices that are imported from the MITRE TAXII collections. Matrices are a collection of tactics and techniques. You can view the matrices to review if your collections are available in the MITRE-ATT&CK repository.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. After you enable the MITRE ATT&CK related feed data sources which are available in the base system, click **Execute Now** to run the integrations and fetch the MITRE related information. For more information on enabling the integrations
2. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK**.
   The MITRE ATT&CK related records are displayed. By default all the records are in enabled state.

   Note: You can enable only those matrices that are relevant to your organization.

3. Select any Matrix record and click **Disable** if you want to disable any specific record.
4. Alternatively, you can create new matrices record by clicking **New** to manually to create the MITRE ATT&CK matrices.
5. Fill in the fields appropriately.

Create New MITRE Mitigation - Details

Field	Description
Name	Enter the name of the matrix.
Source	Specifies the threat source from which this record is created.
Active	Select this check box to active the matrix record.
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.
Insights	
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object type.
Comments	Add any comments that you might have in addition.

Manage Techniques

Manage the techniques that are imported from the MITRE TAXII collections. The techniques contain various ways attackers have developed to employ a given tactic. You can review and deactivate techniques that are not relevant to your organization. In STIX, techniques are known as attack patterns.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.analyst

Techniques represents how an adversary achieves a tactical goal by performing an action.

Procedure

1. After you enable the MITRE ATT&CK related feed data sources which are available in the base system, click **Execute Now** to run the integrations and fetch the MITRE related information. For more information on enabling the integrations
2. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Techniques**.
   The MITRE ATT&CK techniques records are displayed. By default all the records are in enabled state.
3. Select any technique record and click **Disable** if you want to disable any specific record.
4. Alternatively, you can create new techniques records by clicking **New** to manually create the MITRE ATT&CK techniques.
5. Fill in the fields appropriately.

Create New MITRE Mitigation - Details

Field	Description
ID	Unique ID for a technique.
Name	Enter the name of the technique.
Source	Specifies the threat source from which this record is created.
Platforms	Add the platforms required.
Permissions required	Add the required permissions.
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Priority	Indicates the priority level assigned to the MITRE Technique such as Low, Moderate, High, or Critical. **Note:** Priorities can be assigned to techniques to add relevance to your organization.
Description	A description that provides more details and context about the intrusion set, potentially including its purpose and its key characteristics.
Detection	The detection technique is used to identify adversary access to or unauthorized activity on computer networks.
Insights	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object type.
Comments	Add any comments that you might have in addition.
TISC Tags	
Select TISC Tags	Select tags to annotate or earmark records ingested into the system from this source. **Note:** Tags can be assigned to techniques to add relevance to your organization.

Manage Mitigations

Manage the mitigations that are imported from the MITRE TAXII collections. Mitigations enable you to prevent an adversary from successfully executing techniques or sub-techniques against your organization. In STIX, mitigations are known as course of actions.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. After you enable the MITRE ATT&CK related feed data sources which are available in the base system, click **Execute Now** to run the integrations and fetch the MITRE related information. For more information on enabling the integrations.
2. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Mitigations**.
   Click a mitigation to view all the associated information.
3. Click **New** to manually create the MITRE ATT&CK mitigations.
4. Fill in the fields appropriately.

Create New MITRE tools - Details

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.
Name	Enter a descriptive name to identify the object.
Source	Specifies the threat source from which this object record is created.
Aliases	A list of other names to identify this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Description	A description that provides more details and context about the object, potentially including its purpose and its key characteristics.
Contributors	Specifies the contributors.
Insights	
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object.
Comments	Add any comments for this object.

5. Click **Save**.

Manage Groups

Manage the groups that are imported from the MITRE TAXII collections. Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. In STIX, groups are known as intrusion sets.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Groups**.
   You can view the listed groups.
2. Click **New** to manually create the MITRE ATT&CK groups.
3. Fill in the fields appropriately.

Create New MITRE groups - Details

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.
Name	Enter a descriptive name to identify the object.
Source	Specifies the threat source from which this object record is created.
Aliases	A list of other names to identify this object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Description	A description that provides more details and context about the object, potentially including its purpose and its key characteristics.
Insights	
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object.
Comments	Add any comments for this object.

4. Click **Save**.
5. To view how these objects are related, click **Relationships**.

Manage Malware

Manage the malware information that you imported from the MITRE TAXII collections. It is a type of TTP that represents malicious code.

Before you begin

It refers to a program that is covertly inserted into a system. The intent of a malware is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS).

Role required: sn_sec_tisc.analyst

Procedure

1. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Groups**.
   You can view the listed malware.
2. Click a malware to view all the associated information.
3. Click **New** to manually create the MITRE ATT&CK malware.
4. Fill in the fields appropriately.

Create New MITRE Malware - Details

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.
Name	Enter a descriptive name to identify the object.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source	Specifies the threat source from which this object record is created.
Aliases	A list of other names to identify this object.
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Description	A description that provides more details and context about the object, potentially including its purpose and its key characteristics.
Contributors	Specifies the contributors.
Insights	
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object.
Comments	Add any comments for this object.

5. Click **Save**.
6. To view how these objects are related, click **Relationships**.

Manage Tools

Manage the tools information that you imported from the MITRE TAXII collections. Tools are legitimate software that are used by threat actors to perform attacks.

Before you begin

Role required: sn_sec_tisc.analyst

About this task

Tools enable you to know how and when threat actors use them for executing campaigns. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, administrators, network administrators, or even normal users.

Procedure

1. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Tools**.
   You can view the listed tools.
2. Click a tool to view all the associated information.
3. Click **New** to manually create the MITRE ATT&CK tools.
4. Fill in the fields appropriately.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create New MITRE tools - Details

Field	Description
ID	Unique ID for a course of action to prevent an attack.
Revoked	Indicates that the revoked objects are no longer considered valid by the object creator.
Name	Enter a descriptive name to identify the object.
Source	Specifies the threat source from which this object record is created.
Aliases	A list of other names to identify this object.
Created Time In Source	Specifies the time the object is created in the source.
Modified Time In Source	Specifies the time the object is modified in the source.
Description	A description that provides more details and context about the object, potentially including its purpose and its key characteristics.
Contributors	Specifies the contributors.
Insights	
Notes	Any additional information related to the mitigation.
Additional Information	
Additional Context	Add any additional context for this object.
Comments	Add any comments for this object.

5. Click **Save**.
6. To view how these objects are related, click **Relationships**.

Manage MITRE Relationships

Manage the MITRE relationships information that you imported from the MITRE TAXII collections.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. To view the MITRE ATT&CK Repository data, navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **MITRE ATT&CK** > **Relationships**.
   You can view the listed relationships.
2. Click any source object to view all the associated information.
3. Click **New** to manually create the MITRE ATT&CK relationships.
4. Fill in the fields appropriately.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create New MITRE tools - Details

Field	Description
Source MITRE Object	Add the source MITRE object.
Target MITRE Object	Add the target MITRE object.
Source MITRE Type	Enter the source MITRE type.
Target MITRE Type	Enter the target MITRE type.
Relationship Type	Define relationships between objects. A description that provides more details and context about the relationship type. The available options are: Define the relationship direction whether it is direct or inverse. ○ Inverse - This is the type of relationship between the observable and object. ○ Direct - This is the type of relationship between the object and observable.
Source	Select and define the source object.
Relationship ID	Define the relationship ID.

5. Click **Save**.
6. To view how these objects are related, click **Relationships**.

Relationships Objects

Use the relationships objects to link together two observables or an observable and SDO to explain how they relate to each other.

STIX Relationship Objects (SROs) represent types of relationships between various STIX objects. The following relationship objects are available:

- **Observable-Observable Relationship**: This object defines relationships between observables.
- **Object-Object Relationship**: This object defines relationships between SDOs, except the indicator object. An example of an object-object defined relationship is that an attack pattern delivers a malware.
- **Object-Observable Relationship**: This object defines relationships between SDOs and the observable object (SCO). An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.
- **Object-indicator Relationship**: This object defines relationships between SDOs and the indicator object.
- **Indicator-Indicator Relationships**: This object defines relationships between indicator objects.
- **Indicator-Observable Relationship**: This object defines relationships between the indicator object and other SDOs. An example of an object-indicator defined relationship is that an indicator detects evidence of a campaign.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Object Relationships

Relationship Object	Example Source	Example Target	Example Description
Observable-Observable Relationships	IP address, domain name		This relationship describes between the observables.
Object-Object Relationships	Attack-pattern	Malware	This relationship describes that this Attack Pattern is used to deliver this malware instance (or family).
Object-Observable Relationships			This relationship describes between the objects and observables.
Object-Indicator Relationships	Indicator	Attack-Pattern, Campaign, Infrastructure, Intrusion-set, Malware, Threat-actor, Tool	This relationship describes that the indicator can detect evidence of the related attack pattern, campaign, infrastructure, intrusion set, malware, threat actor, or tool. The evidence may not be direct. For example, the indicator may detect secondary evidence of the campaign such as malware that is commonly used by that particular campaign.
Indicator -Indicator Relationships	Infrastructure	Observed data	This relationship describes that the indicator is created based on information from an observed data object. An example of an object-observable defined relationship is that an infrastructure consists of cyber observable objects which provides information of a potential attack.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Object Relationships (continued)

Relationship Object	Example Source	Example Target	Example Description
Indicator-Observable			This relationship describes between the indicators and observables.

Define observable-observable relationships

Define relationships between observables.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Observable-Observable**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

Field	Description
Source Observable	Select and define the source object.
Target Observable	Select and define the target object.
Relationship Type	A description that provides more details and context about the relationship type. The avail able options are: Define the relationship direction whether it is direct or inverse. ○ Inverse - This is the type of relationship be tween the observable and object. ○ Direct - This is the type of relationship be tween the object and observable.
Basis For Correlation	Name of the correlation rule based on which the system has identified as the related records of that observable. This rule is auto populated.

6. Click **Submit**.

Define object-object relationships

Define relationships between SDOs, except the indicator object.

Before you begin

Role required: sn_sec_tisc.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Object-Object**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

Field	Description
Source Object	Select and define the source object.
Source Object Type	Defines the type of source object.
Target Object	Select and define the target object.
Target Object Type	Defines the type of target object.
Relationship Type	A description that provides more details and context about the relationship type. Define the relationship direction whether it is direct or inverse. ○ Inverse - This is the type of relationship be tween the observable and object. ○ Direct - This is the type of relationship be tween the object and observable.
Start Time	Specifies the time when the relationship is created.
Stop Time	Specifies the time when the relationship is stopped or removed.
Description	A brief description about the object relation ships.

6. Click **Submit**.

Define object-observable relationships

Define relationships between SDOs and the observable object (SCO).

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Object-Observable**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Observable	Select and define the observable.
Object	Select and define the object.
Relationship Type	A description that provides more details and context about the relationship type. Define the relationship direction whether it is direct or inverse. ○ Inverse - This is the type of relationship be tween the observable and object. ○ Direct - This is the type of relationship be tween the object and observable.
Start Time	Specifies the time when the relationship is created.
Stop Time	Specifies the time when the relationship is stopped or removed.
Description	A brief description about the object relation ships.

6. Click **Submit**.

Define object-indicator relationships

Define relationships between the indicator object and other SDOs.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Object-Indicator**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

Field	Description
Indicator	Select and define the indicator.
Object	Select and define the object.
Relationship Type	A description that provides more details and context about the relationship type. Define the relationship direction whether it is direct or inverse.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ Inverse - This is the type of relationship be tween the observable and object. ○ Direct - This is the type of relationship be tween the object and observable.
Start Time	Specifies the time when the relationship is created.
Stop Time	Specifies the time when the relationship is stopped or removed.
Description	A brief description about the object relation ships.

6. Click **Submit**.

Define indicator-indicator relationships

Define relationships between the indicator object and other Use the relationships objects to link together two observables or an observable and SDO to explain how they relate to each other..

Before you begin
Role required: sn_sec_tisc.analyst

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Indicator-Indicator**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

Field	Description
Description	Specifies the threat source from which this record is created.
Domain	Defines the scope of the object record. The value in this field is auto populated.
Target Indicator	Select and define the target indicator object.
Relationship Type	A description that provides more details and context about the relationship type. Define the relationship direction whether it is direct or inverse. ○ Inverse - This is the type of relationship be tween the observable and object. ○ Direct - This is the type of relationship be tween the object and observable.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Source Indicator	Select and define the source object indicator.

6. Click **Submit**.

Define indicator-observable relationships

Define relationships between the indicator object and other SDOs.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Relationships** > **Indicator-Observable**.
4. Click **New**.
5. Complete the fields in the form as appropriate.

Field	Description
Observable	Select and define the observable.
Indicator	Select and define the indicator object.

6. Click **Submit**.

Potential Relationships

The application uses automated correlation to establish potentially possible relationships between two SDOs, two Observables or an observable and SDO.

1. Select one or more potentially related records and apply this action on the UI, which will further change the records to the confirmed relationships and visible in Related records section.
2. Any confirmed correlations ingested or manually created by an analyst will override the potential relationships created by auto correlation.

Confirm observable-observable potential relationship

Use this section to confirm the relationships between the observables.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Potential Relationships** > **Observable-Observable**.
4. Select the observable(s) record.
5. Click **Confirm Relation**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A Potential relationship record is ideally created which is identified based on its correlation rules. Once you confirm the relationship, then the observables record will move to the Relationships section which means that the relation between the observables to observables is confirmed. The record shows a confirmed relation only when the correlation rules are matched. For example, a potential relationship can be created when two observables of type URLs has same domain name.

Alternatively, you can also create new observables record by linking the observables from the list of observables and confirm the relationships from the related records tab of each observable.

a. Open any Observable record.

b. Go to **Related Records** tab.

c. Click the **Link** button.

d. Select one or more observable(s).

e. Click **Link**.
This will create a new relationship between the selected observable record and the newly linked observables.

6. Click **Delete** to delete the relationships.

Confirm object-object potential relationships

Define the potential relationships between the objects.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Potential Relationships** > **Object-Object**.
4. Select the observable record.
5. Click **Confirm Relation**.
A Potential relationship record is ideally created which is identified based on its correlation rules. Once you confirm the relationship from this section, then the observables record will move to the Relationships section which means that the relation between the observables to observables is confirmed. The record shows a confirmed relation only when the correlation rules are matched. For example, a potential relationship can be created when two observables of type URLs has the same domain name.

   Alternatively, you can also create new observables record by linking the observables from the list of observables and confirm the relationships from the related records tab of each observable.

   a. Open any Observable record.

   b. Go to **Related Records** tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Click the **Link** button.

d. Select one or more observable(s).

e. Click **Link**.
This will create a new relationship between the selected observable record and the newly linked observables.

6. Click **Delete** to delete the relationships.

Confirm indicator-indicator potential relationships

Define the potential relationships between the objects.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Potential Relationships** > **indicator-indicator**.
4. Select the observable record.
5. Click **Confirm Relation**.
A Potential relationship record is ideally confirmed based on automated correlation rules. Once you confirm the relationship, then the observables record will move to the Relationships section which means that the relation between the observables to observables is confirmed.

   The record shows a confirmed relation only when the correlation rules are matched. For example, a potential relationship is confirmed when two observables of type URLs has the same domain name.

   Alternatively, you can also create new observables record by linking the observables from the list of observables and confirm the relationships from the related records tab of each observable.

   a. Open any Observable record.

   b. Go to **Related Records** tab.

   c. Click the **Link** button.

   d. Select one or more observable(s).

   e. Click **Link**.
   This will create a new relationship between the selected observable record and the newly linked observables.

6. Click **Delete** to delete the relationships.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability relationship mapping

Use many-to-many (M2M) relationship records to map connections between vulnerabilities and other entities.

- **Vulnerability Products**: maps vulnerabilities to products with a status field indicating the relationship (for example, **Known Affected**, **Fixed**, **Under Investigation**).
- **Vulnerability CWEs**: maps vulnerabilities to CWEs. No status field is required for this relationship.

Bulk delete operations are available for all M2M relationship records from the related list view.

Access Vulnerability Downstream actions

Access all downstream actions generated from a vulnerability record to track remediation progress and understand the scope of response activities.

Create Vulnerability Assessment from a Vulnerability

Use this feature to conduct a vulnerability assessment for a specific vulnerability.

Before you begin

Role required: sn_sec_tisc.analyst

About this task

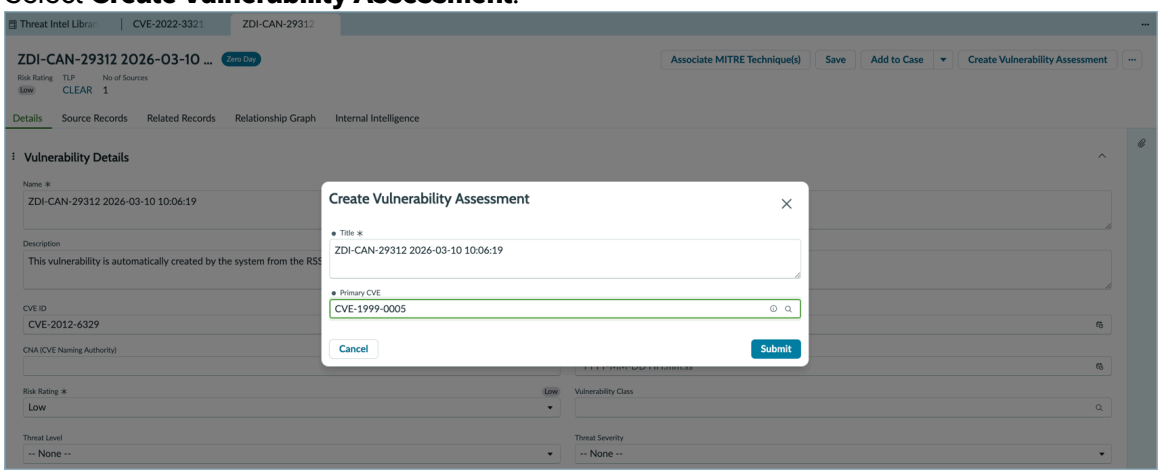
Before you begin, ensure the following:

- The Vulnerability Exposure Assessment application is installed.
- The required role `sn_vul_analyst.emergency_response` is assigned.

> **Note:** This role isn't assigned by default. System administrators must explicitly grant access.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select the **Threat Intel Library** icon on the workspace.
3. Go to **Vulnerability Artifacts** > **All Vulnerabilities**.
4. Open a vulnerability record.
5. Select **Create Vulnerability Assessment**.



6. Fill in the required details such as **Title** and **Primary CVE**.
7. Select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A confirmation message appears indicating that Vulnerability assessment {********} created successfully.

Note:

- When you click the link from the confirmation message, the Vulnerability assessment record opens in read-only mode. The record includes a reference to the originating vulnerability, and relevant fields are automatically populated to maintain consistency.
- A corresponding work note is also added to the vulnerability record. To view it, navigate to the **Details** section and view the **Activity** stream.

Result

Verify your assessments

1. Navigate to the **Internal Intelligence** section on the Vulnerability record.
2. View all associated vulnerability assessments under the **Vulnerability Response** section.



3. Link or unlink existing assessments as needed.

Create Security Incident from a Vulnerability Record

Create a security incident to track and manage remediation efforts for identified vulnerabilities. This process helps prioritize security responses and maintain audit trails.

Before you begin

Role required:

- sn_sec_tisc.analyst
- sn_si.analyst

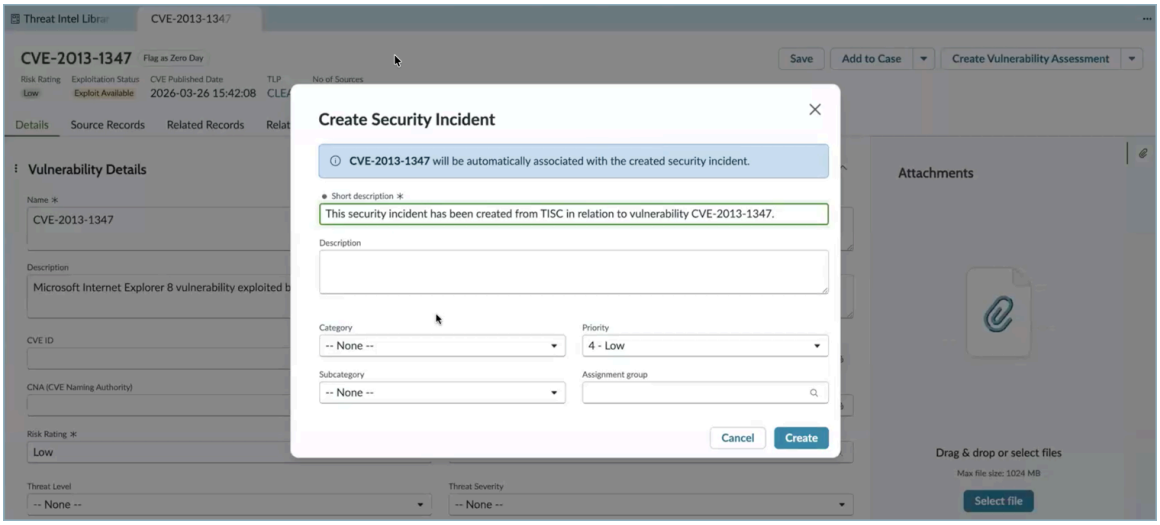
About this task

Before you begin, ensure that Security Incident Response (SIR) application is installed.

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Select the **Threat Intel Library** icon on the workspace.
3. Go to **Vulnerability Artifacts** > **All Vulnerabilities**.
4. Open a vulnerability record.
5. Select **Create Security Incident**.
6. On the form, **Short description** is automatically populated (required) and optionally update category, priority, assignment group, and description as necessary.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Select **Submit**.
   A confirmation message appears indicating that Security incident {********} created successfully, and a link to the Security Incident record is provided.

Note:

- When you click the link from the confirmation message, the Security Incident opens in read-only mode. The record includes a reference to the originating vulnerability, and relevant fields are automatically populated to maintain consistency.
- A corresponding work note is also added to the vulnerability record. To access it, go to the **Details** section of the vulnerability record.
- Additionally, the system records a work note on the activity stream of the Security Incident Response Workspace indicating that the incident record is originated from a TISC vulnerability and providing a link to the related vulnerability record.

The **TISC Context** feature in the Security Incident Response Workspace provides analysts direct access to threat intelligence linked to vulnerabilities associated with incidents. For more information, see Working with TISC Context.

This capability allows analysts to view and investigate related threat objects without leaving the Security Incident Response Workspace, streamlining analysis and enhancing incident response efficiency.

Related topics

TISC integration within SIR Workspace

Deleting threat intelligence library records

Delete threat intelligence library records such as observables, indicators, and objects.

Before you begin

Role required: sn_sec_tisc.analyst

The following example procedure explains how to delete an observable record. You can use the same procedure to delete indicators or objects as well.

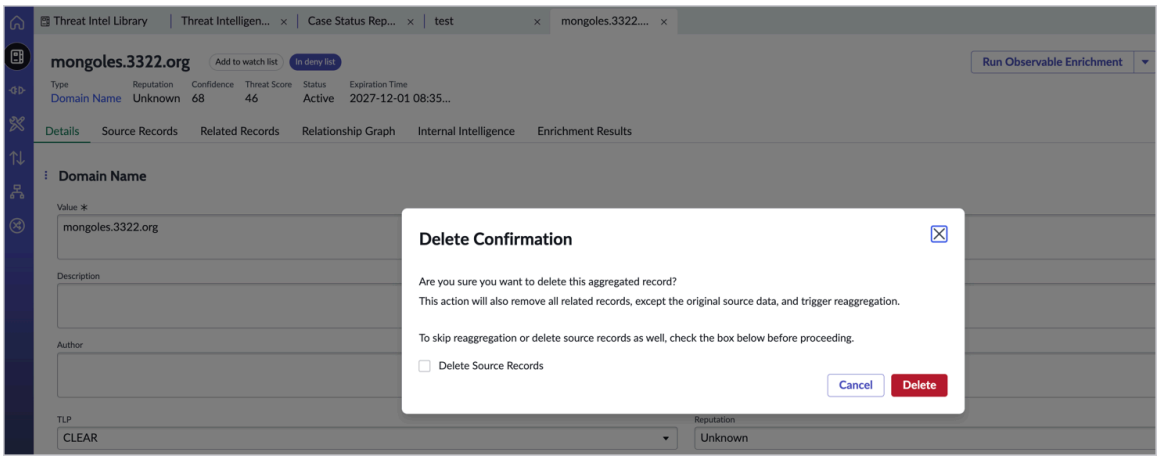
Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Open any observable record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Delete** to delete the aggregated record.
   When you select this action, then it will remove all the related records, except the original source data, and trigger reaggregation.

   A confirmation message will appear to verify that you want to delete the aggregated record. If you also want to delete the source records and prevent re aggregation, select the **Delete Source Records** check box. This action will remove all the associated source records.



4. Select **Delete**.
   The record will be deleted from threat intelligence library.

What to do next
Refer to the section Define an Observable to create a record.

Export intelligence data

Use the export feature to manually export the intelligence data in various formats.

Before you begin
Role required: sn_sec_tisc.analyst

About this task
Currently, the export functionality is limited to observables, indicators, and case management. The following procedure describes how you can export the observables data, and follow the same procedure to export the indicators data.

Procedure
1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Threat Intel Library** > **Observables** > **All Observables**.
2. Select any observable(s).
3. Click **Export** button.

   Note: The **Export** button is enabled only when observables are selected for export. If no observables are selected, the button remains disabled.

4. Select the desired file type for export.
   Currently, the supported export formats are Excel, CSV, and STIX 2.1 JSON. Suppose, if your export type is Excel then the number of records that can be exported at a time is limited to 10,000, regardless of the selected format type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the selection exceeds 10,000 records, then an error message is displayed indicating that the maximum limit for the selected format type has been surpassed, and only the first 10000 records will be exported.

If the export format is CSV and the record limit is exceeded, an alert message will be displayed indicating that the export is **in progress** state, along with a link to view the export status. You can click the link to view the status, refresh the record, and once it moves to **processed** state after refreshing then you can download the attachment.

5. Click **Export**.

Note: You can also view export data from the **Imports/Exports** module.

A confirmation message displayed indicating that the export is successful and your download is complete.

Confirm Potential Relationships from Related Records

Confirm the relationships between the two SDOs.

Before you begin

Role required: sn_sec_tisc.analyst

Procedure

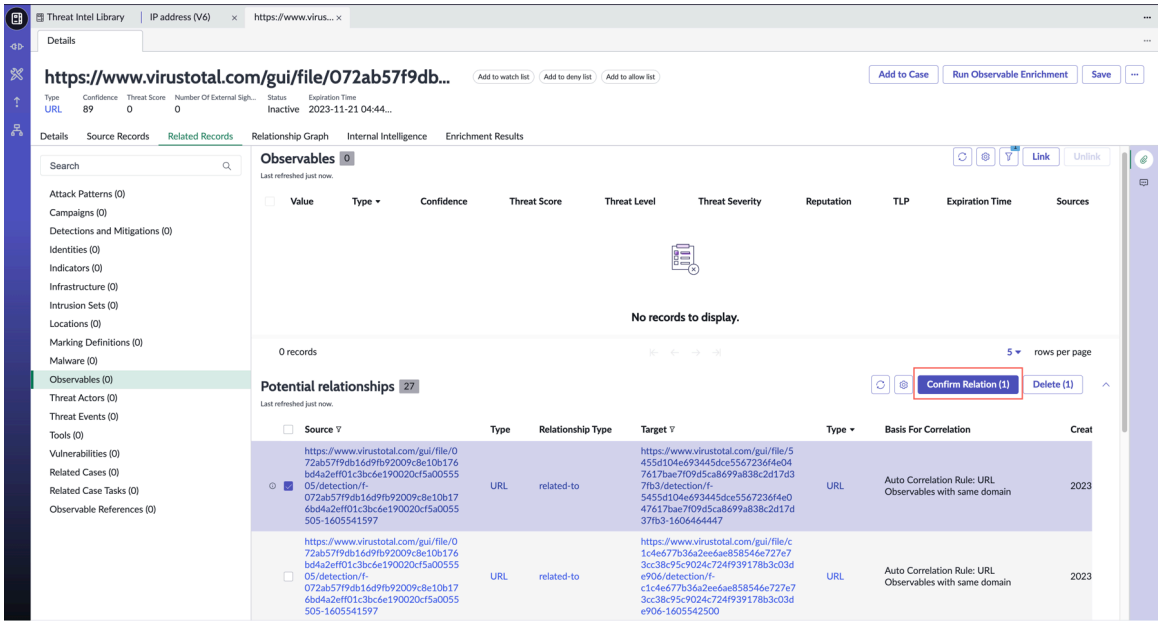
1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Threat Intel Library** icon on the workspace.
3. Go to **Related Records** section.
4. Expand **Potential Relationships**.
5. Open any record such observables, indicators, or any other objects that you wish to confirm the relationships between two SDOs.
6. For example, here select **Observables** from the left navigation.
7. Select the **Observable(s)** records from the list.

Note: The list section shows all the linked observable records of the associated observable.

8. Click **Confirm Relationships** button to confirm the relationships between the objects.

Note: For more information, seeRelationships Objects and Potential Relationships.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Click **Delete** to delete the associated observables.
   For information on how the potential relationships and relationships are established between the SDOs, see Potential Relationships and Relationships Objects.

Automated Correlation

Automated correlation helps you identify the relationships between observables, indicators, and objects.

With the correlation process, the application automatically establishes the correlation between threat intelligence records based on the predefined rules. Based on the type of the rule that is applied, the relationship can be a confirmed relationship or potential relationship. If the relationships between the objects are confirmed, those objects are automatically displayed on the details view of that object under the **Related Records** section.

The following describes the relationships and potential relationships:

- **Relationships**: Use the relationships objects to link together two observables or an observable and SDO to explain how they relate to each other.
- **Potential Relationships**: Use the potential relationships to establish potentially possible relationships between two SDOs, two Observables or an observable and SDO by using the automated correlation.

  Correlation rules for potential relationships identify potential relationships between threat intelligence entities, indicators, and observables.

  Note: The four correlation rules that generate potential relationships are disabled by default (for details, refer the following Correlation rules table). Enabling these rules can result in the creation of large number of potential relationships, depending on the volume of ingested data. Users can enable the rules based on their requirement.

The following are the predefined correlation rules provisioned within the base system:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Correlation rules

Name	Description	Definition	Action	Status
Observables with same file hash	The rule compares the observables' hash values of the same type and identifies if they share the same hash.	The rule compares the hash values of the same type of the indicators and identifies if they share the same hash.	Creates a Relationship	Enabled
URL Observables with same domain	The rule examines the commonalities in the structure of URLs to identify if they share the same base domain.	The rule examines the commonalities in the structure of URLs. Identifies if they share the same base domain and have a similar sub directory structure.	Creates a Potential Relationship	Disabled
Observable found as sources in network object	The rule matches the Network source attribute value with IPV4, IPV6, or domain-name observables in the system and links as the Source of traffic.	The rule matches the Source attribute value with IPV4, IPV6 or domain-name observables in the system and links as Source of traffic.	Creates a Relationship	Enabled
Observable found as destination in network object	The rule matches the Network destination attribute value with IPV4, IPV6, or domain-name observables in the system and links as the destination of the traffic.	The rule matches the destination attribute value with IPV4, IPV6 or domain-name observables in the system and links as destination of traffic.	Creates a Relationship	Enabled
Relate observables based on communication	Based on network objects, the rule identifies all the observables (IPV4, IPV6, and domain name) that have communicated with the same	Based on network objects, the rule identifies all the indicators that have communicated with the same destination (IPV4, IPV6, mac-addr or domain-name)	Creates a Relationship	Enabled

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Correlation rules (continued)

Name	Description	Definition	Action	Status
	destination (IPV4, IPV6, or domain name) and establishes a relationship between these observables. Also, related observables (IPV4, IPV6, and domain name) if they are related to the same network object as the source communicating with the destination.	and establishes a relationship between these indicators as connected to the same C2 infrastructure.		
Related Root domain observables to sub domains	The rule ties together a root domain with sub-domains and vice versa for domain type of observables.	The rule ties together a root domain with sub-domains.	Creates a Relationship	Enabled
Related domains to IPs based on DNS resolutions	Using domain-ipv4 or domain-ipv6 attributes of domain observables, the rule establishes relationships between the domains and IPs.	Using the attributes domain-ipv4 or domain-ipv6, the rule identifies all the domains or sub-domains that resolve to the same IP address and establishes relationships between the indicators, indicating their connection to the same C2 infrastructure.	Creates a Relationship	Enabled
Matching domains with SSL Certificates	The rule analyzes the SSL certificate information associated with the domain observables and establishes a	The rule analyzes the SSL certificate information associated with the indicators and identifies that both	Creates a Relationship	Enabled

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Correlation rules (continued)

Name	Description	Definition	Action	Status
	relation between them.	certificates are issued by the same certificate authority and share the same expiration date and establishes relationships between the indicators, indicating their connection to the same C2 infrastructure or threat campaign.		
Relate entities based on common observables	The rule compares if the same observable is related to two different entities and relates them to each other.	The rule compares if the same observable is related to two different entities and identifies them as related to each other.	Creates a Potential Relationship	Disabled
Relate indicators based on common observables	The rule compares if the same observable is related to two different indicators and relates them to each other.	The rule compares if the same observable is related to two different indicators and identifies them as related to each other.	Creates a Potential Relationship	Disabled
Relate indicators with objects based on common observables	The rule compares if the same observable is related to indicators, and objects and relates them to each other.	The rule compares if the same observable is related to indicators and objects and identifies them as related to each other.	Creates a Potential Relationship	Disabled

Working with Data Exports

Threat Intelligence Security Center supports manual export of observables, indicators, and cases in the recommended formats.

This functionality enables you to easily extract the data for further analysis. The key features are:

- Export observables, indicators, and cases individually or in bulk.
- Output in recommended formats such as CSV, STIX 2.1 for seamless integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Data exports functionality is currently supported only for observables, indicators, and case management. Within the case management, exports are limited to the Observable and Indicator lists under case artifacts.

View all exports

Use this section to view all the manually exported records.

Before you begin
Role required: sn_sec_tisc.export

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Imports/Exports**.
2. Select **Exports** > **All Exports**
   This page displays the export records.
3. Open any record to view the status of the export process.

View my exports

View and download the exports you are authorized to access.

Before you begin
Role required: sn_sec_tisc.export

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center** > **Imports/Exports**.
2. Select **Exports** > **My Exports**
   This page displays the export records.
3. Open any record to view the status of the export process.

Export intelligence system properties

This section describes the record limitations and its properties while exporting data.

Note: TISC provides the following limit for data exports. To set the following properties, navigate to **System Properties** > **Import Export**.

Role required: sn_sec_tisc.export

Format	Property	Description
STIX 2.1 JSON	sn_sec_tisc.stix_export_limit	Maximum number of rows that can be exported to a STIX 2.1 file. The default e is 10000.
STIX 2.1 JSON	sn_sec_tisc.stix_export_payload_streaming_threshold_min_objects_size	If the count of objects in "Objects" array of STIX export payload is greater than the number specified in this property then JSONStreamingAPI will be used for creating attachment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Format	Property	Description
		The default export limit is 4000.
STIX 2.1 JSON	sn_sec_tisc.stix_json_from_json_streaming_api_action_limit	This entity specifies that will be used when triggering flow designer action for generating STIX JSON attachment using JSON streaming API. The default export limit is 900.

Note: For better understanding of export limit on the other format types, see Export limits.

Data migration in TISC

Data migration is a process when you move all your data from a classic UI to TISC.

The purpose of this migration is to allow users to migrate the data from existing threat intelligence data to TISC. To execute this process, a new framework is introduced within TISC which is explained in the further section.

Data migration from SIR TI to TISC

Data Migration Job Configuration in TISC enables you to move the existing Threat intelligence plugin data to TISC plugin data directly.

Before you begin

Role required: sn_sec_tisc.admin

About this task

- **Selective Record Migration**: Only records from the selected table that meet specified conditions are migrated.
- **Include Relationships**: Related records are migrated only if the **Include Relationships** check box is selected.
- **Entity Migration Status**: Once an entity (observable or object) is migrated, it won't be included in further migrations unless it is being migrated as a related record.
- **Case Records**: Only active records are migrated by default, unless the **Include Closed Cases** check box is selected.

Procedure

1. Navigate to **All** > **Threat Intelligence Security Center** > **Data Migration Job Configuration**.
2. Click **New**.
3. On the form, fill the fields as appropriate.

Data Migration Job Configuration

Field	Description
Name	Name of the data migration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Table	Select the table from which the records should be migrated to TISC. The TISC table options for migration are: ○ Observable(sn_ti_observable) ○ Indicator of Compromise(sn_ti_indicator) ○ Security Case(sn_ti_case) ○ STIX V2 objects (sn_ti_stix2_object) (options such as attack patterns, campaigns, course of action) **Note:** ○ When you select the STIX V2 option then all the STIX objects are migrated except the MITRE ATT&CK as TISC has a different framework to migrate the MITRE ATT&CK. ○ When you select to migrate security case then the closed cases won't be migrated but only the active cases are migrated. For example, select **Observable** migration table.
Active	Select this check box if the data migration process is active.
Include Relationships	Select the check box to migrate the relationships of threat intelligence records to TISC records. **Note:** When you select this check box all the related entities are migrated along with the observable and If the check box is not selected, only the single observable will be migrated, without any related entities.
Include Closed Cases	Select this check box if you want to include the closed cases as part of case records migration.
Only Migrate Observables Associated to Security Incident	Select the check box for migrating the observables that are associated with the security incidents and if the check box is not selected, all the observables will be migrated, regardless of their association with security incidents.
Conditions	Option to select the conditions that can be used to filter data being migrated.
Additional Configurations	

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Confidence	Enter the confidence for the migrated TISC entities (observables or objects or indicators). The confidence should be between 0-100 range.
Expiry period (days)	The expiry period for the migrated TISC entities.

Note: The system ignores or skips the records that are already migrated to TISC when fetched again.

4. Click **Submit**.
5. Click **Execute Now** to execute the data migration.
   When you execute the data migration then a background job is run and the migration job gets created. This job creates a migration process and the batch size of these migration records is 5000.
6. Verify the migration job status under the **Migration Job Runs** section.
   The job status will be queued and the maximum limit of the batch size should not be exceeding 5000 records. Click on the record to view the objects that are all migrated for that specific entity.
7. Verify the migration job status under the **Migration Job Runs** related list.
8. Click on the record to view the processing status.
9. Verify the batch migration status under the **Migration Processing Queue** records related list section in the migration job run record.
   The batch size for migration of records is 5000.
10. Verify the TISC entities created as part of batch migration under respective related lists in **Migration Processing Queue** record.

TISC Data Processing Functional Flow

Threat Intelligence Security Center (TISC) provides a solution that automates the data collection and processing which helps reduce the burden on Threat Intel Analysts by avoiding manual steps involved.

Threat Intelligence Security Center (TISC) collects intelligence using one of the following methods:

1. Ingestion from data sources that are preconfigured and run on a schedule.
2. Threat Intel Analysts importing data using the Import Intelligence feature.
3. Manually creating individual records within the application.

Note: The data collected in the application will be processed to normalize, de-duplicate, and aggregate the information before loading into Threat Intel library.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

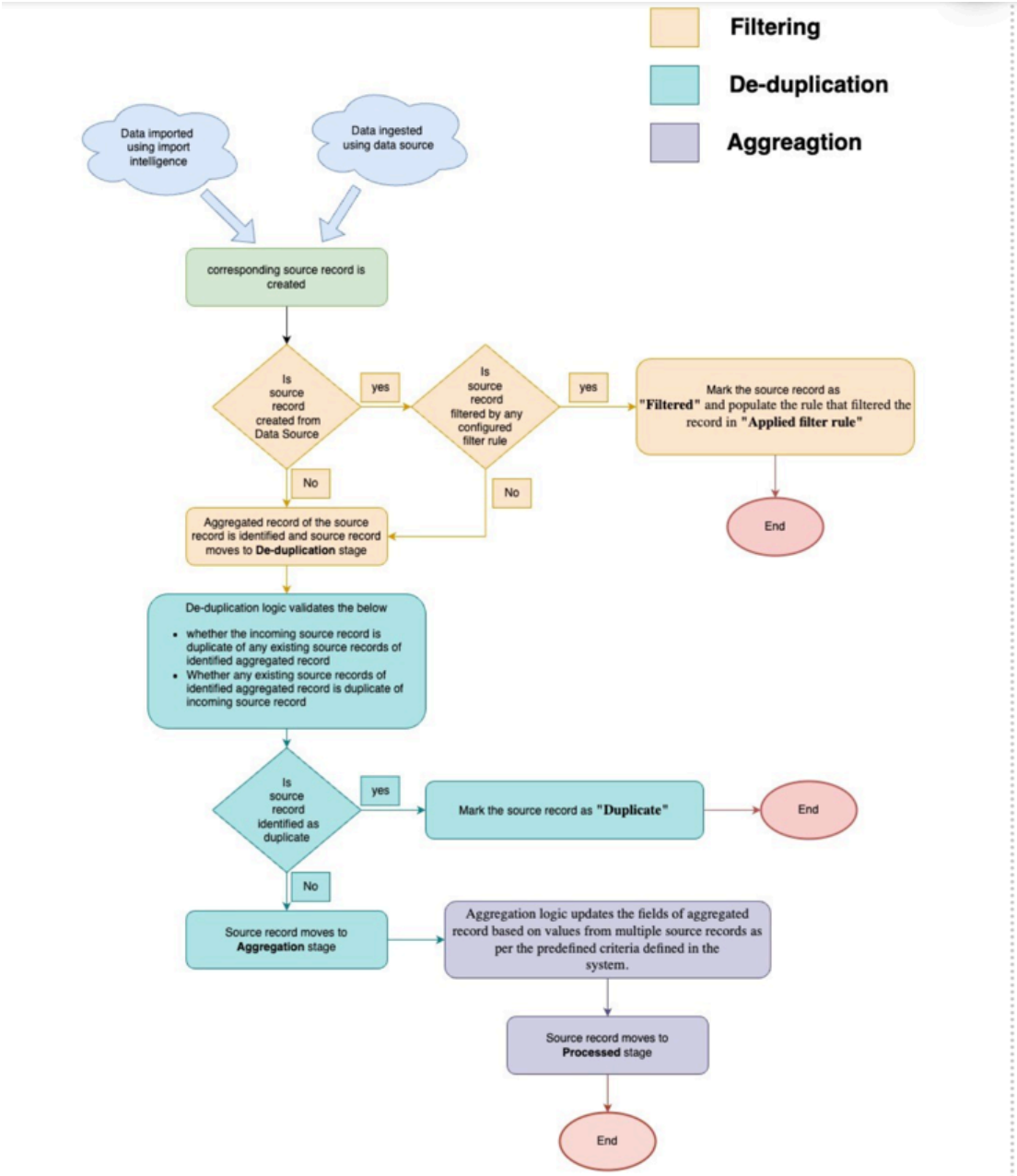
Basic terminology used in Data Processing

1. Source Tables: The Source tables contains the data related to the entities that are fetched from multiple sources, and then the records will be created by each source.
2. Aggregated Records: The Aggregated records tables contains the data related to a specific entity by aggregating the data from all the source records of a specific entity.

TISC Data Flow

1. On a successful execution of import intelligence/Data Source, the records would be created in the corresponding source tables.
2. Once data comes into source table, the data goes through Filtering logic to validate if the record should be filtered based on configured **Inbound Filtering Rules**. (Let's consider SourceRecord1 as a source record for our explanation).
3. If the record gets filtered by any of the configured Inbound Filtering Rules, the corresponding source record (SourceRecord1) is marked as **Filtered** and rule which filtered the record can be found in Applied Filter Rule.
4. Let's assume the source record (SourceRecord1) aggregates to AggregateRecord1.
5. If the record is not filtered, the record is marked for de-duplication by setting processing status to Ready for De-Duplication.
6. De-Duplication logic validates the below:
   a. Whether incoming source record (SourceRecord1) is duplicate of any existing source records for AggregateRecord1.
   b. Any of the existing source records for AggregateRecord1 is a duplicate of incoming source record (SourceRecord1).
7. Every entity has specific fields and relationships based on which the source record is validated for Duplication.
8. If incoming source record (SourceRecord1) is a duplicate of any existing source record of AggregateRecord1, the incoming source record (SourceRecord1) is marked as Duplicate.
9. If any of the existing source record (Existing Source Record1) of AggregateRecord1 is identified as duplicate of incoming source record (SourceRecord1), then existing source record (Existing Source Record1) is marked as Duplicate and incoming source record (SourceRecord1) is marked for aggregation by setting the processing status to Ready for Aggregation.
10. As part of aggregation, fields of aggregated record AggregateRecord1 will be updated based on values from multiple source records will be aggregated as per the predefined criteria defined in the system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



TISC Data Archival

Data grows rapidly in tables with increased adoption of the platform. Some tables come within the base system with various data management policies, but other users are needed to implement them by themselves.

Data Management in TISC

Data is stored and managed in the TISC instance according to the TISC library objects structure for the administrators to view and configure as per their organization's need.

Data Archiving and restoring is one of the key functionality to protect the records for its future use. The following section describes the TISC archival process and records retention as Threat Intelligence contains huge volumes of data and records.

There are a couple of different ways that the users can manage their data in tables:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Delete the data
- Archive the data

Note: If the users don't adopt to any of the ways to manage their data then the usage goes up over time and the data tends to get much larger which will have a large impact on the application instance performance and as well as the storage.

TISC Data Archival

The Threat Intelligence Security Center is provisioned with archival rules in the base system for the TISC table. The related records are also added in the base system to the TISC archive rule.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Archiving** > **Archival Rules**.
   The list of archival rules that are applicable for TISC are displayed. These archival rules are different for every object type and are applicable independently.
2. Filter the tables names starts with sn_sec_tisc.
3. View the TISC related records.

Threat Intelligence Record	Reference Table
Archive Attack Pattern	sn_sec_tisc_attack_pattern
Archive Campaign	sn_sec_tisc_campaign
Archive Course of Action	sn_sec_tisc_course_of_action
Archive Data Component	sn_sec_tisc_aggregated_data_component
Archive Data Source	sn_sec_tisc_aggregated_data_source
Archive Identity	sn_sec_tisc_identity
Archive Infrastructure	sn_sec_tisc_infrastructure
Archive Intrusion Set	sn_sec_tisc_intrusion_set
Archive Malware	sn_sec_tisc_malware
Archive Malware Analysis	sn_sec_tisc_malware_analysis
Archive Marking Definition	sn_sec_tisc_marking_definition
Archive Object Sighting	sn_sec_tisc_object_sighting
Archive Observed Data	sn_sec_tisc_observed_data
Archive Threat Actor	sn_sec_tisc_threat_actor
Archive Threat Event	sn_sec_tisc_threat_event
Archive Threat Grouping	sn_sec_tisc_threat_grouping
Archive Threat Note	sn_sec_tisc_threat_note
Archive Threat Opinion	sn_sec_tisc_threat_opinion
Archive Threat Report	sn_sec_tisc_threat_report

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Threat Intelligence Record	Reference Table
Archive Tool	sn_sec_tisc_tool
Archive Vulnerability	sn_sec_tisc_vulnerability
Artifact	sn_sec_tisc_artifact
AS Number	sn_sec_tisc_as_number
Directory	sn_sec_tisc_directory
Email Address	sn_sec_tisc_email_address
Email Message	sn_sec_tisc_email_message
Email Subject	sn_sec_tisc_email_subject
File	sn_sec_tisc_file
Indicator Archive Rule	sn_sec_tisc_indicator
IPv4 Address	sn_sec_tisc_ipv4_address
IPv4 CIDR	sn_sec_tisc_ipv4_cidr
IPv6 Address	sn_sec_tisc_ipv6_address
Location	sn_sec_tisc_location
MAC Address	sn_sec_tisc_mac_address
MD5 Hash	sn_sec_tisc_md5_hash
Mutex Name	sn_sec_tisc_mutex_name
Other Observable	sn_sec_tisc_other_observable
Process	sn_sec_tisc_process
SHA1 Hash	sn_sec_tisc_sha1_hash
SHA256 Hash	sn_sec_tisc_sha256_hash
SHA512 Hash	sn_sec_tisc_sha512_hash
URL	sn_sec_tisc_url
User Account	sn_sec_tisc_user_account
Windows Registry Key	sn_sec_tisc_windows_registry_key
X.509 Certificate	sn_sec_tisc_x_509_certificate
Object-Object Relationship Archive Rule	sn_sec_tisc_m2m_object
Object-Observable Relationship Archive Rule	sn_sec_tisc_m2m_object_observable
Related Indicator Archive Rule	sn_sec_tisc_m2m_indicator
RSS Feed Archive Rule	sn_sec_tisc_m2m_object_indicator
Imports Archive Rules	sn_sec_tisc_m2m_indicator_observable

Note:

For information on how the archival rules are created, see Create an archive rule.

4. Select an archival rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, select Directory observable record to see the base system archival rule.

5. Update the rule if required.

Archive TISC related records

Use the Archive Related Records related list for TISC to add the related records to the archive rule.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Archiving** > **Archive Rules**.
2. Filter the tables names starts with sn_sec_tisc.
3. Go to **Archive Related Records** related list section to view the TISC related records.

Destroy Rules in TISC

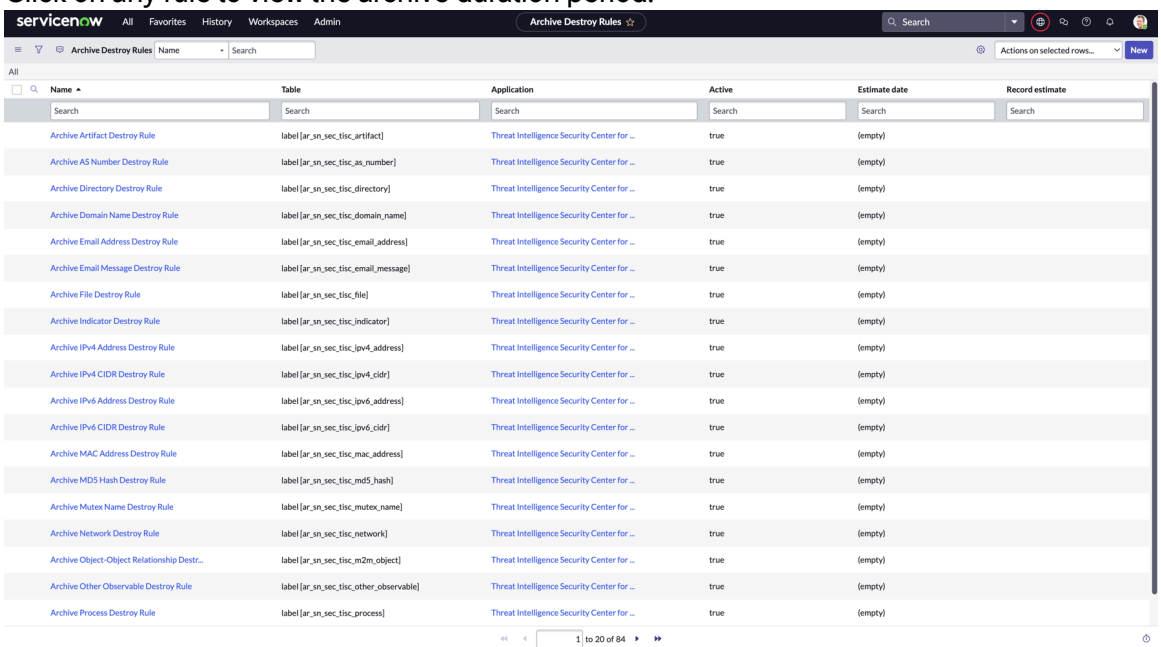
View the destroy rules that are provisioned in the base system.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Archiving** > **Archive Destroy Rules**.
   The list of destroy rules that are applicable for TISC are displayed. These destroy rules are different for every object type and are applicable independently.
2. View the applicable destroy rules for TISC.
3. Click on any rule to view the archive duration period.



Delete intelligence records

Delete records from Threat Intelligence library.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click **Threat Intel Library** icon on the workspace.
3. Open any record.
4. Go to **Source Records** section.
5. Select **Delete** to delete the source records.
6. Delete the library record.

Note:

a. If a library record with associated source records is deleted, then the source records will be reprocessed, and a new library record will be created by aggregating the field values from the source records.

b. To permanently delete the data from the threat intel library, use archival rules instead of deleting the library records. For more information, see TISC Data Archival.

Automated cleanup of duplicate records from same source

The TISC application includes automated logic to manage records that were received repeatedly from the same source. When identical or matching records are ingested multiple times from same source, the application ensures that the most recent record remains active while previously stored instances are identified as duplicates.

Impact of duplicate records

When duplicate records from the same source are retained in the application:

- The deduplication jobs must evaluate a larger number of records during execution.
- Increased record volume can extend job runtime.
- Processing latency may occur as the system identifies and resolves redundant entries.

Table cleaners are implemented for the Observable Source [sn_sec_tisc_observable_source], Indicator Source [sn_sec_tisc_indicator_source], and Object Source [sn_sec_tisc_object_source] tables.

These cleaners remove records from the respective tables based on the following condition:

```
Records where the processing Status is set to Duplicate and Duplicate of Record from Same Source flag is set to true and the record was last updated more than 90 days ago.
```

Navigate to **System Maintenance** > **Table Cleanup** view and manage table cleaners.

Related topics

Observables

Indicators

TISC Data Processing Functional Flow

TISC Data Archival

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data Loss Prevention Incident Response

The Data Loss Prevention Incident Response (DLP IR) application enables you to review and manage the remediation workflow of DLP incidents from multiple sources, such as endpoint, network, email, and cloud.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Data Loss Prevention Incident Response

Explore  Learn about how analysts and administrators use DLP Incident Response	**Install and Configure**  Installing and configuring the DLP Incident Response application	**Administer**  Administration tasks on how to manage the DLP incidents on the ServiceNow AI Platform
Use  Update and manage incidents by leveraging the DLP End User Portal, DLP Ops Portal, and DLP Dashboard.	**Integrate**  Extend DLP capabilities by integrating with third-party applications	

Exploring Data Loss Prevention Incident Response

Explore Data Loss Prevention Incident Response application to learn how to manage sensitive information for your customers, such as the financial and proprietary data, health records, or social security numbers.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data loss occurs when confidential or sensitive information leaves the enterprise network as a result of unauthorized communication. With the DLP application, you can identify, respond, and protect your data loss channels.

By using the Data Loss Prevention Incident Response application, your organization has the following key benefits:

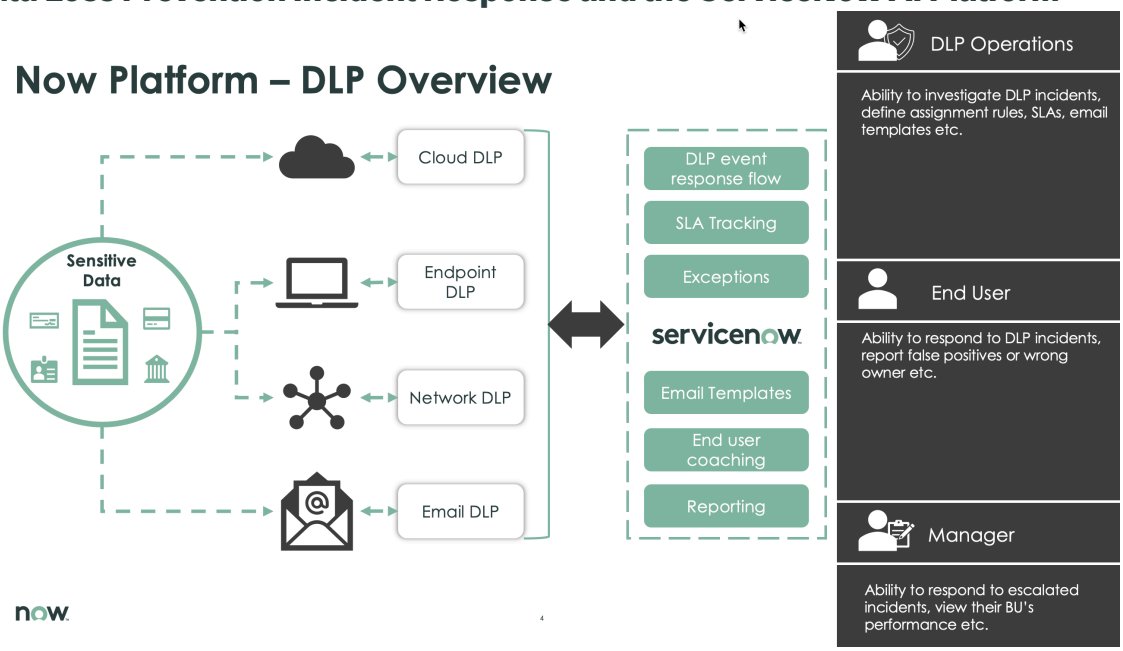
- Integrate with multiple third-party DLP solutions to gain a unified view of the incidents in the ServiceNow AI Platform.
- Monitor and assign incidents to the end users so that you can streamline DLP incident management.
- Coach your employees through the customized email templates and notifications that are sent for each incident as well as in the form of a digest.
- Escalate the overdue DLP incidents from the end users to the managers.
- View summary reports of open incidents by policy, severity, top-offenders, and so on.
- Track DLP incident trends, false positive trends, and remediation trends.

Use this section to learn about the key features, various roles involved in working with DLP incidents.

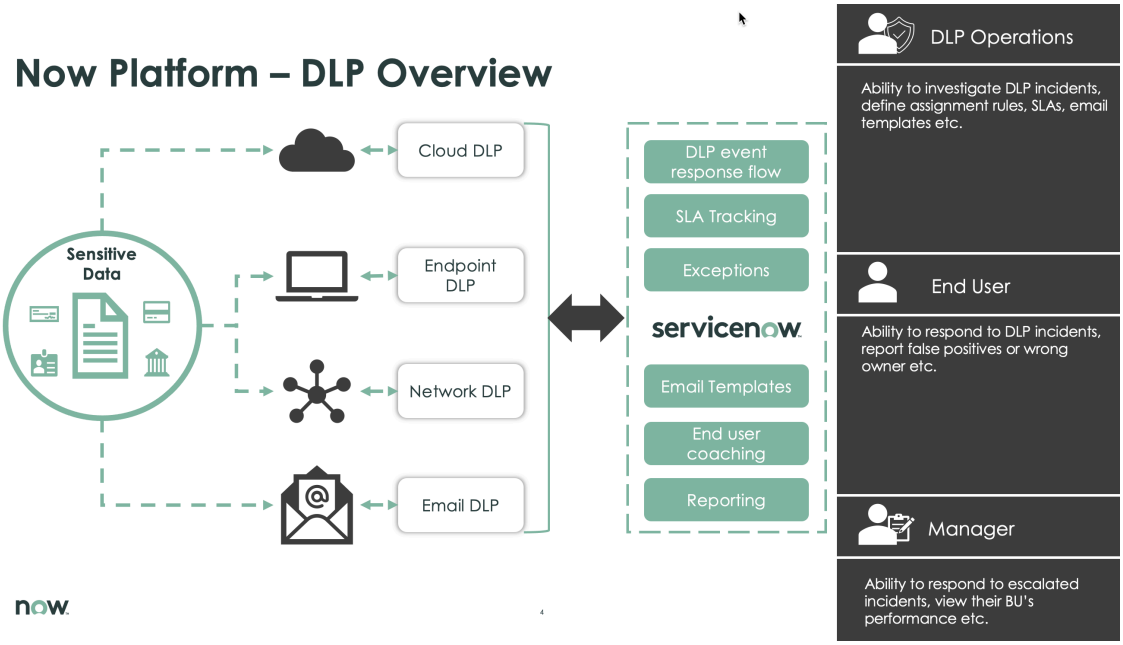
DLP Incident Response overview

Learn how you can use the ServiceNow AI Platform and the Data Loss Prevention Incident Response (DLP IR) application. Manage sensitive information for your customers, such as the financial and proprietary data, health records, or social security numbers. Automate the remediation workflows with the DLP Incident Response application.

Data Loss Prevention Incident Response and the ServiceNow AI Platform



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



1. This is a clickable image, so you can trying clicking on the different sections to learn more about DLP
2. DLP Admin tasks - This is a clickable image, so you can trying clicking on the different sections to learn more about DLP
3. Using the DLP End User portal - This is a clickable image, so you can trying clicking on the different sections to learn more about DLP
4. Using DLP Ops Portal - This is a clickable image, so you can trying clicking on the different sections to learn more about DLP
5. Using DLP dashboard – This is a clickable image, so you can trying clicking on the different sections to learn more about DLP

The Data Loss Prevention Incident Response application includes the following capabilities:

- An end user workspace where your end users or employees can review and respond to the assigned DLP incidents.
- A manager workspace where a manager can review the escalated DLP incidents and act on them appropriately.
- A unified workspace where your DLP operations team can track the trends on the open incidents, top offenders, incidents by scan source, and can view, edit, assign, and close the DLP incidents across multiple sources (endpoints, networks, and email).
- Administrative controls that define the email templates for end-user coaching and communication, assignment rules for automatic assignment of incidents, auto-escalation rules, and delegation for incident responses.

Get started with DLP Incident Response

Review the following information before you start setting up your Data Loss Prevention Incident Response (DLP IR) application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist

Setup task	Description
Verify that you have assigned the required ServiceNow AI Platform and DLP roles.	DLP Incident Response supports the following roles: • The administrator (admin) installs the applications from the ServiceNow Store and assigns the DLP administrator (sn_dlir.admin). • sn_dlir.admin • sn_dlir.analyst
Verify that the ServiceNow core applications that are required to support the Data Loss Prevention Incident Response application are installed and activated.	The Data Loss Prevention Incident Response plugin (com.snc.data_loss_incident) is required to support the Data Loss Prevention Incident Response product. Verify that the following Security Operations applications are installed and activated from the ServiceNow Store. If not installed, install and activate one application at a time in the following order to ensure a smooth installation: • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common For more information on setting up your ServiceNow AI Platform instance for the integration, see Get entitlement for a Security Operations product or application or Activate a ServiceNow Store application.
Domain separation	Verify the Domain separation and DLP Incident Response topic if you intend to separate data, processes, and administrative tasks.

Installing and configuring DLP IR Incident Response

Download the Data Loss Prevention Incident Response (DLP IR) application from the ServiceNow Store and install it on your instance.

Before you invoke the workflows for the integration, install and configure the Data Loss Prevention Incident Response application from the ServiceNow Store on your ServiceNow AI Platform instance.

Install and configure the DLP Incident Response application

Manage sensitive information and automate the remediation workflows by using the Data Loss Prevention Incident Response (DLP IR) application in your ServiceNow AI Platform instance.

Before you begin

Before you can complete the configuration steps, you must download the application from the ServiceNow Store and install it on your instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Roles required: admin and sn_dlir.admin

Procedure

1. Follow the instructions for downloading an application from the ServiceNow Store.
2. After you have downloaded the **DLP Incident Response** application and all of its dependency applications, navigate to **All** > **DLP Administration** > **Default Configuration** to complete the rest of the application configuration.

Domain separation and DLP Incident Response

You can use domain separation with DLP Incident Response to separate the data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level: Standard

- Includes all aspects of **Basic** level support.
- Application properties are domain-aware as needed.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Sample use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

For more information on support levels, see Application support for domain separation.

How domain separation works with DLP Incident Response

- Create a user with the required sn_dlir.admin and sn_dlir.analyst roles in the respective domain.
- Perform the DLP Incident Response configurations in the appropriate domain.

DLP Incident Response Administration

You can set up and assign rules, configure due date rules, use email templates, configure end-user response actions, and much more to manage the Data Loss Prevention Incident Response (DLP IR) incidents on the ServiceNow AI Platform.

The Data Loss Prevention Incident Response application enables you to perform the following configurations.

DLP default configuration settings

Define the default configuration settings for Data Loss Prevention Incident Response (DLP IR) incidents to identify and set up the incident notification and incident assignment preferences for your end users.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can use this module to define the default configuration settings when the core assignment rules and identifier rules are exhausted and unable to match to a condition or user. You can also define and reapply End user lookup rules and Assignment rules to existing Active DLP incidents.

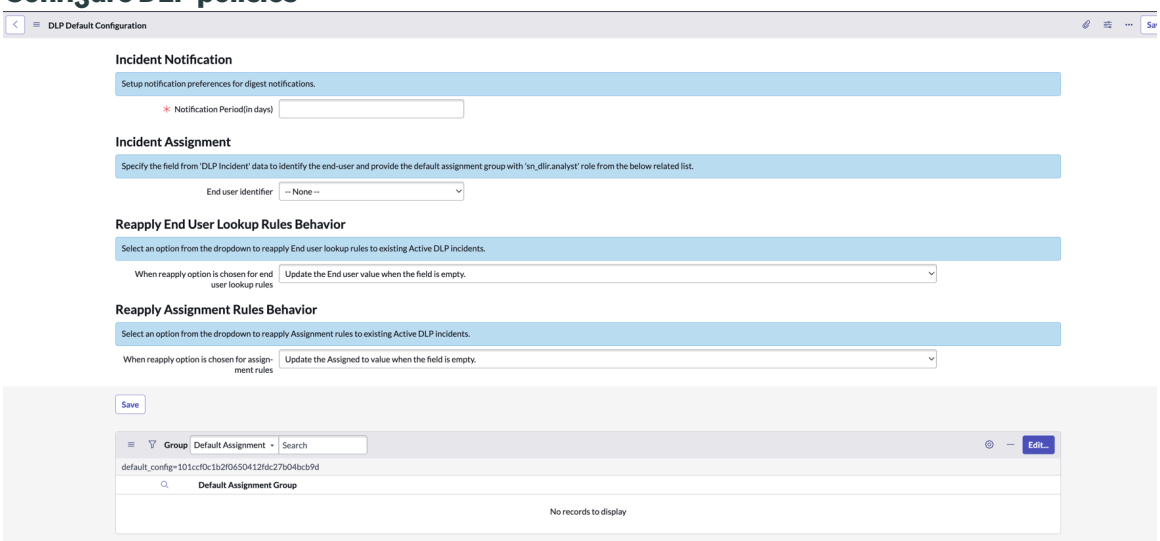
The end user incident notification enables you to specify the frequency at which email notifications are sent to your end users. For example, you can set up notification preferences to accumulate incidents and to send an email digest once a week. By assigning an incident, you can specify which group you initially assign the DLP incidents to. You can also specify how the end users are further identified by the DLP operations team.

For example, let's say that a user has stored credit card information in a file on a network. When the third-party DLP integration product creates an incident for a sensitive data policy violation, the incident data that the ServiceNow AI Platform DLP ingests would contain information about the end user. You would then be able to assign the incident to the right end user.

Procedure

1. Navigate to **All** > **DLP Administration** > **Default Configuration**.

Configure DLP policies



2. On the form, fill in the fields.

DLP Default Configuration form

Configuration Name	Field	Description
End User Incident Notification	Notification Period (days)	Define the number of days after which an email notification should be sent to the end user. The number of days must be between 1–60 days.
	Automatically update parent state based on cloned/child incidents	Option to automatically update the parent state incident based on the cloned or child incidents.
Incident Assignment	End User Identifier	Specify the field to be used from Incident data to identify the end user. Possibles values are the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Name	Field	Description
		○ **Data owner email** ○ **Destination** ○ **File created by** ○ **File modified by** ○ **File owner** ○ **FTP user name** ○ **Sender**
Reapply End User Lookup Rules Behavior	When reapply option is chosen for end user lookup rules	Option to reapply End user lookup rules to existing Active DLP incidents. You can select one of the following option to reapply: ○ **Update the End user value when the field is empty**: Updates the existing active DLP incidents' End user value if that field is empty. ○ **Update the End user value**: Updates the existing active DLP incidents' End user value. ○ **Update the End user and Assigned to values when both fields are empty**: Updates the existing active DLP incidents' End user and Assigned to values if both fields are empty. **Note:** If this option is selected, then the **Update the Assigned to value when the field is empty** option gets disabled automatically in the Reapply Assignment Rules Behavior section as it's applicable for both. ○ **Update the End user and Assigned to values for all the active DLP incidents**: Updates the End user and Assigned to values for all active DLP incidents. **Note:** If this option is selected, then the **Update the Assigned to value for all the active DLP incidents** option gets disabled automatically in the Reapply Assignment Rules Behavior section as it's applicable for both.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Name	Field	Description
Reapply Assignment Rules Behavior	When reapply option is chosen for assignment rules	Option to reapply assignment rules to existing Active DLP incidents. You can select one of the following option to reapply: ○ **Update the Assigned to value when the field is empty.** ○ **Update the Assigned to value for all the active DLP incidents.**

3. Select the **Default Assignment Group** from the related list section where all the DLP incidents are assigned to.
   Click **Edit** to add the user group. When you click **Edit** from the related list section and select an item from the **Collections** columns and then add that selected assignee to the Group columns in the **Edit Members** page, and save the list.

   Note: You can only view and select groups that have been assigned with the sn_dlir.analyst role from the related list. You can only select one group.

4. Click **Save**.

Create end user lookup rules

You can create and configure end user lookup rules and assign the DLP incidents to the respective end users based on those rules.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

The DLP admin defines these end user lookup rules to automatically assign the end users to DLP incidents using only the end user field. The DLP end user lookup rule enables you to assign the end user on DLP incidents based on End user identifier, Custom attributes, or Script.

Procedure

1. Navigate to **All** > **DLP Administration** > **DLP End User Lookup Rules**.
2. Click **New**.
3. On the form, fill in the fields.

DLP End User Lookup Rule form

Field	Description
Name	Name for the end user lookup rule.
Active	Option to indicate whether the end user lookup rule is active.
Execution order	The end user lookup rule priority. This field indicates the order in which the end user

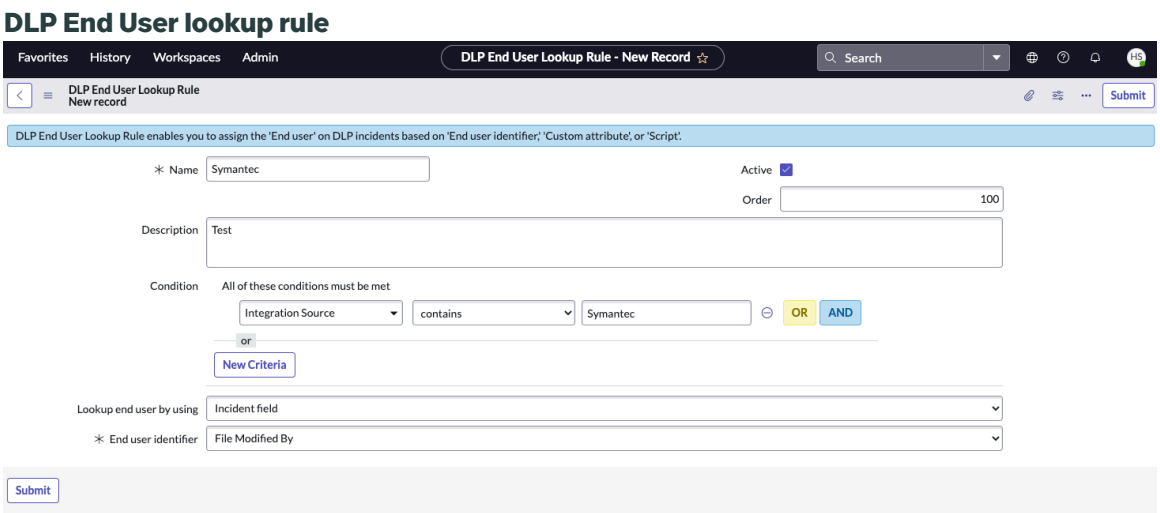
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	lookup rules are executed when two or more rules share the triggering conditions. The end user lookup rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, and so on. The default value is 100.
Description	Unique description for the end user lookup rule.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the end user lookup rule, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. For example, you can set the conditions for this end user lookup rule by selecting the condition as **Integration Source**, **contains**, **Symantec**. **Note:** The conditions in the condition builder are case sensitive.
Lookup end user by using	Option to lookup end user by using **Incident field** or **Script**.
End User Identifier	The end user identifier of the DLP incident. This field appears when **Incident field** is selected from the **Lookup end user by using** field. You can select an end user identifier from the following: ○ **Data owner email** ○ **Destination** ○ **File created by** ○ **File modified by** ○ **File owner** ○ **FTP user name** ○ **Sender**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The above listed end user identifiers are configurable using the system property `sn_dlir.assignment.fields`. For more information, see Configure advanced settings. ○ **Custom user from incident**
Custom attribute	Option to specify a custom attribute from the incident that has the reference to a user. This field appears only when **The a** is selected from the **End User Identifier** field.
Script	You can use the script editor to customize and format the field values during the end user lookup rule creation. For example, you can use the email address field to identify the end user.

Example
The following example shows an end user lookup rule with the name 'Symantec'. The condition builder requires the 'Integration Source' as 'Symantec'. The **Lookup end user by using** option is set to 'Incident field', and **End user identifier** option is set to 'File Modified by'.



4. Click **Submit**.
   You also have an option to select one or more end user lookup rules and reapply it on all existing DLP incidents.
5. To reapply an end user lookup rule on all existing DLP incidents, click **Reapply**.

Create assignment rules

Create assignment rules and assign the Data Loss Prevention Incident Response (DLP IR) incidents to user groups, end users, managers, or user from incident.

Before you begin
Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_dlir.admin
- sn_dlir.analyst and sn_dlir.analyst_read

About this task

Use assignment rules to assign DLP IR incidents to user groups, end users, or to managers. The assignment of the DLP incidents occur when the conditions in the assignment rule are met.

Procedure

1. Navigate to **All** > **DLP Administration** > **Assignment Rules**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Assignment Rule form

Field	Description
Name	Name for the assignment rule.
Active	Option to indicate whether the assignment rule is active.
Execution order	The assignment rule priority. This field indicates the order in which the assignment rules are executed when two or more rules share the triggering conditions. The assignment rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, and so on. The default value is 100.
Description	Unique description for this assignment rule.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the assignment rule, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. For example, assume you create a DLP assignment rule for an endpoint. You can specify that the condition scan source is an

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

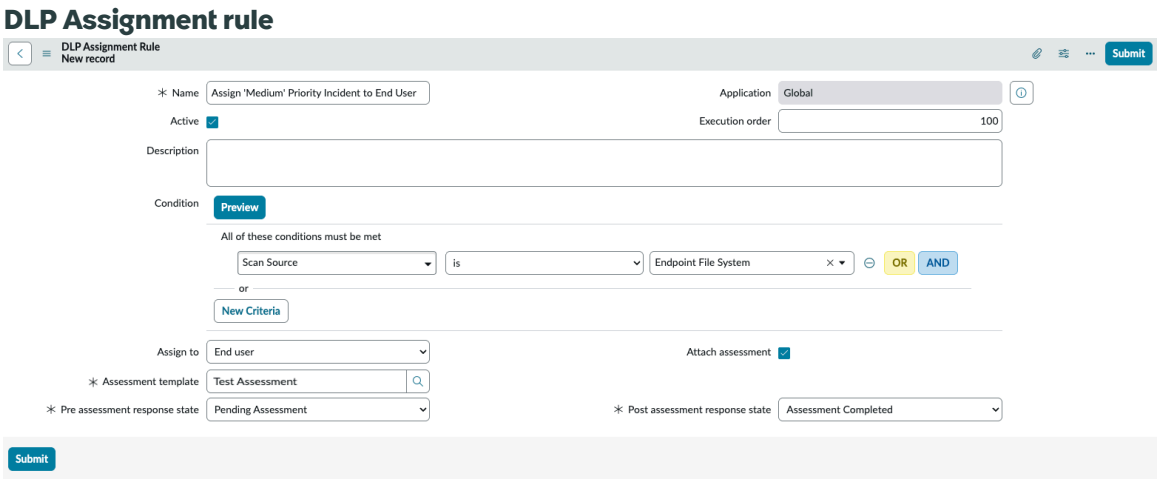
Field	Description
	endpoint file system that must be met before assigning an incident. **Note:** The conditions in the condition builder are case sensitive.
Assign to	Assignment to either one of the following: ○ User group ○ End user ○ Manager ○ User from incident The assignment occurs when the conditions in the condition builder are met.
User group	Option to search and select a user group to assign the DLP incidents to. This field appears when **User group** is selected from the **Assign to** field. **Note:** You can only view and select groups that have been assigned with the sn_dlir.analyst role.
End user	Option to assign the DLP incident to the end user. The assignment occurs when the conditions in the condition builder are met.
Assign using Manager fields	Manager of the end user. This field appears when **Manager** is selected from the **Assign to** field. You can assign the DLP incidents to a particular manager by selecting one of the Manager fields, such as Last name, Email, City, Employee number.
User Identifier	The user identifier of the incident. This field appears when **User from Incident** is selected from the **Assign to** field. You can select an user identifier from the following: ○ **Data owner email** ○ **Destination** ○ **File created by** ○ **File modified by** ○ **File owner** ○ **FTP user name** ○ **Sender** ○ **Custom user from incident**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Custom attribute	Option to specify a custom attribute from the incident that has the reference to a user. This field appears only when the **Custom User from Incident** is selected from the **User Identifier** field.
Attach Assessment	Option to indicate whether you want to attach an assessment to the incident.
Pre assessment response state	Option to select which state that the incident should be in before the end user responds. It can also be a custom state. The default value is Pending assessment.
Post assessment response state	Option to select which state that the DLP incident should be in after the user responds. The default value is Assessment Completed.
Advanced	Advanced option to identify the end user. This field appears only when the **Custom User from Incident** is selected from the **User Identifier** field. You can use the script editor to customize and format the field values during the assignment rule creation to identify the end user. Then, you pick whom you want to assign the DLP incident to, which could be an End user or the End user's Manager. For example, you can use the email address field to identify the end user.

Example

The following example shows an assignment rule with the name `Assign 'Medium' Priority Incident to End User`. The condition builder requires the Scan Source to be `Endpoint File System`, and the `Assign to` field is set to `End user`. Then, you can look up the 'Email' of the End user.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select the **Assign to** field from the related list section where all the DLP incidents are assigned to.
   Click **Edit** to add the user group. When you click **Edit** from the related list section and select an item from the **Collections** columns and then add that selected assignee to the Group columns in the **Edit Members** page, and save the list.

   Note: You can only view and select groups that have been assigned with the sn_dlir.analyst role from the related list. You can only select one group.

5. Click **Submit**.
   You can select one or more assignment rules and reapply it on all existing DLP incidents.
6. To reapply an assignment rule on all existing DLP incidents, click **Reapply**.

Create incident consolidation rules

Create incident consolidation rule to consolidate multiple incidents of similar nature under one parent incident.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only)

About this task

The DLP admin defines these incident consolidation rules to automatically consolidate the DLP incidents of same nature under one parent incident. The DLP incident consolidation rule enables you to consolidate the DLP incidents based on configuration provided for Consolidation duration and Consolidation identification.

Note:

When a consolidated incident is created, it becomes a child of the parent DLP incident. If the severity of the consolidated incident is higher than that of the parent, then the parent incident severity will be updated to match with the child incident.

Procedure

1. Navigate to **All** > **DLP Administration** > **DLP Incident Consolidation Rules**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Assignment Rule form

Field	Description
Name	Name for the incident consolidation rule.
Active	Option to indicate whether the incident consolidation rule is active.
Execution order	The incident consolidation rule priority. This field indicates the order in which the incident consolidation rules are executed when two or more rules share the triggering conditions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The incident consolidation rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, and so on. The default value is 100.
Description	Unique description for the incident consolidation rule.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the incident consolidation rule, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. For example, you can set the conditions for this incident consolidation rule by selecting the condition as **Integration Source**, **contains**, **Symantec**. **Note:** The conditions in the condition builder are case sensitive.
Consolidation duration	Option to set the duration for the incident consolidation. Incidents in this period with same values for the selected fields will be consolidated under the first incident. The first incident matching this rule will be the parent incident and rest of incidents will be child incidents.
Consolidate incidents by	Select DLP incident field to consolidate the incidents when having the same value in selected field for different incidents. Select at least one field. Select at least one field.

The following example shows an incident consolidation rule with the name Consolidate incidents for Symantec Integration. The condition builder requires the Integration Source as

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Symantec. The **Condition duration** option is set to 1 hour, and Policy Name option is selected for **Consolidate incident by**.

At the time of Symantec DLP Incident ingestion, this rule will be executed and when multiple Incidents have the same Policy Name, the Incident will be consolidated under the first ingested incident matching this rule.

4. Click **Submit**.
   Incidents consolidated based on the consolidation rule will be available under the Child incidents list on DLP Analyst Workspace.

Create response due date rules

Set up the response due date rules to determine the time you want to give your end users to respond to the assigned Data Loss Prevention Incident Response (DLP IR) incidents.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

You can use this module to define the response due date rules for the different types of DLP incidents and the rules to start counting the due date. After the due date has expired, the users get notified about the overdue incident. You're also provided with an option to escalate the overdue incident to one of the following:

- Manager
- Custom User from Incident
- User group

For example, when you escalate the overdue incident to a Manager, and you've specified a maximum of three levels of escalation. The first level of Manager gets notified first. If the incident is overdue again, then the second level of Manager gets notified, followed by the third level if the incident is still overdue. If the Manager has a Delegate, then the Manager has the option to assign the escalation or overdue incident to the Delegate.

You're also provided with the ability to create multiple response due date rules.

Procedure

1. Navigate to **All** > **DLP Administration** > **Response Due Date Rules**.
2. Click **New**.
3. On the form, fill in the fields.

Response Due Date Rule form

Field	Description
Name	Name of the response due date rule.
Active	Option to indicate whether the response due date rule is active.
Due in (days)	Number of due days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

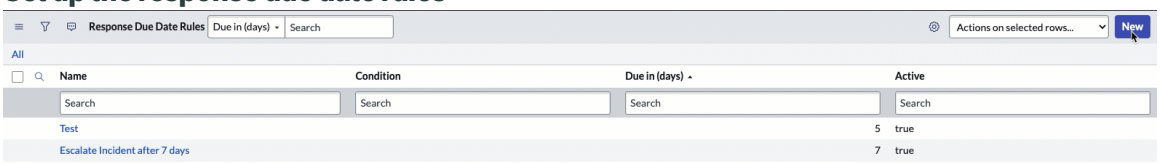
Field	Description
Due date counted from	Start date that is used to calculate the due date. The due date can be calculated from either the first time that the user was notified about the incident, or from the incident assignment date.
Notify before due date	Option to notify the end user about the DLP incident before the due date.
Notify on (days before due date)	Number of days before the due date when the rule triggers a notification to the end user.
Description	Unique description for this response due date rule.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the response due date rule, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. **Note:** The conditions in the condition builder are case sensitive.
Escalate	Option to escalate the DLP incident to someone if the response due date has been breached. For more information, see Add multiple users to access DLP incidents
Escalate overdue incident to	Option to specify if the incident should be escalated to a Manager, a Custom user, or a User group. This field appears only when the **Escalate** option is enabled.
Assign using	Specify how a manager should be identified. This field appears only when **Manager** is selected from the **Escalate overdue incident to** field.
Maximum Escalation Levels	Option to define the maximum number of escalation levels for a Manager, and a Custom user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	As a Manager or Custom user, you can define any number of escalation levels. By default, three levels of escalation are provided. ○ As a Manager, you can define any number of escalation levels by updating the value in this field. ○ As a Custom user, you can use the + icon to define any number of escalation levels.
Custom attribute	Option to specify a custom attribute from the incident that has the reference to a user. This field appears only when **Custom User from Incident** is selected from the **Escalate overdue incident to** field.
User group	Option to search and select a user group to escalate DLP incidents to. This field appears only when **User group** is selected from the **Escalate overdue incident to** field. **Note:** You can only view and select groups that have been assigned with the sn_dlir.analyst role.

Example
The following example shows the response due date rule to determine how much time you want to give your end users to respond to the assigned Data Loss Prevention Incident Response (DLP) incidents. After the end user is first notified, the response due date is in two days. The conditions builder shows that the Scan Source must match the Endpoint File System to proceed with creating the response due date. The escalation option is selected. The incident is escalated to the manager if the response due date is breached.

Set up the response due date rules



4. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add multiple users to access DLP incidents

Use the escalation chain feature to allow all the respective users who are involved in the incident to access the DLP incidents from the list view, though the incident is assigned to a different user.

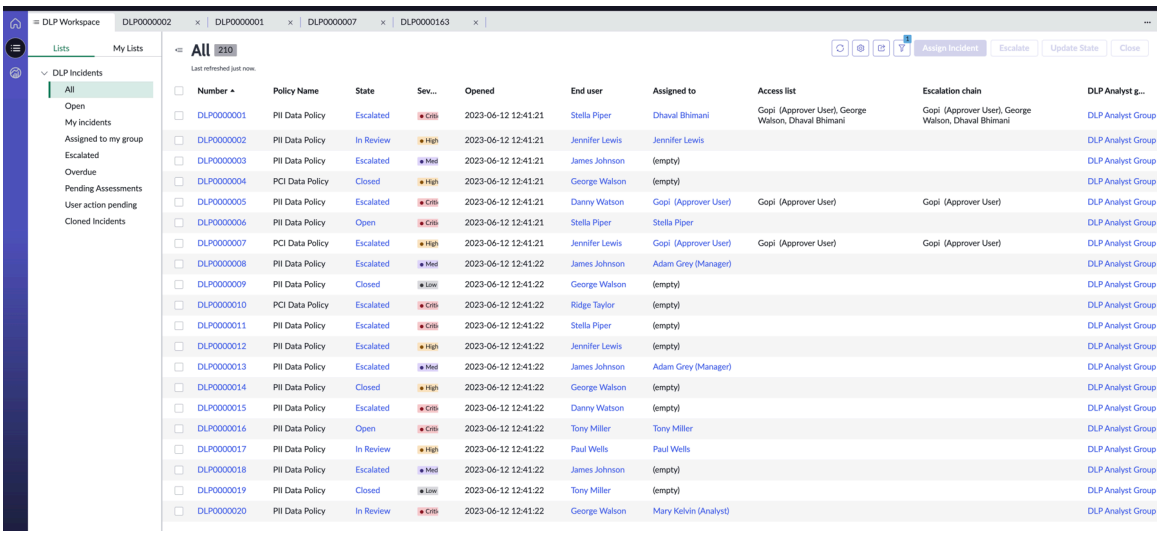
Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.read, sn_dlir.analyst, and sn_dlir.analyst_read - View (read-only).

Procedure

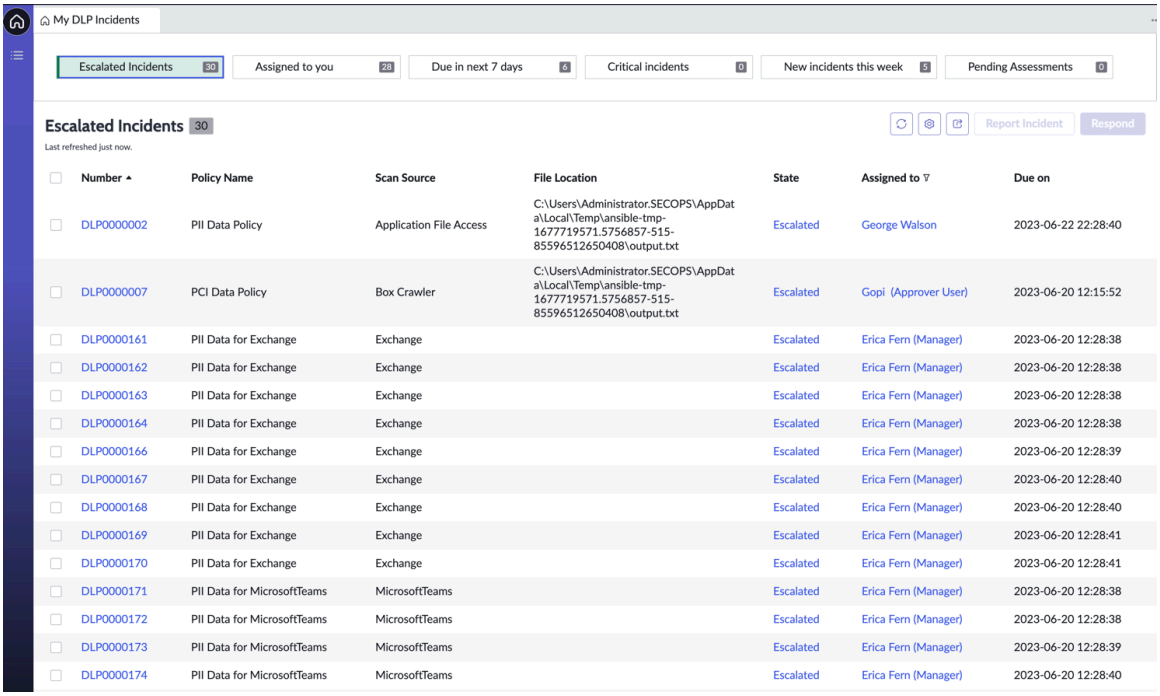
1. Navigate to **DLP** > **DLP Analyst Workspace**.
   On the list view, the users and their delegates should be able to view the DLP incident under **Escalated** incidents tab on the end user portal.
2. Open any incident.
3. Click **Escalate** button to escalate an incident.
4. Select the user or user group from the drop down list.
   You can add multiple users to the escalation chain, all the users who has access are listed on the Details section of the form view and also under the **All** incidents tab. The escalation chain is displayed based on the configuration settings. For more information, see Configure advanced settings



Number	Policy Name	State	Sev...	Opened	End user	Assigned to	Access list	Escalation chain	DLP Analyst g...
DLP0000001	PII Data Policy	Escalated	Critical	2023-06-12 12:41:21	Stella Piper	Dhaval Bhimani	Gopi (Approver User), George Walson, Dhaval Bhimani	Gopi (Approver User), George Walson, Dhaval Bhimani	DLP Analyst Group
DLP0000002	PII Data Policy	In Review	High	2023-06-12 12:41:21	Jennifer Lewis	Jennifer Lewis			DLP Analyst Group
DLP0000003	PII Data Policy	Escalated	Medium	2023-06-12 12:41:21	James Johnson	(empty)			DLP Analyst Group
DLP0000004	PCI Data Policy	Closed	High	2023-06-12 12:41:21	George Walson	(empty)			DLP Analyst Group
DLP0000005	PII Data Policy	Escalated	Critical	2023-06-12 12:41:21	Danny Watson	Gopi (Approver User)	Gopi (Approver User)	Gopi (Approver User)	DLP Analyst Group
DLP0000006	PII Data Policy	Open	Critical	2023-06-12 12:41:21	Stella Piper	Stella Piper			DLP Analyst Group
DLP0000007	PCI Data Policy	Escalated	High	2023-06-12 12:41:21	Jennifer Lewis	Gopi (Approver User)	Gopi (Approver User)	Gopi (Approver User)	DLP Analyst Group
DLP0000008	PII Data Policy	Escalated	Medium	2023-06-12 12:41:22	James Johnson	Adam Grey (Manager)			DLP Analyst Group
DLP0000009	PII Data Policy	Closed	Low	2023-06-12 12:41:22	George Walson	(empty)			DLP Analyst Group
DLP0000010	PCI Data Policy	Escalated	Critical	2023-06-12 12:41:22	Ridge Taylor	(empty)			DLP Analyst Group
DLP0000011	PII Data Policy	Escalated	Critical	2023-06-12 12:41:22	Stella Piper	(empty)			DLP Analyst Group
DLP0000012	PII Data Policy	Escalated	High	2023-06-12 12:41:22	Jennifer Lewis	(empty)			DLP Analyst Group
DLP0000013	PII Data Policy	Escalated	Medium	2023-06-12 12:41:22	James Johnson	Adam Grey (Manager)			DLP Analyst Group
DLP0000014	PII Data Policy	Closed	High	2023-06-12 12:41:22	George Walson	(empty)			DLP Analyst Group
DLP0000015	PII Data Policy	Escalated	Critical	2023-06-12 12:41:22	Danny Watson	(empty)			DLP Analyst Group
DLP0000016	PII Data Policy	Open	Critical	2023-06-12 12:41:22	Tony Miller	Tony Miller			DLP Analyst Group
DLP0000017	PII Data Policy	In Review	High	2023-06-12 12:41:22	Paul Wells	Paul Wells			DLP Analyst Group
DLP0000018	PII Data Policy	Escalated	Medium	2023-06-12 12:41:22	James Johnson	(empty)			DLP Analyst Group
DLP0000019	PII Data Policy	Closed	Low	2023-06-12 12:41:22	Tony Miller	(empty)			DLP Analyst Group
DLP0000020	PII Data Policy	In Review	Critical	2023-06-12 12:41:22	George Walson	Mary Kelvin (Analyst)			DLP Analyst Group

5. Click **Submit**.
   After you submit, the incident will then be assigned to a manager however the end user can still view the incident.
6. To verify this, navigate to the **DLP User Workspace** as an end user.
   All the incidents that are assigned to the end user are displayed.
7. View the escalated incidents list under the **Escalated Incidents** section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Number	Policy Name	Scan Source	File Location	State	Assigned to	Due on
DLP0000002	PII Data Policy	Application File Access	C:\Users\Administrator.SECOPS\AppData\Local\Temp\ansible-tmp-1677719571.5756857-515-85596512650408\output.txt	Escalated	George Walson	2023-06-22 22:28:40
DLP0000007	PCI Data Policy	Box Crawler	C:\Users\Administrator.SECOPS\AppData\Local\Temp\ansible-tmp-1677719571.5756857-515-85596512650408\output.txt	Escalated	Gopi (Approver User)	2023-06-20 12:15:52
DLP0000161	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000162	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000163	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000164	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000166	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:39
DLP0000167	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40
DLP0000168	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40
DLP0000169	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:41
DLP0000170	PII Data for Exchange	Exchange		Escalated	Erica Fern (Manager)	2023-06-20 12:28:41
DLP0000171	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000172	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:38
DLP0000173	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:39
DLP0000174	PII Data for MicrosoftTeams	MicrosoftTeams		Escalated	Erica Fern (Manager)	2023-06-20 12:28:40

You can also view the users access list under the **Escalation Chain**column on the list view.

8. Open any incident.
9. Click **Respond** button to submit incident response.
10. Select the response from the drop down list.
11. Click **Submit**.

Create Approval Rules

Create approval rules to take approval from various levels of approver users whenever an advanced type of response option is selected.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

The DLP admin defines these approval rules to grant consent on requests raised by end users for the approval of advanced type of response option. DLP admin can also define multiple levels of approval from here.

Procedure

1. Navigate to **All** > **DLP Administration** > **DLP Approval Rules**.
2. Click **New**.
3. On the form, fill in fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP Assignment Rule form

Field	Description
Name	Name for the approval rule.
Active	Option to indicate whether the approval rule is active.
Execution order	The approval rule priority. This field indicates the order in which the approval rules are executed when two or more rules share the triggering conditions. The approval rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, 300, and so on. The default value is 100.
Description	Unique description for the approval rule.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the approval rule, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. For example, you can set the conditions for this incident consolidation rule by selecting the condition as **Integration Source**, **contains**, **Microsoft**.
Applicable for response options	Option to select the response option of type advanced. You can select the multiple response options.
Approver	Select which type of approver user you want to set.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **User Table**: Select this option if you want to select approver user from the Users (sys_user) table. ○ **Custom Approval List**: Select this option if you want to configure multiple levels of custom approver for a single request
Approver identifier	This field will appear when **User Table** is selected for **Approver** option. Select field to identifier the approver from the Users(sys_user) table.
Number of levels	This field will appear when **User Table** is selected for **Approver** option. End number in this field to define the levels of approval. For example, if 3 is added in the Number of levels field and Manager is selected in the Approver identifier field then approval request will traverse to three levels of approval.

The following example shows the approval rule created for one of the advance response options. The condition requires the Integration source name contains the Microsoft keyword that then triggers this configuration.

4. For the **Approver** option, select **Custom Approval List**.
5. Click **Submit**.
6. **Approval Levels** related list will populate on the form view.
7. In the **Approval Levels** section, click **New**.
8. On the form, fill in the fields.

Approval Level form

Field	Description
Name	Name for the approval level.
Active	Option to indicate whether the approval level is active.
level	The level for the approval rule. This field indicates the order in which the approval levels are executed when two or more levels are configured. The approval level with the lowest number has the highest priority. To set the level of operation, enter a value. For example, 100, 200, 300, and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The default value is 100.
Approval Rule	Approval Rule for which you want to define this configuration. This will be read-only field.
Description	Unique description for the approval rule.
Approvals required	Select option to define whether approval from all the configured users/groups are required or only required from any one user.
Approvers	Option to select the approvers. **a.** Users and Groups: **i. Users**: Click the  icon to add a particular user from the list. You can also add a user by using their email address or search option. To add yourself as the user to whom the DLP conditions are applicable, click the  . **ii. Groups**: Click the <add_icon> icon to add a particular group from the list. You can also add a group by using the search option. **b. Find by using script**: You can use the script editor to customize and format the field values during the approval level creation. For example, you can use the email address field to identify the approver user.

9. Click **Submit**.

Create user instructions templates

Create and manage user instructions template for DLP incidents to help the users understand the instructions involved incident resolution and the next steps involved in the resolution process.

Before you begin

The user instructions card template displays two different headers which provides you more information about a specific incident on the form view.

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

When an incident is assigned to the end user then the user might be required to know the additional instructions on how to respond to the incidents, introduce the users to the terminology and provide any additional information about the incident. These templates can guide the users to provide the accurate response to the DLP incidents.

Procedure

1. Navigate to **All** > **DLP Administration** > **User Instructions Templates**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Incident Assessment

Field	Description
Name	Name of the user instruction template.
Short Description	Unique description of this user instruction template.
Active	Option to indicate whether the user instruction template is active.
Execution Order	Priority of the incident user instruction template. This field indicates the order in which the order is executed to evaluate the user instruction template when an incident is created. The option with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default is 100.
Incidents matching condition	Incidents that match the defined conditions in the condition builder will be displayed. These conditions are based on the DLP incident data. To build a condition for a user instruction, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click AND or OR: If AND is selected, all conditions must be matched. If OR is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. **Note:** The conditions in the condition builder are case sensitive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Applies to	Select the user or user groups that the template is applicable for. The other available options are: ○ **All end users**: Select this check box if the instructions template applies to all the users. ○ **All reviewers of escalated incidents**: Select this check box if the template applies to all the reviewers of the escalated incidents. ○ **Specific users**: Click the icon to add a particular user from the list to whom the DLP incident conditions are applicable. You can also add a user by using their email address or search option. For example, Legal Manager. To add yourself as the user to whom the DLP conditions are applicable, click the **Add me** icon. ○ **Specific user groups**: Click the icon to add a particular group from the list to whom the DLP incident conditions are applicable. You can also add a group by using the search option. For example, Survey creators.
Instructions Template: Instructions	Add instructions in the rich text editor with variables available at an incident level.

4. Drill down to the **Instructions Template** section, enter the template instruction and add incident level information under this section, if required.
5. Drag-and-drop the required variables to dynamically display certain fields.
6. Click **Submit**.
   The user instructions templates are now created and you can click on any user instruction header to know the additional details of a DLP incident.

   For more information, see Data Loss Prevention Incident Response User Workspace.

Configure DLP UI user instructions

Configure the system UI messages to add detailed user instruction headers as required.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System UI** > **Messages**.
2. Search for **user_instruction_card_heading**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By default, user_instruction_card_heading and user_instruction_modal_window_heading are the two UI message configurations provisioned to the users.

3. Click on any of the user instruction to update or modify.

Create email templates

Create and manage the preconfigured email templates for sending notifications to your end users, user groups, or managers. With these templates, you can coach and communicate with your end users about the Data Loss Prevention Incident Response (DLP IR) incidents.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

Important: For Analysts to view email communications of a DLP Incident on the activity stream, you should add or append the 'sn_dlir.analyst' role in the global system property `glide.ui.activity.email_roles`.

About this task

Email notifications are categorized by the incident notifications that are sent to the end users, the escalation notifications that are sent to the managers, or the due date notifications. You can send email notifications about the due dates for DLP incidents, or even coach the end users about what to do when certain conditions are met in the email conditions filter.
DLP email templates enable you to send the email notification for end users, managers, and analysts. You can configure the templates to be sent per incident or as a digest. Your email subject and body can contain variables so that you can reuse your existing content.

DLP provides the following preconfigured email templates based on the categories:

- **DLP Email template - Per incident approval notification:** Notify users about the approval for their requests.
- **DLP Email template - Escalation notification:** Send escalation notifications to managers in the form of digests.
- **DLP Email template - Pending approval notification:** Notify approvers about pending items.
- **DLP Email template - Per incident approval request cancellation notification:**Notify users about an approval request that has been cancelled by DLP analyst team.
- **DLP Email template - User response completion notification:** Notify DLP analyst team about the response submitted by users.
- **DLP Email template - User incident notification:**This is a default template for user digest notification. Send incident notifications to the end users in the form of digests every few days, even if there are no new incidents, to inform the users about the total number of incidents on the particular user's name. You can also send digest notifications to notify the users about the nearest upcoming due dates of DLP incidents with the severity as critical, high, medium, or low.
- **DLP Email template - Per incident pending approval notification**: Notify approvers about pending approvals.
- **DLP Email template - rejection notification:** Send reject notification to requester.
- **DLP Email template - Due date notification:** Send incident due date notification. If a DLP incident is assigned to the end user, and if the end user has not taken any action before the due date, then an email notification is sent to the end user. You also have an option to escalate

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the DLP incident to a manager, a custom user, or a user group if the response due date has been breached.

Note: Due date notifications must be in the form of digests.

- **DLP Email template - Per incident user response notification:** Notify analysts about the response submitted users per incident.
- **DLP Email template - Per incident escalation notification:** Notify managers about escalations per incident.
- **DLP Email template - Per incident user notification:** Notify users about assignment per incident.

Procedure

1. Navigate to **All** > **DLP Administration** > **Email Templates**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Email Template form

Field	Description
Name	Name of the email template.
Active	Option to indicate whether the DLP email template is active. If this option is not enabled, then notifications are not sent for this email template.
Category	Email notification category. DLP supports the following options: ○ **Incident notification to end users**: Sent when the incidents are assigned to the end users. ○ **Escalation notification to managers**: Sent when the response due date is breached or manually assigned to the manager through DLP Ops portal. ○ **Due date notification**: Sent when the response due date is breached. ○ **User response notification to analysts**: Sent when the end user takes any action on the DLP incident. ○ **Pending approvals notification**: Notify approvers about pending items. ○ **Approval notification to the requester**: Notify users about the approval for their requests. ○ **Reject notification to the requester**: Notify users about the rejection for their requests. ○ **Cancel notification to the requester**: Notify users about the cancellation for their requests.
Type	Option to indicate whether the email is sent per incident or as a digest.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If you selected **Due date notification** from the **Category** field, then you can use only digests. Select this option.
Description	Unique description for this email template.
Execution Order	Email template priority. This field indicates the order in which the email templates are executed when two or more email templates share the triggering conditions. The email template with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default value is 100.
Template Condition	Options in the template conditions that are based on the DLP incident table. You can select any of the incident fields for building the email template trigger condition. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**. ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. **Note:** The conditions in the condition builder are case sensitive.
Target Users	Target users for the template when the conditions are met. The target users can be one of the following: ○ **All recipients**: Send the email to target users. ○ **Recipients in the group:** Send the email only to recipients within a particular group by using the filter option. ○ **Recipients matching the criteria**: Send the email to target users who match the criteria. You can use the filter to drill down target users based on the conditions. For example, city.
Email Template	Email template that you can select. You can define the variables to reuse existing content to add to the email notification. The **Category** and **Type** fields determine the variables that are available for selection. For example, let's say that the email category is set to incident notification and that the email type is a digest, then the variables for selection are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

	digest fields to accommodate the accumulation of multiple DLP incidents.
	
	Here is an example Email Body HTML of each email template:
	○ **Default template for Per incident approval notification**:
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	
	`- Date protection team`
	○ **Per incident approval request cancellation notification**
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	
	`- Data protection team`
	○ **Default template for Due date notification**:
	`Dear ${target_user.name},`
	
	`Following incidents require your response.`
	
	`${due_days_table}`
	
	`- Data protection team`
	○ **Default template for Per Incident user notification**:
	`Dear ${assigned_to.name},`
	
	`DLP Incident ${number} is assigned to you.`
	
	`Please review and submit your response.`
	
	`- Data protection team`
	○ **Default template for User incident notification**:
	`Hello ${target_user.name},`

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	``` You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_seve rity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ``` ○ **Default template for Escalation - Digest**: ``` Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table} - Data protection team ``` ○ **Default template for Escalation - Per Incident**: ``` Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team ``` ○ **Default template for Pending approval notification**: ``` Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

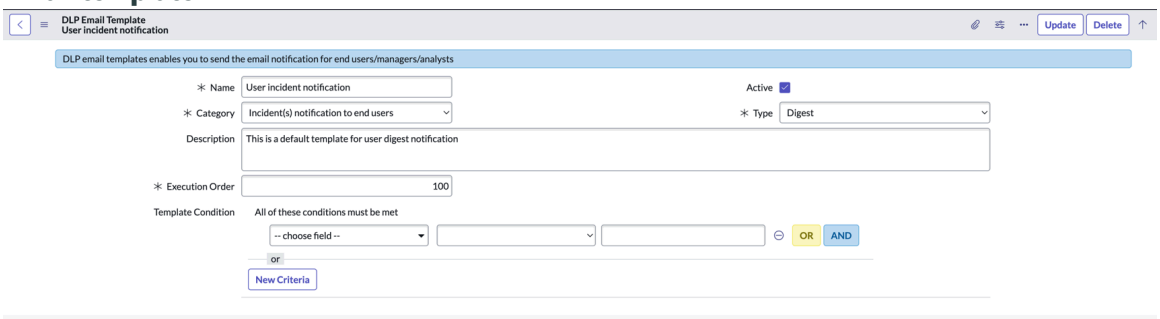
Field	Description
	``` - Data protection team ```
	○ **Default template for Per incident pending approval notification**: ``` Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team ```
	○ **Default template for Per incident rejection notification**: ``` Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team ```
	○ **Default template for Per incident user response notification**: ``` Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ```
	○ **Default template for User response completion notification**: ``` Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_respo nse_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_r esponse_completed}. ```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

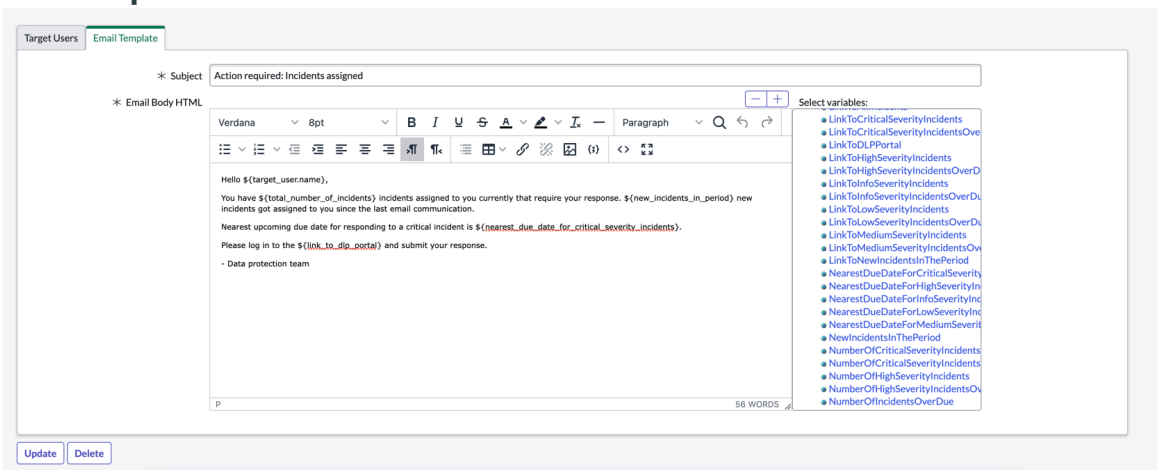
Example
The following example shows the DLP Email Template with the target users defined as all recipients.

Email template



The following example shows an email template with the subject "User incident notification" and a variable *new_incidents_in_period*. The email body contains multiple variables that are added from the Select variables column.

Email template variables



4. Click **Submit**.

Result
The end user receives a digest notification email with all the selected variable fields in the template.

Create a Data Loss Prevention Incident Response SLA trigger

Create a Data Loss Prevention Incident Response SLA trigger condition that enables a prompt and efficient response to an incident when triggered.

Before you begin
Role required:

- sn_dlir.admin - Create, update, and delete DLP SLA Triggers.
- sn_dlir.analyst.read - Read Trigger Table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **DLP Administration** > **SLA Triggers**.
2. Select **New** to create the SLA trigger.

Field	Description
Name	Name of the trigger
Order	Order in which the trigger is considered.
Active	Option to evaluate the SLA trigger.
Trigger when a DLP incident is updated	Option to evaluate the trigger condition on each update of the DLP incident.

3. Configure a condition by selecting the rule record and defining conditions in the **Trigger Condition** field.
   For example, the trigger condition to set SLAs on DLP incidents from an email scan source would be **[Scan Source][is][Email SMTP]**.
4. Select **Submit**.

Result

Once a task SLA record for a Data Loss Prevention Incident Response incident is created, the SLA records tab becomes visible for that particular incident in the workspace. This tab enables you to use an SLA system for your organization's task.

Create a Data Loss Prevention Incident Response SLA definition

Create a Data Loss Prevention Incident Response SLA definition that outlines the conditions and duration for responding to data breaches. Establishing clear expectations and protocols helps ensure a swift response to incidents, minimizing potential damage and enhancing overall data protection strategies.

Before you begin

Role required:

- sn_dlir.admin - Create, update, and delete DLP SLA definitions.
- sn_dlir.analyst.read - Read DLP SLA definitions.

Procedure

1. Navigate to **All** > **DLP Administration** > **SLA Definitions**.
2. Create an SLA definition.
   For a description of the field values, see DLP SLA Definition form.
3. Select **Submit**.

> **Note:** Due date rules, escalations and SLA definitions are mutually exclusive. An SLA definition primarily determines when a particular SLA will start to be effective, stop, pause, or be triggered.

Create assessments

Create and manage assessments to enable end users to respond to DLP incidents. You can use the assessments to gather information about the sensitive data exposed or leaked from the DLP incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task
DLP incident assessments help you identify potential threats and vulnerabilities to your data based on the end-user response. You can use this information to determine your end users' existing gaps, concerns, and expectations.

Procedure
1. Navigate to **All** > **DLP Administration** > **Assessments**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Incident Assessment

Field	Description
Name	Name of the DLP incident assessment.
Active	Option to indicate whether the DLP incident assessment is active.
Description	Unique description for this DLP incident assessment.
Assessment Introduction	Provide an introduction or context for your assessment. You can also use variables from the Select variables section to dynamically display certain fields.

4. Click **Submit**.
5. After creating an assessment, open the assessment and click **Assessment Designer**.
6. In the New Assessment section, select a type of assessment question under the Controls section.
7. Drag-and-drop the required assessment question type under the New Assessment section. For example, you can drag-and-drop the **Choice** control under the New Assessment or New Category section.
8. To add more categories for the assessment, click the  icon.
9. To modify an existing category, click the  icon.
10. After creating the different assessment questions for the first time, click **Save**, and then **Publish**.

Configure response option for your DLP incidents

Use this feature to configure the type of response that an end user or analyst should perform.

Before you begin
The base system DLP Incident Response application provides the following response options:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Assessment Complete
2. Deleted Content
3. Deleted File
4. Encrypted File
5. Masked Content
6. Report false positive
7. Report wrong owner
8. Request email release from quarantine

   Note: This option is available for the DLP Microsoft Exchange records.

9. Required for Business Process
10. Reviewed Entitlements

Role required:

- sn_dlir.admin
- sn_dlir.analyst and sn_dlir.analyst_read

Procedure

1. Navigate to **All** > **DLP Administration** > **Response Options**.

   By default, the base system provides two types of response option:

   a. **Basic**: A manual response option submitted by the user.

   b. **Advanced**: An automated response option triggers a flow designer sub flow when the user submits the response option.

2. Click **New**.
3. On the form, fill in the fields.

Response Option form of Type: Basic

Field	Description
Name	Enter the name of the incident response option.
Type	Option to select the response option type.

Response Option form of Type: Advanced

Field	Description
Name	Enter the name of the incident response option.
Type	Option to select the response option. By default, this field displays the following two types of options:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **Basic**: When you select this option while creating a new response option, you may have to add a response option name and the type. ○ **Advanced**: When you select this option, the following fields will be available for you to select: ▪ **Flow**: Select the flow designer sub flow. ▪ **Requires MID Server**: Select this check box if the selected flow uses the MID Server.
Flow	Select the required flow designer flow to activate the MID Application and MID Capability. When you are creating a sub flow for the response option, add the following sub flow inputs: **a. Name**: ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Type**: ▪ Reference (to DLP incident table) ▪ Sys ID for both MID Server application and MID Server Capability
Requires MID Server	Option to determine that MID server configuration. By enabling the **Requires MID Server** checkbox **MID Server Application** and **MID Server Capability** fields you can configure the MID Application and MID Capability. **Note:** Based on the MID Server Application and MID Server Capability configuration and if any MID is up and running then only the Response Option will be visible in the workspace.
MID Server Application	Select the required MID Server Application from the drop down list.
MID Server Capability	Select the required MID Server Capability from the drop down list.

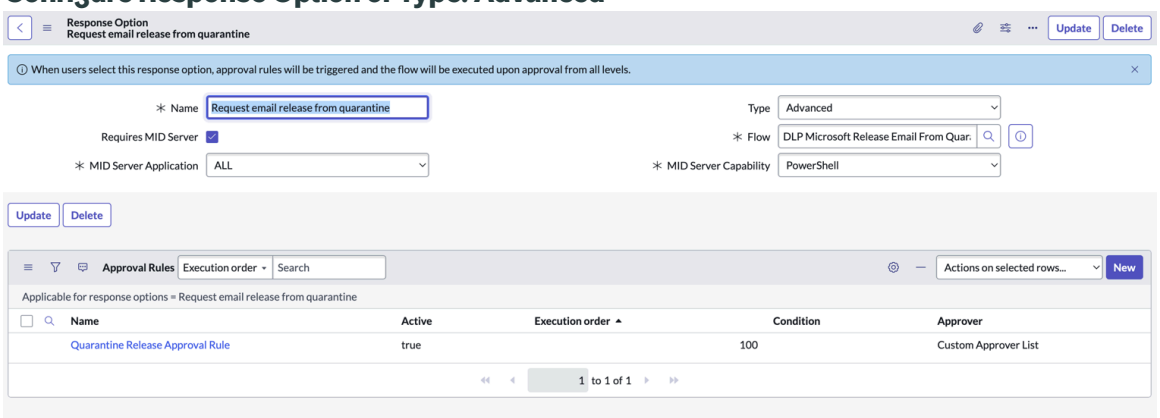
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If there is no MID server available for the selected MID Server Capability, the response option will not be visible. If you want a specific MID server from the list then you have to configure the MID app and make it visible in the list, and then at least one MID server which is configured should be up and running from the selected mid applications and should have the selected MID Server Capability.

4. Click **Submit**.

Note: If you are creating an **Advanced** type of response option, then the **Approval Rules** related list will be populated for you to configure the approval rule for that new response option. For more information, see Create Approval Rules.

Configure Response Option of Type: Advanced



Create incident response option rules

Create the incident response option rules that end user or analyst can use while responding to an incident.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

You can configure the type of response that an end user should perform based on the type of DLP incident. The base system DLP Incident Response application provides the following response options for users:

- Assessment Complete
- Deleted Content
- Deleted File
- Encrypted File
- Masked Content
- Report false positive
- Report wrong owner
- Required for Business Process
- Reviewed Entitlements

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, let's say that an end user reports a DLP incident as a false positive. The state for this incident is then automatically marked as closed because the target state that is configured by you is closed.

Procedure

1. Navigate to **All** > **DLP Administration** > **Incident Response Option Rules**.
2. Click **New**.
3. On the form, fill in the fields.

Incident Response Option Rules form

Field	Description
Name	Name of the incident response option.
Active	Option to indicate whether the incident response option is active.
Execution order	Priority of the incident response option. This field indicates the order in which the incident response options are executed when two or more incident response options share the triggering conditions. The incident response option with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default is 100.
Description	Unique description for this incident response option.
Default target state	The default target state that you configured.
Condition	Conditions in the condition builder. These conditions are based on the DLP incident table. To build a condition for the incident response options, select any of the incident fields. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**: ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**.

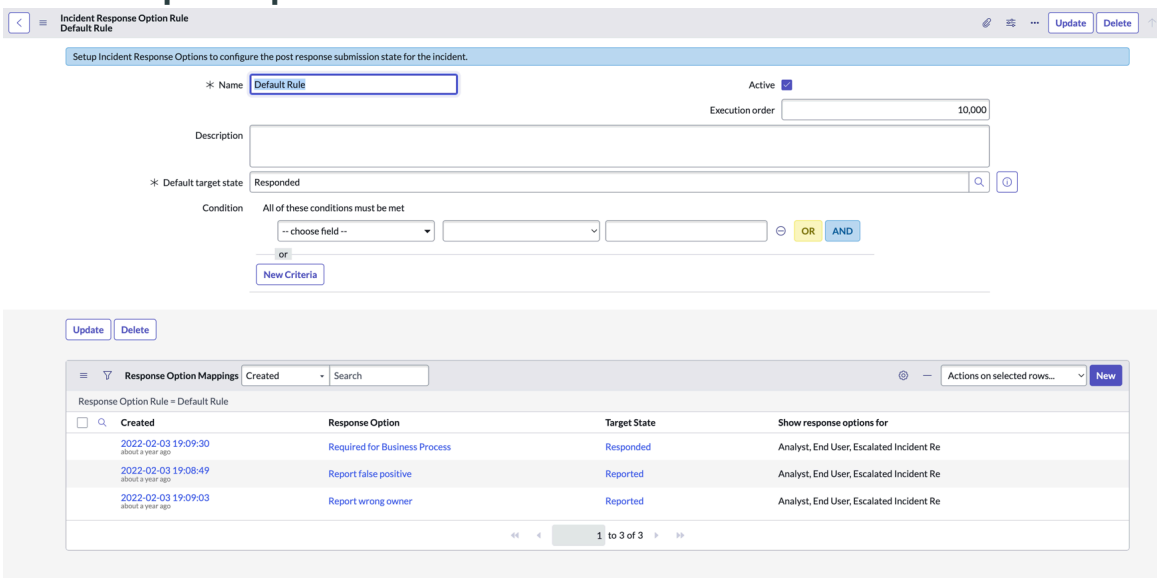
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The conditions in the condition builder are case sensitive.

Example

The following example shows the end-user action configuration for an endpoint. The condition requires the scan source to be an endpoint file system that then triggers this end-user action configuration. The mapping shows that the report wrong owner, report false positive, and deleted file are the response options available to the end user.

Incident Response Option Rule



4. In the **Response Option Mappings** section, click **New**.
5. On the form, fill in the fields.

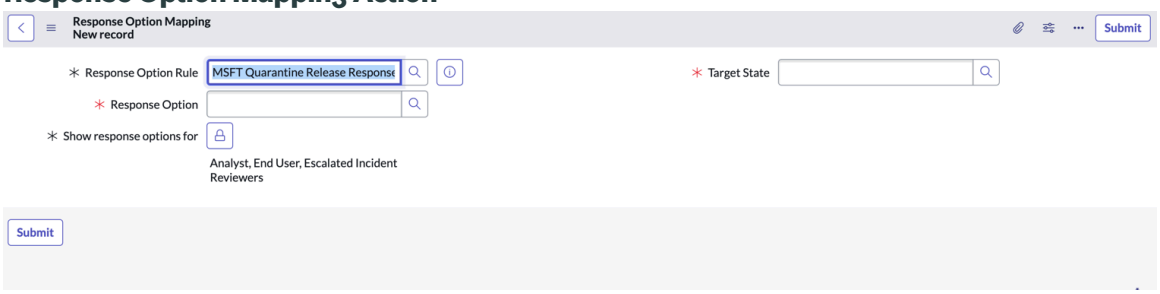
Response Option Mapping form

Response Option Rule	Name of the incident response option rule. For example, `SharePoint` implies that the scan source is SharePoint. You can either enter the name of the incident response or look up using search.
Response Option	Option to select the response option. You can either enter the response option or look up using search.
Target State	The target state of the DLP incident after the end user selects the appropriate action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

	Note: **a.** The **Target State** field will appear only when you select **Response Option** which is of **Type: Basic**. For more information on how the target state types are configured, see Configure response option for your DLP incidents. **b.** When a Response Option which is of **Type: Advanced** is selected, you will not be able to set the Target State and will be hidden. The Target State will be assigned based on the custom state that is configured from the flow designer sub flow.
Show response options for	Option to determine the user roles to show the response options for. You can choose from **Analyst**, **End user**, and **Escalated Analyst Reviewers** by using the unlock option. You are allowed to choose one or all the roles.

Response Option Mapping Action



6. Click **Submit**.

Create age chart configurations

Configure the age chart that appears in the Data Loss Prevention Incident Response (DLP IR) Ops portal. This chart shows the count of open incidents by the number of days.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

Procedure

1. Navigate to **All** > **DLP Administration** > **Age Chart Configuration**.
2. Review the age chart entries in the following table and customize the entries for your environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP Age Chart Configurations form

Name	Condition
0-30 days	Age of the open incident that is between 0 through 30 days.
31-60 days	Age of the open incident that is between 31 through 60 days.
61-90 days	Age of the open incident that is between 61 through 90 days.
90+ days	Age of the open incident that is over 90 days.

3. Add a new age chart configuration by clicking **New**.
4. In the Name field, enter a **Name** for the DLP age chart configuration.
5. Set the conditions for the DLP age chart configuration.

   a. To add conditions, click **AND** or **OR**.
      - If **AND** is selected, all conditions must be matched.
      - If **OR** is selected, either condition can be matched.

      Note: The conditions in the condition builder are case sensitive.

   b. To set a second filter condition, click **New Criteria**.

6. Click **Submit**.

Create user delegate configurations

Prevent certain executives in the organization from receiving notifications about the incidents assigned or escalated to them.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

Consider a scenario where the executive is a user who belongs to a leadership or executive group. The executive should not be sent emails about incident assignment or escalation. A delegated user can then take the necessary action on behalf of the executive.

Once a user has assigned a particular person, Henry, as a delegate, another user cannot assign Henry as a delegate again. Similarly, a delegate cannot assign another user as a delegate.

Procedure

1. Navigate to **All** > **DLP Administration** > **Delegate Configuration**.
2. Click **New**.
3. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Delegate Configuration form

Field	Description
User	Name of the user who needs a delegate for DLP incidents.
Delegate	Name of the user who can respond to the DLP incident on behalf of the original end user.

4. Click **Submit**.

Create repeat offender identification rules

Create repeat offender identification rules to identify users who repeat the same issue multiple times.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

You can identify repeat offenders by using certain rules or criteria. Data Loss Prevention Incident Response provides fields that you can use to identify repeat offenders.

Procedure

1. Navigate to **All** > **DLP Administration** > **Repeat offender identification rules**.
2. Click **New**.
3. On the form, fill in the fields.

Repeat offender identification rules form

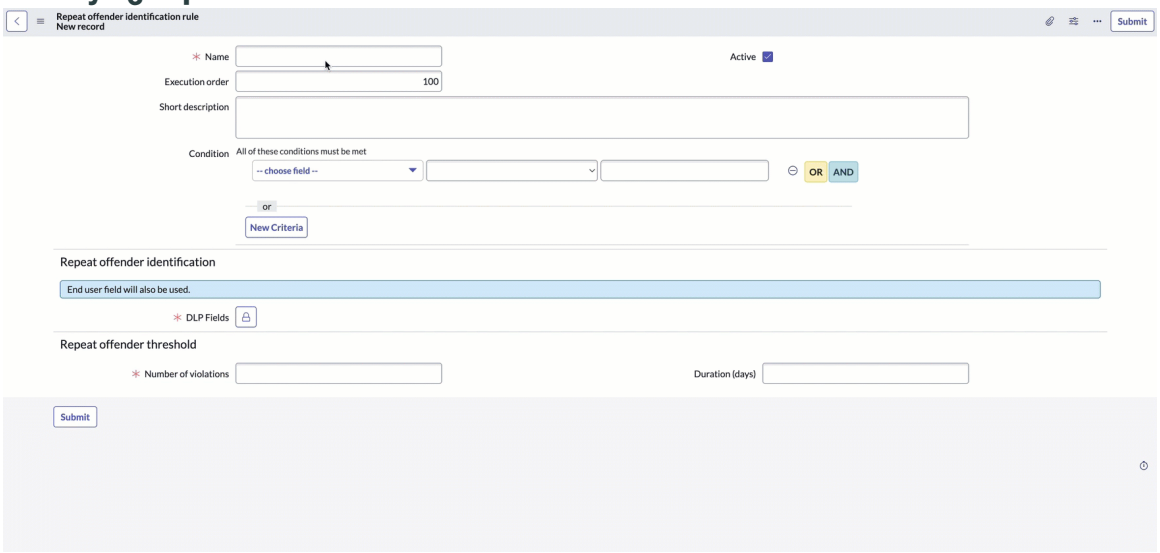
Field	Description
Name	Name of the repeat offender identification rule.
Execution order	Priority of the repeat offender identification rules. This field indicates the order in which the repeat offender identification rules are executed when two or more rules share the triggering conditions. The repeat offender identification rule with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default value is 100.
Short description	Unique description for this repeat offender identification rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Condition	Conditions in the condition builder that are based on the DLP incident table. You can select any of the incident fields for building the trigger condition for the repeat offender identification rule. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**: ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. **Note:** The conditions in the condition builder are case sensitive.
DLP fields	Identify repeat offenders based on the required DLP fields. Click on the  icon next to the DLP Fields to view the list of available DLP fields. Select the DLP fields that you want to use from the Available column and move them to the Selected column. For example, you can select the**File Name** and **File Owner** fields from the Available column and move them to the Selected column. Then, you can identify the repeat offenders based on the **File Name** and **File Owner** fields. Thus, if a user breaches the repeat offender threshold (number of violations and duration), and if the same user matches with the DLP fields, then that particular user is identified as a repeat offender.
Number of violations	Define the repeat offender threshold limit value. After the user repeats the same actions and breaches the specified number of violations, the user is identified as a repeat offender.
Duration (in days)	Define the repeat offender threshold limit in the form of days. After the user repeats the same actions and breaches the threshold duration, the user is identified as a repeat offender.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Identifying Repeat Offenders



4. Click **Submit**.

Create Additional Incident Data Fields

Create your Additional Incident Data Fields for the DLP incidents. You can create different types of Additional Incident Data Fields such as string, number, check box, choice, date and time, and use them in the DLP incident forms.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

Important: Additional Incident Data Fields for DLP incidents are supported only on the San Diego version or later.

About this task

Additional Incident Data Fields are associated with Field level restrictions, so if there are any Field level restrictions then it applies to Additional Incident Data Fields on the DLP Ops portal and End user portal.

Procedure

1. Navigate to **All** > **DLP Administration** > **Additional Incident Data Fields**.
2. Create an Additional Incident Data Fields by clicking **New**.
3. On the form, fill in the fields.

DLP Additional Incident Data Fields form

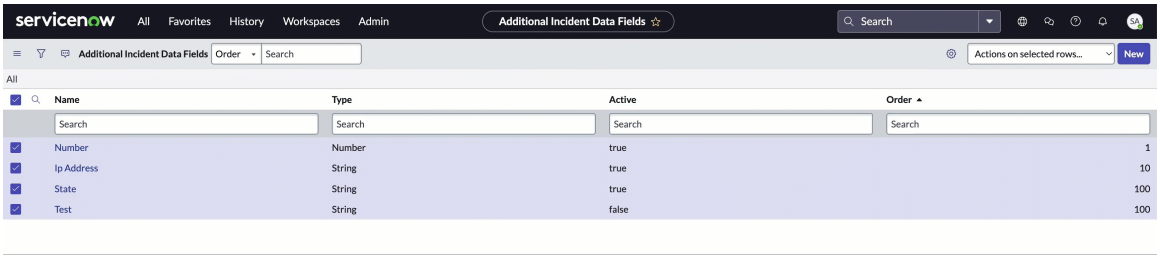
Field	Description
Name	Name of the Additional Incident Data Fields.
Type	Option to select the type of Additional Incident Data Fields. You can choose one of the following types:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **String** ○ **Number** ○ **Check box** ○ **Choice** If you select the Additional Incident Data Fields type as **Choice**, then after creating the Additional Incident Data Fields you can define the Additional Incident Data Fields choice options. To create an Additional Incident Data Fields choice option: **a.** Open the required Additional Incident Data Fields. **b.** In the Custom Choice Field Options section, click **New**. **c.** In the Option Name field, define the required option name. **d.** Click **Submit**. ○ **Date** ○ **Date/Time** **Note:** After you select a type for your new Additional Incident Data Fields, you are not allowed to modify it. If you want to modify the type, then you have to create a new Additional Incident Data Fields again with the required type.
Order	Option to choose the order in which the Additional Incident Data Fields should be displayed. You can define the order value for each Additional Incident Data Fields. The Additional Incident Data Fields are sorted based on the order values that you define. By default, the Additional Incident Data Fields are sorted in ascending order. You can sort the Additional Incident Data Fields in descending order by clicking on the **Order** column.
Active	Option to indicate whether the Additional Incident Data Fields is active.
Description	Description for the Additional Incident Data Fields you created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP Additional Incident Data Fields



4. Click **Submit**.

DLP SLA Definition form

Field descriptions for the DLP SLA Definition form used to create an SLA record.

Field	Description
Name	Name of the definition.
Type	Type of agreement, which in this case is SLA.
Target	Target used for filtering, searching and reporting on the agreement being defined. The available options are: • None • Response • Resolution
Table	Table that determines the records tracked by the SLA, which should be DLP SLA Task [sn_dlir_incident_sla_task].
Flow	Flow to run when the SLA definition attaches to a Task record, which should be Default SLA flow.
Duration Type	Method to calculate the duration of the SLA. The available options are: • User specified duration • 2 business days by 4pm • 3 business days by 4pm • Breach on Due Date • End of next business day • Next business day by 4pm
Duration	Length of time the SLA runs before it's marked Breached. This field is available only when User specified duration is selected from **Duration Type**.
Schedule source	Schedule to use while creating the task SLAs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Schedule	Hours during which the SLA timer runs. This set of schedules is defined in the core configuration.
Timezone Source	Timezone source to be used when creating task SLAs. The available options are: • The caller's timezone • The SLA definition's timezone • The CI location's timezone • The task location's timezone • The caller location's timezone
Active	Option to make the trigger effective when the start condition is met.
Tabs	
Start condition	Condition that initiates the SLA timer and activates the SLA.
Pause condition	Conditions under which the SLA is suspended, which increases the total elapsed time.
Cancel condition	Conditions under which the SLA is cancelled.
Reset condition	Conditions under which the active SLA is completed and a new SLA is established when the value of any field on the task record changes, changes to, or changes from a specific value in the record. For example, say the value of the **Location** field in the task record is 101 Broadway East, Seattle, WA. If you set the SLA reset condition to **[Location][changes from][101 Broadway East, Seattle, WA]**, any change in the value of the **Location** field resets the SLA of the task record.

Related topics

Create a Data Loss Prevention Incident Response SLA definition

Configure advanced settings

Configure the advanced settings to customize the incident display and behavior. For example, enable displaying the sensitive data on an incident and its clone, or specifying fields on the incident to identify the end users. In addition, activate and customize the evidence files preview properties.

Before you begin

Role required:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_dlir.admin
- sn_dlir.analyst and sn_dlir.analyst_read

About this task

Configure the advanced settings on the Data Loss Prevention Incident Response to customize the details to display for an incident or control the duration to identify a repeat offender.

Procedure

1. Navigate to **All** > **DLP Administration** > **Advanced Settings**.
2. On the form, fill in the fields.

Advanced Settings form

Field	Description
Should sensitive data which caused the violation be displayed on the incident	Option to choose whether you want to display the sensitive data that caused the violation on the DLP incident. By default, this option is enabled.
Should sensitive data which caused the violation be displayed on the cloned incidents as well?	Option to choose whether you want to display the sensitive data that caused the violation on the DLP cloned incident as well. By default, this option is turned off.
List of fields on the incident that are used to identify the end user	The list of fields on the incident of the Assignment Rule module that are used to identify the end user. You can also specify your own custom attributes to identify the end user.
Maximum number of incidents in a digest email	The maximum number of incidents that can be sent in a digest email. By default, the value is 100.
Repeat offense maximum duration (in days)	The maximum duration to identify a repeat offender. By default, the value is 90 days.
Quick mode to send emails	Option to validate emails and identify issues. You can perform the validation by enabling the **Yes** option. By default, this option is enabled.
This property is for setting the log verbosity of the application	The log verbosity level of the application, meaning the name of the type of information. You can also update the value to the following options: ○ **error** ○ **warn**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ **info** ○ **debug** By default, the value is **info**.
Should downloading the violating file of the reported incident be allowed	Option to download the violating file of the reported incident. By default, this option is **Yes**.
Exclude cloned and child incidents from reports	Option to exclude the cloned and child incidents from the reports. By default, this option is **Yes**.
Day(s) to wait for deleting match content on cloud storage after incident gets closed	Option to choose the number of wait days to clean up the match content of those incidents that are inactive for a specific time duration. By default, the value is 90. If the DLP incident is inactive after 90 days, the match content is cleaned up from the cloud storage.
Assign Incident to DLP Analyst group after last escalation level	Select this check box to assign the incident to the analyst after the last escalation level.
Allow users to access incidents post escalation	Select this check box to enable the assigned users to access the incidents after the escalation. When you select this option, all the users that were added to the escalation chain list can access the incidents.
List of fields on the "sys_user" table that are used to uniquely identify the user in DLP workspaces	Options to uniquely identify the user in the DLP workspaces. The options are email and user_name.
Allow analyst to edit completed assessment	Select this check box to enable the analyst to edit the completed assessment. When you select this option, the analysts can edit the Assessments, when unselected you can view the assessments in the Read-Only mode.
List of valid file extensions. This property is a comma separated string. Each token indicates an extension.	List of the valid file extensions. Keep the field empty to allow all file extensions.
Enabling this system property will display the Playbook tab under DLP Incidents and provide the option to manually trigger a playbook via the Add Playbook action	Option to display the Playbook tab and manually add the Playbook action. By default, this option is **Yes**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Evidence Files Preview Properties	
Enabling this system property activates the evidence file preview feature in the DLP analyst workspace. sn_dlir.enable_evidence_file_preview	Option to choose whether you want to preview the evidence files directly in the workspace. By default, this option is **Yes**.
This will allow DLP users to download the previewed evidence files. Once this property is enabled, users will see a download button in the document viewer to download the evidence file. sn_dlir.enable_download in_preview	Option to display the download button in the document viewer. The download button enables you to download the previewed evidence files. By default, this option is **Yes**.
This property determines the duration for which files will be temporarily retained for evidence file preview purposes. (in minutes) sn_dlir.preview_temp_files_cleanup_interval	The maximum duration for which files are temporarily stored for evidence file preview. By default, the value is 10. If the DLP incident is inactive after 10 minutes, the evidence file is cleaned up from the analyst workspace.
Enabling this property will extend the cleanup interval if evidence files are in use. This will allow the system to extend the expiry time of evidence files based on the value set in the system property "sn_dlir.preview_temp_files_cleanup_interval". sn_dlir.extend_cleanup_interval_on_usage	Option to extend the time before evidence files are deleted if they're being used. By default, this option is **Yes**.
The maximum duration to extend the cleanup interval of evidence files (in minutes). sn_dlir.max_extension_duration_for_cleanup	Option to select how long, in minutes, the system keeps your evidence files before cleaning them up. By default, the value is 60.

3. Select **Save**.

Monitor DLP Integration Run process

Track and monitor the ongoing ingestion or the integration run process. The integration run processes contains the statistics on how much the data was processed and the integration status.

Role required: sn_dlir.admin.

The integration run process lists the details on how many records are ingested. For example:

1. In Symantec integration, the process contains both child and parent integration runs. The parent record indicates the ingestion data and child record indicates the enrichment calls and custom attribute records.
2. In Microsoft integration, there is only parent record ingestion process to be run.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP Integration Run Processes: This displays the queue entries, status of queue entries, and fetched records.

The integration run contains the Source for which the integration profile and the integration run record is created, profile polling intervals, ingestion states and substates, incident count which indicates the number of records that are ingested.

1. Navigate to **DLP Administration** > **Integration Runs**.
2. Select the integration run from the list.
3. Navigate to the **DLP Integration Run Process**.
4. View the queue entry status of the record.

DLP Incident Access Restrictions

Manage the visibility of a particular DLP incident that contains sensitive information. You can use incident access restrictions to define who can access a particular DLP incident and restrict specific users or groups from accessing that incident.

Create field level restrictions

Set field level restrictions in DLP incidents to protect sensitive information from being exposed. You can use field level restrictions to control the users or groups who can access specific fields in the DLP incidents.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

Field level restrictions enable you to display only certain fields for specific users or groups, providing a more granular way to control the data a user can access. You can create a Field level restriction by defining the DLP incident matching conditions, selecting the users or groups to which these conditions apply, and then choosing the DLP fields that these users or groups can view.

Procedure

1. Navigate to **All** > **DLP Administration** > **Incident Access Restrictions** > **Field level restrictions**.
2. Click **New**.
3. On the form, fill in the fields.

DLP Field Level Restriction form

Field	Description
Name	Name of the field level restriction.
Active	Option to indicate whether the field level restriction is active.
Execution order	Priority of the field level restrictions. This field indicates the order in which the field level restrictions are executed when two or more field level restrictions share the triggering conditions.

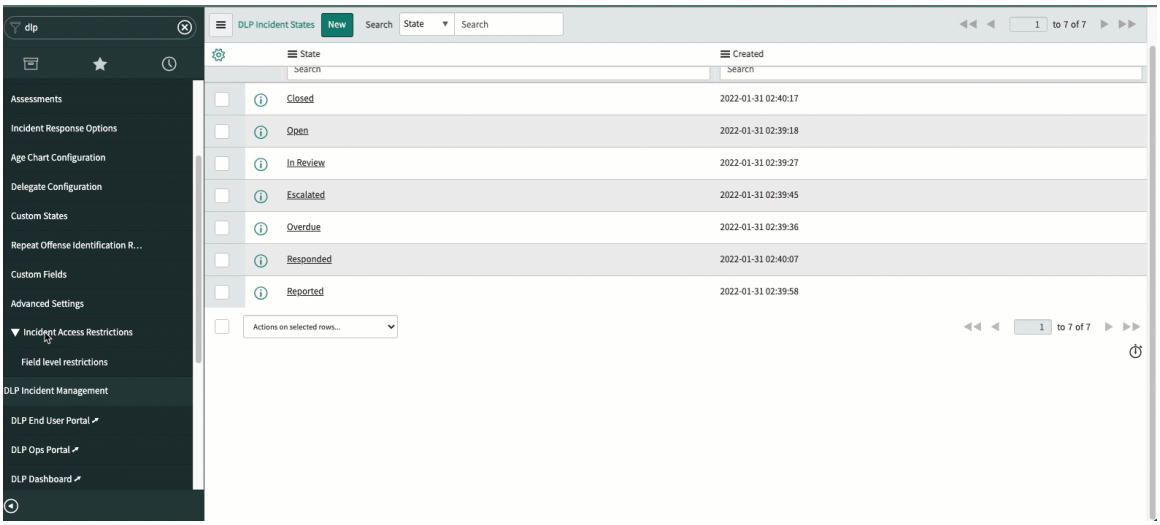
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	The field level restriction with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default value is 100.
Short description	Unique description for this field level restriction.
Incident matching condition	Options in the incident that matches the defined conditions. You can select any of the incident fields for defining the trigger condition for the field level restrictions. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**: ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**. For example, you can select the field as `Policy name`and set the condition as `in`, and `Name of the policy`. **Note:** The conditions in the condition builder are case sensitive.
Applies to	Option to apply the incident matching conditions to specific users or groups. You can apply the conditions to the following: ○ **All end users**: Option to select all end users to whom the DLP incident conditions are applicable. ○ **All reviewers of escalated incidents**: Option to select all reviewers of escalated incidents to whom the DLP incident conditions are applicable. This refers to all DLP incidents escalated to the Manager. ○ **Users**: Click the  icon to add a particular user from the list to whom the DLP incident conditions are applicable. You can also add a user by using their email address or search option. For example, Legal Manager. To add yourself as the user to whom the DLP conditions are applicable, click the  ○ **Groups**: Click the  icon to add a particular group from the list to whom the DLP incident conditions are applicable. You can also add a group by using the search option. For example, Survey creators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Allow access to following fields only	○ **DLP Fields**: Option to define the DLP fields that you want allow access to the selected users or groups. Select the DLP fields that you want to allow access to from the Available column and move them to the Selected column. **Note:** The selected users or groups will be able to access only the selected DLP fields. For example, you can select the**Assigned to** and **Opened** fields from the Available column and move them to the Selected column. Then, the selected users or groups have access only to the Assigned to and Opened fields. ○ **Upload attachments**: Option to indicate whether you want to allow the selected users or groups to upload attachments. ○ **Custom Fields**: Option to define the custom fields that you want allow access to the selected users or groups. You can view the custom fields that you have created under the Available column. Select the custom fields that you want to allow access to from the Available column and move them to the Selected column. **Important:** ▪ Custom fields for DLP incidents are supported only on the San Diego version or later. ▪ The selected users or groups will be able to access only the selected Custom fields.

DLP Field Level Restriction



4. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create record level restrictions

Set record level restrictions in DLP incidents to protect sensitive records from being exposed. You can use record level restrictions to control the users or groups who can access specific records in the DLP incidents.

Before you begin

Role required:

- sn_dlir.admin - Create, edit, and delete.
- sn_dlir.analyst and sn_dlir.analyst_read - View (read-only).

About this task

Record level restrictions enable you to provide access to records only for specific users or groups, providing a more granular way to control the records a user can access. You can create a record level restriction by defining the DLP incident matching conditions, selecting the users or groups to which these conditions apply, and then choosing the DLP records that these users or groups can view.

Procedure

1. Navigate to **All** > **DLP Administration** > **Incident Access Restrictions** > **Record level restrictions**.
2. Click **New**.
3. On the form, fill in the fields.

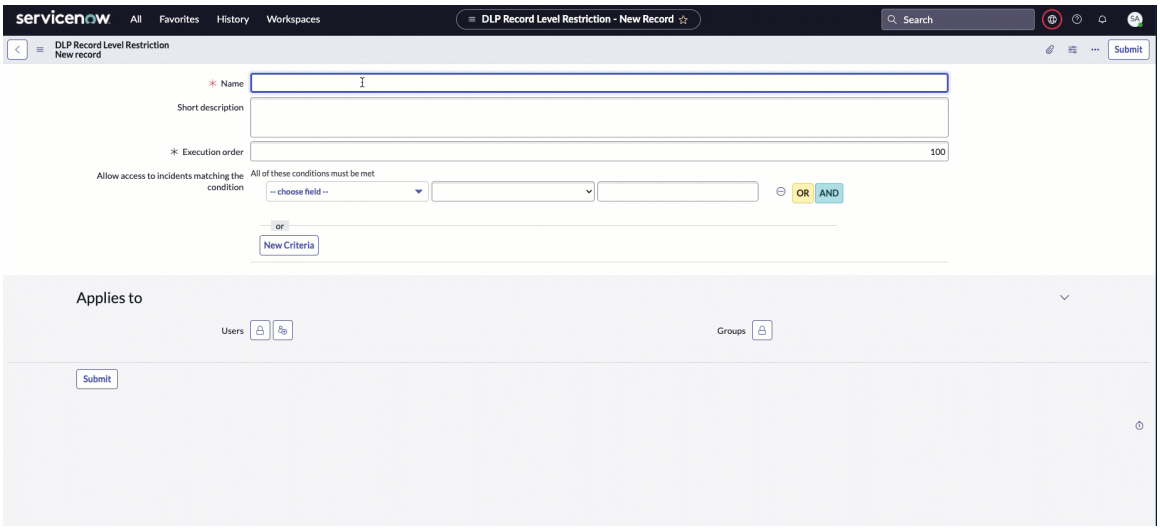
DLP Record Level Restriction form

Field	Description
Name	Name of the record level restriction.
Short description	Unique description for this record level restriction.
Execution order	Priority of the record level restrictions. This field indicates the order in which the record level restrictions are executed when two or more record level restrictions share the triggering conditions. The record level restriction with the lowest number has the highest priority. To set the order of operation, enter a value. For example, 100, 200, or any other number. The default value is 100.
Allow access to incidents matching the condition	Options enable access to the incidents that matches the defined conditions. You can select any of the incident fields for defining the trigger condition for the record level restrictions. Use the lists and fields of the conditions builder to set the filters for the first row. To add more conditions, click **AND** or **OR**: ○ If **AND** is selected, all conditions must be matched. ○ If **OR** is selected, either condition can be matched. To set a second filter condition, click **New Criteria**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: The conditions in the condition builder are case sensitive. For example, you can select the field as `Active`and set the condition as `is`, and `true`.
Applies to	Option to apply record level restrictions to specific users or groups. You can apply the conditions as follows: ○ **Users**: Click the icon to add a particular user from the list to whom the selected record is applicable. You can also add a user by using their email address or search option. For example, Legal Manager. To add yourself as the user to whom the record is applicable, click the . For example, System Administrator. ○ **Groups**: Click the icon to add a particular group from the list to whom the selected record is applicable. You can also add a group by using the search option. For example, Survey creators.

DLP Record Level Restriction



4. Click **Submit**.

DLP Incidents Archival

The Data Loss Prevention Incident Response is provisioned with one archival rule in the base system for the DLP incident table. The related records are also added in the base system to the DLP incident archive rule.

Before you begin

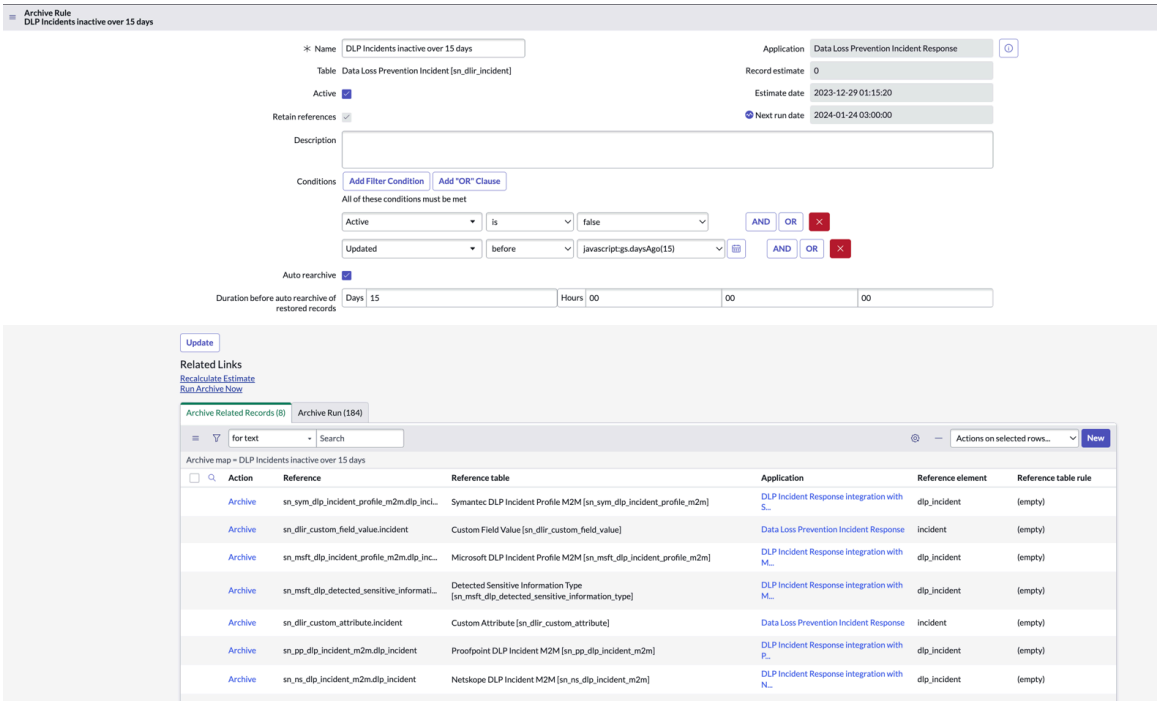
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Archiving** > **Archive Rules**.
   The system archiving rules that are in the base system are displayed.
2. View the DLP archiving rule.

> **Note:** **DLP Incidents inactive over 15 days** is the default base system archiving rule for DLP incidents. You can modify the archiving rule if necessary. This rule signifies that the incidents that are inactive above 15 days are automatically archived.



> **Note:** For information on how the archival rules are created, see Create an archive rule.
>
> For information on how to view the archived incidents, see View archived DLP incidents.

3. **Optional:** **Update** the rule.

Archive DLP related records

Use the Archive Related Records related list for DLP incidents to add the related records to the archive rule.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Archiving** > **Archive Rules**.
2. Select **DLP Incidents inactive over 15 days** archiving rule.
3. Go to **Archive Related Records** related list.
4. View the DLP related records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Reference Table
DLP Incident Response integration with Symantec	Symantec DLP Incident Profile M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Custom Field Value [sn_dlir_custom_field_value]
DLP Incident Response integration with Microsoft	Microsoft DLP Incident Profile M2M [sn_msft_dlp_incident_profile_m2m]
DLP Incident Response integration with Microsoft	Detected Sensitive Information Type [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	Custom Attribute [sn_dlir_custom_attribute]
DLP Incident Response integration with Proofpoint	Proofpoint DLP Incident M2M [sn_pp_dlp_incident_m2m]
DLP Incident Response integration with Netskope	Netskope DLP Incident M2M [sn_ns_dlp_incident_m2m]
DLP Incident Response integration with Symantec	Detected Sensitive Information Type [sn_sym_dlp_detected_sensitive_information_type]

Note: All the system tables such as Emails, Assessments, Attachments will automatically direct to the archived DLP record.

5. Select the archive related record rule you want to archive.

Note: For more information on how to add more related records, see Archive DLP related records on ServiceNow AI Platform.

Data Loss Prevention Incident Response Incident Management

Use the Data Loss Prevention Incident Response Incident Management to update and manage incidents by leveraging the DLP User Workspace, DLP Analyst Workspace, and DLP Dashboard.

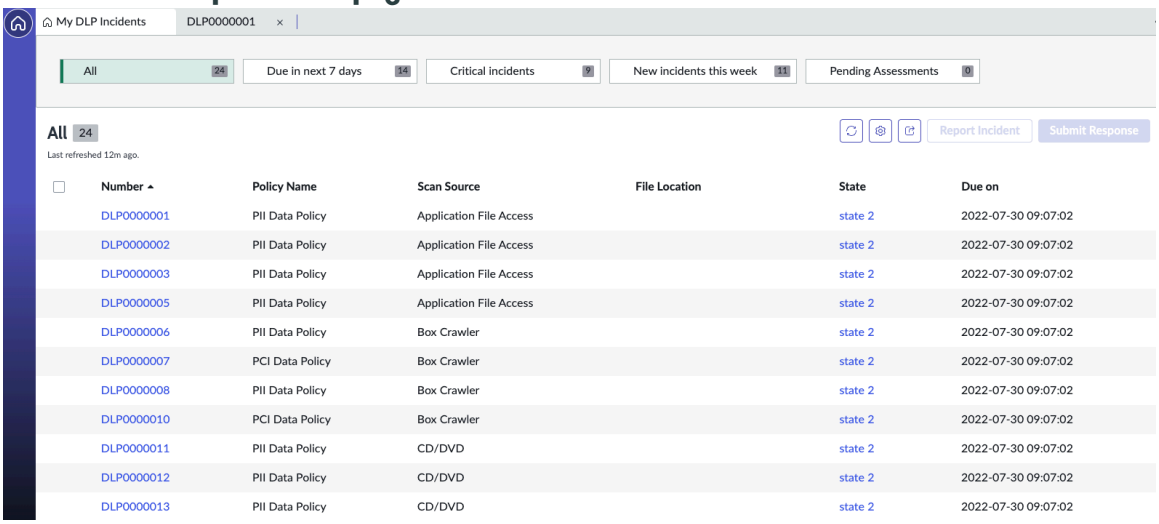
Data Loss Prevention Incident Response User Workspace

The Data Loss Prevention Incident Response (DLP IR) User Workspace is a workspace where end users, managers, and approvers can respond to the assigned DLP incidents. The end users, managers, and approvers can then respond to the incidents by specifying the correct actions.

You can also create and manage assessments to enable end users to respond to DLP incidents. The workspace consists of a landing page and list views that let you see the assigned DLP incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP User Workspace homepage



Report or respond to DLP incidents

Access the Data Loss Prevention Incident Response (DLP) User workspace, review the assigned DLP incidents, and report or respond to the incidents.

Before you begin

Role required:

- Any valid user/employee

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP User Workspace**.
   The My DLP Incidents page opens in a new tab.
2. Click a list view to review the incidents that are assigned to you.

List view	Description
All	View all the assigned incidents.
Due in the next 7 days	View all the incidents that are due in the next 7 days.
Critical incidents	View all the incidents with the severity label critical.
New incidents this week	View all the incidents that are assigned this week.
Pending Assessments	View all the assessments that are still pending.

3. You can review the DLP incidents using two ways:

   a. The first way is to locate and select one or more DLP incidents that you want to review, and click the check box next to the incidents.

   b. Choose the option that is appropriate for you.

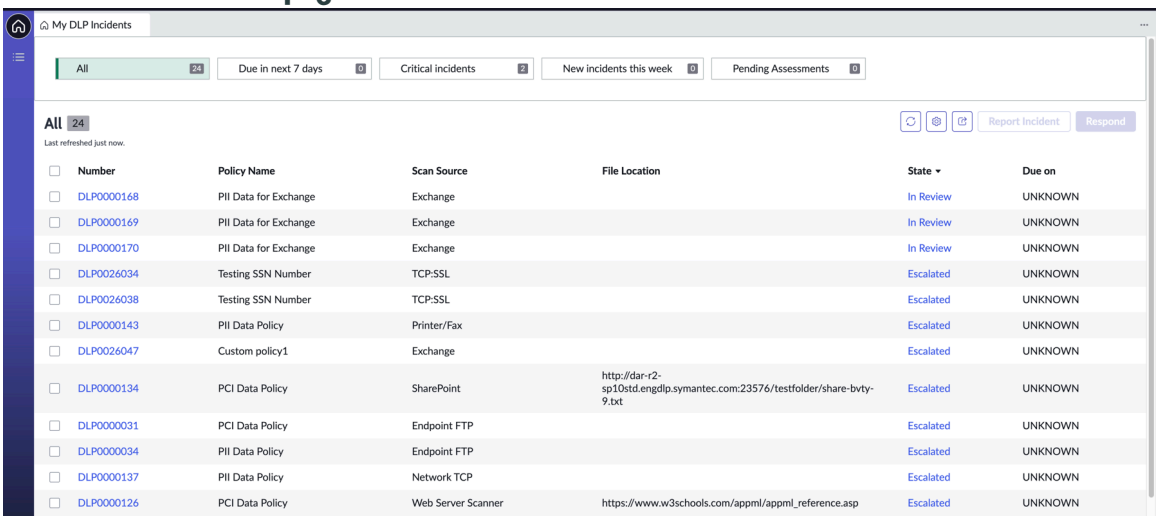
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP End User portal homepage

Option	Description
Refresh List	Option to refresh the list of DLP incidents if you made an update.
List Actions	List of actions that you can perform. Choices are as follows: ▪ **Save as** ▪ **Edit columns** ▪ **Reset widths** **Note:** When you have your own custom list which is created under **My Lists** section configured for your workspace, you will be able to perform the below additional list actions as well: ▪ **Rename** ▪ **Save** ▪ **Delete**
Copy URL for All	Option to copy the URLs of all the DLP incidents.
Report Incident	Action to report the incident as false positive or wrong owner. For example, you can report a wrong owner and suggest another owner or report the incident as a false positive.
Respond	Respond to an incident by selecting an incident response option. For example, user delete a file violating a DLP policy, the user can choose the option **Deleted File** to submit manual acknowledgement that the file has been deleted and provide comments. From here you can also select advanced response options. For example, **Request email release from quarantine**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DLP User Portal homepage



c. The second way is to click a particular DLP incident to open it.
The **Details** tab displays the following sections:

- Details: You can view the details of the DLP incident such as incident number, severity, file name.
- Compose: To add comments about the DLP incident that is visible to everyone, enter the comments in the Comments tab. To add comments that are visible to certain people, enter the comments in the Work notes (Private) tab.
- Activity: You can view the details of the different activities on the DLP incident.
- Attachments: If you have any attachments related to the DLP incident, click **Browse** and select the attachment from your local drive.

  The **Additional Details** tab displays all the additional information about the DLP incident including custom fields.

  Important:
  - Custom fields for DLP incidents are supported only on the San Diego version or later.
  - If there are any custom fields data available for a particular DLP incident, you can view them under the **Additional Details** tab. If there are no custom fields for the DLP incident, you would see a blank page.

- **Detected Sensitive Information Type**: Displays the incident detected sensitive information.

  Note: This related list is visible only for the DLP Incidents created for Microsoft or Symantec integrations. Within the Microsoft or Symantec incident record, whenever the user accesses the detected sensitive information type record, the highlighted match content with respect to that integration is displayed.

d. Choose the option that is appropriate for you.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

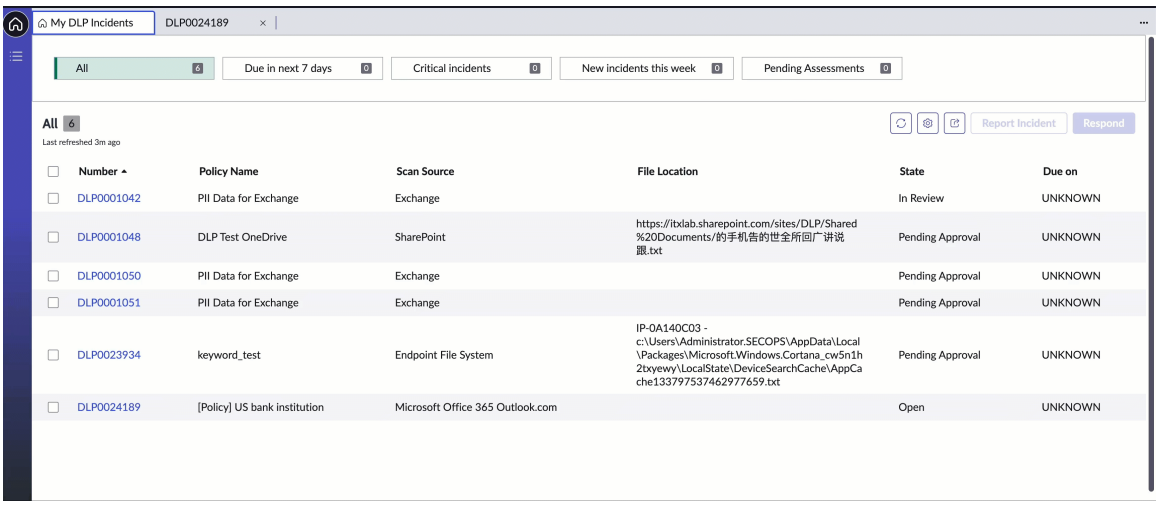
Option	Description
Report False Positive	Action to report that the DLP incident has been wrongly triggered or created. You can mention the details of why you've marked the incident as false positive in the Comments field.
Report Wrong Owner	Action to report that the DLP incident has been assigned to the incorrect user. If you know the correct owner for the incident, you can select the owner's name in the Suggest Owner field. To add any additional details, use the Comments field.
Respond	Respond to an incident by selecting an incident response option. For example, user delete a file violating a DLP policy, the user can choose the option **Deleted File** to submit manual acknowledgement that the file has been deleted and provide comments. From here you can also select advanced response options. For example, **Request email release from quarantine**.

e. Select the **Respond** button after answering the analyst query.
A pop-up to submit an incident response appears. Select the response from the drop-down menu and add comments.

f. Select **Submit**.
A banner appears confirming that your response has been submitted successfully.

Note: The incident is assigned to the corresponding approver or analyst and the end user will loose the access to the incident.

DLP Incident Actions

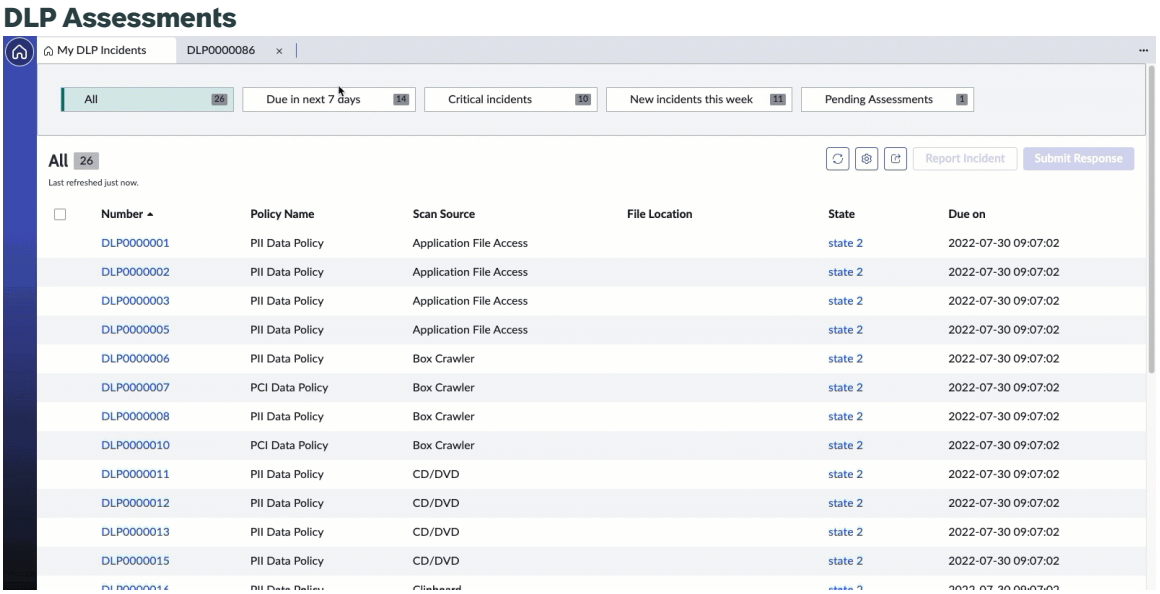


4. To take assessments, select the **Pending Assessments** list view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Click a particular assessment number to open it.

b. Answer the assessment questions, and click **Save** or **Submit** based on your requirements.



5. Click on the **Instructions** card section which is displayed on top of all the fields in the DLP incident form view, to view the additional information about a particular incident.

   Note: This section on the workspace guides the users on the incident information, which helps in understanding the next steps of the incident resolution.

   The user instructions card displays two different headers which provides you more information about a specific incident on the form view. Click on any user instruction header to know the additional details.

   For more information, see Create user instructions templates and Configure DLP UI user instructions.

Working with my approvals module

My Approvals module will be available on DLP Users Workspace to the logged in users. Users can approve or reject the assign approval requests from here.

Before you begin

Role required:

- End user
- Manager
- Approver

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP User Workspace**.
   The **My DLP Incidents** page will be displayed in a new tab.
2. Click on the **My Approvals** module present under **My DLP Incidents** module.
   My Approvals list view will be displayed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Approver can approve or reject the requests from the list view of **My Approvals** page. One can approver or reject the multiple requests from the list view.

Approver can view the details of assigned request on the form view. By clicking the **Approve** or **Reject** action from the form view, one can approve or reject the Individual request.

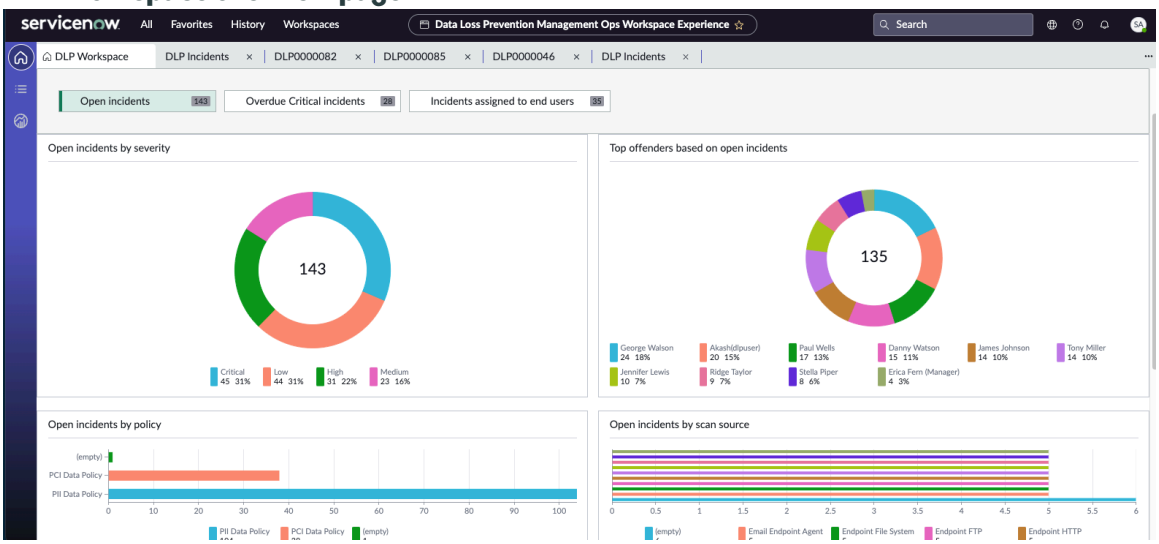
Note: To view the DLP Incident details, click on info icon available on the **Approve** field.

Data Loss Prevention Incident Response Analyst Workspace

Use the Data Loss Prevention Incident Response (DLP IR) Analyst Workspace to view the DLP incidents. Assign the incidents to end users for resolution and more.

The DLP workspace consists of a home page with dashboards, list views, and form views that let you monitor DLP incidents.

DLP Workspace overview page



Review and assign your DLP incidents

Access the Data Loss Prevention Incident Response (DLP IR) Analyst Workspace so that you can review the DLP incidents and assign or resolve them. You can track trends on incidents by severity, top offenders, incidents by scan source, and incidents by policy.

Before you begin

Role required:

- sn_dlir.analyst - Edit and view DLP incidents.
- sn_dlir.analyst_read and sn_dlir.read - View DLP Incidents.

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
   The DLP Workspace My Incidents ops list page opens in a new tab.
2. Click on the **DLP Workspace** home icon to view the workspace homepage view.
3. Review the dashboard widgets to identify trends by incidents by severity, top offenders, incidents by scan source, and incidents by policy.
4. Click the appropriate filters on the home page to view the widgets by their various categories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Filters	Description
Open incidents	View all open incidents.
Overdue critical incidents	View the incidents that have the critical severity label and that are overdue.
Incidents assigned to end users	View the incidents that are assigned to end users.

5. You can review and assign the DLP incidents using two ways:

   a. The first way is to locate and select one or more DLP incidents that you want to review, and click the check box next to the incidents.

   b. Choose the option that is appropriate for you.

Option	Description
Refresh List	Option to refresh the list of DLP incidents when you make an update.
List Actions	List of actions that you can perform. Choices are as follows: ▪ **Save as** ▪ **Edit columns** ▪ **Reset widths** **Note:** When you have your own custom list which is created under **My Lists** section configured for your workspace, you will be able to perform the below additional list actions as well: ▪ **Rename** ▪ **Save** ▪ **Delete**
Copy URL for All	Option to copy the URLs of all the DLP incidents.
Show filter panel	Option to drill down the required incidents using the filter option. i. Click the filter on the top-left of the page, and select **Advanced view**. ii. Use an existing filter or build your own by adding conditions that contain a field, operator, and values. iii. To add more conditions, click **AND** or **OR**:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	▪ If **AND** is selected, all conditions must be matched. ▪ If **OR** is selected, either condition can be matched. **iv.** Click **Update**.
Assign Incident	Action to determine whom to assign the DLP incident to. Choices are as follows: ▪ **Assign incident to**: Option to assign the incident to an analyst, end user, or someone else. ▪ **User**: Option to determine which user that the incident should be assigned to. ▪ **Incident state pre-user response**: Option to determine which state that the incident should be in before the user responds. It can also be a custom state. ▪ **Attach assessment**: Option to indicate whether you want to attach an assessment to the incident. If enabled, below options will be available: ▪ **Assessment template**: Option to select an assessment template for the DLP incident. ▪ **Incident state post user response** Option to select which state that the DLP incident should be in after the user responds.
Respond	Respond to an incident by selecting an incident response option. For example, user delete a file violating a DLP policy, the user can choose the option **Deleted File** to submit manual acknowledgement that the file has been deleted and provide comments. From here you can also select advanced response options. For example, **Request email release from quarantine**.
Escalate	Action to escalate the incident. You can escalate the incident by selecting the user that you want to escalate it to. You can also any additional information in the Comments field.
Update State	Action to update the state of the incident. You can update the state of the incident by select one of the states from the drop-down options. It can also be a custom state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Close	Action to close the incidents. Select the corresponding **Closure code** from the drop down list and add closure comments. The **Close** feature in Data Loss Prevention Incident Response is done both asynchronously and synchronously from the list view. **i.** Synchronous closure: When closing incidents synchronously, it means that the closure action is performed immediately. When you select multiple incidents for closure and if the incident count is less than or equal to 100 then the incidents are closed foreground from the DLP incidents list view. Here 100 is the default value. **ii.** Asynchronous closure: This implies that the closure request is submitted and the application runs the request in the background if the selected incidents count is greater than 100. You need to refresh the DLP incidents list view to see the updated the incidents status. **Note:** ▪ The selected incidents count for both asynchronous or synchronous closure is configured using the system property *sn_dlir.closure_sync_count_limit*. ▪ By default the incident count is set to 100.

c. The second way is to click a particular DLP incident to open it.

- **Details** tab: Displays the following sections:
  - **Details**: You can view the details of the DLP incident such as Incident number, Severity, File name, and so on. You are also provided with the ability to modify the Severity, State, End user, and DLP Analyst group fields respectively and save them.
  - **Compose**: To add comments about the DLP incident that is visible to everyone, enter the comments in the Comments tab. To add comments that are visible to certain people, enter the comments in the Work notes (Private) tab.
  - **Activity**: You can view the details of the different activities on the DLP incident.
  - **Attachments**: If you have any attachments related to the DLP incident, click **Browse** and select the attachment from your local drive.
- **Additional Details** tab: Displays all the additional information about the DLP incident including custom fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important:

- Custom fields for DLP incidents are supported only on the San Diego version or later.
- You can use the **Additional Details** tab to see if any custom fields have been created for a particular DLP incident or not.

- **Custom attributes** tab: Displays the list of custom attributes related to the DLP incident.
- **Other incidents from end user**: Displays the incident from the same end user. One can consolidate incidents by performing the **Add as child incident** action from this related list.
- **Detected Sensitive Information type**: Displays the incident detected sensitive information.

  Note: This related list is visible only for the DLP Incidents created for Microsoft or Symantec integrations. Within the Microsoft or Symantec incident record, whenever the user accesses the detected sensitive information type record, the highlighted match content with respect to that integration is displayed.

- **Child Incidents**: Displays the child incidents created manually (by performing the 'Add as child incident' action) or from the DLP consolidation rules. One can unlink the child incident by performing the 'Unlink child incident' from this related list.
- **Cloned incidents**: Displays the cloned incidents from the parent incident. By clicking on the **Clone incident** action of the form view, you can create a new cloned incident.
- **Assessments** tab: Displays the list of assessments that are assigned to the DLP incident.

d. Choose the option that is appropriate for you.

Option	Description
Assign Incident	Action to determine whom to assign the DLP incident to. Choices are as follows: ▪ **Assign incident to**: Option to assign the incident to an analyst, end user, or someone else. ▪ **User**: Option to select which user that the incident should be assigned to. ▪ **Incident state pre-user response**: Option to select which state that the incident should be in before the user responds. It can also be a custom state. ▪ **Attach assessment**: Option to indicate whether you want to attach an assessment to the incident. If enabled, below options will be available:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	▪ **Assessment template**: Option to select an assessment template for the DLP incident. ▪ **Incident state post user response**: Option to select which state that the DLP incident should be in after the user responds.
Cancel Approval	Action to cancel the approval request. This action will be visible to analysts on the form view only when the DLP Incident is in **Pending Approval** state. The available options are: ▪ **Assign incident to**: Option to assign the incident to no one, to an analyst, or to someone else. ▪ **User**: Option to select which user that the incident should be assigned to. ▪ **Post cancellation incident state**: Option to select which state that the incident should be in after canceling the request. ▪ **Comments**: To provide additional details for cancellation.
Assign Assessment	Action to attach an assessment while assigning the incident. Choices are follows: ▪ **Assessment template**: Option to select an assessment template for the DLP incident. ▪ **Incident state post user response**: Option to select which state that the DLP incident should be in after the user responds.
Download File	Action to download the file or email that has the violating content. This action can be performed for incidents created for Microsoft OneDrive, SharePoint Online, or Exchange Online.
Save	Action to save any changes that you made. You have an option to modify the Severity, State and End user fields of the DLP incident and save them.
Respond	Respond to an incident by selecting an incident response option. For example, user delete a file violating a DLP policy, the user can choose the option **Deleted File** to submit manual acknowledgement that the file has been deleted and provide comments.

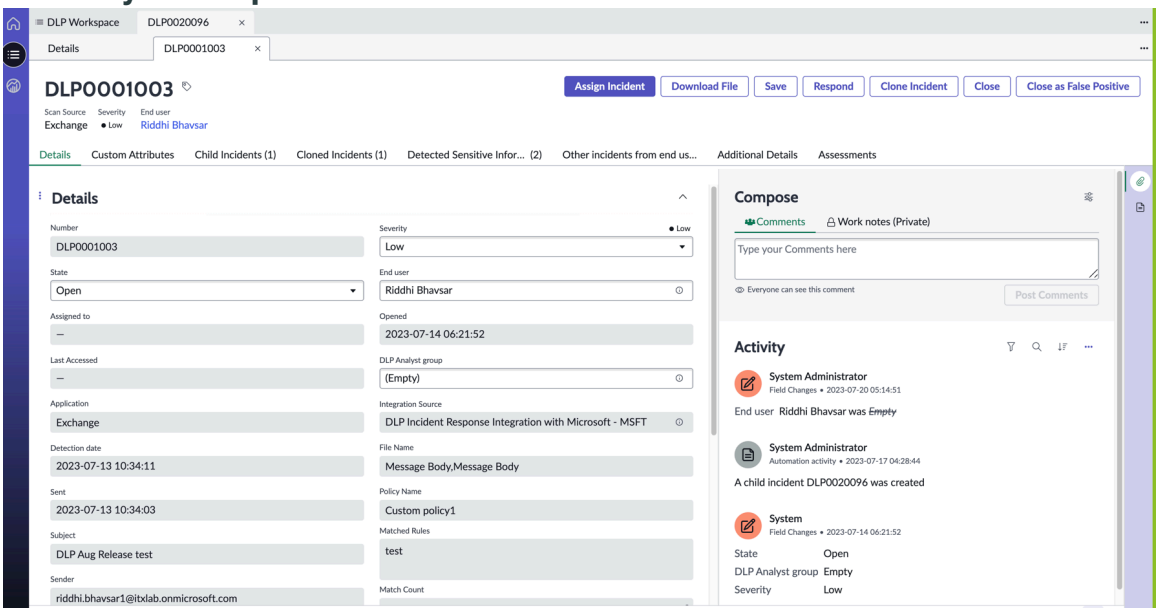
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	From here you can also select the advanced response options. **For example: Request email release from quarantine**.
Escalate	Action to escalate the incident. You can escalate the incident by selecting the user that you want to escalate it to. You can also any additional information in the Comments field.
Clone Incident	Action to create a clone incident if the incident record impacts multiple users. You can assign the cloned incidents to multiple stakeholders such as legal/IT. After you create a clone incident record, a new **Cloned Incidents** tab gets created under the parent DLP incident and all the cloned incidents are listed in this view. **Note:** ▪ If the parent DLP incident record is closed, then all the cloned incident records will close automatically. ▪ If a DLP incident record contains a cloned incident, it cannot be assigned to end users. The Parent DLP incident records can be managed only by users with the Analyst role. ▪ You also have an option to automatically update the parent state based on the state of the cloned incidents in the Default Configuration module. For example, if all the cloned incidents are moved to the Escalated state, then the parent incident will also be moved to the Escalated state.
Close	Action to close the incident. You must select the corresponding **Closure code** from the drop down list and add any closure comments, if required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Close as false positive	Action to close the incident as false positive. You can also add any additional comments before closing the incident.

DLP Analyst Workspace



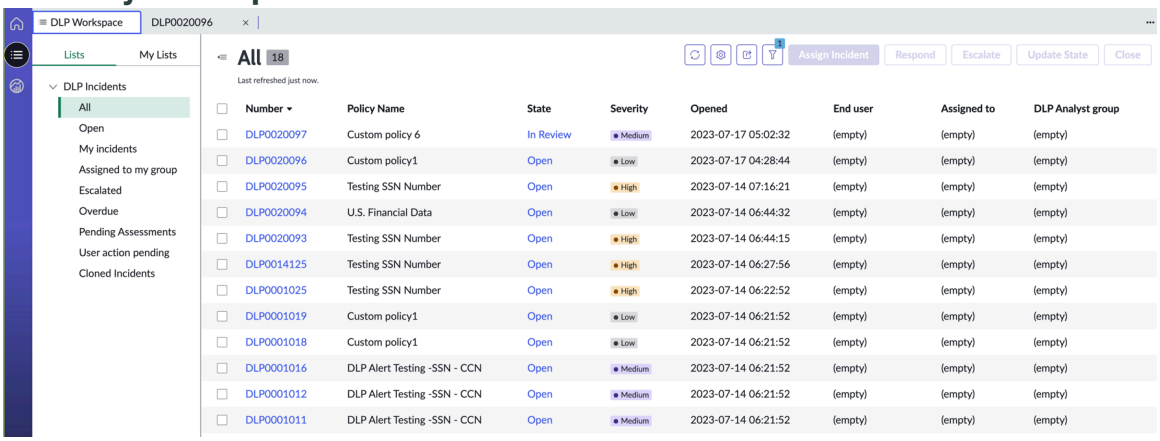
6. You can see the List view from the homepage by going to the top-left of the page and clicking the **Lists** tab.
   The Lists category consists of the default and customized list pages for DLP incidents.
   - **Lists** tab: Default lists for DLP incidents. The following are the default lists:
     - All
     - Open
     - My Incidents
     - Assigned to my group
     - Escalated
     - Overdue
     - Pending Assessments
     - User action pending
     - Cloned Incidents
     - Archived Incidents
   - **My Lists** tab: Displays any lists that you've renamed and any lists that you created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Example

The following example shows the DLP workspace with the list view categories. The **All** list view option is selected.

DLP Analyst Workspace Lists view



Preview evidence files

Preview Data Loss Prevention Incident Response evidence files in the DLP IR Analyst workspace.

Before you begin

Important: While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format. If you don't want to store the evidence files, disable the Evidence Files preview feature. For more information, see Configure advanced settings.

Role required: sn_dlir.analyst

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. From the contextual sidebar, select the Evidence files icon ( ).
4. On the **Evidence Files** tab, select the **Evidence File** card to preview the evidence files in the document viewer.

   The preview feature is different for each file type, as listed in the following table.

File Format	File Extension
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp. Image files open in the document viewer mode.
Microsoft Office files	.doc, .docx, .ppt, .pptx, .xls, and .xlsx Office files open in the document viewer mode.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File Format	File Extension
Text files	.txt Text files open in text editor mode.
Mail files	.eml **Note:** The file size must be less than 5MB. You must first download the file to preview its content.
PDF files	.pdf ○ Enter a keyword to search the document. ○ Zoom-in and zoom-out features to adjust the view for better readability. ○ Rotate the page clockwise or counterclockwise to view the content more clearly.

Note:

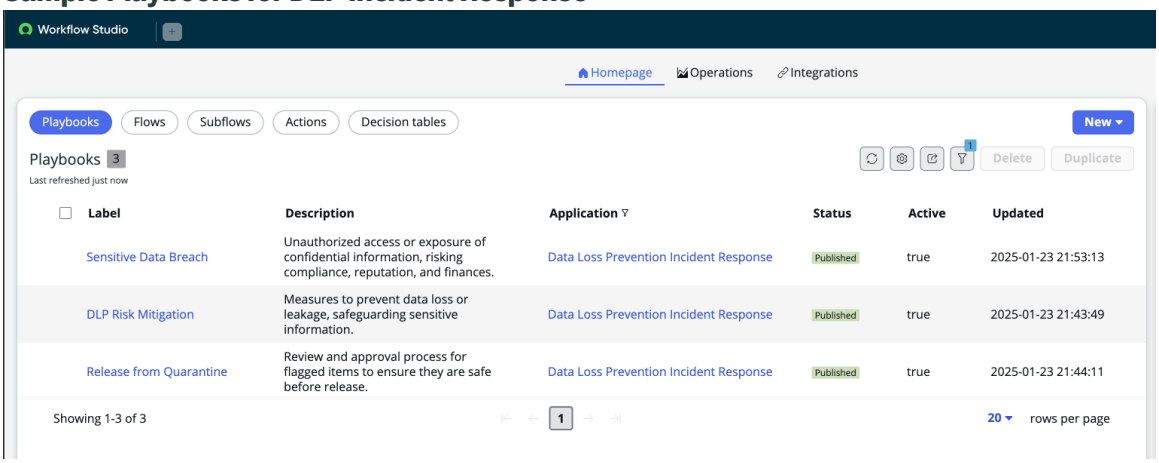
Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

Playbook for Data Loss Prevention Incident Response

A Data Loss Prevention Incident Response Playbook is a step-by-step guide for addressing and mitigating data loss incidents, which can include unauthorized exposures, leaks, or breaches of sensitive information that can compromise your organization's security.

The following image shows the sample Playbooks available for DLP IR.

Sample Playbooks for DLP Incident Response



The following table lists the activities and stages available for creating a DLP Playbook. For more information, see Add a DLP Playbook:

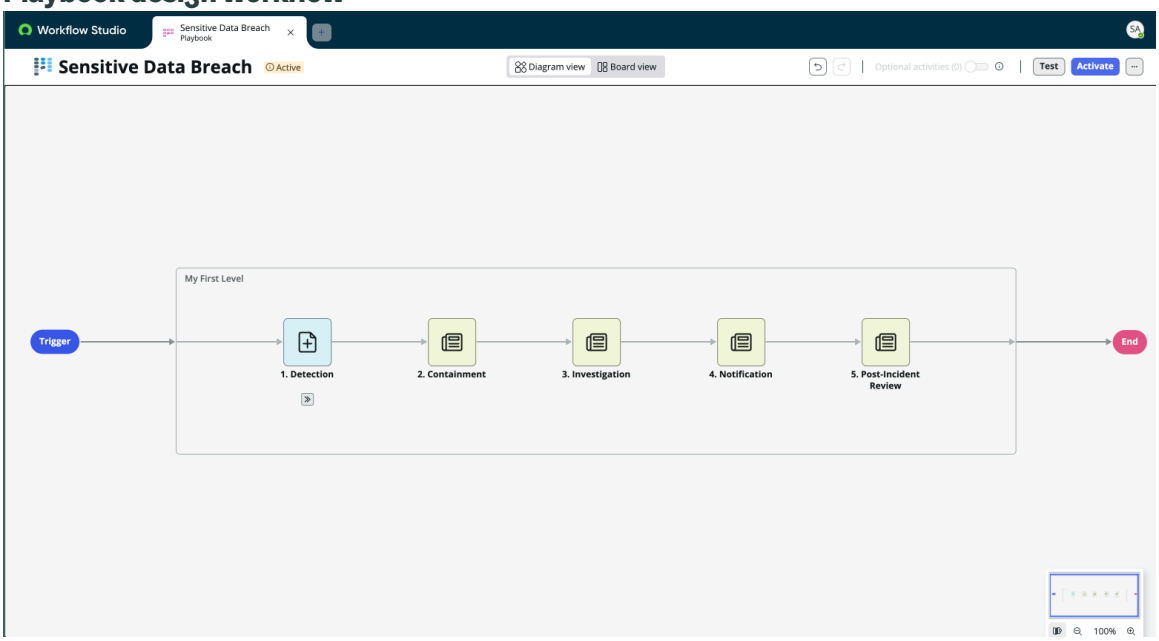
Activity	Description
Detection	Identify and confirm unauthorized access or exposure of sensitive data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activity	Description
Containment	Isolate affected systems or users to prevent further data leakage or unauthorized access.
Investigation	Investigate the breach to understand how it occurred, what data was affected, and the potential impact.
Notification	Notify internal teams, external stakeholders, and regulatory bodies as required by law or policy.
Remediation	Apply corrective measures to address vulnerabilities, update policies, and prevent future breaches.
Recovery	Restore systems from secure backups and validate the integrity of data post-incident.
Post-Incident Review	Analyze the incident to identify root causes, improve security controls, and strengthen policies.

The following figure shows the workflow of activities and stages involved in the creation of the Sensitive Data Breach Playbook. Playbook steps vary depending on the workflow.

Playbook design workflow



Related topics

- Add a DLP Playbook
- Cancel a DLP Playbook

Add a DLP Playbook

Add a Playbook in the Data Loss Prevention Incident Response Analyst workspace that can act as a guide for addressing and mitigating data loss incidents that can compromise your organization's security.

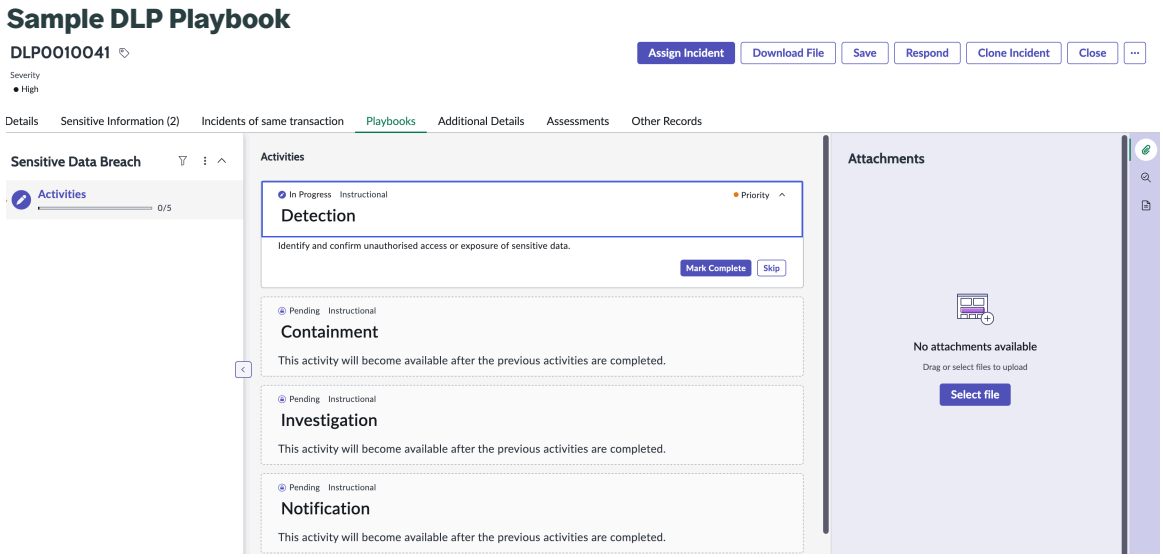
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Role required: sn_dlir.analyst - Add or view Playbooks in the DLP workspace.

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. On the DLP Analyst Workspace - My Incidents page, open any DLP incident.
3. Add the Playbook.
   a. Navigate to the **Playbooks** tab.
   b. In the UI actions menu, select the More actions icon ( ) and select **Add Playbooks**.
   c. In the dialog box, select a Playbook from the drop-down menu.
   d. Select **Add Playbooks**.
4. Select each lane to explore the tasks this Playbook performs.



Cancel a DLP Playbook

Cancel a Data Loss Prevention Incident Response Playbook to stop a business flow when it is no longer valid.

Before you begin

Note: Playbooks are automatically canceled when the associated DLP incident is closed.

Role required: sn_dlir.admin.

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open any DLP incident.
3. Navigate to the **Playbooks** tab.
4. In the header of the Playbook that you want to cancel, select the Playbook actions icon ( ) and then select **Cancel Playbook**.
5. Provide a reason for canceling the Playbook.
6. Select **Cancel Playbook**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
A banner appears below the Playbook header confirming that the Playbook has been canceled.

View archived DLP incidents

Use the DLP Analyst workspace to view or reactivate the archived DLP incidents.

Before you begin
Role required:

- sn_dlir.analyst
- sn_dlir.analyst_read and sn_dlir.read

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
   By default, My Incidents section is displayed.
2. Click **Archived Incidents**.
   The archived DLP incidents list is displayed.
3. Click **Show Incidents Count** button to view the archived incidents count.

   Note:
   - By default, the archived incidents count is hidden to improve the list loading time. Select the **Show Incident Count** button to view the incidents count. An information message is displayed that shows the incidents count.
   - The system property glide.ui.list.seismic.omit.count is enabled in the base system for the archived incidents to hide the incidents list count.

4. Select one or more DLP incidents that you want to view.
   The DLP incident displays the incident details section.

   Note:
   - **Other incidents from end users** includes the archived incidents.
   - **Match Content** is supported for all the archived incidents (which will be supported in all the integrations as well) but **Download file** is supported only for Microsoft integrations.

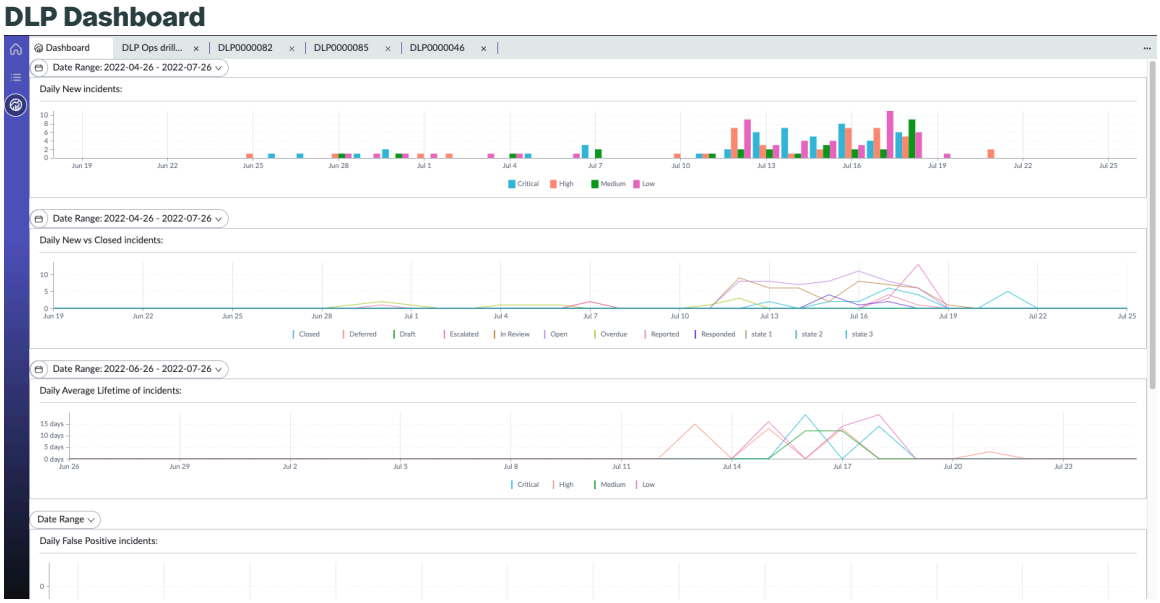
5. **Optional:** To reactivate an incident, change the **State** field to an active state, such as Open or In Progress.

Data Loss Prevention Incident Response Dashboard

The Data Loss Prevention Incident Response (DLP IR) Dashboard provides a high-level overview of your DLP incidents and daily incidents trends in your instance in the form of graphical charts. These charts help you effectively view, manage, and remediate the DLP incidents.

The Data Loss Prevention Incident Response dashboard provides key insights about your DLP incidents daily. You can set up indicators and regularly collect data snapshots of the incidents matching the conditions in the indicator properties. The collected data is then visualized using widgets in the dashboard. To analyze the DLP incidents in different time intervals, you can apply different date ranges.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Analyze daily incident trends in your DLP incidents

Access the Data Loss Prevention Incident Response (DLP IR) dashboard to analyze the daily trends in your DLP incidents and effectively remediate them.

Before you begin

Role required:

- sn_dlir.analyst - Edit and View DLP incidents.
- sn_dlir.analyst_read and sn_dlir.read - View DLP Incidents.

About this task

You can visualize the daily trends using widgets in the DLP dashboard. The data or statistics for the daily trends of your DLP incidents are collected from the daily incidents indicator properties that are defined by your organization. You can gain key insights by applying different data ranges to analyze the DLP incidents in different time intervals for the following charts:

- **Daily New incidents**: Data of the overall DLP incidents created daily irrespective of the incidents' state. The DLP incidents are categorized based on the severities, including Medium, Critical, High, and Low. Each DLP incident severity is represented by a particular color on the chart.
- **Daily New vs Closed incidents**: The different states of the DLP incidents and a comparison between the daily new incidents and daily closed incidents. The Daily New category includes all the DLP incidents in Open, Draft, Escalated, In Review, Overdue, Reported, Responded, or Custom (if any) states. The Closed incident category includes the closed DLP incidents. Each DLP incident state is represented by a particular color on the chart.
- **Daily Average Lifetime of incidents**: The lifetime of an incident is the time period between the opening and closing of a specific DLP incident. The daily average lifetime is calculated only for the closed DLP incidents.
- **Daily False Positive incidents**: Data of all the DLP incidents reported as daily false positives. The daily false positive incidents are categorized based on the severities, including Medium, Critical, High, and Low. Each daily false positive incident severity is represented by a particular color on the chart.
- **Age vs Severity of incidents**: Data comparison of all the DLP incidents, categorized by the age and configured with the severity of the DLP incidents. The Age category includes all the DLP incidents under the age that your organization defines. For more information on Age charts,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

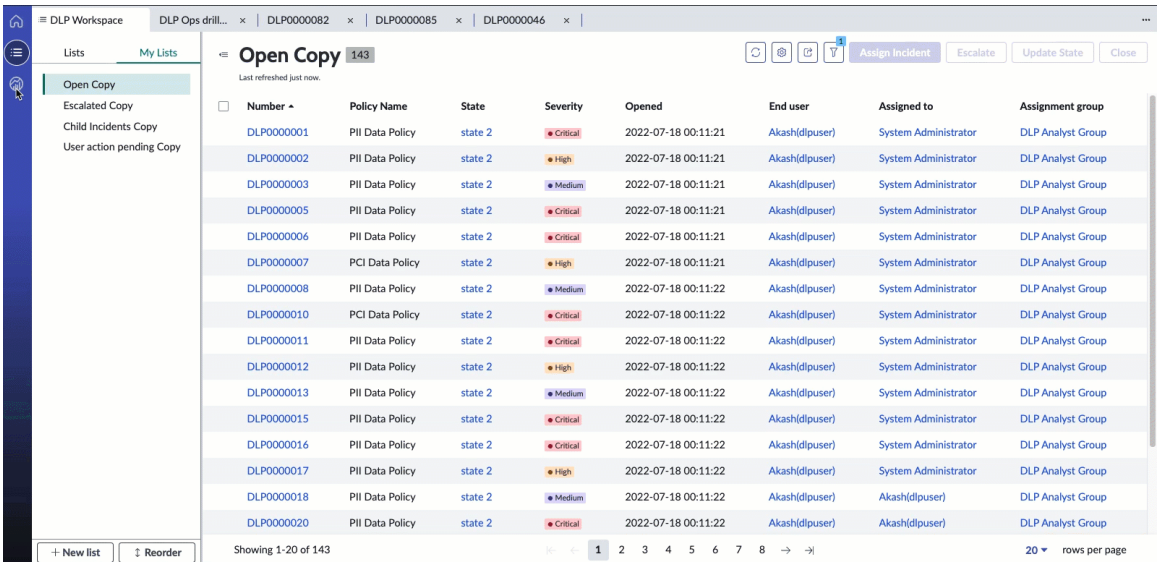
see Create age chart configurations. The Severity of incidents includes all the DLP incidents in the High or Low category. Each severity is represented by a particular color on the chart.

- **Daily Escalated incidents**: Data of all the escalated DLP incidents daily. The daily escalated incidents are categorized based on the severities, including Medium, Critical, High, and Low. Each daily escalated incident severity is represented by a particular color on the chart.

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Dashboard**.
   The My DLP Dashboard page is displayed in a new browser tab.
2. Select a dashboard widget for which you want to perform a daily trend analysis.
   For example, the Daily New Incidents chart.
3. Review the dashboard widgets to identify trends.
4. Click **Date Range**.

DLP Dashboard Overview



5. Select a date range from the calendar, and click **Apply**.

   Example
   For example, the Daily New Incidents chart gets updated for the selected data range.
6. Use the filters below the chart to drill down and perform a more in-depth analysis.

Inbound Integration for Data Loss Prevention Incident Response

Create single or multiple DLP incidents by using the Inbound REST API.

Create a single DLP incident

Role required: sn_dlir.api_integration_user.

To create a single DLP incident, define the following parameters as necessary:

Field	Description
HTTP Method	*POST*

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
URL	`https://{instance}/api/now/import/sn_dlir_incident_import`
Request Header	**Accept:** *application/json* **Content-Type:** *application/json*

Sample Payload	{
	"application_window_title": "<value>",
	"assigned_to": "<value>",
	"attachments": "<value>",
	"data_owner_email": "<value>",
	"destination": "<value>",
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "",
	"file_created": "",
	"file_created_by": "",
	"file_location": "",
	"file_modified_by": "",
	"file_name": "",
	"file_owner": "",
	"file_permissions": "",
	"ftp_user_name": "",
	"last_modified": "",
	"machine_ip": "",
	"machine_name": "",
	"match_count": "",
	"policy_id": "",
	"policy_name": "",
	"printer_name": "",
	"printer_type": "",
	"print_job_name": "",
	"recipients": "",
	"scanned_machine": "",
	"scan_source": "",
	"seen_before": "",
	"sender":"",
	"source":"",
	"source_file":"",
	"source_ip":"",
	"source_ip_port":"",
	"subject":"",
	"url":"",
	"user_justification":""
	}

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

Sample Response	{
	"import_set": "ISET0010003",
	"staging_table":
	"sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value":
	"DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id":
	"7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Create multiple DLP incidents

Role required: sn_dlir.api_integration_user.

To create multiple DLP incidents from the same request, define the following parameters as necessary:

Field	Description
HTTP Method	*POST*
URL	`https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple`
Request Header	**Accept:** *application/json* **Content-Type:** *application/json*
Sample Payload	{ "records": [{ "file_name": "<value>", "file_modified_by": "<value>", "work_notes": "<value>", "url": "<value>", "scan_source": "<value>", "data_owner_email": "<value>", "file_created_by": "<value>",

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description

	"file_owner": "<value>",
	"policy_name": "<value>"
	},
	{
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "<value>",
	"file_created": "<value>",
	"file_created_by": "<value>",
	"file_location": "<value>",
	"file_modified_by": "<value>",
	"file_name": "<value>",
	"file_owner": "<value>",
	}
	]
	}

Sample Response	{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id": "e78f69229734dd1056a43d1e6253af75"
	}

Note: By default, the transformation is asynchronous. To set synchronous transformation, create a new record in the REST Insert Multiples [sys_rest_insert_multiple] table, select the source table as **sn_dlir_incident_import**, and set the transformation to **synchronous**.

DLP integrations

The Data Loss Prevention Incident Response base system includes integrations to third-party data loss prevention software packages.

This section provides instructions for activating the plugins and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.

Integration Configurations

The base system includes a series of cards for each of the integration implementations you can activate and use. Also, cards are displayed for any integrations posted on the ServiceNow Store that have dependencies on Security Operations plugins. The integration cards can be viewed by selecting **Security Operations** > **Integration Configurations**.

Data Loss Prevention Incident Response supports the following third-party data loss prevention software packages:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Symantec Integration for Data Loss Prevention Incident Response

The Symantec DLP integration supports the ingestion of Data Loss Prevention Incident Response incidents created on the Symantec Data Loss Prevention Incident Response deployment. After ingestion, you can use the incident management functionalities to remediate the DLP incidents.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview and key features

The Symantec DLP integration helps companies to track the usage and movement of sensitive data on various platforms.

This integration includes the following key features:

- Ability to create multiple integration profiles for different Symantec API endpoints.
- Scheduled ingestion of DLP incidents from Symantec into your ServiceNow instance.
- Ability to apply API filters to retrieve the incidents that match the filter criteria and also specify the filter for Symantec DLP incidents that are required to be imported.
- Ability to store the evidence file internally in the ServiceNow instance.
- Ability to map the DLP incident states in your ServiceNow instance to DLP incident states in Symantec.
- Automatically update incident status in Symantec when the state changes in your ServiceNow instance.
- Ability to customize and define the severity mapping between Symantec DLP incidents with ServiceNow incidents.
- Ability to download the evidence file for Symantec incidents from directly Symantec server or from internal ServiceNow storage.
- Supports smart response rules from ServiceNow.

To learn more about the integration, see the Symantec product documentation.

Getting started with Symantec DLP integration for Data Loss Prevention

Before you can use the integration, you must download it from the ServiceNow® Store.

Checklist

Review the following information before you start setting up your Symantec DLP integration for data loss prevention.

Check list

Field	Description
Verify you have assigned the required ServiceNow AI Platform, Data Loss Prevention Application, MID application roles.	Following roles are used across the Symantec DLP integration on the ServiceNow AI Platform:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Check list (continued)

Field	Description
	• The Administrator(admin) install the applications from the ServiceNow® Store and assigns the Data Loss Prevention admin (sn_dlir.admin). • The user with sn_dlir.admin role can configure the integration and setup the incident profiles. • The users with sn_dlir.analyst role will have read roles across the integration.
Assign the required Symantec DLP user roles.	Review the Symantec DLP integration roles and permissions.
Verify you are using Symantec DLP 15.8	The Symantec DLP integration for Data Loss Prevention is tested with 15.8 version of Symantec Data Loss Prevention. **Note:** Ensure that you are using Symantec DLP 15.8
Verify that ServiceNow® core application that is required to support the Symantec DLP integration are installed and activated.	Verify that the following DLP applications and security support common applications are installed and activated from ServiceNow Store. If not installed, install, and activate on application. • Security Support Common • Data Loss Prevention Incident Response

Install and configure the Symantec DLP integration for Data Loss Prevention

Install and configure the#Symantec DLP integration from the#ServiceNow® Store on your #ServiceNow AI Platform instance. Start investigating DLP incidents using the#Symantec DLP incident data.

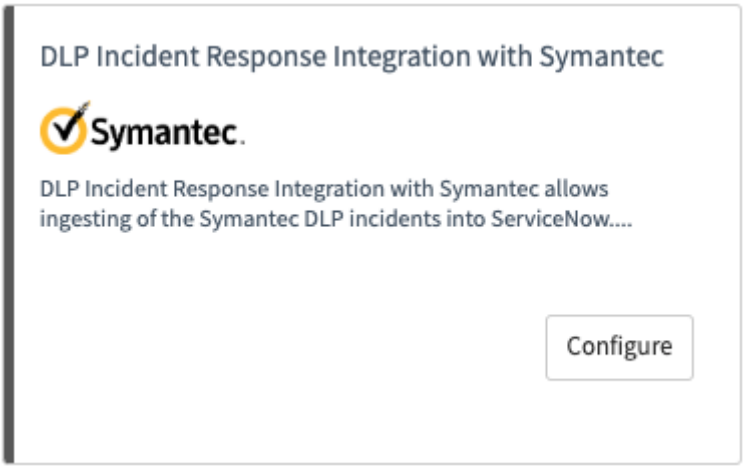
Before you begin

Role required: sn_dlir.admin

Procedure

1. Download the#Symantec DLP integration from the#ServiceNow® Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the#DLP Incident Response Integration with Symantec tile and click#**Configure**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

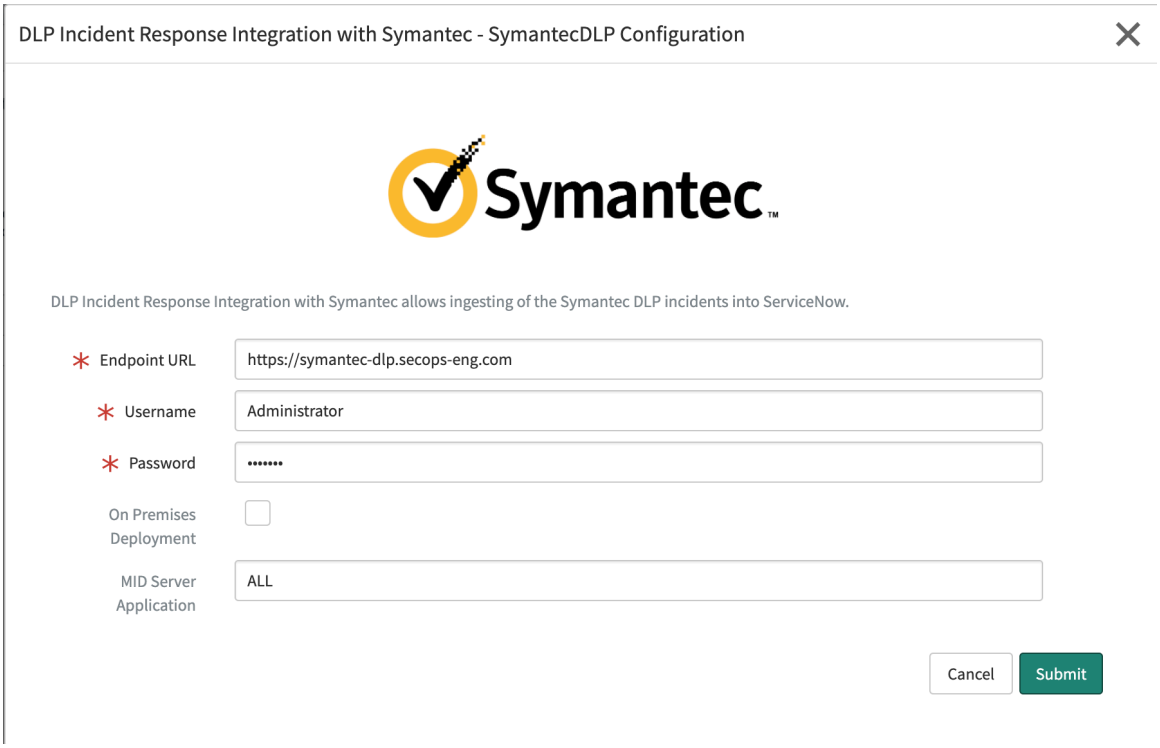


4. On the form, fill in the fields.

Symantec DLP Integration Configuration form

Field	Description
Name	Name of the Symantec DLP integration configuration.
Endpoint URL	Symantec REST API endpoint.
Username	Symantec account name. For information on the Roles and Permissions required, see Roles and Permissions.
Password	Symantec account password.
On-Premises Deployment	Option that you can select if your Symantec is deployed in an on-premises instance. When you select this option, you must use the MID Server to connect to Symantec.
MID Server Application	The MID Application name that is used to communicate with Symantec. This field is needed when you select the **On-Premises Deployment** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.

Result

Note: Please connect symantec sub prod to the ServiceNow sub prod. Keep all the username and passwords in sync across the instances to avoid accounts getting logged out.

After you successfully validate and submit the configuration, the Symantec DLP Integration is saved on the Security Integrations page as a tile.

Create a profile for Symantec DLP integration

Create an incident profile in your#ServiceNow AI Platform instance. Determine the#Symantec DLP incidents that are suitable for creating DLP incidents.

Before you begin

Role required: sn_dlir.admin

About this task

Configure the ServiceNow AI Platform® to fetch the DLP incidents from the Symantec endpoint. Store these incidents into your ServiceNow® instance as DLP incidents.

Procedure

1. Navigate to **Symantec DLP integration** > **Incident Profile**.
2. Click **New**.
3. On the form, fill the fields in the Name section.

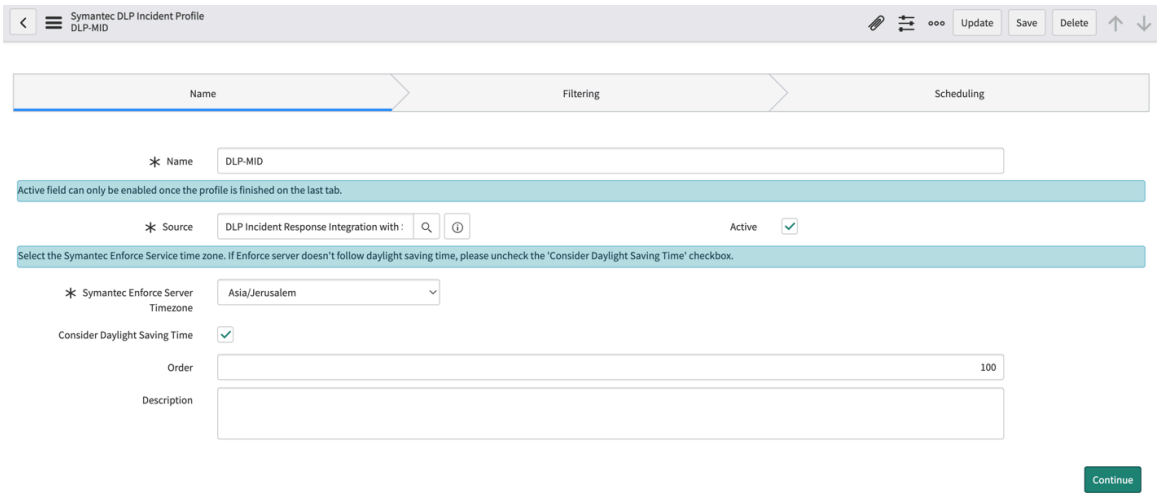
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create a profile

Field	Description
Name	Name of the profile. This field helps you to identify the profile. **Note:** The name must be unique for each profile.
Source	Symantec DLP instance that you configured to ingest incidents. If you have multiple instances configured, select the appropriate instance for the incident types that you are planning to ingest for the profile.
Active	Option to indicate if the profile is active. This field can only be enabled after you click the **Finish** in the Scheduling section. When the profile is active, it implies that the #ServiceNow AI Platform is actively polling Symantec DLP incidents. The corresponding DLP incidents are created in#DLP #when the filtering conditions are matched based on the Scheduling parameters that you have provided.
Symantec Enforce Server Timezone	Select the time zone for symantec enforce server in the profile so that incidents are not missed due to the time zone issues.
Consider Daylight Saving Time	Select this check box if the enforce server follows the daylight saving time.
Order	Order of the profile execution. The profile with the lowest order considered as the highest priority. By default, the value is 100.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Description	Unique description for this profile.



What to do next
To move to the Filtering section,#click **Continue**.

Define filters to apply for the Incident creation

Define and set filter conditions to drill down the incoming#Symantec DLP#ncidents. Determine the incidents that should be created as DLP incidents in ServiceNow®.

Before you begin
Role required: sn_dlir.admin

About this task
Filtering helps you to isolate DLP incidents and to limit the number of DLP incidents that you create. If additional filtering criteria are set, only incidents that match the conditions are created.

Procedure
1. Select **API based filter for incident ingestion** checkbox to apply the API filters and retrieve the incidents that match the filter criteria.
2. Add the API filters.
   The following is an example that shows the API filters.

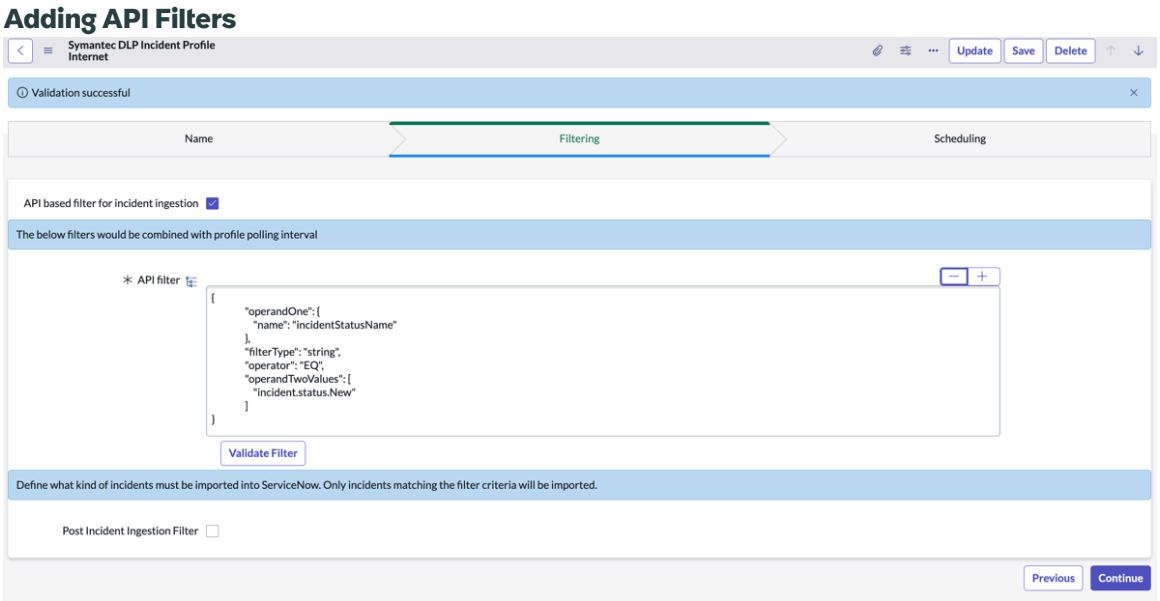
```
{
                "operandOne": {
                    "name": "incidentStatusName"
                },
                "filterType": "string",
                "operator": "EQ",
                "operandTwoValues": [
                    "incident.status.New"
                ]
            }
```

Note: For more information on the API filters on Symantec integration, see Incident Lists: Parameters - Request object details.

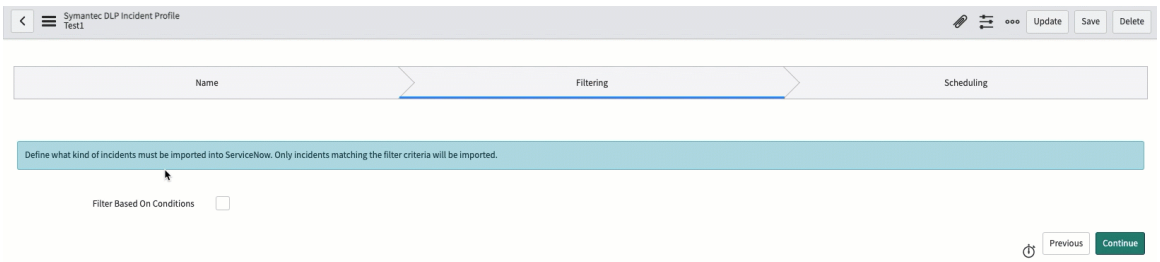
3. Click **Validate Filter** after you apply the API filters.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If the validation is unsuccessful then an error message is displayed that the validation is failed and this happens when the filters are not properly entered as per the Symantec APIs.



4. Select **Post Incident Ingestion Filter** checkbox to define the criteria that an incoming Symantec DLP incident must satisfy so that a DLP incident is created.
   The options in the first field in the Filter Conditions match the fields that are available in the DLP incident. The criteria that you enter are case-sensitive. Verify that the criteria you define match the values of the incident.
5. In the condition builder, set the filters in the **Filter Conditions** field.



6. To add more conditions, click#**AND**# or#**OR**.
   - If#**AND**#s selected, all conditions must be matched.
   - If#**OR**#s selected, either condition can be matched.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
To configure the schedule, click **Continue**.

Configure evidence file storage

Configure evidence file storage to securely store the evidence file for the DLP Incidents.

Before you begin
Role required: sn_dlir.admin

Verify that the Symantec user that you are configuring for ServiceNow Symantec DLP integration must have Body, Attachments and Original Message options enabled from Roles configuration page on Symantec DLP portal. For more information, see Display Attributes section available on Configuring Roles document for more information.



About this task
You can configure the evidence file storage to securely store files. This provides an option for internal storage in ServiceNow instance, ensuring that files are stored and encrypted using ServiceNow's Column Level Encryption. For more information, see Field Encryption on NowPlatform documentation.

When DLP analyst performs the Download evidence files for DLP Incidents action from analyst workspace, the file will be downloaded from the selected storage if evidence file storage option is enabled. Otherwise, the file will be downloaded directly from the Symantec source and will not be persisted in ServiceNow instance.

> **Note:** When a DLP analyst performs the Download evidence files for DLP Incidents action from analyst workspace, the file will be downloaded from the selected storage if evidence file storage option is enabled. Otherwise, the file will be downloaded directly from the Symantec source and will not be persisted in ServiceNow instance.

Procedure
1. Navigate to **All** > **Symantec DLP Integration** > **Incident Profile**.
2. Click on **Evidence Storage** section on the Incident Profile form.
3. Select **Evidence File Storage** check box to enable the file storage.
4. Select the preferred storage type.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Type	Description
Evidence File Storage	Option to enable the Evidence file storage.
Storage Type	Option to select the preferred storage type. **Note: ServiceNow Storage**: This will store the evidence files in the Service Now instance in an encrypted format.

5. Click **Continue** and move to the **Scheduling** section.

Result
The evidence files are stored as per the configuration, after the incident ingestion is completed.

Schedule the Symantec DLP Incident Retrieval

Set a schedule to retrieve the incident data and ingest Symantec DLP incidents that match the criteria in the profile. Configure the schedule to define how and when you pull incidents from Symantec.

Before you begin
Role required: sn_dlir.admin

About this task
You can plan how often you will poll for future incidents that match the incident profile configuration. To enable automated incident ingestion, you must configure the scheduling and incident retrieval before you activate the profile. The profile can be configured to do one-time retrieval using the **One-Time Retrieval** check box. The historical date can be up to the last three months from the current date.

The polling interval is configured for each profile individually. The different polling intervals may impact the performance of the Symantec DLP incident integration. When scheduling, plan to balance the system load against the urgency of an incident.

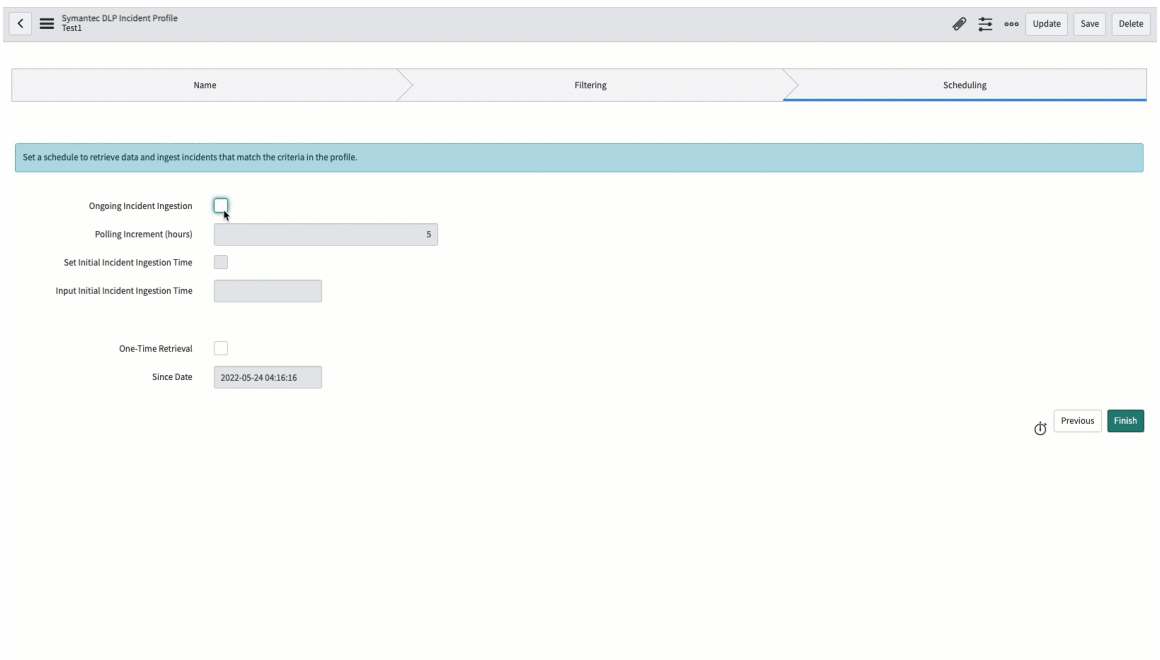
Procedure
1. Set a schedule to retrieve data and ingest incidents that match the criteria in the profile.
2. On the form, fill the fields.

Schedule for the DLP incident

Field	Description
Ongoing Incident Ingestion	The ongoing incident ingestion that the ServiceNow AI Platform instance pulls from the#Symantec for new incidents. DLP incidents are created if triggered incidents are found and the incident generation filtering criteria matches.
Polling increment (minutes)	The polling frequency that is defined in minutes. This field is automatically set to 300 minutes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Set Initial Incident Ingestion Time	Option to define a date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.
Input Initial Incident Ingestion Time	Date and time that you specify for the incident ingestion.
Initial Incident Ingestion Time	First time when the data is ingested. You can see the that values start showing up when the initial incident ingestion time is set.
Next Incident Ingestion Time (estimated)	Next period for an estimated incident ingestion.
One-Time Retrieval	Option to enable one-time historical data pull. If this field is selected, then historical data will be pulled from Symantec DLP according to the date added in the **Since Date** field.
Since Date	Date from when data is supposed to be retrieved from Symantec. This field can be set to at most three months.



3. To save the created profile configuration, click **Finish** on the pop-up window.
4. To activate the profile, open the created profile.
5. Enable **Active** option.
6. Click **Update**.

Result

After successful creation and activation of the profile, the incidents are retrieved periodically as per the configuration set in the profile and added into DLP incidents table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mapping Symantec DLP incident statuses with ServiceNow incident Status

Synchronize the status of the DLP incidents ingested on the ServiceNow with the DLP incidents of the Symantec. Map the **ServiceNow Incident Status** field with the **Symantec Incident Status** field.

Before you begin

Role required: sn_dlir.admin

About this task

The incident status is retrieved dynamically from the Symantec Endpoint Source which is added in the mapping. You need to perform a one-to-one incident status mapping.

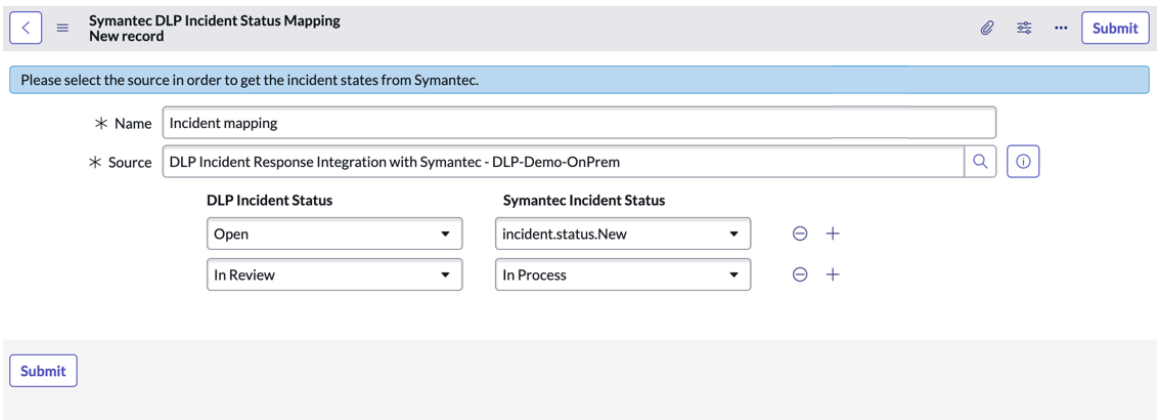
Procedure

1. Navigate to **Symantec DLP integration** > **Incident Status mapping**.
2. Provide a **Name** to identify the mapping.
3. Select the **Source** integration from where you want to fetch the status.
4. Map the **DLP Incident Status** with **Symantec Incident Status**.

> **Note:** It is not necessary to map all the states, you can map only the required states.

Symantec DLP Incident Status Mapping

Field	Description
Name	Name of the mapping record.
Source	The configured Symantec Endpoint source from where you want to fetch the incident status.
DLP Incident Status	List of Status of DLP incidents.
Symantec Incident Status	List of Status fetched from the Source (Symantec Endpoint).



5. Click **Submit**.

Result

After successfully creating the record for mapping statuses of the ServiceNow incidents, the ServiceNow incidents status will be synced with Symantec DLP incidents status.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you change the status of any DLP incident on your ServiceNow instance, then the status of associated Symantec DLP incidents will be changed on the source Symantec platform based on the mapping set in the record.

Severity mapping between Symantec DLP incidents with ServiceNow incidents

Use the severity mapping feature to configure and synchronize the mapping between Symantec incidents and ServiceNow AI Platform® incidents.

Before you begin

Role required: sn_dlir.admin

About this task

DLP Severity mapping allows you to map the source severity with the DLP incident severity. You can customize and define the source severity value and map it to the desired DLP incident severity value.

Procedure

1. Navigate to **Symantec DLP integration** > **Incident Severity Mapping**.
2. Click **New**.
3. On the form, fill in the fields.

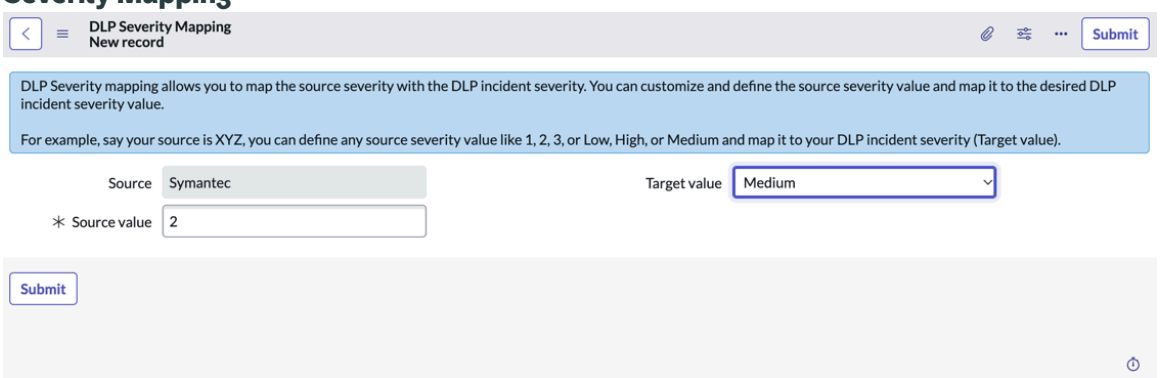
DLP Severity Mapping

Field	Description
Source	The configured Symantec Endpoint source from where you want to fetch the incident.
Target Value	Target value is the DLP incident severity ID. The available values are Critical, High, Medium, Low, and Info (used as the info severity in Symantec).
Source Value	Source value is the Symantec incident severity.

Note: Within the base system, there are four severity mappings that are shipped to the DLP users.

4. Click **Submit**.

Severity Mapping



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure Smart Response Rules

Configure the Symantec smart response rule(s) to perform response actions on the ingested Symantec DLP incidents.

Before you begin

Role required: sn_dlir.admin

About this task

Verify that the Symantec user that you are configuring for ServiceNow Symantec DLP integration must have those Smart Response Rules selected under the **Roles configuration** page. For more information, see **Actions** section available on Configuring Roles document.

For the fetched smart response rule(s), DLP admin can create the Incident Response Option Rule(s) and Response Option Mappings to configure the response action(s) to be performed on ingested Symantec DLP Incidents.

Procedure

1. Navigate to **All** > **Symantec DLP Integration** > **Smart Response Rules**.
   You will see all the available smart response options for each configured integration configuration. For more information see, Install and configure the Symantec DLP integration for Data Loss Prevention and follow the procedure explained on how to configure Symantec integration: configuration source if this was not configured.
2. Click on any of the Smart Response Rules to open its form view.

   Follow Create incident response option rules to create Incident Response Option Rules and Response Option Mappings to display this smart response rule on Respond modal of DLP workspace.
3. Create the approval rules for the Smart Response Rule using the **Approval Rules** tab in the related list or by following the procedure explained in the Configure Approval Rules section. Approval Rules for each Smart Response Rules will be visible in the Approval Rules related list.
4. After creating the Incident Response Option Rule(s), you can see the record in the related list of the Smart Response Rule record.
5. Use the **Refresh Smart Response Rule** button in the list view to manually update the source. The smart response rules will add, update, or delete automatically each day for every source.

Execute Smart Response Rules

Use this feature to execute Smart Response Rules for the Symantec DLP incidents.

Before you begin

You need to configure the Smart Response Rules by following procedure explained here in this section, Configure Smart Response Rules.

Role required: sn_dlir.admin

Note:

The response options on the workspace will be available for the end user or analyst or manager based on the configuration mentioned in the section Configure response option for your DLP incidents.

Procedure

1. Navigate to **All** > **DLP** > **DLP User Workspace**.
2. Open any DLP incident created from the DLP workspaces.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Respond**.
4. Select the response option from the Response drop down list.
   The response options will be visible based on the configuration of the **Incident Response Option Rule** and **Response Option Mappings**.
5. Click **Submit**.

> **Note:** You can also configure the approval rule(s) for the Response Options by following the procedure explained in the Create Approval Rules section. When an approval rule is configured for the Smart Response Rule, the approval flow will be triggered first and after receiving all the approvals, the Smart Response Option flow will be triggered. The state of the DLP Incident will be updated as per the target state of the Response Option mapping after successful execution of the response option.

Download evidence files on Symantec

Download the DLP incident evidence files that violate the DLP policy on Symantec.

Before you begin

Download this file onto your local machine from the DLP IR Analyst workspace and DLP IR End user workspace. Download Files action will be available only for the approvers on the DLP IR End User workspace.

Role required:

- sn_dlir.analyst
- sn_dlir.secure_file_download (any approver with this role)

Procedure

1. Navigate to **All** > **Symantec DLP Integration** > **Settings**.
2. Enable **Should downloading the violating file of the reported incident be allowed** property.
   After you enable this property, you will now be able to see the **Download File** action on the DLP Analyst Workspace for any Symantec DLP incident.
3. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
4. Open a DLP incident record which is ingested from Symantec source.
5. Click **Download File**.

> **Note:** The file that violated the DLP policy on Symantec will be downloaded to the user's local machine.

For the approver to view the Download File action, follow below mentioned steps:

6. Navigate to **All** > **DLP Incident Management** > **DLP User Workspace**.
   My DLP Incidents page will be displayed in a new tab.
7. Select **My Approvals** module available under My DLP Incidents module.
   My Approvals list view will be displayed.
8. Open an approval request record which is raised for Symantec DLP Incident.
9. Click on info icon (i) available on the DLP Incident field in the form view.
10. Click **Download File**.

Result

After performing this action, the evidence file in either ZIP format (if the incident has violations in multiple components and/or the original message data is also available) or a single file (if

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

incident has violations in single component or only original message data is available) will be downloaded to the user's local machine.

Note: As a DLP admin, you can control the access of **Download File** action by disabling the **Should downloading the violating file of the reported incident be allowed** option from the **Advanced Settings** page. For more information, see Configure advanced settings for Data Loss Prevention Incident Response.

Preview evidence files

Preview Data Loss Prevention Incident Response evidence files in the DLP IR Analyst workspace.

Before you begin

Important: While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format. If you don't want to store the evidence files, disable the Evidence Files preview feature. For more information, see Configure advanced settings.

Role required: sn_dlir.analyst

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. From the contextual sidebar, select the Evidence files icon ( ).
4. On the **Evidence Files** tab, select the **Evidence File** card to preview the evidence files in the document viewer.

   The preview feature is different for each file type, as listed in the following table.

File Format	File Extension
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp. Image files open in the document viewer mode.
Microsoft Office files	.doc, .docx, .ppt, .pptx, .xls, and .xlsx Office files open in the document viewer mode.
Text files	.txt Text files open in text editor mode.
Mail files	.eml **Note:** The file size must be less than 5MB. You must first download the file to preview its content.
PDF files	.pdf

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File Format	File Extension
	○ Enter a keyword to search the document. ○ Zoom-in and zoom-out features to adjust the view for better readability. ○ Rotate the page clockwise or counterclockwise to view the content more clearly.

Note:

Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

Configure the Symantec DLP#ntegration settings

Modify the#Symantec DLP#ntegration default system properties.

Before you begin

Role required: sn_dlir.admin

Procedure

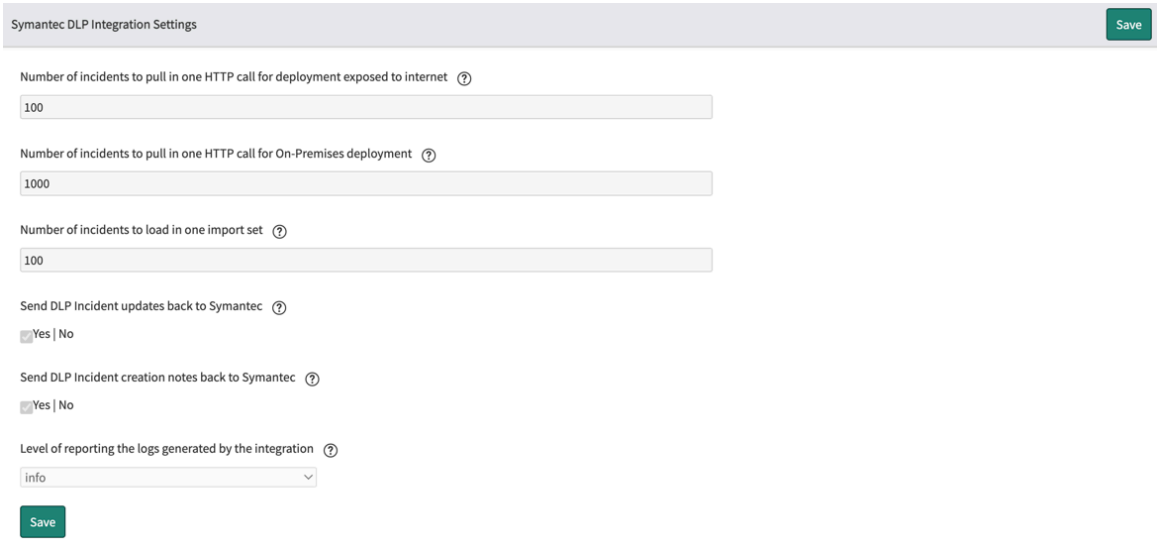
1. Navigate to **Symantec DLP Integration** > **Settings**.
2. Modify the following settings as required.

Settings

Field	Description
Enforce a limit on Number of incidents to pull in one HTTP call for On-Premises deployment sn_sym_dlp.page_size_on_prem	Maximum number of incidents to be fetched in one HTTP call for On-Premise deployment of Symantec. ○ Type: integer ○ Default value: 1000
Enforce a limit on Number of incidents to pull in one HTTP call for deployment exposed to internet sn_sym_dlp.page_size_on_internet	Maximum number of incidents to be fetched in one HTTP call for Symantec deployment exposed to internet. ○ Type: integer ○ Default value: 100
Number of incidents to load in one import set sn_sym_dlp.incidents_per_attachment	Number of records to store in one attachment file for processing. ○ Type: integer ○ Default value: 100
Send DLP Incident updates back to Symantec sn_sym_dlp.incident_update	This property enables you to restrict any state synchronization between ServiceNow and Symantec DLP incidents. ○ Type: Boolean ○ Default value: **true**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Send DLP Incident creation notes back to Symantec sn_sym_dlp.incident_creation_notes	This property enables you to send a note back to Symantec as soon as an incident is created in ServiceNow. ○ Type: Boolean ○ Default value: **true**
Level of reporting the logs generated by the integration sn_sym_dlp.logging.verbosity	Property that defines the reporting of the logs generated by the integration.



3. Click **Save**.

Domain Separation in the Symantec DLP integration

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with Symantec DLP integration

Follow these steps to achieve domain separation:

- Create a user with the required role in the respective domain.
- Perform the Symantec DLP integration procedures in the appropriate domain.

Data Loss Prevention Incident Response Integration with Proofpoint

The Proofpoint DLP integration supports the ingestion of Data Loss Prevention incidents created on the Proofpoint Data Loss Prevention deployment. After ingestion, you can use the incident management functionalities to remediate the DLP incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview and key features

The Proofpoint DLP integration helps companies to track the usage and movement of sensitive data on various platforms.

This integration includes the following key features:

- Multiple profile creation for different Proofpoint endpoints.
- Automating the creation of DLP incidents.
- Mapping of the Proofpoint DLP incident state field to DLP incident state field.
- Filtering of Proofpoint DLP incidents.
- Ingestion of incidents in your ServiceNow instance as soon as the alerts are generated on Proofpoint DLP tenant.
- Proofpoint DLP integration supports both endpoints and email type of incidents.
- Automatic updates for the Proofpoint DLP incident status and comments for DLP incident creation, and for state change and closure on ServiceNow side.
- Downloading evidence file for email alerts directly from Proofpoint or from internal ServiceNow storage.
- Performing remediation actions such as Release Encrypted Email with Scan, Delete Email, Release Email without Scan and Release Email with Scan from ServiceNow side.

Learn about this integration

Document identifier	Document title
Proofpoint product documentation website	Proofpoint product documentation
ServiceNow® product documentation website	ServiceNow Product Documentation website

Getting started with Proofpoint integration for Data Loss Prevention

The Proofpoint DLP integration supports the ingestion of Data Loss Prevention alerts created on the Proofpoint dashboard. After ingestion, the incident management functionalities that remediate the DLP incidents will be used.

Checklist

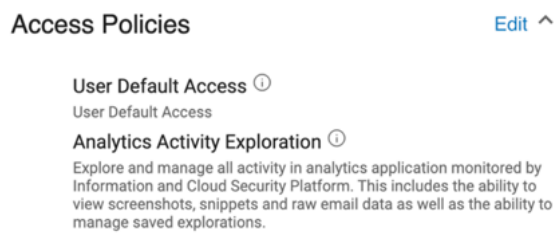
Review the following information before you start setting up your Proofpoint DLP integration for Data Loss Prevention.

Checklist

Field	Description
Verify you have assigned the required ServiceNow AI Platform and Data Loss Prevention Incident Response application roles.	The following roles are used across the Proofpoint DLP integration on the ServiceNow AI Platform:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

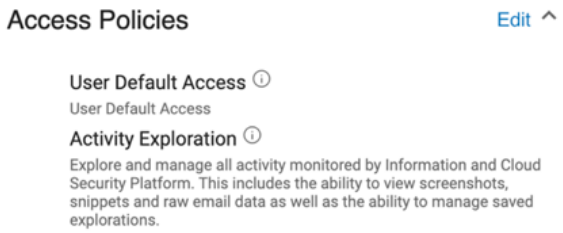
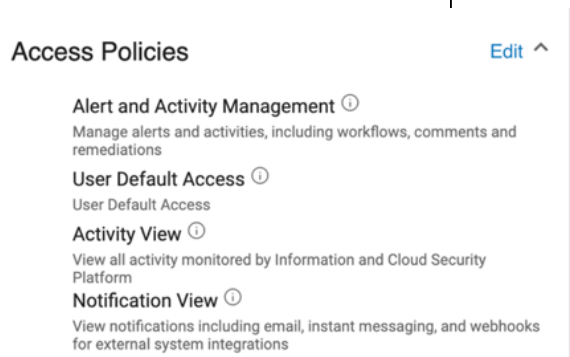
Checklist (continued)

Field	Description
	• The administrator (admin) installs the applications from the ServiceNow® Store and assigns the Data loss prevention admin (sn_dlir.admin). • The user with sn_dlir.admin role can configure the integration and set up the incident profiles. • The users with sn_dlir.analyst role have read roles across the integration.
Assign the required Proofpoint DLP user roles.	Assign any High Level access or Granular access to the created DLP User. **High level access**: Assign either of the below listed access policy. • **Analytics Activity Exploration:** Explore and manage all activity monitored by Information and Cloud Security Platform. This includes the ability to view screenshots, snippets, and raw email data and to manage saved explorations. **Analytics Activity Exploration - Access Polices**  • **Activity Exploration:** Explore and manage all activity in analytics application monitored by Information and Cloud Security Platform. This includes the ability to view screenshots, snippets and raw email data and to manage saved explorations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Field	Description

	Activity Exploration - Access policies
	 
	• **Granualar access:**: Assign all the below listed access policies.
	  ○ **Notification View**: View notifications including email, instant messaging, and webhooks for external system integrations.
	  ○ **Activity View**: View all activity monitored by Information and Cloud Security Platform.
	  ○ **Alert and Activity Management**: Manage alerts and activities, including workflows, comments and remediations.
	Granualar access - Access Policies
	 
	For more information navigate to Administration > User Management > Access Policies > Predefined Access Policies Descriptions on Proofpoint Documentation.

Verify that the end-user core application required to support the Proofpoint DLP integration is installed and activated.	Verify that the following DLP applications and security support common applications are installed and activated from ServiceNow Store. If not installed, install, and activate on application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Field	Description
	• Security Support Common • Data Loss Prevention Incident Response

Install and configure the Proofpoint integration for Data Loss Prevention

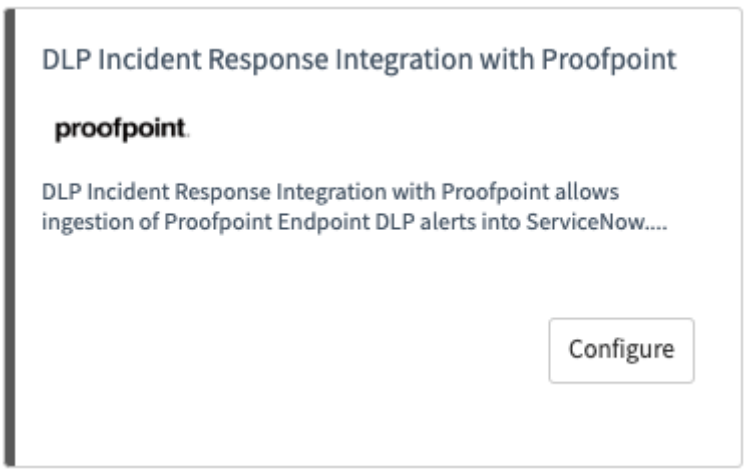
Install and configure the#Proofpoint DLP integration from the#ServiceNow® Store on your #ServiceNow AI Platform instance. Start investigating DLP incidents using the#Proofpoint DLP incident data.

Before you begin

Role required: sn_dlir.admin

Procedure

1. Download the#Proofpoint DLP integration from the#ServiceNow® Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the#DLP `Incident Response Integration with Proofpoint` tile, and click#**Configure**.

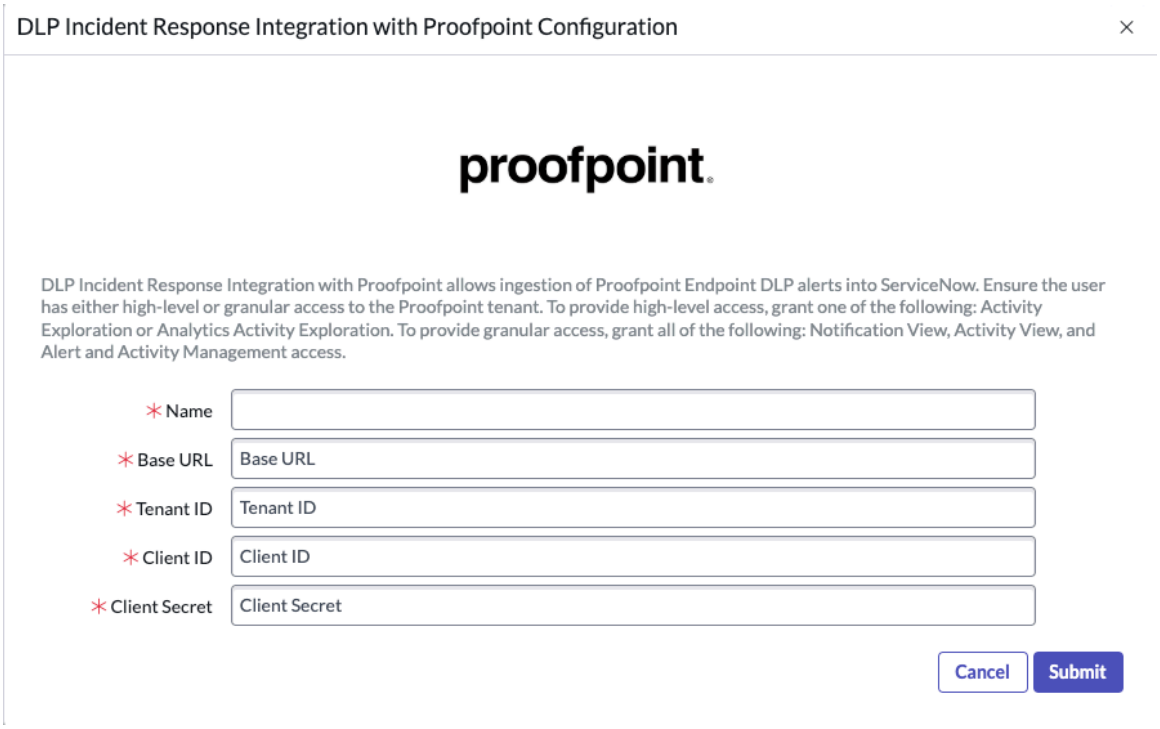


4. On the form, fill in the fields.

Proofpoint DLP Integration Configuration form

Field	Description
Name	Name of the Proofpoint DLP integration configuration.
Base URL	URL for the Proofpoint that serves as the REST endpoint.
Tenant ID	The ID of Proofpoint tenant.
Client ID	The ID of Proofpoint client to be used.
Client Secret	The secret configured for your user account on Proofpoint.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

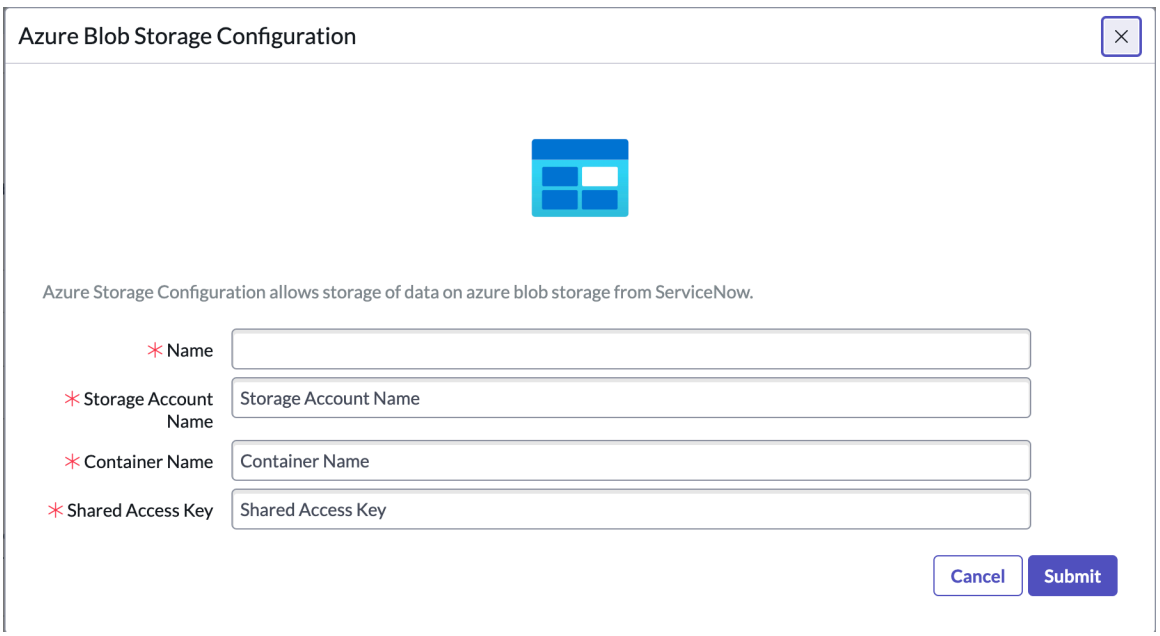


Note: For the existing customers, we continue to support Basic Authentication to ensure that the existing child tiles which have basic authentication function as expected. However, if a customer wishes to add OAuth to a child tile, they must not remove the existing Basic Authentication credentials (username and password). While they can replace these values with dummy entries, leaving the fields empty will prevent the tile from being submitted successfully.

5. Update the Azure Storage Configuration.

   a. In the Security Integrations page, search for **Azure Storage Configuration** tile.

   b. In the Azure Storage Configuration tile, click **Update**.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. On the form, fill in the fields.

Azure Storage Configuration form

Field	Description
Name	Name of the Azure Storage configuration.
Storage Account Name	Storage account name created on Azure portal
Container Name	Container name created in storage account on Azure portal.
Shared Access Key	Shared access key for the Storage account.

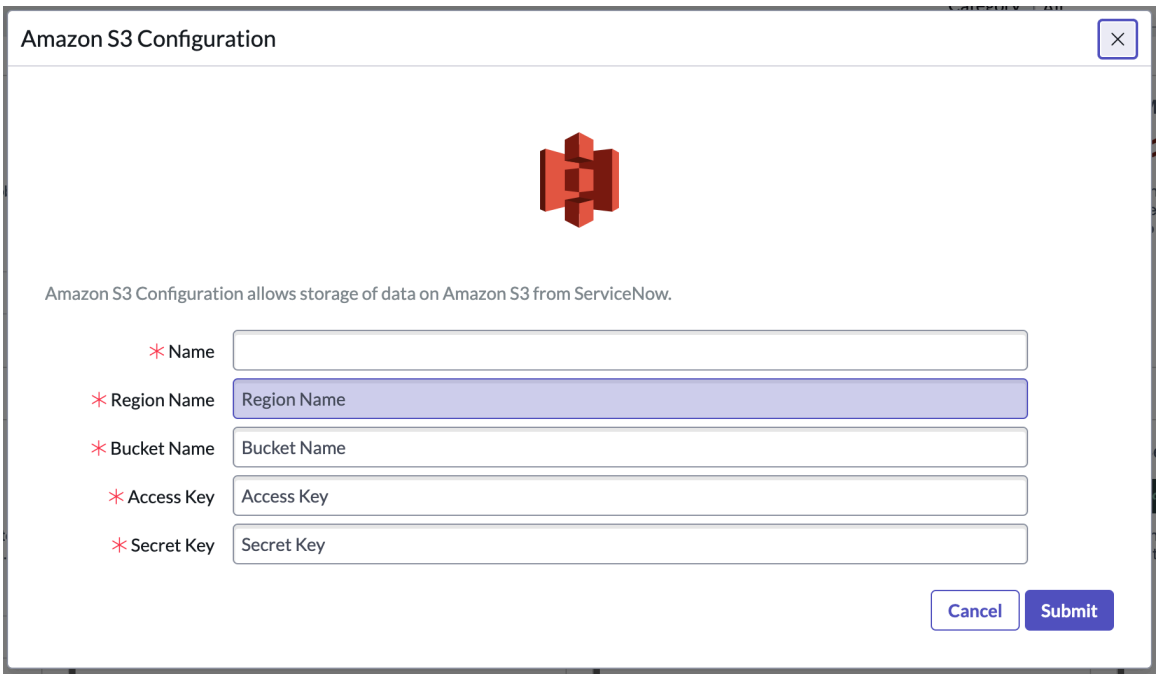
d. Click **Submit**.

After you successfully validate and submit the configuration, the Azure Storage Configuration is saved on the Security Integrations page as a tile.

6. Update the AWS Storage Configuration.

a. In the Security Integrations page, search for **AWS Storage Configuration** tile.

b. In the AWS Storage Configuration tile, click **Update**.



c. On the form, fill in the fields.

AWS Storage Configuration form

Field	Description
Name	Name of the AWS Storage configuration.
Region Name	Region name of the AWS Storage account.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Bucket Name	Bucket name created on the AWS portal.
Access Key	Access key with read and write access.
Secret Key	Secret key with read and write access.

7. Click **Submit**.

Result
After you successfully validate and submit the configuration, the Proofpoint DLP Integration is saved on the Security Integrations page as a tile.

Create an Application in Proofpoint and Obtain Client Credentials

Create an Application in Proofpoint and configure the required settings to obtain client credentials. These credentials enable secure access to Proofpoint's API for seamless integration and automation.

Before you begin
Role required: admin

Procedure
1. Log in to the Proofpoint Console.
   Access the Proofpoint Console using your credentials.
2. Create a New Application.
   a. In the **Developer** section, select Authorization.
   b. Select **Create**.
   c. Enter an application name.
   d. In Allowed Scopes, add scopes to your Application as required.
   e. In Allowed Grants, select **Client Credentials**.
   f. Select **Save**.
   Client ID and Client Secret are generated.
3. Configure Application details.
   a. Select the newly created Application.
   b. In the Access Policies, select **Edit**.
   Select either High Level or Granular access policies.
   c. Select **Done**.

Result
Use the generated Client ID and Client Secret to configure the integration in the DLP Proofpoint (PPT) application and start using it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure the Webhook on the Proofpoint DLP tenant for alert notifications to ServiceNow

Configure a webhook on Proofpoint using the REST API endpoint to start getting the alerts from the Proofpoint DLP tenant. Your ServiceNow instance creates DLP incidents from these alerts. The Proofpoint DLP integration provides a REST API endpoint for end users to configure the webhook.

Before you begin

Role required: sn_pp_dlp.api_integration_user

Procedure

1. Log in to **Proofpoint**.
2. Navigate to **Proofpoint Tenant** > **Administration Application** > **Integration** > **Notification Policies**.
3. Create a notification policy with an appropriate name.
4. Click the **Notification policy** and manage the webhooks configured on the notification policy.
5. Create a new webhook configuration by clicking **Add Webhooks**.
6. Select the webhook type as **Generic**.
7. In URL Input, enter a URL using the format: `https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts`.
8. Keep the method as **POST**.
9. Add the following headers to the webhook:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the
      ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D not change the other values.
11. Click **Save**.
12. Navigate to **Proofpoint Tenant** > **Administration Application** > **Policies** > **Rules**.
13. In the Actions section, select the rules for which the webhook notification should be generated.
14. Add the newly created Notification policies that have a webhook configured.
15. Click **Save**.

Create a Profile for Proofpoint DLP integration

Create an incident profile in your#ServiceNow AI Platform instance. Determine the#Proofpoint DLP incidents that are suitable for creating DLP incidents.

Before you begin

Role required: sn_dlir.admin

About this task

Configure the ServiceNow AI Platform to populate DLP alerts of Proofpoint. Store the alerts as DLP incidents in your ServiceNow instance.

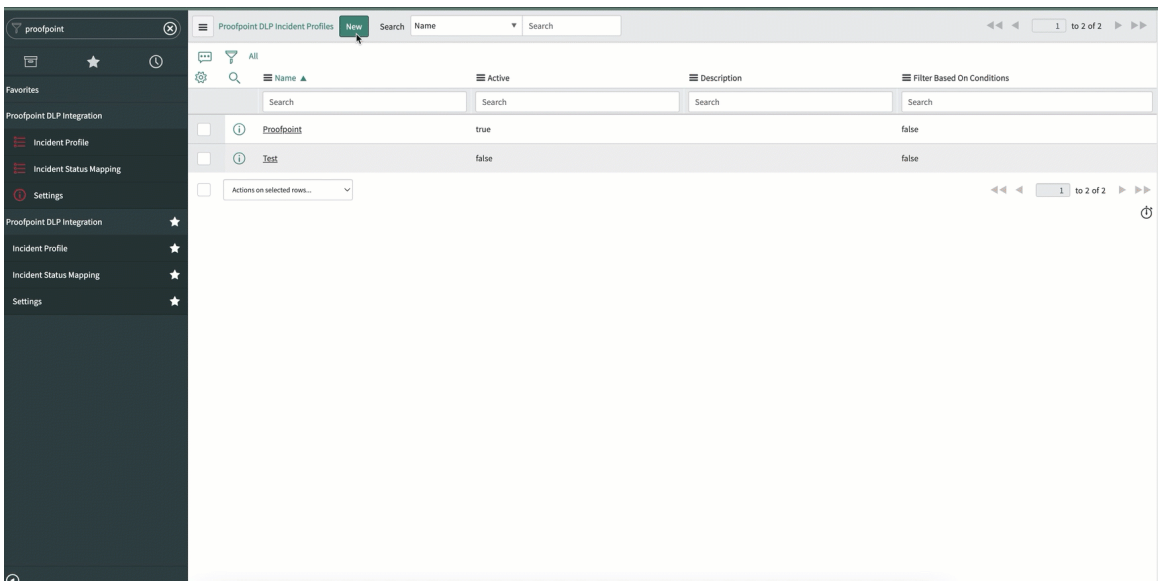
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Proofpoint DLP integration** > **Incident Profile**.
2. Click **New**.
3. On the form, fill the fields in the **Name** section.

Create a profile for Proofpoint DLP integration form

Field	Description
Name	Name of the profile. This name helps you to identify the profile. **Note:** The name must be unique for each profile.
Source	The Proofpoint DLP instance that you configured to ingest incidents. If you have multiple instances configured, select the appropriate instance for the incident types that you are planning to ingest for the profile.
Active	Option to make the profile active. When the profile is active, your ServiceNow AI Platform instance is ready to receive the incidents from Proofpoint.
Description	Description to help distinguish this profile from other profiles.



4. Click **Continue** and move to the Filtering section.

Define filters to apply for the Incident creation

Define and set filter conditions to filter the incoming#Proofpoint DLP#ncidents. Control which DLP incidents should be created on ServiceNow®.

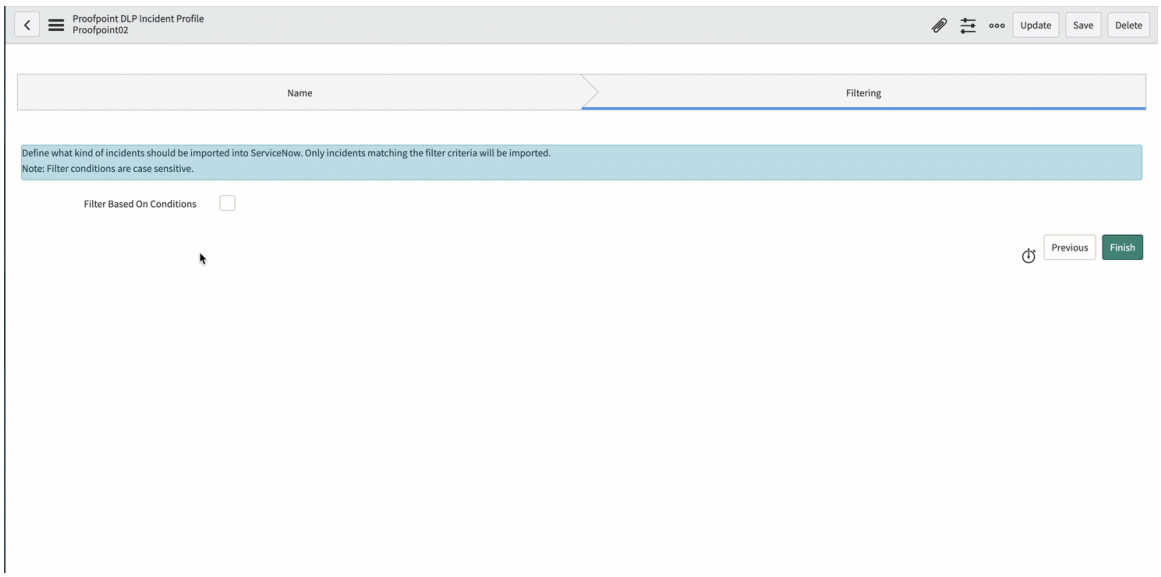
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_dlir.admin

About this task
This type of filtering helps you to isolate DLP incidents and to limit the number of DLP incidents that you create. If additional filtering criteria are set, only incidents that match the conditions are created.

Procedure
1. Select the **Filter based on conditions** option and define the criteria that an incoming Proofpoint DLP incident must satisfy so that a security incident is created.
2. Using the lists and fields of the condition builder, set the filters in the **Filter Conditions** field.

   The options in the first field in the **Filter Conditions** matches the fields that are available in the DLP incident. The criteria that you enter are case-sensitive. Verify that the criteria you define match the values of the incident.



3. Add more conditions by clicking#**AND**# or#**OR**.
   - If#**AND**#s selected, all conditions must be matched.
   - If#**OR**#s selected, either condition can be matched.
4. Click **Finish**.

Configure evidence file storage

Configure evidence file storage to securely store the evidence files in the ServiceNow instance or external for the Proofpoint email DLP Incidents.

Before you begin
Role required: sn_dlir.admin

About this task
You can configure the evidence file storage to securely store files. This provides an option for internal storage in ServiceNow instance or store externally, ensuring that files are stored and encrypted using Column Level Encryption. For more information, see Field Encryption on NowPlatform documentation.

When a DLP analyst performs the Download evidence files for DLP Incidents action from analyst workspace, the file will be downloaded from the selected storage if evidence file storage option

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

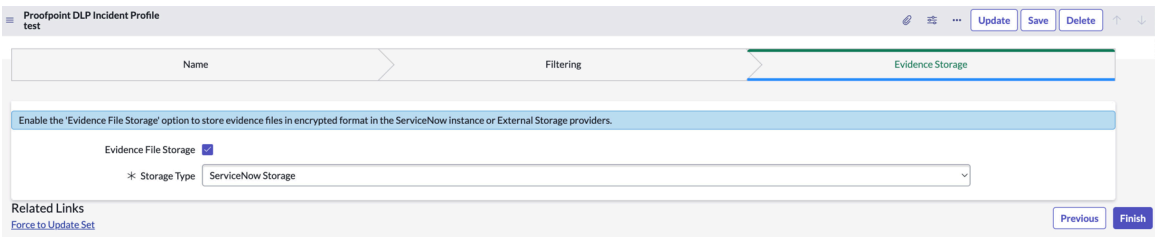
is enabled. Otherwise, the file will be downloaded directly from the Proofpoint source and will not be persisted in ServiceNow instance. For more information, see Download DLP incidents evidence files on Proofpoint.

Procedure

1. Select **Evidence Storage** section on the Incident Profile form.
2. Select **Evidence File Storage** check box to enable the file storage.
3. Select the preferred storage type.

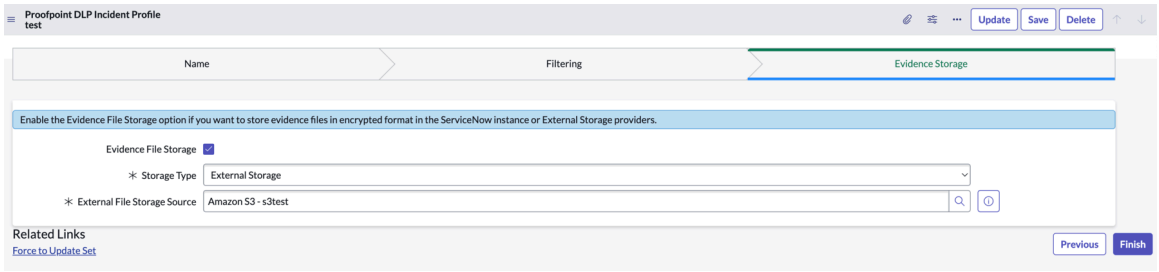
Field	Description
Evidence file storage	Option to enable the evidence file storage.
Storage type	Option to select the preferred storage type. You can use either internal or external stor age to store the evidence files. ○ **ServiceNow Storage**: This will store the ev idence files in the ServiceNow instance in an encrypted format. ○ **Evidence File Storage**: This storage provides a flexibility to man age the evidence files, allows you to choose the preferred storage method. Inter nal storage offers quick access within the application, while external storage supports both Blob storage and Amazon S3 storage options and allows the increased capacity and backup options. When you select this storage type, a new field is displayed: **Exter nal File Storage Source**.
External File Storage Source	This field supports both Blob storage and Amazon S3 storage options. This is in refer ence to the existing DLP Core configuration tiles for S3 or blob storage which are being used in Microsoft integration for match con tent storage.

Internal Storage



External Storage

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Click **Finish**.

Result

If the **Evidence File Storage** option is enabled and ServiceNow Storage is selected then the evidence files will be stored internally in an encrypted format, after the incidents from Proofpoint are fetched and if you perform **Download File** action for any of these Proofpoint incident then the system will get the evidence file from this table.

Download DLP incidents evidence files on Proofpoint

Download DLP incident evidence files that violate the DLP policy on Proofpoint.

Before you begin

Download this file onto your local machine from the DLP IR Analyst workspace and DLP IR End user workspace.

Note: **Download File** action will be available only for the approvers who has the secure file access role (applicable only for ServiceNow storage type and there is no role needed for external storage) on the DLP IR End User workspace.

Make sure to enable **Should downloading the violating file of the reported incident be allowed** property available under the **Settings** is enabled (or set to active true).

Role required:

- sn_dlir.analyst
- sn_dlir.secure_file_download

Note: Any approver with this role for internal storage only can download the file.

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a Proofpoint DLP incident with the Scan source as **Email SMTP**.
3. Click **Download File**.

For the approver to view the Download File action, follow the below steps:

4. Navigate to **All** > **DLP Incident Management** > **DLP User Workspace**.
   My DLP Incidents page will be displayed in a new tab.
5. Select **My Approvals** module available under My DLP Incidents module.
   My Approvals list view will be displayed.
6. Open an approval request record which is raised for Proofpoint DLP Incident with Scan source Email SMTP.
7. Click on info icon (i) available on the DLP Incident field on the form view.
8. Click **Download File**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result

After performing this action, the file that violated the DLP policy on Proofpoint will be downloaded to the user's local machine.

Note:

DLP admin can also control the access of **Download File** action by disabling the **Should downloading the violating file of the reported incident be allowed** setting from the Advanced Settings page. For more information, see Configure advanced settings for Data Loss Prevention Incident Response.

Preview evidence files

Preview Data Loss Prevention Incident Response evidence files in the DLP IR Analyst workspace.

Before you begin

Important: While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format. If you don't want to store the evidence files, disable the Evidence Files preview feature. For more information, see Configure advanced settings.

Role required: sn_dlir.analyst

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. From the contextual sidebar, select the Evidence files icon ( ).
4. On the **Evidence Files** tab, select the **Evidence File** card to preview the evidence files in the document viewer.

   The preview feature is different for each file type, as listed in the following table.

File Format	File Extension
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp. Image files open in the document viewer mode.
Microsoft Office files	.doc, .docx, .ppt, .pptx, .xls, and .xlsx Office files open in the document viewer mode.
Text files	.txt Text files open in text editor mode.
Mail files	.eml **Note:** The file size must be less than 5MB. You must first download the file to preview its content.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File Format	File Extension
PDF files	.pdf ○ Enter a keyword to search the document. ○ Zoom-in and zoom-out features to adjust the view for better readability. ○ Rotate the page clockwise or counterclockwise to view the content more clearly.

Note:

Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

Email remediation actions

Perform the remediation action on the email quarantined for Proofpoint.

Before you begin

Proofpoint provides four remediation actions:

1. Release Email with Scan
2. Release Email without Scan
3. Release Encrypted Email with Scan
4. Delete Email

By default, **Release Email with Scan**, **Release Email without Scan, Release Encrypted Email with Scan**, and **Delete Email response options** and **Proofpoint Remediation Action Rule** to perform the remediation action on the email. These response options also have the **Proofpoint Email Release Approval Rule** configured with it to leverage the approval functionality for these actions. These remediation actions are available to the End Users, Analysts, Escalated Incident Reviewers for execution.

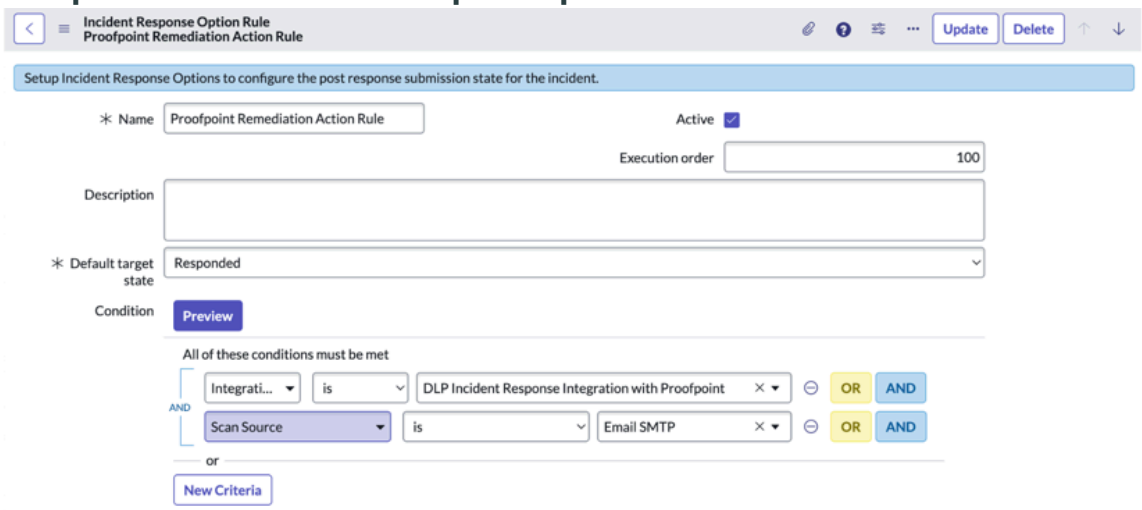
For more information, see Set up incident response option rules for your DLP incidents, Configure response option for your DLP incidents, and Configure Approval Rules.

Role required:

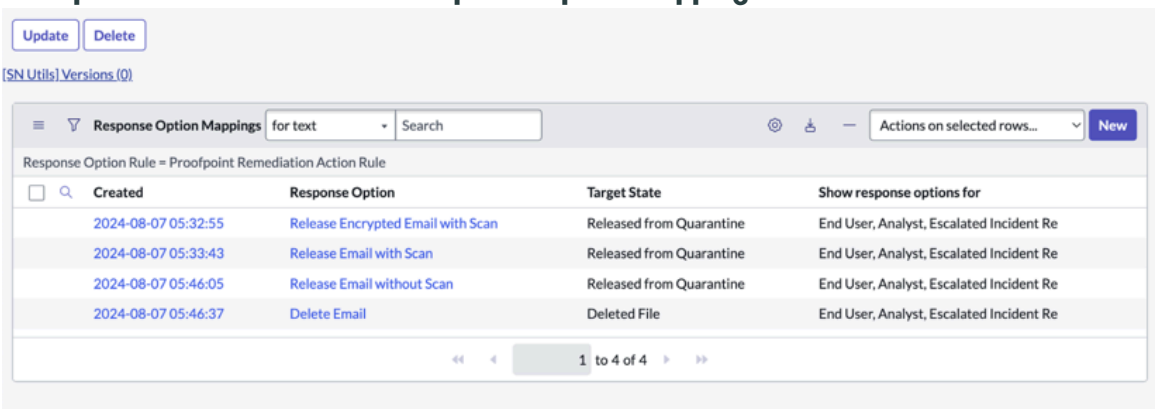
- sn_dlir.admin
- sn_dlir.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Proofpoint Quarantine Release Response Option Rule



Proofpoint Quarantine Release Response Option Mappings



Procedure

The following procedure explains how to submit the remediation action from the DLP Analyst Workspace. As a DLP Admin and DLP Analyst, you can:

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open any Proofpoint DLP incident with **Scan source** as Email SMTP.
3. Click **Respond**.
4. Select the response option from the **Response** drop down list.
5. Click **Submit**.

The following procedure explains how to submit the remediation action from the DLP User Workspace. As an end user, you can:

6. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
7. Open any Proofpoint DLP incident with **Scan source** as Email SMTP.
8. Click **Respond**.
9. Select the response option from the **Response** drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Click **Submit**.

Note:

- When an approval rule is configured for this action, the approval flow will be triggered first and after receiving all the approvals, the email remediation flow will be triggered, and then the action will be performed.
- If **Delete Email** is performed, then the state of the DLP incident is updated to **Delete File**. For any other response option, the DLP incident state will be updated to **Released Email from Quarantine** after the email is successfully released.

Map Proofpoint DLP incidents status with ServiceNow incident status

Synchronize the status of the DLP incidents ingested on your ServiceNow instance and DLP incidents of the Proofpoint. Map the ServiceNow Incident status with the Proofpoint Incident status.

Before you begin

Role required: sn_dlir.admin

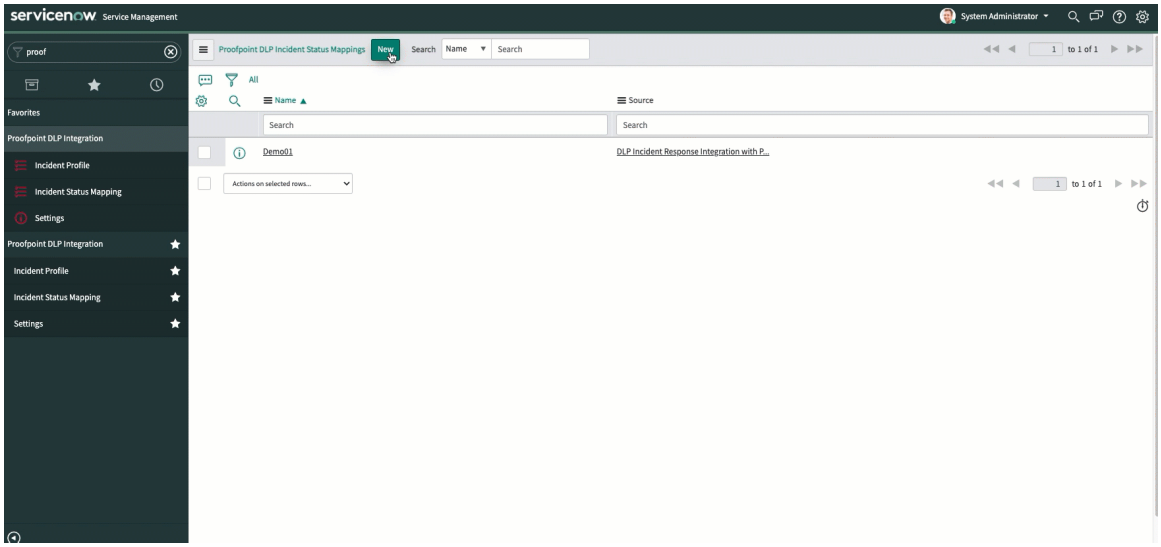
Procedure

1. Navigate to **Proofpoint DLP integration** > **Incident** > **Incident Status Mapping**.
2. Provide a **Name** to identify the mapping.
3. Select the **Source** (integration configuration) tile for which the Status Mapping should be applied.
4. Map the **ServiceNow DLP incident Status** with **Proofpoint Incident Status**.

Map Proofpoint DLP incidents status with ServiceNow incident status form

Field	Description
Name	Placeholder for the mapping record.
Source	Configured Proofpoint Endpoint source from where you want to fetch the incident status.
ServiceNow Incident Status	List of Status of DLP incidents.
Proofpoint Incident Status	Default mapped values for default states available in DLP incidents. For custom states, the default Proofpoint status is **New**. You can modify and add the required Proofpoint status in the input field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Click **Submit**.

Result

A record for mapping is successfully created. The statuses of the ServiceNow incidents will be synchronized with Proofpoint DLP incidents.

When you change the status of any DLP incident on your ServiceNow instance, then the status of the associated Proofpoint DLP incident will be changed on the source Proofpoint platform as per the mapping set in the record.

Configure Proofpoint DLP integration settings

Modify the#Proofpoint DLP#ntegration default system properties.

Before you begin

Role required: sn_dlir.admin

Procedure

1. Navigate to **Proofpoint DLP Integration** > **Settings**.
2. Modify the following settings as required.

Field	Description
Maximum Timeout for HTTP calls sn_pp_dlp.maximum_http_time_out	Maximum Timeout for HTTP calls (in sec onds). ○ Type: integer ○ Default value: 30
Send DLP Incident updates back to Proof point sn_pp_dlp.incident_update	This property enables restricting any synchro nization from your ServiceNow instance to Proofpoint DLP incidents. ○ Type: Boolean ○ Default value: true
Level of reporting the logs generated by the integration sn_pp_dlp.logging.verbosity	The level of reporting logs generated by the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Should downloading the violating file of the reported Proofpoint incident be allowed sn_pp_dlp.enable_file_download	Option to choose whether you want to enable download of the file. By default, this option is enabled. The default value is: True (enable).

3. Click **Save**.

Result
Your modified integration settings are applied in the next polling interval as defined in the profile.

Domain Separation in Proofpoint DLP integration

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with Proofpoint DLP integration

Follow these steps to achieve domain separation:

- Create a user with the required role in the respective domain.
- Perform the Proofpoint DLP integration procedures in the appropriate domain.

Data Loss Prevention Incident Response Integration with Netskope

The Netskope DLP integration supports the ingestion of Data Loss Prevention incidents created on the Netskope Data Loss Prevention deployment. Netskope DLP helps companies to track the usage and movement of sensitive data on various platforms.

After ingestion, you can use the incident management functionalities to remediate the DLP incidents.

Key features

This integration includes the following key features:

- Multiple profile creation for different Netskope tenants.
- Automating the creation of ServiceNow DLP incidents from Netskope DLP incidents.
- Filtering of Netskope DLP incidents.
- Scheduled ingestion of Netskope DLP incidents that create DLP incidents in ServiceNow.
- Automatically update object status on Netskope when the DLP state changes in your ServiceNow instance.
- View the forensic details (violating content) of the DLP Incident on DLP IR Analyst workspace and DLP End user workspace.

Note: The violating content doesn't persist in ServiceNow. The content is pulled when the incident is in opened in the workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Downloading evidence file directly from Netskope on demand.

  Note: The evidence file doesn't persist in ServiceNow. The evidence file is pulled when the analyst click on the **Download File** in the workspace.

- Notification via email to DLP Admin users on Netskope token expiration.
- Notification via email is sent to DLP Admin users if it exceeds the defined retry limit for incident API call failures.
- Netskope also supports integration run process. For more information, see Monitor DLP Integration Run process.

Getting started with Netskope DLP integration for Data Loss Prevention

Review the following information before you start setting up your Netskope DLP integration for Data Loss Prevention.

Setup Task	Description
Verify you have assigned the required ServiceNow AI Platform, Data Loss Prevention Application.	The following roles are used across the Netskope DLP integration on the ServiceNow AI Platform: • The Administrator (admin) installs the applications from the ServiceNow Store and assigns the Data loss prevention admin (sn_dlir.admin). • The user with sn_dlir.admin role can configure the integration and set up the incident profiles. • The users with sn_dlir.analyst role will have read roles across the integration.
Assign the required privileges for Netskope API v2 token.	The following endpoint privileges are used across the Netskope API v2 tokenization. • Read: /api/v2/incidents/dlpincidents • Read: /api/v2/events/dataexport/events/incident • Read + Write: /api/v2/incidents/update
Verify that the end-user core application required to support the Netskope DLP integration is installed and activated.	Verify that the following DLP applications and security support common applications are installed and activated from ServiceNow Store. If not installed, install, and activate on application. • Security Support Common • Data Loss Prevention Incident Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Install and configure the Netskope DLP integration for Data Loss Prevention

Install and configure the Netskope DLP integration from #ServiceNow Store #ServiceNow AI Platform instance. You can start investigating DLP incidents using the#Netskope DLP incident data.

Before you begin

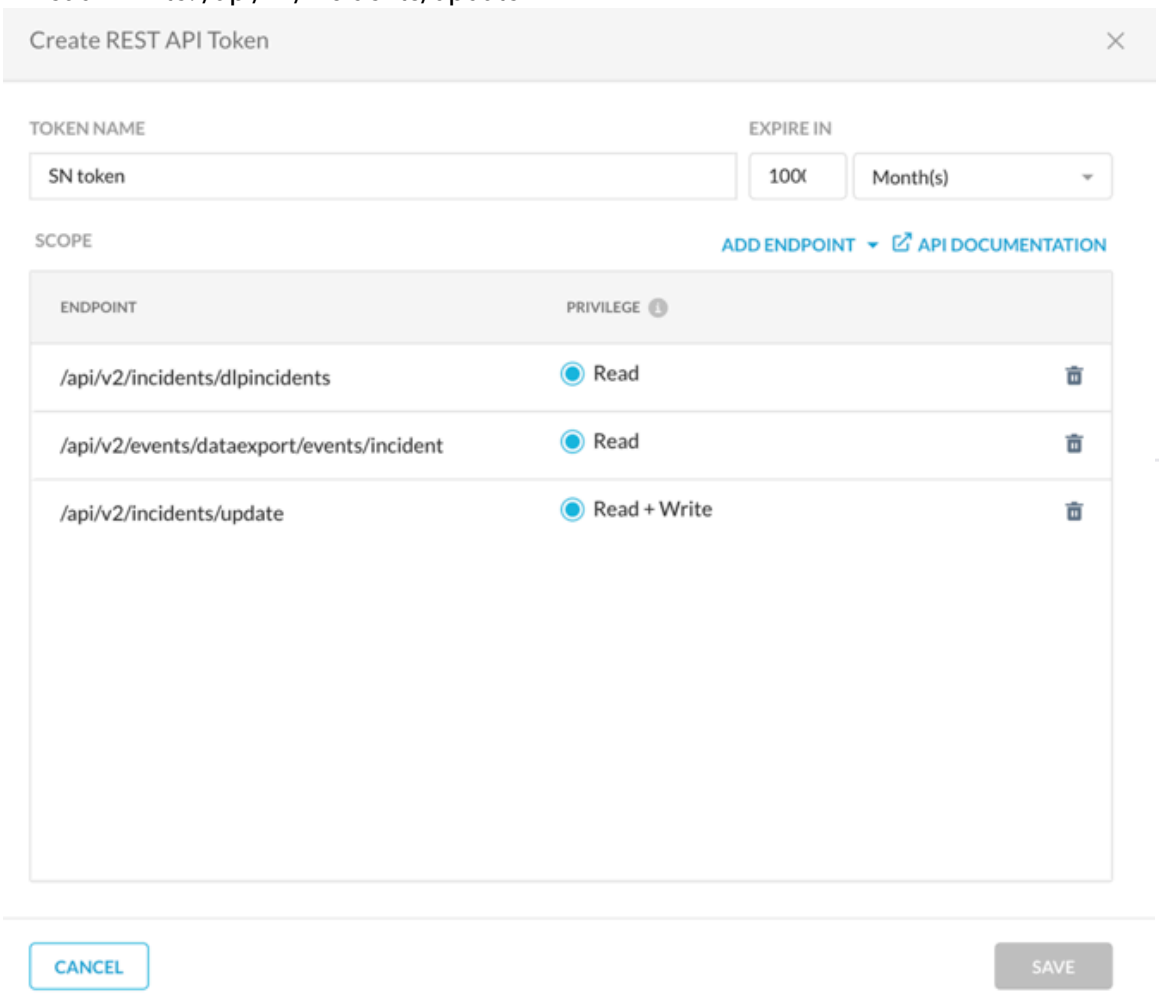
Role required: sn_dlir.admin

Procedure

1. Download the#Netskope DLP integration from the ServiceNow Store and install it.
2. Navigate to#**Security Operations** > **Integrations** > **Integration Configurations**
3. Search for#DLP `Incident Response Integration with Netskope` tile, and click #**Configure**.
4. On the form, fill in the fields.

Note: Make sure your Netskope API v2 Token has the below endpoint privileges:

- Read: /api/v2/incidents/dlpincidents
- Read: /api/v2/events/dataexport/events/incident
- Read + Write: /api/v2/incidents/update



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Name	Name of the Netskope DLP integration configuration.
Netskope Tenant	The Netskope base URL for the Netskope tenant.
Netskope API v2 Token	Token configured for REST API v2 on your user account at Netskope.

5. Click **Submit**.

Result

Note: Please connect netskope sub prod to the ServiceNow sub prod. Keep all the username and passwords in sync across the instances to avoid accounts getting logged out.

After you successfully validate and submit the configuration, the Netskope DLP Integration is saved on the Security Integrations page as a tile.

Create a Profile for Netskope DLP integration

Create an incident profile in your ServiceNow AI Platform instance.

Before you begin

Role required: sn_dlir.admin

About this task

Configure ServiceNow AI Platform to retrieve the DLP incidents from the Netskope endpoint. Store the incidents into your ServiceNow instance as DLP incidents.

Procedure

1. Navigate to **Netskope DLP integration** > **Incident Profile**.
2. Click **New**.
3. On the form, fill in the fields.

Create a Profile

Field	Description
Name	Name of the profile. The name must be unique for each profile. This name helps you to identify the profile.
Source	Netskope DLP instance that you configured to ingest incidents. If you have multiple instances configured, select the appropriate instance for the incident types that you are planning to ingest for the profile. **Note:** Only one active profile is allowed per source.
Active	Indicator that the profile is active.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: This field is available only after you click **Finish** in the last Scheduling section. When the profile is active, your ServiceNow AI Platform instance is actively polling Netskope DLP incidents. Corresponding DLP incidents are created as ServiceNow DLP incidents when the filtering conditions are matched based on the Scheduling parameters you have provided.
Order	Order of the profile execution. The profile with the lowest order considered as the highest priority. By default, the value is 100.
Description	Description to help you distinguish this profile from other profiles.

4. Click **Continue** and move to the Filtering section.

Define Filters to apply for the Incident creation

Define and set filter conditions to filter the incoming#Netskope DLP#incidents. Control which of these incidents should be created as DLP incidents on your ServiceNow instance.

Before you begin
Role required: sn_dlir.admin

About this task
This type of filtering helps you to isolate DLP incidents and to limit the number of DLP incidents that you create. If additional filtering criteria are set, only incidents that match the conditions are created.

Procedure
1. Select the **Filter based on conditions** option and define the criteria that an incoming Netskope DLP incident must satisfy so that a DLP incident is created.
2. Using the lists and fields of the condition builder, set the filters in the **Filter Conditions** field.

   The options in the first field in the **Filter Conditions** match the fields that are available in the **Netskope DLP incident import** table. The criteria that you enter are case-sensitive. Verify that the criteria you define match the values of the incident.
3. Add more conditions by clicking#**AND**# or#**OR**.
   - If#**AND**#is selected, all conditions must be matched.
   - If#**OR**#is selected, either condition can be matched.
4. Click **Continue** and move to the Scheduling section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Schedule the Netskope DLP incidents retrieval

Set a schedule to retrieve Netskope DLP incidents that match the criteria in the profile.

Before you begin

Role required: sn_dlir.admin

About this task

You can plan how often you will poll for net new Netskope incidents that match the incident profile configuration. To enable automated incident ingestion, you must configure the scheduling and incident retrieval before you activate the profile. The profile can be configured to do one-time retrieval using the **One-Time Retrieval** check box. The historical date can be up to one month from the past.

Procedure

1. Configure the schedule to define how and when you pull incidents from Netskope.
2. On the form, fill in the fields.

Schedule the Netskope DLP incidents

Field	Description
Ongoing Incident Ingestion	Ongoing incident ingestion that your ServiceNow AI Platform instance pulls from #Netskope for new incidents. If there are triggered incidents found, which match with the incident filtering criteria, then DLP incidents are created.
Polling increment (minutes)	Polling frequency that is defined in minutes. This default value is set to **5**.
Set Initial Incident Ingestion Time	Option to set initial incident ingestion based on the configured date and time. You can use this option to define a specific date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.
Input Initial Incident Ingestion Time	Date and time that you specify for the incident ingestion.
Initial Incident Ingestion Time	The first time when data is ingested. **Note:** The value is visible only if the **Set Initial Incident Ingestion Time** option is selected.
Next Incident Ingestion Time (estimated)	The next estimated incident ingestion time.
One-Time Retrieval	Option to enable one-time historical data pull.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: If selected, then historical data will be pulled from Netskope DLP according to the date added in **Since Date**.
Since Date	Date from when data is fetched from Netskope. **Note:** At most the last 30 days of data can be fetched from Netskope.

3. Click **Finish**.
4. On the pop-up, save the created profile configuration by clicking **Finish**.
5. Activate the profile.
   a. Open the created profile.
   b. Set **Active** to **true**.
   c. Click **Update**.

Result
After the successful creation activation of the profile, incidents will be fetched periodically as per the configuration set in the profile. The incidents will be added into the DLP incidents table.

Mapping DLP incident status with Netskope

The incident status mapping section enables the users to provide the mappings between the DLP Incident status in ServiceNow and Netskope Object status.

Before you begin
The mapping will be used when ingesting any DLP incident from Netskope to ServiceNow as well as syncing any state change of DLP incident in ServiceNow back to Netskope.

Synchronize the status of the DLP incidents ingested on the ServiceNow with the DLP incident of Netskope. Map the ServiceNow Incident Status field with the Netskope Object Status field.

Role required: sn_dlir.admin

About this task
You need to create a one-to-one incident status mapping of Netskope and ServiceNow status.

Procedure
1. Navigate to **Netskope DLP integration** > **Incident status mapping**.
2. Provide a Name to identify the mapping.
3. Select the Source integration.
4. Map the DLP Incident Status with Netskope Object Status (Duplicate Netskope state can also be mapped).
   The status sync from ServiceNow to Netskope will be disabled if you don't create a mapping record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

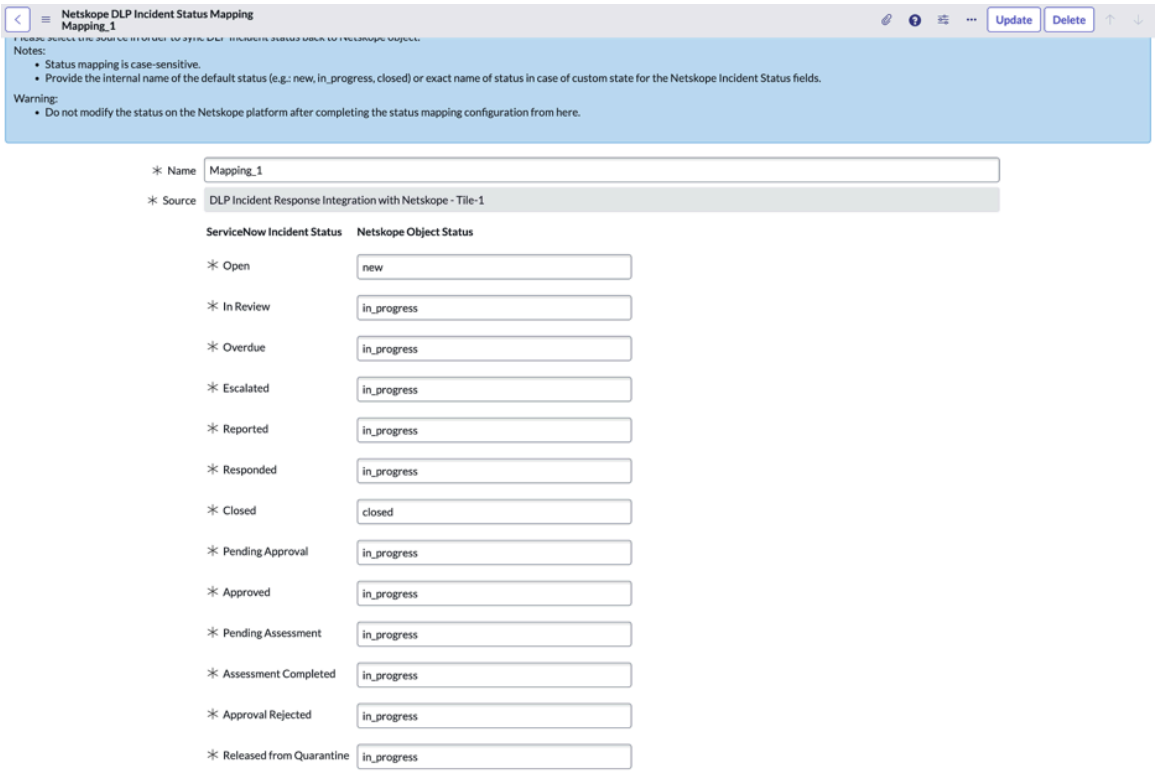
Important: You need to map all the Netskope object statuses to all ServiceNow statuses. Select the source in order to sync DLP Incident status back to Netskope object.

The following information and alert messages are displayed when you map the incident status, review the messages and proceed further.

Note:

- Status mapping is case-sensitive.
- Provide the internal name of the default status (For example: new, in_progress, closed) or exact name of status in case of custom state for the Netskope Object Status fields.

Warning: Do not modify the status on the Netskope platform after completing the status mapping configuration from here.



Netskope DLP Incident Status Mapping

Field	Description
Name	Name of the mapping record.
Source	The configured Netskope Endpoint source from where you want to sync the incident status.
DLP Incident Status	Indicates the list of DLP incidents status.
Netskope Object Status	Indicates the list of Netskope object status.

5. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
After successfully creating the record for status mapping, whenever there is an update on ServiceNow DLP incident's state then it will automatically reflect it on Netskope side as per the mapping.

Note: If you change the status of any DLP incident on Netskope tenant directly, then the status sync from SN to Netskope will not work considering the API limitations. Ensure you map all the DLP incident status with Netskope object status carefully.

Configure Netskope DLP integration settings

Modify the#Netskope DLP#integration default system properties.

Before you begin
Role required: sn_dlir.admin

Procedure
1. Navigate to **Netskope DLP Integration** > **Settings**.
2. Modify the following settings as required.

Configure Netskope DLP integration settings

Field	Description
Should downloading the violating file of the reported incident be allowed sn_ns_dlp.enable_file_download.	Option to choose whether you want to enable download of the file. By default, this option is enabled.
Maximum Timeout for HTTP calls, in seconds sn_ns_dlp.maximum_http_time_out.	Maximum Timeout for HTTP calls, in seconds. This field is automatically set to 30.
Maximum number of retries to be performed for API failures. sn_ns_dlp.maximum_retry.	Maximum number of retries to be performed for API failures. The default value is set as 3.
Level of reporting the logs generated by the integration sn_ns_dlp.logging.verbosity.	Define the level of reporting logs generated by the integration. This field is automatically set to **info**.

3. Click **Save**.

Result
Your modified integration settings are applied in the next polling interval as defined in the profile.

Download evidence files

Download files that violate the DLP policy on Netskope. Download this file onto your local machine from the DLP IR Analyst workspace and DLP IR End user workspace for approvers.

Before you begin
Role required:

- sn_dlir.analyst
- sn_dlir.secure_file_download (any approver with this role)

About this task
You need to enable file download for Netskope before moving ahead.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Netskope DLP Integration** > **Settings**.
2. Enable the property **Should downloading the violating file of the reported incident be allowed**.
   You will be able to see the **Download File** button in the DLP IR Analyst Workspace and DLP IR End user workspace.
3. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
4. Open a DLP incident record which is ingested from Netskope source.
5. Click **Download File**.
   The file that violates the DLP policy on the Netskope will be downloaded to the user's local machine.

> **Note:** DLP admin can control the access of **Download File** action for all integrations by disabling the **Should downloading the violating file of the reported incident be allowed** option from the **Advanced Settings** page of DLP Administration. For more information, see Configure advanced settings.

Preview evidence files

Preview DLP incident evidence files in the DLP IR Analyst workspace.

Before you begin

- Navigate to **All** > **DLP Administration** > **Advanced Settings**.
- Make sure the **sn_ns_dlp.enable_evidence_file_preview** property is already enabled.

> **Important:** While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format for the duration you have selected using **sn_dlir.preview_temp_files_cleanup_interval** property from the **Advanced Settings** page. You can disable the **Evidence Files** preview feature if you don't want to store any data in the ServiceNow database. For more information, see Configure advanced settings.

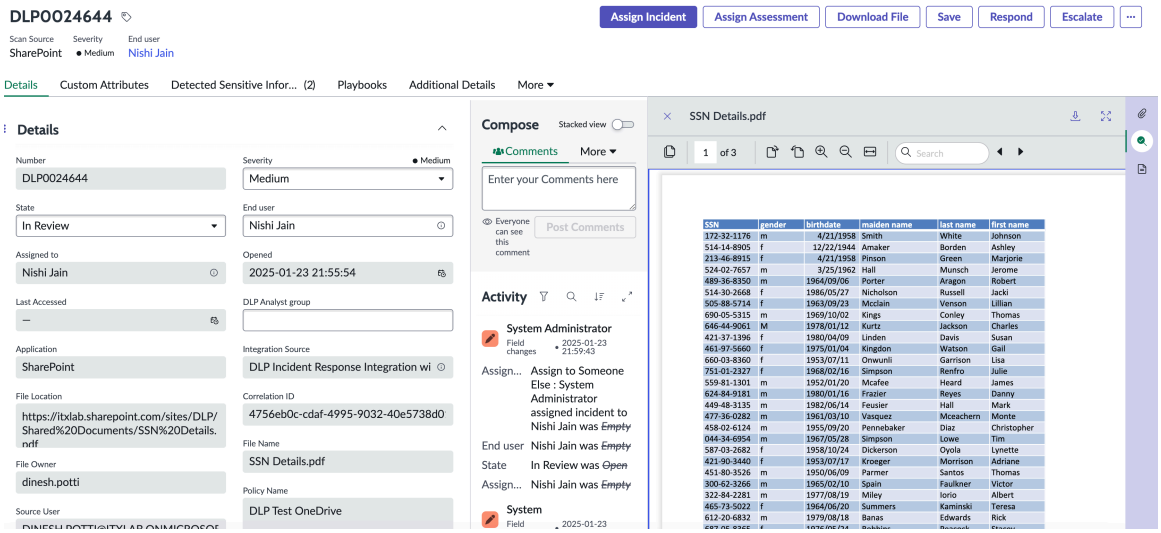
Role required: sn_dlir.analyst

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. Select the **Evidence Files** icon, which is available on the contextual menu.
   A tab opens which fetches all the evidence files. Once the download is finished, you can view all the evidence files in the **Evidence Files** tab.
4. Select the **Evidence File** card which you want to preview.
   The preview feature is different for each file type.
5. Preview pdf and office docs in the document viewer by selecting the **Expand** icon on the top right of the evidence file to open the pdf in full screen.
   Office Extensions for which the document viewer opens the evidence files include- doc, docx, ppt, pptx, xls, xlsx.
   a. Locate the search bar and enter the keyword you're looking for.
   b. Use the zoom-in and zoom-out features to adjust the view for better readability.
   c. Rotate the page clockwise or counterclockwise to view the content more clearly.

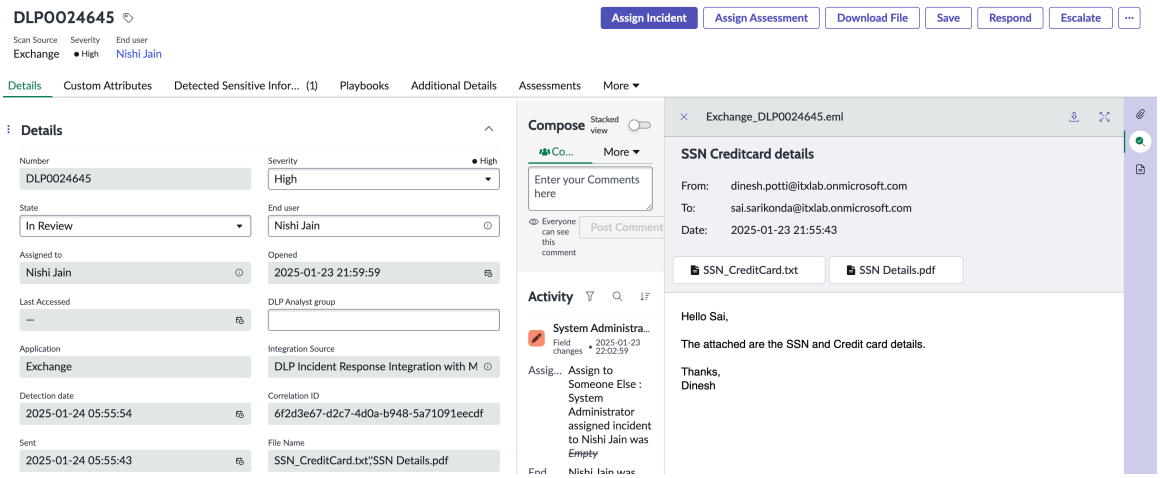
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These control options enhance your ability to understand the evidence file comprehensively. Only the pdf has control options in the header.



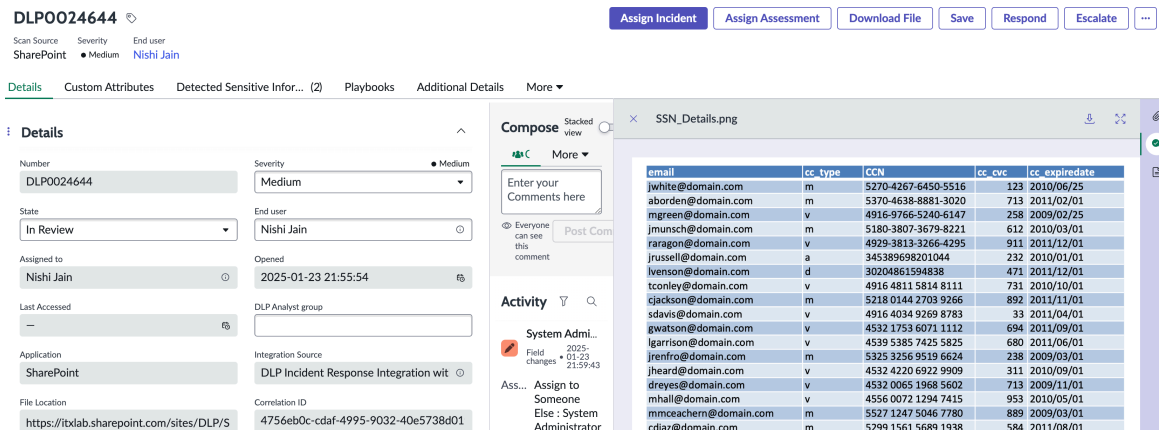
6. Preview eml files.
   Select the attachments in the email and preview them.

> **Note:** If the selected evidence file exceeds the 5-MB limit, it can't be previewed in the analyst workspace. You have to download the file to preview its content. This limit is only for .eml files.

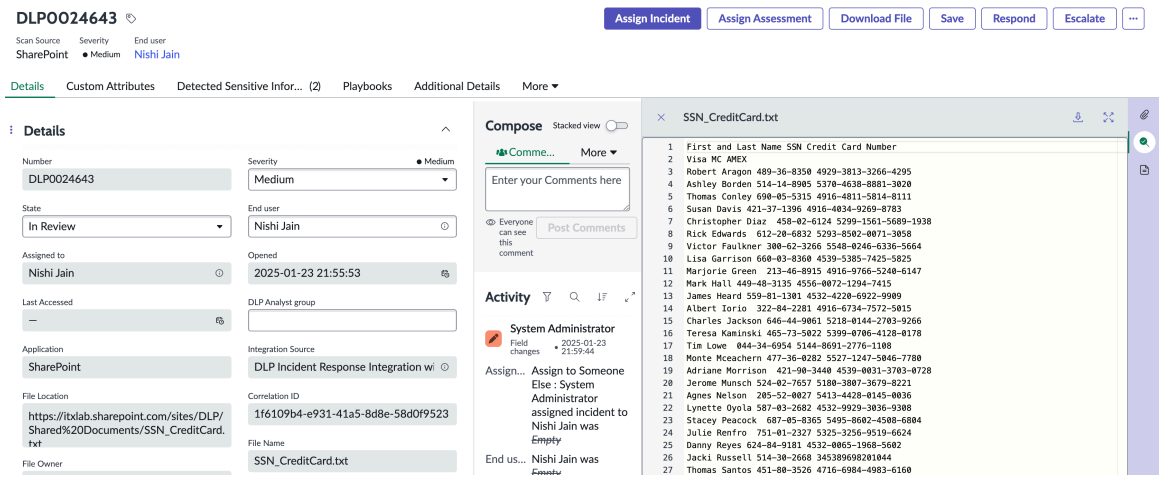


7. Preview images in the DLP analyst workspace.
   Images only with the .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp extensions are supported.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. Preview text files in the text editor by selecting the **Expand** icon on the top right of the evidence file.



Note: Evidence Files apart from the office docs, eml files, text, and image extensions won't be supported for preview. Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

Notifications for users on retry mechanism

Netskope integration will retry the configured number of times in case of API failures during DLP Incident ingestion.

Once the maximum retry limit is exceeded, Netskope integration sends out an email notification to users who have the DLP Admin (sn_dlir.admin) role.

After you complete the integration setup and configuration, provide the DLP Admin (sn_dlir.admin) role to the users who should be notified when the maximum retry limit exceeds.

Once the maximum retry limit is exceeded, the profile will skip ingestion for a duration of up to one hour. The maximum retries are configured using the property: `Maximum number of retries to be performed for API failures`. For more information, seeConfigure Netskope DLP integration settings.

Email notifications on credential expiration

When the token used in the ServiceNow instance expires, Netskope integration sends out an email notification to users with the DLP Admin (sn_dlir.admin) role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the setup of the integration configuration is completed, provide the DLP Admin (sn_dlir.admin) role to the users who should be notified if the token expired.

If the token expires, the data ingestion for associated profiles would be on hold until the Netskope integration configuration is updated with a valid token.

You must create a token or renew the old one on Netskope, and then update the token on the ServiceNow instance. If you renew the token by extending the expiry time, then the Netskope application automatically detects the renewal and will continue with the data collection. If you create a token, you must update the token in the configuration.

Domain Separation in Netskope DLP integration

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with Netskope DLP integration

Follow these steps to achieve domain separation:

- Create a user with the required role in the respective domain.
- Perform the Netskope DLP integration procedures in the appropriate domain.

Internet Content Adaption Protocol (ICAP) integration for DLP IR

The Internet Content Adaption Protocol (ICAP) DLP integration supports the ingestion of Data Loss Prevention Incident Response alerts, allows the fetching of match content, and evidence files from Amazon S3 created on the ICAP supported Data Loss Prevention Incident Response deployment.

After the alerts are ingested, you can use the DLP workspace to view the required key information such as match content, alert severity, and various incident management functionalities to remediate the DLP incidents.

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview and key features

The Internet Content Adaption Protocol (ICAP) integration helps you to track the usage and movement of sensitive data on various platforms.

This integration includes the following key features:

- Ingestion of DLP Alerts: Users would be able to configure and schedule the ingestion of DLP alerts from specified Amazon S3 buckets. This includes the capability to perform delta imports to ensure only new data is ingested.
- Display ingested alerts in the DLP Workspace: Once the alerts are ingested, they should be displayed in the DLP workspace, providing key details about each alert such as match content, alert severity, and relevant metadata.
- Match content: Sensitive information records are created during ingestion, match content is fetched when the record is opened.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Evidence file download: The system would allow users to download associated evidence files directly from the DLP workspace for further investigation or review.
- Ability to customize and define the severity mapping between ICAP DLP incidents with ServiceNow incidents.

Getting started with ICAP DLP integration for Data Loss Prevention

Before you can use the integration, you must download it from the ServiceNow® Store

Checklist

Review the following information before you start setting up your provider ICAP DLP integration for data loss prevention.

Checklist

Field	Description
Verify you have assigned the required ServiceNow AI Platform, Data Loss Prevention Application application roles.	Following roles are used across the ICAP DLP integration on the ServiceNow AI Platform: • The Administrator (admin) install the applications from the ServiceNow® Store and assigns the Data Loss Prevention admin (sn_dlir.admin). • The user with sn_dlir.admin role can configure the integration and setup the incident profiles. • The users with sn_dlir.analyst role will have read roles across the integration configurations.
Verify you have assigned the required Amazon S3 bucket policies.	You can follow the official AWS documentation for creating and managing IAM users, policies, and permissions through the following links: • Creating an IAM User • Creating IAM Policies • Amazon S3 Permissions **Note:** Using the above links, you can learn more on the detailed instructions and further options for managing IAM users and S3 permissions in AWS, also how to create an IAM user in your AWS account - AWS Identity and Access Management, and the basic overview of the process used to create an IAM user and credentials in AWS Identity and Access Management.
Verify that ServiceNow® core application that is required to support the ICAP DLP integration are installed and activated.	Verify that the following DLP applications and security support common applications are installed and activated from ServiceNow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Field	Description
	Store. If not installed, install, and activate on application. • Security Support Common • Security Case Management common workspace components. • Data Loss Prevention Incident Response

Install and configure the ICAP DLP integration

Install and configure the#provider ICAP DLP integration from the#ServiceNow® Store on your #ServiceNow AI Platform instance. Start investigating DLP incidents using the#provider ICAP DLP incident data.

Before you begin

Role required: sn_dlir.admin

Procedure

1. Download the#provider ICAP DLP integration from the#ServiceNow® Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Search for the#DLP Incident Response Integration with ICAP tile and click#**Configure**.



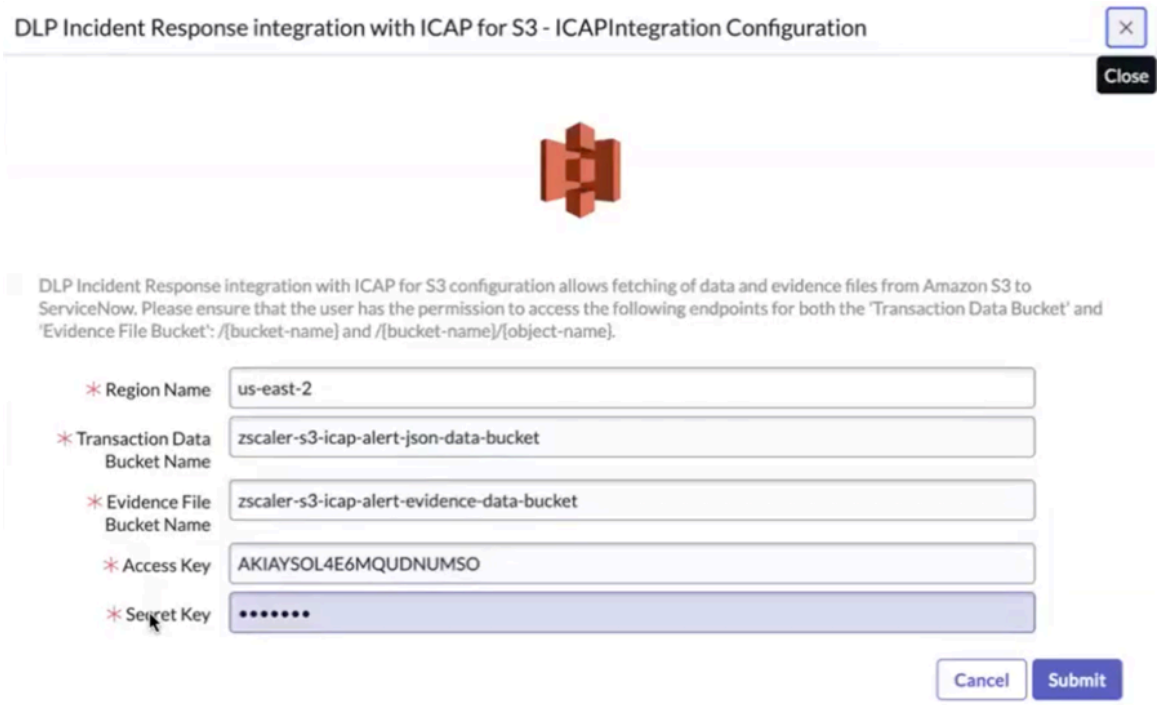
4. On the form, fill in the fields.

ICAP DLP Integration Configuration form

Field	Description
Region Name	Region name of the Amazon S3 bucket name.
Transaction Data Bucket Name	Transaction data bucket name is the bucket where a DLP violation transaction has occurred.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Evidence File Bucket Name	Evidence file bucket name is the bucket where you can find the DLP file that caused the violation.
Access Key	AWS IAM access key for the ICAP configuration.
Secret Key	AWS IAM secret key for the ICAP configuration.



5. Click **Submit**.

Result

Note: Please connect ICAP sub prod to the ServiceNow sub prod. Keep all the username and passwords in sync across the instances to avoid accounts getting logged out.

After you successfully validate and submit the configuration, the ICAP DLP Integration configurations is saved.

Create a profile for ICAP DLP integration

Create an incident profile in your#ServiceNow AI Platform instance. Determine the#CAP DLP alerts that are suitable for creating DLP incidents.

Before you begin

Role required: sn_dlir.admin

About this task

Configure the NowPlatform to fetch the DLP alerts from Amazon S3 configuration. Store these alerts into your ServiceNow instance as DLP incidents.

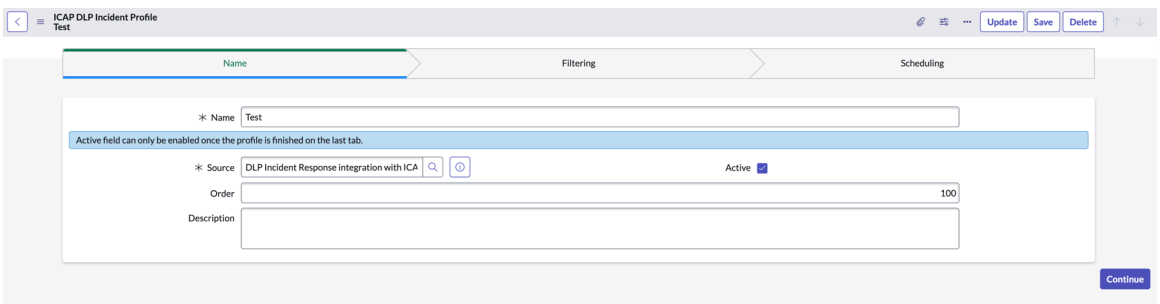
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **ICAP DLP Integration** > **Incident Profile**.
2. Click **New**.
3. On the form, fill the fields in the Name section.

Create a profile

Field	Description
Name	Name of the profile. This field helps you to identify the profile. **Note:** The name must be unique for each profile.
Source	Amazon S3 configuration that you configured to ingest incidents. If you have multiple sources configured, select the appropriate source for the incident type that you are planning to ingest for the profile. **Note:** Only a single source is allowed for the active profile.
Active	Option to indicate if the profile is active. This field can only be enabled after you click the **Finish** in the Scheduling section. When the profile is active, it implies that the#ServiceNow AI Platform is actively polling ICAP DLP alerts. The corresponding DLP alerts are created in#DLP #when the filtering conditions are matched based on the Scheduling parameters that you have provided.
Order	Order of the profile execution. The profile with the lowest order considered as the highest priority. By default, the value is 100.
Description	Description for this profile.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
To move to the Filtering section, click **Continue**.

Define filters to apply for the Incident creation

Define and set filter conditions to filter the incoming DLP alerts. Determine the alerts that should be created as DLP incidents in ServiceNow.

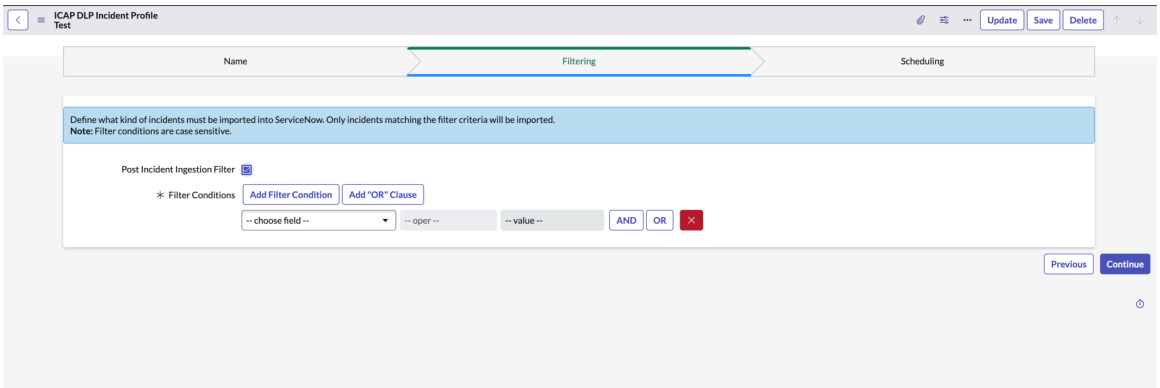
Before you begin
Role required: sn_dlir.admin

About this task
Filtering helps you to isolate DLP alerts and to limit the number of DLP alerts that you create. If additional filtering criteria are set, only alerts that match the conditions are created.

Procedure
1. Select **Post Incident Ingestion Filter** check box to apply the post incident ingestion filters and retrieve the incidents that match the filter criteria.
2. Select the **Filter based on conditions** option and define the criteria that an incoming ICAP DLP incident must satisfy so that a DLP incident is created.
3. Set the filters in the **Filter Conditions** field.

   The options in the drop down **Filter Conditions** match the fields that are available in the **ICAP DLP incident import** table. The criteria that you enter are case-sensitive. Verify that the criteria you define match the values of the incident.

4. Add more conditions by clicking **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.



What to do next
To configure the schedule, click **Continue**.

Schedule the ICAP DLP incidents retrieval

Set a schedule to retrieve ICAP DLP alerts that match the criteria in the profile.

Before you begin
Role required: sn_dlir.admin

About this task
You can plan how often you will poll for net new ICAP incidents that match the incident profile configuration. To enable automated incident ingestion, you must configure the scheduling and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

incident retrieval before you activate the profile. The profile can be configured to do one-time retrieval using the **One-Time Retrieval** check box.

Procedure

1. Configure the schedule to define how and when you pull incidents from ICAP.
2. On the form, fill in the fields.

Schedule the ICAP DLP incidents

Field	Description
Ongoing Incident Ingestion	Ongoing incident ingestion that your ServiceNow AI Platform instance pulls from #CAP for new incidents. If there are triggered incidents found, which match with the incident filtering criteria, then DLP incidents are created.
Polling increment (minutes)	Polling frequency that is defined in minutes. This default value is set to **5**.
Set Initial Incident Ingestion Time	Option to set initial incident ingestion based on the configured date and time. You can use this option to define a specific date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period.
Input Initial Incident Ingestion Time	Date and time that you specify for the incident ingestion.
Initial Incident Ingestion Time	The first time when data is ingested. **Note:** The value is visible only if the **Set Initial Incident Ingestion Time** option is selected.
Next Incident Ingestion Time (estimated)	The next estimated incident ingestion time.
One-Time Retrieval	Option to enable one-time historical data pull. **Note:** If selected, then historical data will be pulled from ICAP DLP according to the date added in **Since Date**.
Folder Name	Name of the folder from which you want to retrieve the data. All the folders whose names are lexicographically greater than the provided folder name will be ingested in one-time retrieval.

3. Click **Finish**.
4. On the pop-up, save the created profile configuration by clicking **Finish**.
5. Activate the profile.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Open the created profile.

b. Set **Active** to **true**.

c. Click **Update**.

Result

After the successful creation activation of the profile, incidents will be fetched periodically as per the configuration set in the profile. The alerts will be added into the DLP incident table.

View sensitive information for DLP alerts

View the detected sensitive information for DLP alerts.

Before you begin

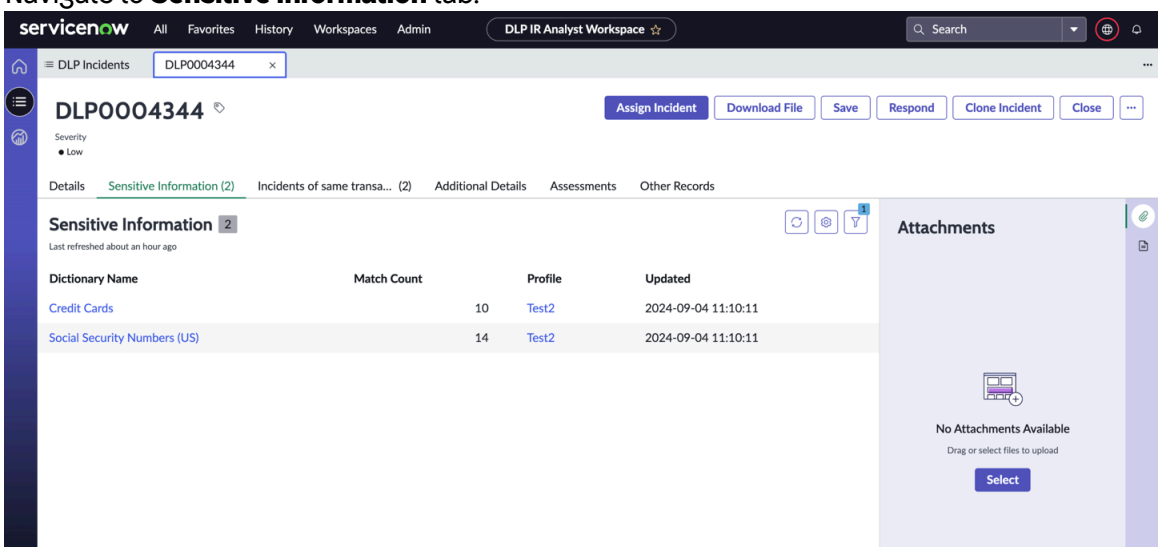
There are certain rules and policies configured in the respective integration and if anytime you are violating the defined policies then a DLP incident gets created and the match content displays that violated information under the Sensitive Information section of that DLP incident record.

Role required: sn_dlir.analyst

Note: End users can also view the sensitive information by logging into DLP User Workspace.

Procedure

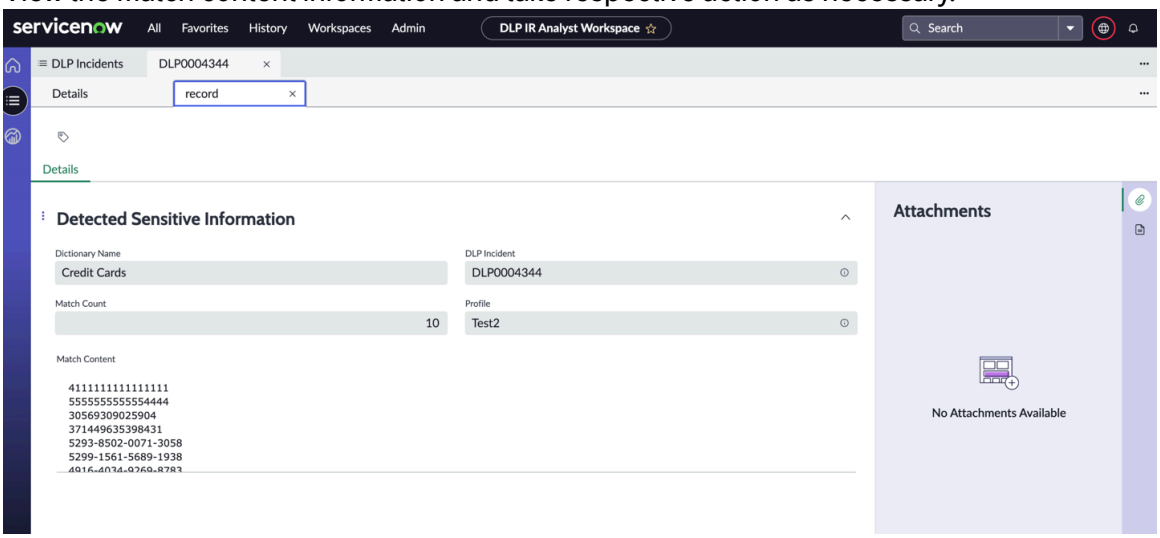
1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
   The DLP Workspace - My Incidents page displays on the DLP Analyst Workspace for the analysts.
2. Open any DLP incident.
3. Navigate to **Sensitive Information** tab.



4. Click on the violated record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. View the match content information and take respective action as necessary.



Download evidence files for DLP alerts

Download files that violate the DLP policy on provider that supports ICAP. Download this file onto your local machine from the DLP IR Analyst workspace and DLP IR End user workspace for approvers.

Before you begin

Role required:

- sn_dlir.analyst and approvers can download

About this task

You need to enable file download for ICAP before moving ahead.

Procedure

1. Navigate to **All** > **ICAP DLP Integration** > **Settings**.
2. Enable the property sn_icap_dlp.enable_file_download **Enabling this property allows downloading the evidence file of the reported ICAP incident**.
   You will be able to see the **Download File** button on the DLP IR Analyst Workspace and DLP IR End user workspace.
3. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
4. Open a DLP incident record which is ingested from ICAP provider source.
5. Click **Download File**.

> **Note:** DLP admin can control the access of **Download File** action for all integrations by disabling the **Should downloading the violating file of the reported incident be allowed** option from the **Advanced Settings** page of DLP Administration. For more information, see Configure advanced settings.

Preview evidence files for ICAP

Preview DLP incident evidence files in the DLP IR Analyst workspace.

Before you begin

- Navigate to **All** > **DLP Administration** > **Advanced Settings**.
- Make sure the **sn_icap_dlp.enable_evidence_file_preview** property is already enabled.

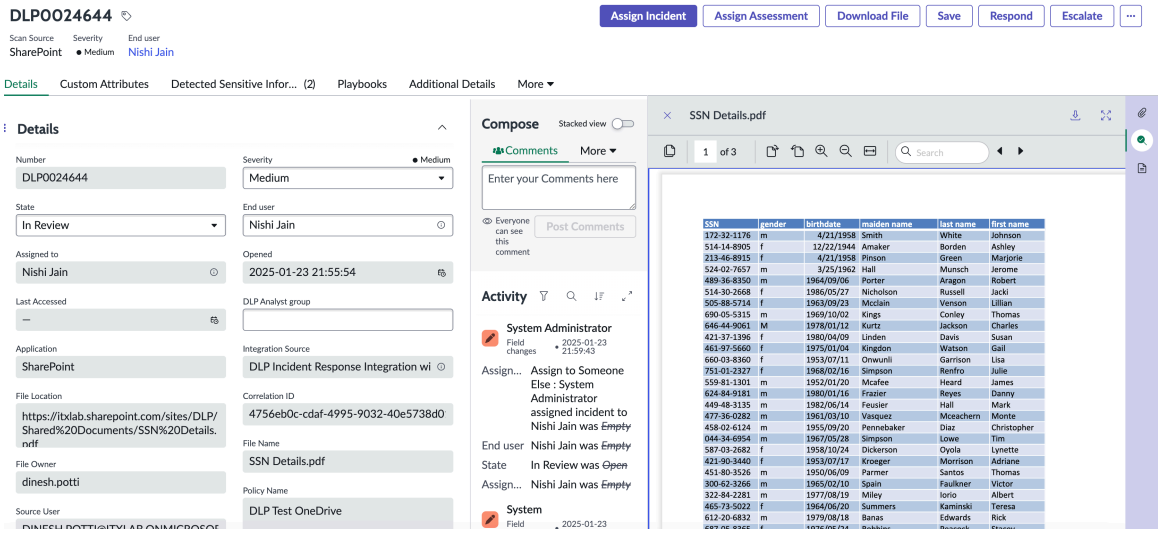
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format for the duration you have selected using **sn_dlir.preview_temp_files_cleanup_interval** property from the **Advanced Settings** page. You can disable the **Evidence Files** preview feature if you don't want to store any data in the ServiceNow database. For more information, see Configure advanced settings.

Role required: sn_dlir.analyst

Procedure

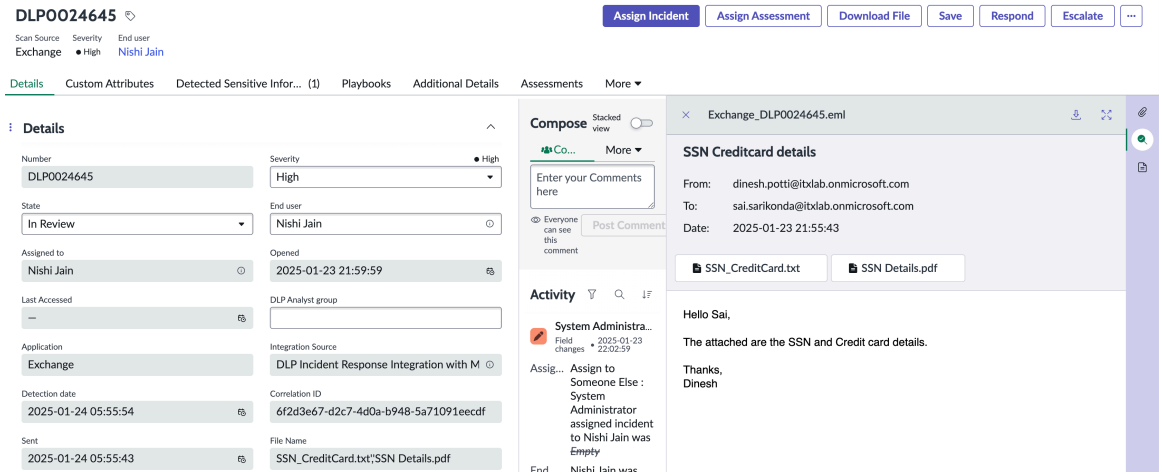
1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. Select the **Evidence Files** icon, which is available on the contextual menu.
   A tab opens which fetches all the evidence files. Once the download is finished, you can view all the evidence files in the **Evidence Files** tab.
4. Select the **Evidence File** card which you want to preview.
   The preview feature is different for each file type.
5. Preview pdf and office docs in the document viewer by selecting the **Expand** icon on the top right of the evidence file to open the pdf in full screen.
   Office Extensions for which the document viewer opens the evidence files include- doc, docx, ppt, pptx, xls, xlsx.
   a. Locate the search bar and enter the keyword you're looking for.
   b. Use the zoom-in and zoom-out features to adjust the view for better readability.
   c. Rotate the page clockwise or counterclockwise to view the content more clearly.
   These control options enhance your ability to understand the evidence file comprehensively. Only the pdf has control options in the header.



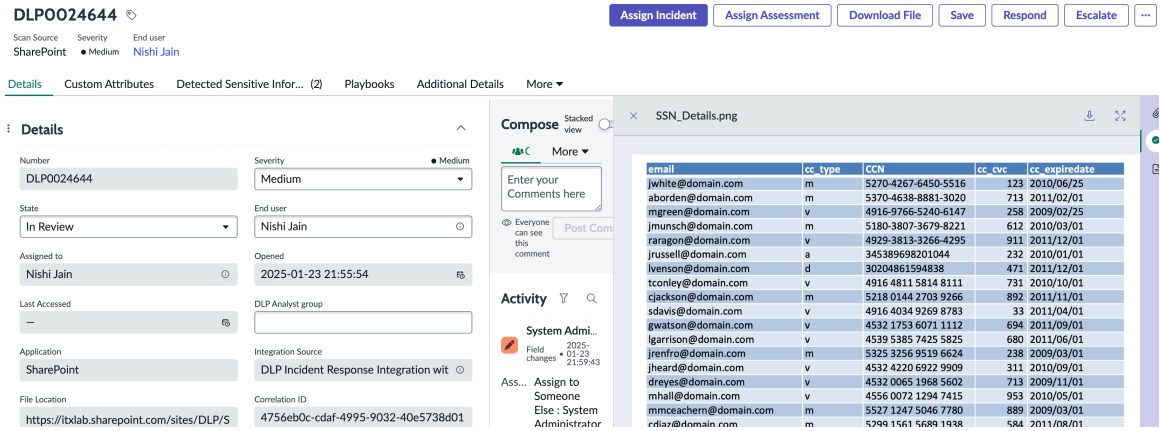
6. Preview eml files.
   Select the attachments in the email and preview them.

Note: If the selected evidence file exceeds the 5-MB limit, it can't be previewed in the analyst workspace. You have to download the file to preview its content. This limit is only for .eml files.

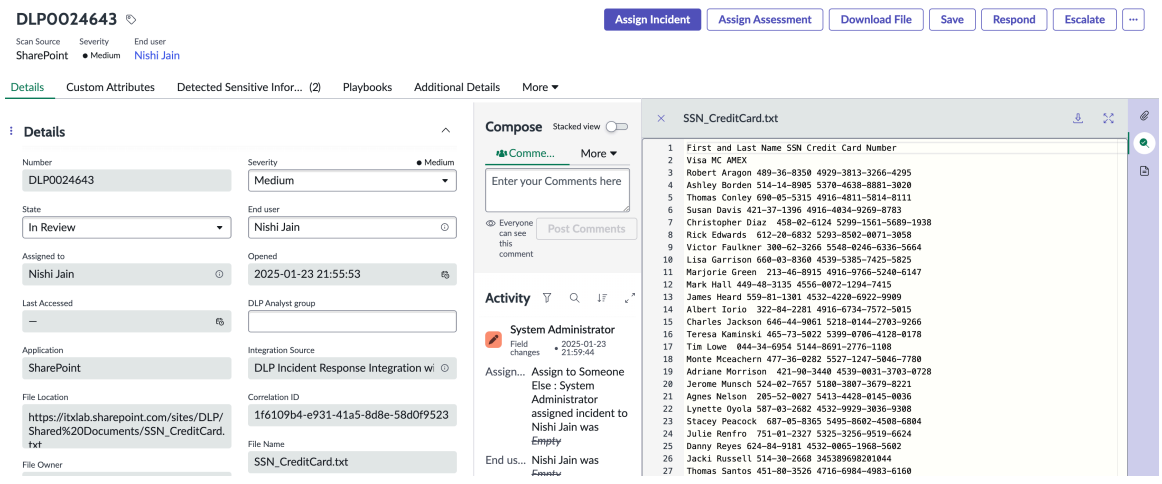
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Preview images in the DLP analyst workspace.
Images only with the .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp extensions are supported.



8. Preview text files in the text editor by selecting the **Expand** icon on the top right of the evidence file.



Note: Evidence Files apart from the office docs, eml files, text, and image extensions won't be supported for preview. Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Review the ICAP DLP integration settings

Review the provider ICAP DLP integration settings and modify the default system properties to suit your environment.

Before you begin

Role required: sn_dlir.admin

Procedure

1. Navigate to **All** > **ICAP DLP Integration** > **Settings**.
2. Review and modify the settings are required.

Property name	Description
sn_icap_dlp.maximum_retry	Option to chose maximum number of retries to be performed for AWS Get object failures.
sn_icap_dlp.logging.verbosity	Define the level of reporting the logs generat ed by the integration. The default value is set as 4.
sn_icap_dlp.enable_file_download	Option to enable this property allows down loading the evidence file of the reported ICAP incident. By default, this option is enabled.
sn_icap_dlp.presigned_file_expiry_time	Specify the duration in seconds, for which the presigned file will be available for down load or preview. The file will only be accessi ble within this time frame. This field is automat ically set to 300.

Data Loss Prevention Incident Response with Microsoft

The Data Loss Prevention Incident Response with Microsoft provides a core framework to import Data Loss Prevention (DLP) incidents from multiple sources, such as Microsoft Purview apps, Microsoft Teams, Exchange Online, SharePoint Online, OneDrive for Business, and other event types.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Overview and key features

The Data Loss Prevention Incident Response integration with Microsoft enables organizations to gain a unified view of incidents across email, network, endpoint, and cloud sources. Endpoint devices enable remediation workflow involving end users, managers, and#DLP#operations team with automated incident assignment and escalations.

Use the key features of this integration to do the following actions:

- Create multiple profiles for different accounts.
- Automate the creation of DLP IR incidents.
- Map the Microsoft DLP IR event fields to DLP IR incident fields.
- Filter Microsoft DLP IR events.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Schedule the ingestion of DLP IR events that create DLP IR incidents periodically.
- Store the matching content of each Microsoft DLP event in external cloud storage.
- Delete matching content at external cloud storage on the deletion of the DLP IR incident in ServiceNow.
- Download files for DLP IR incidents of type Exchange, OneDrive, and SharePoint.
- Store evidence files for DLP IR incidents of type Exchange, OneDrive and SharePoint in the internal ServiceNow storage.

Learn about this integration

Document identifier	Document title
Microsoft product documentation website	Microsoft Product Documentation website
ServiceNow product documentation website	ServiceNow Product Documentation website

Getting started with Microsoft DLP IR integration for data loss prevention

Review the following information before you start setting up your Microsoft DLP IR integration for data loss prevention.

Checklist

Setup task	Description
Get the Microsoft Purview credentials to fetch the event data and AWS/Azure Storage account credentials to store the match content Register an application with the Microsoft identity platform	Register an application on the Microsoft Azure platform from here to get the Client ID, Client Secret, and Tenant ID. For information on the Roles required for creating an application, see Prerequisites. For information on the API Permissions/Roles required on a Microsoft Azure application to configure it on ServiceNow Microsoft DLP integration, refer to the following table.
Permissions required for Azure user to get the access of read/write/delete blob on Azure Storage	1. Assign the **Storage Blob Data Contributor** role to an existing Azure user to read, write, and delete blobs on Azure Storage. For information about the role, see Azure built-in roles: Storage Blob Data Contributor. Alternatively, create a custom role and specify the actions. For information about creating custom roles, see Azure custom roles. 2. Assign a shared access key to the user that has the role privileges. For information about account access keys, see View account access keys.
Permissions required for AWS user to get the access of read/write/delete object on AWS Storage	Create a policy that gives list, read, write, and delete access for the object in AWS S3 Storage.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Checklist (continued)

Setup task	Description
	1. Create and configure an Amazon S3 bucket. For information about creating an S3 bucket, see Create an S3 bucket. 2. Provide read and write access to Amazon S3 bucket objects. For information about the object accesses, see the example policy. For information about creating policies, see Create IAM policies. 3. Provide the access key and the secret key to the user. For information about authentication, see Authenticating the AWS tools.

Assign and verify if you have the required roles for ServiceNow AI Platform and Data Loss Administration roles.	The following roles are required for configuration and verification of the expected results:
	• The admin role installs the integration from the ServiceNow Store and assigns the sn_dlir.admin role.
	• The sn_dlir.admin role performs the following tasks:
	  ○ Configures the integration.
	  ○ Sets up the incident profiles.

Verify that the ServiceNow core applications required to support the Microsoft DLP IR integration are installed and activated before you configure this integration.	Verify that the following DLP IR applications and security support common applications are installed and activated from the ServiceNow Store. If not installed, then install and activate on the application. • Security Support Common • Data Loss Prevention Incident Response

Required API Permissions/Roles on a Microsoft Azure application

You need the following API Permissions/Roles on a Microsoft Azure application to configure it on **ServiceNow** *Microsoft DLP integration.*

API	Permission name	Type	Description	Required for which ServiceNow functionality?	Is Admin consent required?
Office 365 Management API	ActivityFeed.ReadDlp	Application	Read DLP policy events including detected	To ingest the DLP events from MSFT Purview to ServiceNow.	Yes

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required API Permissions/Roles on a Microsoft Azure application

You need the following API Permissions/Roles on a Microsoft Azure application to configure it on **ServiceNow** *Microsoft DLP integration.*

(continued)

API	Permission name	Type	Description	Required for which ServiceNow functionality?	Is Admin consent required?
			sensitive data.	**Note:** This permission is a must to get the MSFT data into ServiceNow.	
Microsoft Graph API	Files.Read.All	Application	Read files in all site collections that you can access.	Download File: To download the attachment on the ServiceNow instance that caused the DLP event from OneDrive or SharePoint **Note:** This is optional. You can skip this API permission if you don't want to allow the analysts to download the attachment that caused the DLP event.	Yes
	Mail.Read	Application	Read mail in all mailboxes.	Download File: To download the email content (body and attachment) on the ServiceNow instance that caused the DLP event from Exchange. **Note:** Optional. You can skip this API permission if you don't want to allow the analysts to download the email content (body, attachment) that caused the DLP event.	Yes

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Required API Permissions/Roles on a Microsoft Azure application

You need the following API Permissions/Roles on a Microsoft Azure application to configure it on **ServiceNow** *Microsoft DLP integration.*

(continued)

API	Permission name	Type	Description	Required for which ServiceNow functionality?	Is Admin consent required?
	User.Read	Delegated	Sign in and read user profile.	Default permission available for all new applications.	No

Detected Sensitive Information (Optional)

The match content is stored externally in Azure Blob Storage or Amazon S3 bucket and will be pulled from external storage when the user views an incident.

Any one of the following permissions are required if the users would like to view Match Content/ Detected Sensitive Information in the DLP Core application:

1. If you're a Microsoft Azure user, you must have the role Storage Blob Data Contributor to read, write, and delete blobs on Azure Storage.
2. If you're an Amazon S3 user, you must create a policy that gives list, read, write, and delete access for the object in Amazon S3 Storage.

Install and configure the Microsoft DLP integration

Install and configure the#DLP Incident Response integration with Microsoft DLP from the #ServiceNow® Store on your#ServiceNow AI Platform instance. Start investigating DLP incidents using the#Microsoft DLP event data.

Before you begin

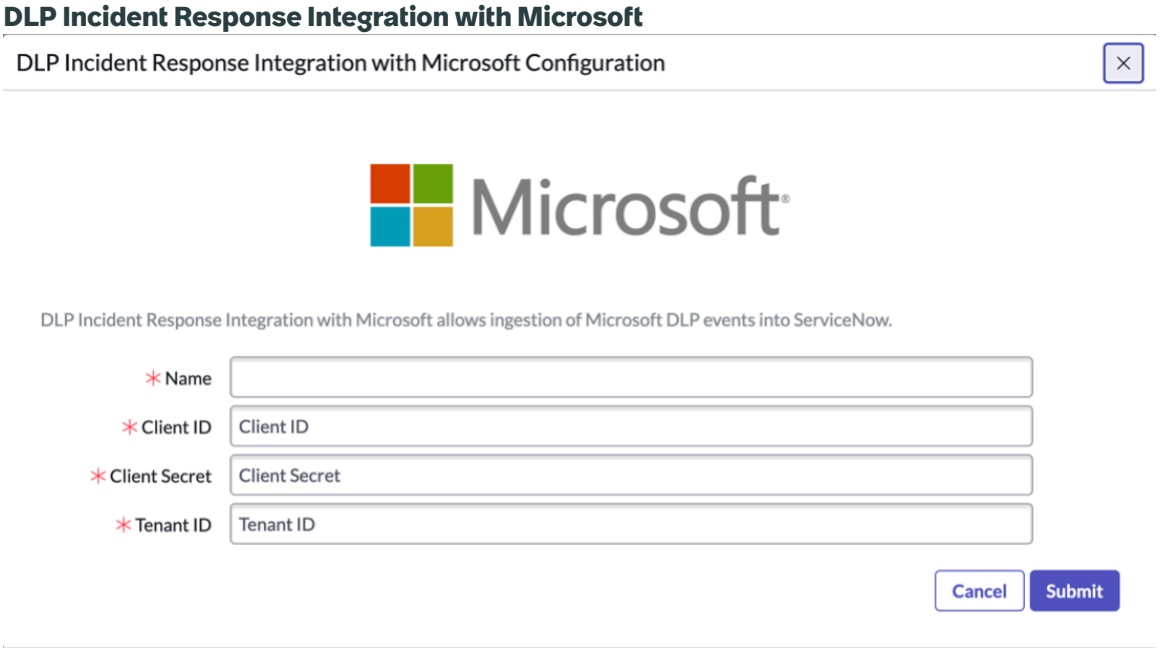
Role required: sn_dlir.admin

Procedure

1. Download the#Microsoft DLP integration from the#ServiceNow® Store and install it.
2. Navigate to **Security Operations** > **Integrations** > **Integration Configurations**.
3. Configure the Microsoft DLP integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Search for **DLP Incident Response Integration with Microsoft** tile and click#**Configure**.



b. On the form, fill in the fields.

Microsoft DLP Integration Configuration form

Field	Description
Name	Name of the Microsoft DLP integration configuration.
Client ID	Client ID of the app created on Microsoft Azure portal.
Client Secret	Client Secret of the app created on Microsoft Azure portal.
Tenant ID	Tenant ID of the user.

c. Click **Submit**.

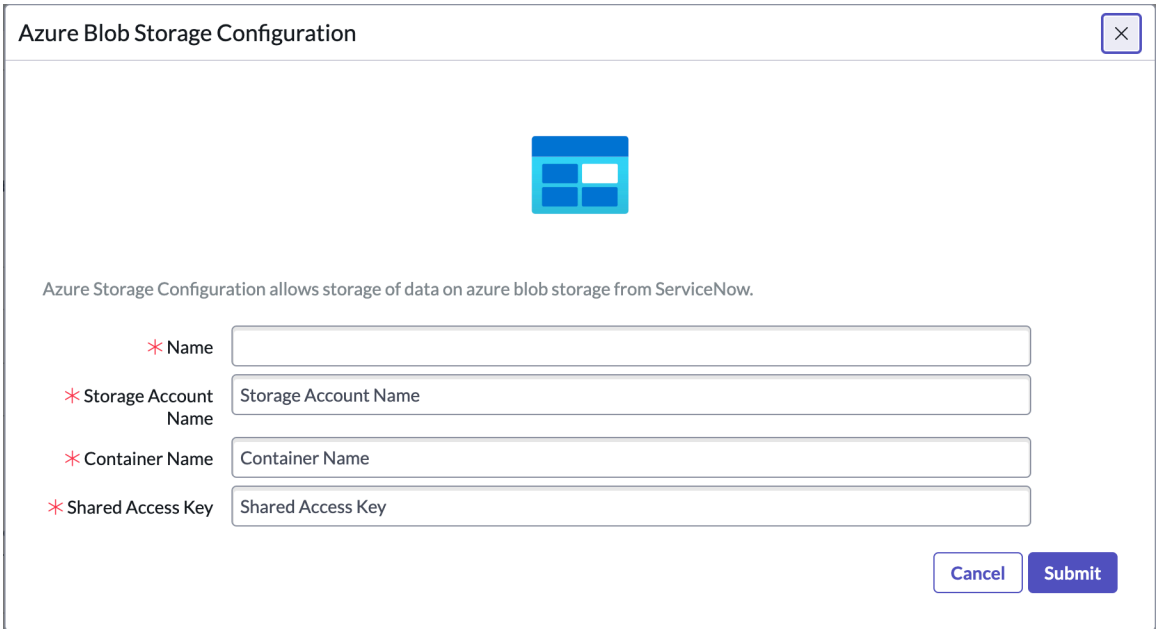
After you successfully validate and submit the configuration, the Microsoft DLP Integration is saved on the Security Integrations page as a tile.

4. Update the Azure Storage Configuration.

a. In the Security Integrations page, search for **Azure Storage Configuration** tile.

b. In the Azure Storage Configuration tile, click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. On the form, fill in the fields.

Azure Storage Configuration form

Field	Description
Name	Name of the Azure Storage configuration.
Storage Account Name	Storage account name created on Azure portal
Container Name	Container name created in storage account on Azure portal.
Shared Access Key	Shared access key for the Storage account.

d. Click **Submit**.

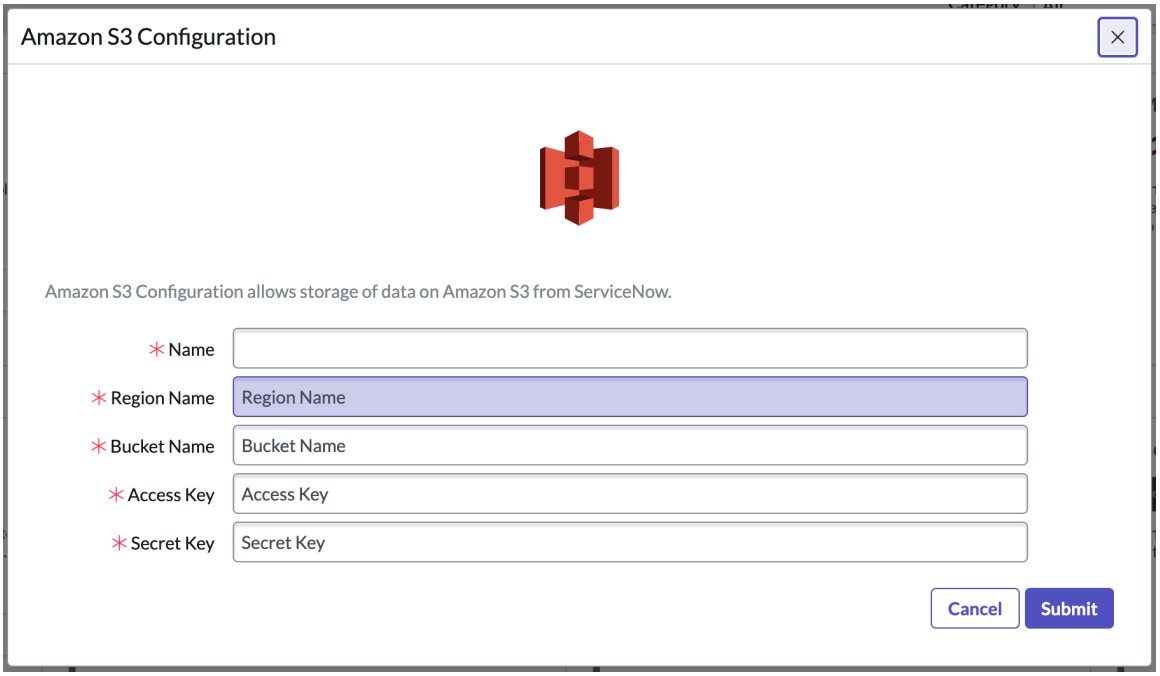
After you successfully validate and submit the configuration, the Azure Storage Configuration is saved on the Security Integrations page as a tile.

5. Update the AWS Storage Configuration.

a. In the Security Integrations page, search for **AWS Storage Configuration** tile.

b. In the AWS Storage Configuration tile, click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



c. On the form, fill in the fields.

AWS Storage Configuration form

Field	Description
Name	Name of the AWS Storage configuration.
Region Name	Region name of the AWS Storage account.
Bucket Name	Bucket name created on the AWS portal.
Access Key	Access key with read, write, and delete access.
Secret Key	Shared key with read, write, and delete access

d. Click **Submit**.

Result
After you successfully validate and submit the configuration, the AWS S3 Configuration is saved on the Security Integrations page as a tile.

Create a new incident profile for Microsoft DLP integration

Create an incident profile in your#ServiceNow AI Platform instance to retrieve the data from the Microsoft Purview and add the data into the ServiceNow DLP IR incident table.

Before you begin
Role required: sn_dlir.admin(Create, edit, and delete)

sn_dlir.analyst - View (read-only)

About this task
Configure the ServiceNow AI Platform® to retrieve the events from the Microsoft Purview. Store these events on the DLP IR Incident table on your ServiceNow® instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **Microsoft DLP integration** > **Incident Profile**.
2. Click **New**.
3. On the form, fill the fields in the Name section.

Create a profile form

Field	Description
Name	Name of the profile. This field helps you to identify the profile. **Note:** The name must be unique for each profile.
Source	The Microsoft DLP IR instance that you configured to ingest incidents. If you have multiple integration configurations, select the appropriate integration configuration record for the incident types that you are planning to ingest for the profile.
Active	Option to indicate if the profile is active. This field can only be enabled after you click the **Finish** field in the Scheduling section. When the profile is active, it implies that the#ServiceNow AI Platform is actively polling Microsoft DLP IR events based on the configuration defined in the profile.
Order	Order of the profile execution. The profile with the lowest order considered as the highest priority. By default, the value is 100.
Description	Unique description for the profile.

What to do next

To move to the Filtering section,#click **Continue**.

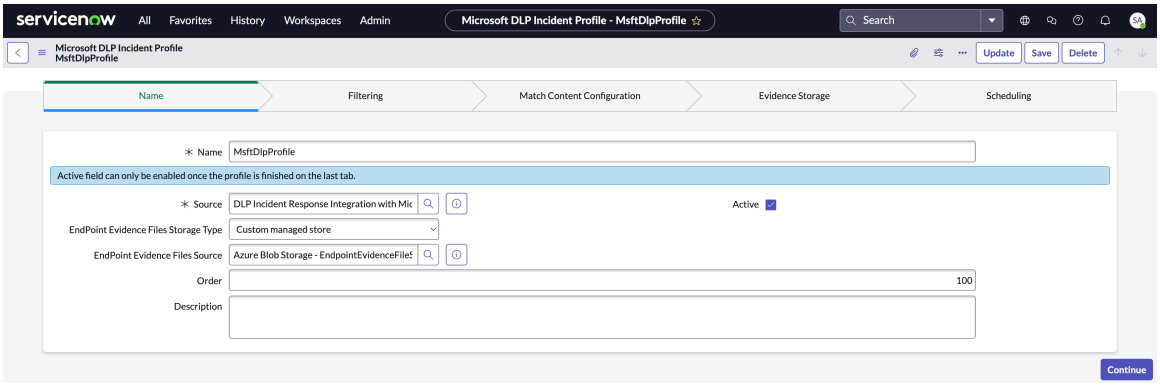
Microsoft purview endpoint storage configuration

Microsoft Purview endpoint evidence files storage configuration tells you where the endpoint evidence files are being stored by the purview- Custom managed store or Microsoft managed storage environments.

In case of Microsoft managed store, Microsoft itself stores the evidence files in some location and for Custom managed store, you need to specify the container in which the evidence files will be stored by the purview when an alert gets generated.

Select either of the two storage types based on what is being configured at the purview end for the system to fetch the evidence files of the corresponding endpoint DLP incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: We recommend using the **Custom Managed Store** because Microsoft currently does not provide any APIs to retrieve evidence files from the **Microsoft Managed Store**. As a result, preview and download functionality is not supported for evidence stored in the Microsoft Managed Store. We have raised a case with Microsoft regarding this limitation.

Define filters to apply for the Incident creation

Define and set filter conditions to filter the incoming#Microsoft DLP #events. Control which of these events should be created as DLP IR incidents on your ServiceNow instance.

Before you begin

Role required: sn_dlir.admin(Create, edit, and delete)

sn_dlir.analyst - View (read-only)

About this task

This type of filtering helps you to isolate Microsoft DLP #events to limit the number of DLP IR incidents that you create. If the filtering criteria is set, only events that match the conditions are created as DLP incidents.

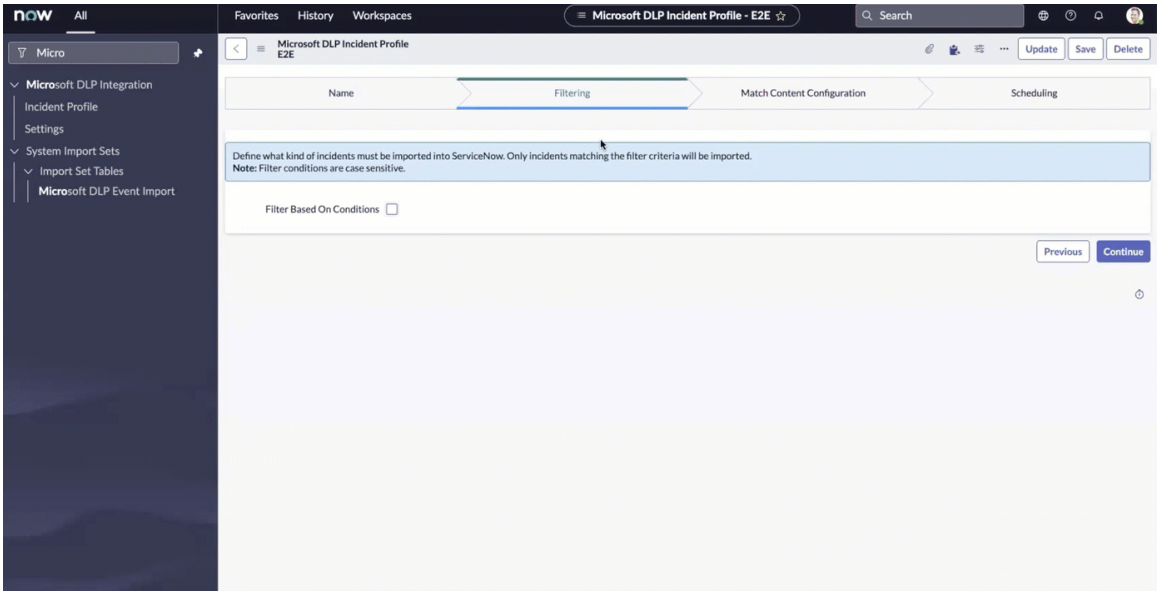
Procedure

1. Select the **Filter based on conditions** option.
2. Using the lists and fields of the condition builder, set the filters in the **Filter Conditions** field.

   Define the criteria that an incoming Microsoft DLP event must satisfy so that a DLP incident is created.

   The options in the first field in the **Filter Conditions** match the fields that are available in the Microsoft DLP event. The criteria that you enter are case-sensitive. Verify that the criteria you define match the values of the event.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Add more conditions by clicking **AND** or **OR**.
   - If **AND** is selected, all conditions must be matched.
   - If **OR** is selected, either condition can be matched.
4. Click **Continue** and move to the Match Content Configuration section.
   Earlier, UserID was mapped only to the Source User field but, the UserID field is currently available as a lookup attribute for all Purview events, including Endpoint events.

Configure the match content for the incident

Provide the configuration to store the sensitive information internally, on the ServiceNow® storage, or on the external cloud storage, such as Azure Storage or AWS S3 bucket. Retrieve the stored content while accessing the DLP IR Incident.

Before you begin

Role required:

- sn_dlir.admin
- sn_dlir.analyst

Procedure

1. On the progress bar, click the **Match Content Configuration** step.
2. On the form, fill in the fields.

Match Content Configuration

Field	Description
Store Match Content	Option to store the matched content.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Important: Enable this option to store the match content, and retrieve and display the match content when a DLP incident is opened in the workspace. For information on the External Cloud Storage configuration, see Install and configure the Microsoft DLP integration.
Storage Source for Match content	Option to choose whether to store the matched content internally, on the ServiceNow® storage, or externally, on the cloud storage.
External Cloud Credentials	The External Cloud Storage where the match content gets stored. You can refer to the External Cloud Credentials added for the Storage configuration. This option is visible only when the **Store Match Content** field is selected.
Delete Match Content on Incident Deletion	Option to delete the incident match content from the external cloud storage. This option is visible only when the **Store Match Content** field is selected.

3. Click **Continue** and move to the Scheduling section.

Schedule the DLP IR Microsoft incident retrieval

Set a schedule to retrieve the incident data and ingest Microsoft DLP IR incidents that match the criteria in the profile. Configure the schedule to define how and when you pull incidents from Microsoft.

Before you begin

Role required: sn_dlir.admin(Create, edit, and delete)

sn_dlir.analyst - View (read-only)

About this task

You can plan how often you'll poll for future incidents that match the incident profile configuration. To enable automated incident ingestion, you must configure the scheduling and incident retrieval before you activate the profile. The profile can be configured to do one-time retrieval using the **One-Time Retrieval** check box. The historical date can be up to the last three months from the current date.

The polling interval is configured for each profile individually. The different polling intervals may impact the performance of the Microsoft DLP IR incident integration. When scheduling, plan to balance the system load against the urgency of an incident.

Procedure

1. Set a schedule to retrieve data and ingest incidents that match the criteria in the profile.
2. On the form, fill in the fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Schedule for the DLP incident form

Field	Description
Ongoing Incident Ingestion	The ongoing incident ingestion that the ServiceNow AI Platform instance pulls from Microsoft for new incidents. DLP IR incidents are created if triggered incidents are found and the incident generation filtering criteria matches.
Polling increment (minutes)	The polling frequency from Microsoft. This field is automatically set to 300 minutes.
Set Initial Incident Ingestion Time	Option to define a date and time for the initial ingestion. Subsequent ingestions are based on the polling interval period. This option is visible only when the **Ongoing incident ingestion** field is selected.
Input Initial Incident Ingestion Time	Date and time that you specify for the incident ingestion. ○ If the value is set, then data retrieving from Microsoft will start from the added future date. ○ This field is visible only when the **Set Initial ingestion time** is selected.
Initial Incident Ingestion Time	First time when the data is ingested. You can see the that values start showing up when the initial incident ingestion time is set.
Next Incident Ingestion Time (estimated)	The next period for an estimated incident ingestion.
One-Time Retrieval	Option to enable one-time historical data pulls. If this field is selected, then historical data is pulled from Microsoft DLP IR according to the date added in the **Since Date** field.
Since Date	Date from when data is supposed to be retrieved from Microsoft. This field can be set to a maximum of 7 days.

3. Save the created profile configuration by clicking **Finish** on the pop-up window.
4. Activate the profile.
   a. Open the created profile.
   b. Enable the **Active** option.
   c. Click **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
After the successful creation and activation of the profile, the incidents are retrieved periodically as per the configuration set in the profile and added into the DLP incidents table.

Configure Microsoft DLP IR integration settings

Modify the#Microsoft DLP IR #integration default system properties.

Before you begin
Role required: sn_dlir.admin

Procedure
1. Navigate to **Microsoft DLP Integration** > **Settings**.
2. Modify the following properties as required.

Microsoft DLP Integration Settings

Field	Description
Maximum Timeout for HTTP calls (sn_pp_dlp.maximum_http_time_out)	Maximum Timeout for HTTP calls (in seconds). ○ Type: integer ○ Default value: 30
Level of reporting the logs generated by the integration (sn_pp_dlp.logging.verbosity)	The level of reporting logs generated by the integration, meaning the name of the type of information. You can also update the value to the following options: ○ **error** ○ **warn** ○ **info** ○ **debug** ○ **off** By default, the value is **info**.
Destination of reporting the logs generated by the integration (sn_pp_dlp.logging.destination)	The destination for the logs that are generated by the integration. You can also update the value to the following options: ○ **db** ○ **file** ○ **none** By default, the value is **db**.
Should downloading the violating file of the reported incident be allowed (sn_msft_dlp.enable_file_download)	Option to choose whether you want to enable download of the file. By default, this option is enabled. By default, the value is **True** and enabled.

3. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
Your modified integration settings are applied in the next polling interval as defined in the profile.

Configure evidence file storage for Microsoft

Configure evidence file storage to securely store the evidence file in the ServiceNow instance for the Microsoft incidents of type OneDrive, Exchange and SharePoint.

Before you begin
Role required: sn_dlir.admin

About this task
You can configure the evidence file storage to securely store files. This provides an option for internal storage in ServiceNow instance, ensuring that files are stored and encrypted using ServiceNow Column Level Encryption. For more information, see Encryption Support on ServiceNow AI Platform documentation.

When a DLP analyst or approver performs the Download evidence files for DLP Incidents action from analyst workspace, the file will be downloaded from the selected storage if evidence file storage option is enabled. Otherwise, the file will be downloaded directly from the Microsoft source and will not be persisted in the ServiceNow instance. For more information, see Download files for DLP incidents of type Exchange Online, OneDrive, and SharePoint.

Procedure
1. Select **Evidence Storage** section on the **Incident Profile** form.
2. Select **Evidence File Storage** check box to enable the file storage.
3. Select the preferred storage type.

Field	Description
Evidence file storage	Option to enable the evidence file storage.
Storage type	Option to select the preferred storage type. **ServiceNow Storage**: Option that stores the evidence files in the ServiceNow instance in an encrypted format.

4. Click **Continue** and move to the **Scheduling** section.

Result
If the **Evidence File Storage** option is enabled and ServiceNow and the **Storage** option is selected then the evidence files will be stored internally in the ServiceNow instance in an encrypted format. The **Download file** action will get the file from the ServiceNow instance after the files are stored.

Request release email from quarantine

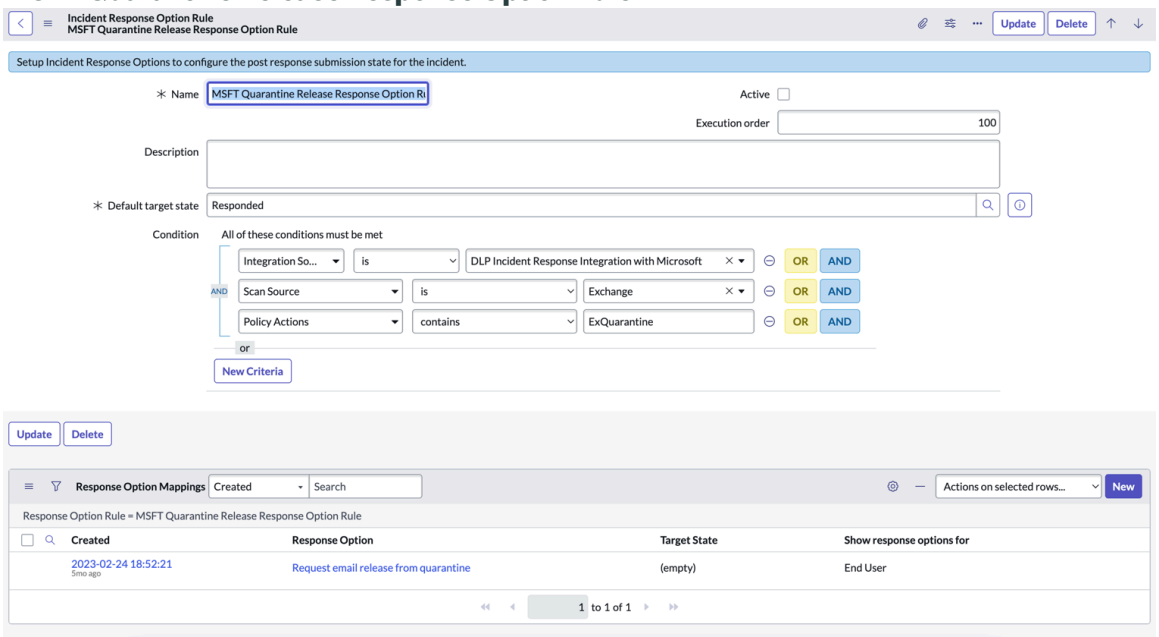
Use this feature to release the email that is quarantined from the Microsoft Purview compliance portal.

Before you begin
By default, the base system provides the **Request email release from quarantine** response option and **MSFT Quarantine Release Response Option Rule** to release the email from quarantine. This default record also has the **Quarantine Release Approval Rule** configured with it to leverage the approval functionality for this action. For more information, see Create incident

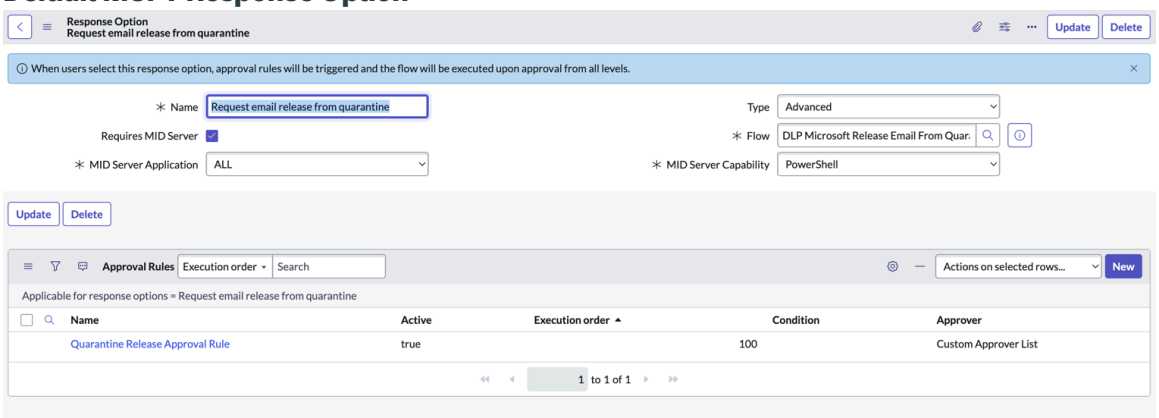
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

response option rules, Configure response option for your DLP incidents, and Create Approval Rules.

MSFT Quarantine Release Response Option Rule



Default MSFT Response Option



Prerequisites:

1. Exchange Online PowerShell module need to be installed on the MID server. For more information, see Install and maintain the Exchange Online PowerShell.
2. The MID server needs to communicate with the Exchange server, which is also a cloud service. Therefore, the MID server requires continuous internet access.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you are using this response option then make sure the mid server is up and running with PowerShell capability. If a mid server is not up and running and doesn't have PowerShell capability then the end user will not be able to select **Request email release from quarantine** action from the DLP Users workspace. For more information, see Create incident response option rules and Configure response option for your DLP incidents.

- If you want a specific MID server from the list then you have to configure the MID app and make it visible in the list, and then at least one MID server which is configured should be up and running from the selected mid applications and should have the Power Shell capability.
- For you to use the Release from quarantine option, you need API permissions.
  On the Microsoft API permissions page, verify **Office 365 Exchange Online** > **Exchange.ManageAsApp** is listed and contains the following values:
  - **Type**: **Application**.
  - **Admin consent required**: **Yes**.
  - **Status**: The current incorrect value is **Not granted for <Organization>** for the **Office 365 Exchange Online** > **Exchange.ManageAsApp** entry and change the status value. For further steps on the API permissions, see Assign API permissions to the application on the Microsoft documentation site.

    Note: This step is required to connect to Exchange online using Service principle.
- You should also need **Security Administrator** role in Service Principle,
  - Search for **Microsoft Entra ID roles and Administrators** in Microsoft Azure portal, and add assignment to the registered app (Service Principle) and then follow the procedure explained on the Microsoft Documentation on how to assign a role.
- This option is applicable only for Microsoft Exchange incidents which have the **Policy Action** option as **ExQuarantine** on the incident form view.

Role required: End user

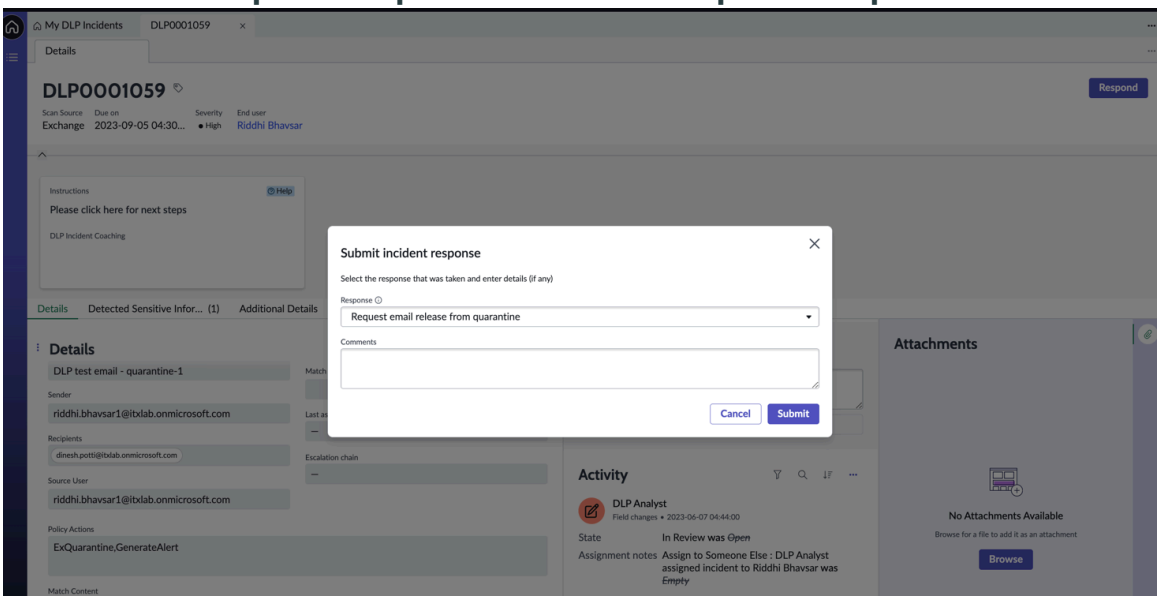
The following procedure explains on how to submit this action from the DLP User Workspace.

Procedure

1. Navigate to **DLP** > **DLP User Workspace**.
2. Open any Microsoft Exchange DLP incident.
   Verify that the incident **Policy Action** is set to ExQuarantine.
3. Click **Respond**.
4. Select **Request release mail from Quarantine** option from the Response drop down list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Submit incident response - Request email release from quarantine option



5. Click **Submit**.

> **Note:** When an approval rule is configured for this action, the approval flow will be triggered first and after receiving all the approvals, the Request email release from quarantine flow will be triggered and the email will be released from quarantine. The state of the DLP Incident will be updated to **Released from Quarantine** after successful release.

Download files for DLP incidents of type Exchange Online, OneDrive, and SharePoint

Download files or email that violates the DLP policy on Microsoft Purview. Download this file or email on to your local machine from the DLP IR Incident view. You can download the files for DLP IR incidents of type Scan source Exchange Online, OneDrive, and SharePoint.

Before you begin

Role required:

- sn_dlir.admin, sn_dlir.analyst
- Any valid approver

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record of type Scan source Exchange Online or OneDrive or SharePoint which is ingested from Microsoft source.
3. Click **Download File**.
   The file or email that violated the DLP policy on the Microsoft Purview side will be downloaded to the user's local machine.

> **Note:** DLP admin can control the access of **Download File** action by disabling the **Should downloading the violating file of the reported incident be allowed** setting from the Advanced Settings page. For more information, see Configure advanced settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Download files approval flow

The below approval flow describes the procedure for the approvers to view the Download File action.

Before you begin

Role required: any valid approver

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP User Workspace**.
2. Select **My Approvals** module available under My DLP Incidents module.
3. Open an approval request record which is raised for Microsoft DLP Incident with application any of OneDrive, SharePoint or Exchange.
4. Click on info icon (i) available on the DLP Incident field on the form view.
5. Click **Download File**.

Result

After performing this action, the file that violated the DLP policy on Microsoft will be downloaded to the user's local machine.

DLP admin can control the access of Download File action by disabling the Should downloading the violating file of the reported incident be allowed setting from the Advanced Settings page. For more information, see Configure advanced settings for Data Loss Prevention Incident Response.

Preview Evidence files for DLP incidents of type Exchange Online, OneDrive, and SharePoint

Preview Data Loss Prevention Incident Response evidence files in the DLP IR Analyst workspace.

Before you begin

Important: While using the Evidence files action in the DLP analyst workspace, the evidence files are temporarily stored in the ServiceNow database in an unencrypted format. If you don't want to store the evidence files, disable the Evidence Files preview feature. For more information, see Configure advanced settings.

Role required: sn_dlir.analyst

Procedure

1. Navigate to **All** > **DLP Incident Management** > **DLP Analyst Workspace**.
2. Open a DLP incident record.
3. From the contextual sidebar, select the Evidence files icon ( ).
4. On the **Evidence Files** tab, select the **Evidence File** card to preview the evidence files in the document viewer.

   The preview feature is different for each file type, as listed in the following table.

File Format	File Extension
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg, and .webp.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

File Format	File Extension
	Image files open in the document viewer mode.
Microsoft Office files	.doc, .docx, .ppt, .pptx, .xls, and .xlsx Office files open in the document viewer mode.
Text files	.txt Text files open in text editor mode.
Mail files	.eml **Note:** The file size must be less than 5MB. You must first download the file to preview its content.
PDF files	.pdf ○ Enter a keyword to search the document. ○ Zoom-in and zoom-out features to adjust the view for better readability. ○ Rotate the page clockwise or counterclockwise to view the content more clearly.

Note:

Binary files won't be rendered and have to be downloaded to preview their content. The preview evidence file feature also works for archived incidents.

Domain separation in Microsoft DLP integration

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Support level

Support: Basic.

How domain separation works with Microsoft DLP integration

Follow these steps to achieve domain separation:

- Create a user with the required role in the respective domain.
- Perform the Microsoft DLP integration procedures in the appropriate domain.

Security Operations common functionality

Whenever any of the plugins for the main Security Operations applications (Security Incident Response, Vulnerability Response, Threat Intelligence, or Configuration Compliance) are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

activated, the Security Support Common plugin is activated. This plugin loads various modules that provide functionality that is common across all Security Operations applications.

Note: Only users with the [sn_sec_cmn.admin] can view and use the Security Operations module. This role is inherited when you are assigned an administrative role in any of the Security Operations applications.

Security Operations Modules

Feature	Description
Security Operations Integration Reference, Threat Intelligence integrations, Vulnerability Response integrations	Several integrations are included with the Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response). This section provides instructions for activating the plugins and configuring both ServiceNow and third-party integrations. Also included are some basic guidelines for developing your own integrations, as well as details on specific integrations included in the base system.
Security Operations email processing	You can set up the integration of information from external detection systems, provide granularity in processing security operations records, handle unmatched emails, and prevent duplication of records using Email Processing.
Groups	• **Filter Groups** Create and use filter groups to locate records from any table on your instance. For example, you can create a group of all computers by the same manufacturer. You can also filter configuration items (CIs) that have similar vulnerabilities or that fall within a particular subnet IP address range. • **Escalations** You can create an escalation path for security incidents for issues requiring more attention or expertise. Once an escalation group exists, a button appears on any security incident in that group.
Security Tags	**Tags**: Security tag rules provide filtering for security tag access.
Workflows	• **View Security Workflows** You can view the many workflows included with the Security Operations applications. You can create workflows from templates and in the Workflow Editor. • **Workflow Triggers**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Feature	Description
	Security Operations workflow triggers contain a condition on a table. All workflows attached to the workflow trigger record run when the condition is met.
Utilities	• **Enrichment Data Mapping** Enrichment Data Mapping transforms data from XML, JSON, or Properties files to ServiceNow records. Security Operations workflows use enrichment data maps and provide output data to security incidents. • **Field Value Transforms** Transforms unique customer field values into field values recognized by Security Operations email parsing, data enrichment or tables using field maps. Supports choice fields, references, and aligns external data into the standard terminology and format for your new record. • **Field Mapping** Security Operations tables can be mapped to and from other tables, linking a security incident to a customer service case or a problem to other parts of the Security Operations system. For example, you can integrate a plugin to a Security Incident Response task. • **On-Demand Orchestration** During Security Incident Response analysis, a security analyst may want to perform a task that is driven by a security incident workflow. For example, run a process dump on a particular CI. This can be accomplished with on-demand orchestration. • **Operating Systems Groups** NA. • **SecOps Application Registry** NA.
CMDB	**CI Identifier Rules**: CI identifiers are rules used to lookup a configuration item (CI) in the CMDB that contains matching information from a third-party integration. These rules define the fields that contain matching data and the order of precedence

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Feature	Description
	by which they are evaluated. The lowest **Order** value is evaluated first.

Create and define filter groups in Security Operations

Create and use filter groups to locate records from any table on your instance. For example, you can create a group of all computers by the same manufacturer. You can also filter configuration items (CIs) that have similar vulnerabilities or that fall within a particular subnet IP address range.

Before you begin

Role required: sn_sec_cmn.write

About this task

Filter groups can contain dynamically updated records, a series of static records that are not filtered using conditions, or a combination of dynamically updated and static records. Some filter groups are included in the base system, for example, CI exclusions.

Procedure

1. Navigate to **All** > **Security Operations** > **Groups** > **Filter Groups**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the filter group.
Active	Box to activate the group.
Description	Description for the filter group.
Network IP Address	The network IP address that contains the IP addresses of the CIs you want to add to the group. This field appears only if you selected Configuration Item [cmdb_ci] or a table that extends configuration item in the **Table** field.
Subnet Mask	The subnet that contains the IP addresses of the CIs you want to add to the group,for example, 255.255.255.0. This field appears only if you selected Configuration Item [cmdb_ci] or a table that extends configuration item in the **Table** field.
Table	The table to be filtered on.
Condition	Use the condition builder to define the criteria to be filtered.

4. Right-click the form header and select **Save**.
   An **Advanced Conditions** tab appears.

   More tabs appear depending on the type of table you specified in the **Table** field, as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Table	Tabs Displayed
Configuration Item [cmdb_ci] or a table that extends the configuration item table	**Manually Added CIs** and **Matching CIs**
Task [task] or a table that extends the task table	**Manually Added Tasks** and **Matching Tasks**
A table not related to a CI or task	**Manually Added Record**

5. To define more conditions for your filter group:
   a. Click **Advanced Conditions**.
   b. Insert a new row into the **Additional Filter Group Conditions** embedded list to select other prebuilt filter groups that you want to combine with the filter group being updated.
   If you want the selected filter group to filter records based on a reference field, a mapped field is automatically selected when the current record is saved.

   Note: The **Mapped field** value cannot be edited from the **Additional Filter Group Conditions** embedded list. To change the field, click the information icon to open the record.

   c. Click **Update**.
6. To manually add more CIs or tasks to the filter group:
   a. Click the **Manually Added CIs** or **Manually Added Tasks** tab.
   b. Click **Edit**.
   c. Select the CIs or tasks you want to add.
   d. Click **Save**.
7. To view the CIs or tasks that match your selection criteria:
   a. Click the **Matching CIs** or **Matching Tasks** tab.
   b. If you changed the criteria, refresh the list by right-clicking in the form header and selecting **Refresh List**.

Shared data transformation

The Security Incident Response, Vulnerability Response, and Threat Intelligence plugins share common features, for relationship data and duplication rules, used to import external and internal information into Security Operations.

Email Parsing, Duplication Rules, and Field Mapping take input data (an email, JSON or XML file, or a record) and transform that data into the correct format to create a new record. Each of these features pulls data in their own way but, it is transformed into the new record using many of the same processes.

Relationship data

When you add information to a related list (such as an associated observable in a security incident), you can create a relationship record consisting of an m2m table. Sometimes, there is additional data on that relationship record to set. For example, an observable being a Source

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IP (as opposed to a destination IP). That information goes in the **Relationship data** field in the **Field Transform** form used by **Email Parsing** or a **Field Mapping Fields** related list in the **Field Mapping** form.

The **Relationship data** field is usually empty. It is most commonly used for IP addresses on observables in **Email Parsing**.

You can transform data from any ServiceNow record to any other ServiceNow record using **Field Mapping Fields** in the **Field Mapping** feature. For example, to transform data from an incident to a security incident, or a security incident to a PRB.

Security Operations duplication rules

Use Duplication Rules to handle duplicate records for security, vulnerability, IoCs, and so on.

Duplication rules have two purposes. They prevent too many duplicate records from being created and, when a duplicate is detected, they specify which fields in the record are updated. Only active duplicates are looked for. If the record is not active, for example, if the incident is closed, then any new identical problem becomes a new incident.

Duplication rules are used by **Email Parsing**, **Field Mapping**, and **Enrichment Data Mapping**.

Related topics

- Create email parsers in Security Operations
- Map tables to tables with Security Operations field mapping

Create duplication rules in Security Operations

You can use Duplication Rules to identify new email, enrichment data, or field maps with active duplicate records and process them appropriately.

Before you begin

Role required: sn_sec_cmn.write

Procedure

1. Navigate to **All** > **Security Operations** > **Duplication Rules**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate:

Duplication rule

Field	Description
Name	The name of the duplication rule.
Table	Table where records are created and used to determine duplication.
Identifying fields	Select a set of fields that indicate a duplicate security incident, observable, vulnerability, and so on, when the values in these fields are identical.
Duplicate action	Governs how to handle duplicate emails. Choices are: **Create as child** Creates a record as a child of the original. The field linking the child to the parent is the **Parent** field. **Do not create nor update records** (default) Does nothing. Ignores duplicates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Update duplicate record Updates the fields in the existing record as specified in **Duplication Actions.** **Note:** If you choose **Update duplicate record**, the **Duplication Actions** related list appears.
Active	Select this check box to activate the rule.
Description	Describes the purpose and application of this duplication rule; when it should be used, for example a rule designed for IP-based observable, or security incidents from the firewall.

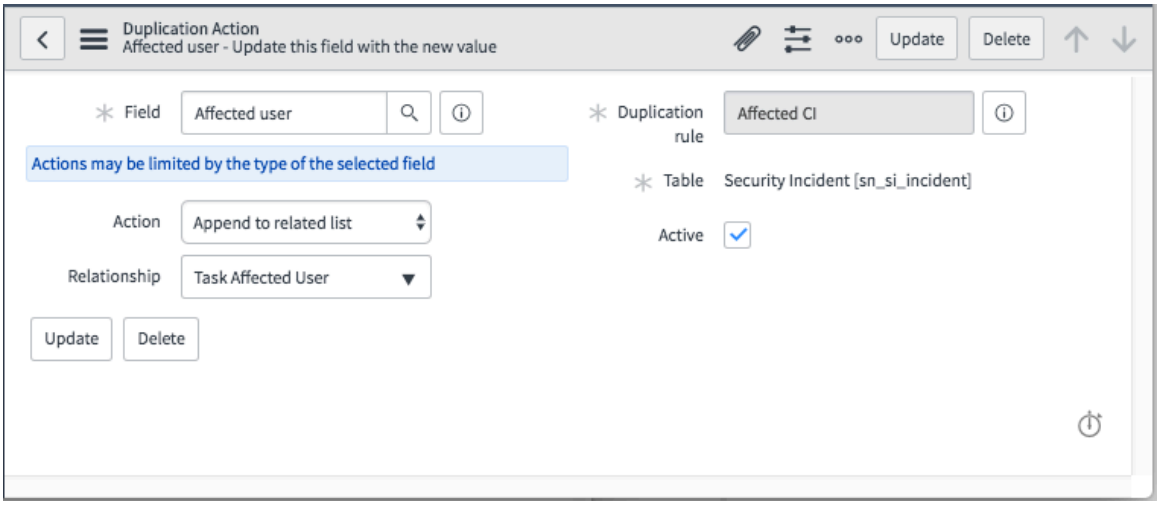
4. Right-click in the record header and select **Save** or click **Update**.
5. To set duplication actions, if you have chosen **Update duplicate record**, click **New** to create duplication actions for each field you want to update in the incident.
6. Fill in or edit the fields on the form, to describe how to update the field:

Duplication actions

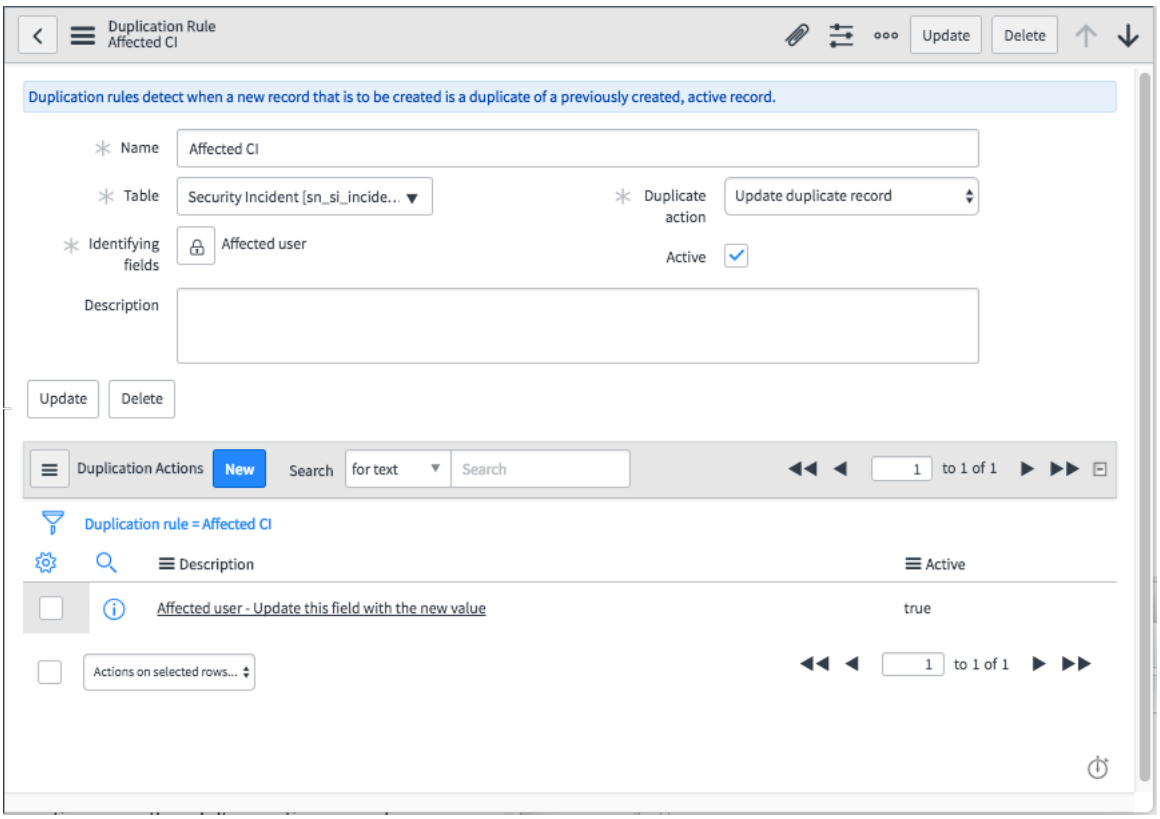
Field	Description
Field	The name of the field to use for the duplication action.
Action	The actions supported vary by field type. Choices are: **Update this field with the new value** Replaces the previous value in the existing record with this value. **Append the new value to a comma separated list, if unique** Treats the value as an entry in a comma-separated list and adds the new data (if any) as a new entry in that list. If the data is already in the list, it is not added twice. **Append the new value to this field** Appends the new value to the end of the existing text in the field. **Add one to a counter field** Adds one to the numeric field. **Set the field to today** Sets the field to the current date and time. **Append to related list** Adds the related record with this value to the related list of the current record. Appears when there is a many-to-many table, with a column of the same type, linked to the table being updated. For example, **Affected CI** or **Affected User**.
Relationship	[Optional] This field appears only when the **Append to related list** action is chosen. It is the name of the related list you want to associate with this rule.
Duplication rule	Rule that this action is part of.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Table	Table where records are created. Displays as information only.
Active	Select this check box to activate the action.



7. Click **Submit**.



Security Operations email processing

You can set up the integration of information from external detection systems, provide granularity in processing security operations records, handle unmatched emails, and prevent duplication of records using Email Processing.

Email Processing consists of these features:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Feature	Description
Email Parsing	Generate new Security Operations records from external system emails.
Duplication Rules	Identifies new email with known incidents and processes them appropriately.
Properties	Specifies accounts used as input in Email Parsing for security, vulnerability, and IoCs. Provides for granularity in processing Security Operations records.
Unmatched Emails	Lists emails that do not match any Security Operations record.

Security Operations email properties

Email Properties specify which inboxes are used as input in Email Parsing to import information from external detection systems to create records for security, vulnerability, and IoCs. You can set up a general account for all external detection systems to use, or individual email accounts for Security Incident Response, Threat Intelligence, or Vulnerability Response.

Create Security Operations email properties

You can specify email addresses for reports and control automatic email behaviors using email Properties.

Before you begin

Role required: sn_sec_cmn.admin
Set up external detection tools to send emails to your email parsing inbox.

Procedure

1. Navigate to **All** > **Security Operations** > **Email Processing** > **Properties**.
2. Enter your recipient mailboxes as appropriate:
   These are inbound email addresses to be processed by **Email Parsing**, rather than **Inbound Actions**.

   Email parsing properties

Field	Description
Inbox for Security Operations tools	Full email address for Security Operations. For example, secops_support@yourcompany.com.
Inbox for Security Incident tools	Full email address for Security Incident Response. For example, sir_support@your.company.com.
Inbox for Vulnerability Response tools	Full email address for Vulnerability Response. For example, vuln_resp@yourcompany.com.
Inbox for Threat Intelligence tools	Full email address for Threat Intelligence. For example, threat_intel@yourcompany.com.

3. Click **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations email parsing

Generate new Security Operations records from external detection systems using Email Parsing. This feature provides a method for integrating information from external tools such as malware detection, vulnerability detection, firewalls, threat intelligence, and more.

How emails are parsed

Any system that can send an email, can create Security Operations records, for example, security incidents, requests, vulnerable items, vulnerabilities, security incident observables, attack methods, and more.

All Security Operations plugins (Security Incident Response, Threat Intelligence, and Vulnerability Response) have a property (**email_to**) that defines the email address where external integrations should send emails to, to be parsed by the email parsers. See **Email Processing** > **Properties** for more information.

Email sent to any of the Security Operations email addresses is stored in an email events table. These emails are processed to determine whether they match any email parser.

Emails that have a match are flagged and the transform and duplication rules create or update a Security Operations record. The email is linked to that record and flagged as `matched`.

Emails that do not match are listed in Unmatched Emails as a Security Operations record. They can be reviewed to help build email parsers to handle these emails. A Reprocess action allows you to run the unmatched email through the parsers again. The original email log is linked to that record.

The duplication rules for the email transform manage multiple emails relating to the same issue. These rules define what makes a duplicate record and can prevent duplicate records from being created. When a duplicate is detected, the rule specifies what action to take: no action (do not create a new record), create the new record as a child record of the existing record, or update the existing record. When updating the duplicate rule specifies which fields in the existing record are updated.

Note: A Security Operations email parser works in conjunction with platform inbound actions and does not replace them. It does not support setting values on indirect fields for example, **sys_journal_field** entries.

By default, email events are deleted after 30 days.

Multiple records

External detection systems (malware detectors, vulnerability, and so on) can send emails that report on multiple items at one time. The email parser supports separators within the email.

For example, a malware detector could send you an email report about all systems within your network infected by one particular malware with information about the malware first, followed by a list of the systems affected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample malicious email

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

In this example, when the **Record Separator** is set within your **Email Transform**as **==========**, it splits the email into four sections that are evaluated separately. This creates a Security Incident for each of the three affected systems.

Note: The header section is detected but does not have any affected systems so, it is used in all three records and does not create a fourth record.

Field Transforms pull in data from each section. If something in the header or footer of the email applies to all records, such as Malware Hash, Malware Name, and Type in this example, the field transform for them should set **Search for value** to a value that searches within the email body either **At the start of a line in the email body** or **Anywhere in the email body**.

Field Transforms must be set to search **At the start of a line within the record section** or **Sec** for data that is defined within each section, such as System, IP address, or Status. The record section options are only available when there is a record separator defined within the email transform.

When parsing an email with a separator defined, records are only created for sections with at least one piece of section-specific data.

In this example, three records are created, even though there are four sections defined. The first section is a header, and it lacks anything specific to only one system. If any of the fields within the first section were filled in (System, IP, or Status), then a record would be created for that section, as well.

Related topics

- Create email parsers in Security Operations
- Security Operations enrichment data mapping
- Security Operations field mapping

Create email parsers in Security Operations

Email Parsing creates Security Operations records from your email for security, vulnerability, and observables to expedite threat response and remediation.

Before you begin

- Set up external detection tools to send emails to a central email address.
- Set the email address in Security Operations Properties. For more information, see Create Security Operations email properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Assign a user account to this email address and give that user security access controls to create and update the email event records.
- Have a copy of the relevant email from your external detection tool in front of you.
- Decide what type of record you want to create, a security incident, vulnerability record, task and so on. This choice determines the table you select.

Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Email Parsing**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

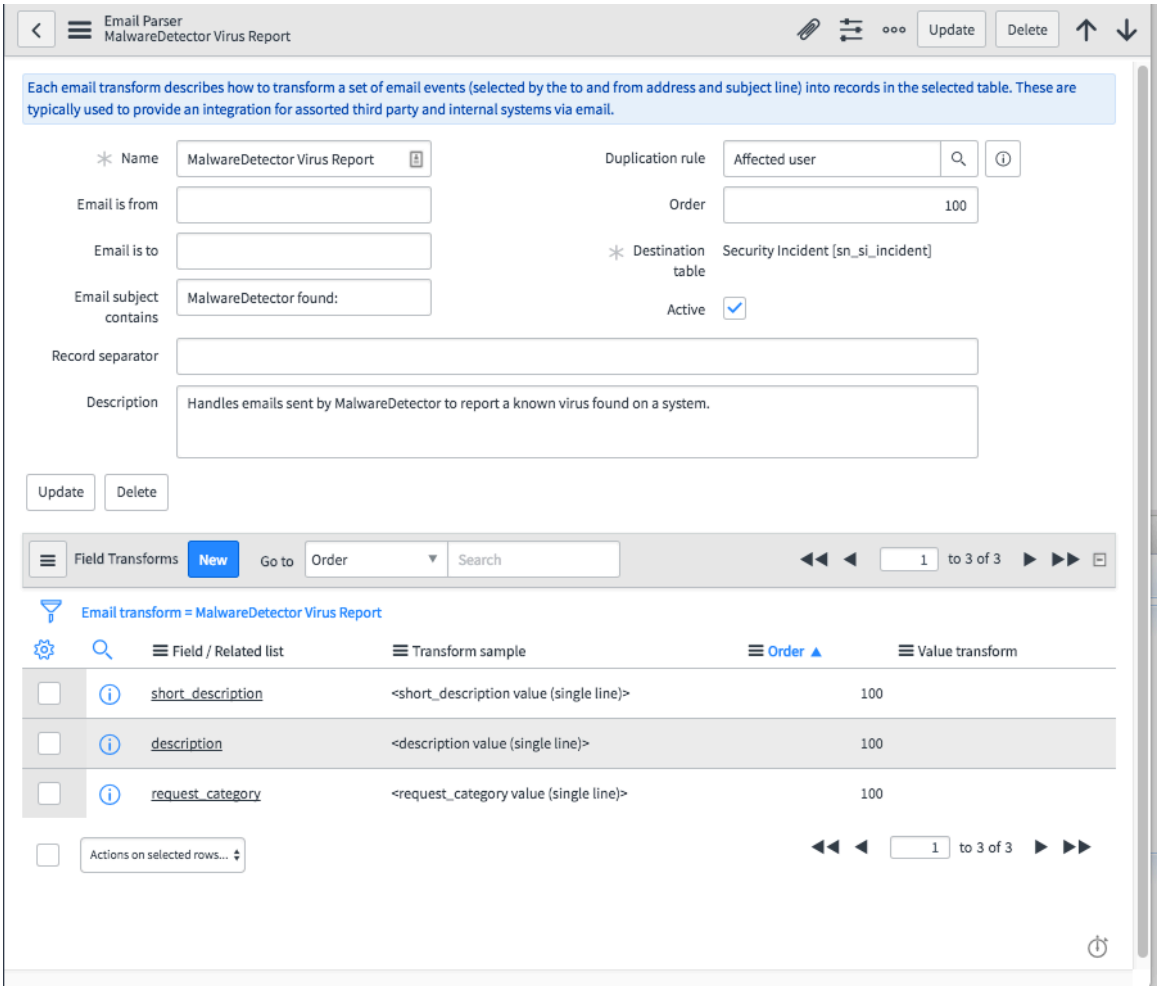
   Note: If more than one field is specified, all fields must match the email to create a record.

   Email parser

Field	Description
Name	The name of the email parser.
Email is from	If filled in, only emails from this address are transformed by this email parser.
Email is to	If filled in, only emails from this address are transformed by this email parser.
Email subject contains	If filled in, only emails where the subject contains this phrase are transformed by this email parser.
Duplication rule	Governs how to handle duplicate emails for any email this transform handles. For more information, see Shared data transformation.
Order	In what order to consider the transforms. The first matching email transform is used. Typically, you want to set up the most specific email parsers in the lower numbers, with some fallback. Give catchall email parsers higher **Order** numbers so they run if nothing else matches. Default is 100. When everything matches, the most specific email parser (matches **from**, **to**, and **subject**) is used.
Destination table	The table where you want to create records.
Active	Whether this transform is active, in use, or not active. If unchecked, no emails are transformed with this code.
Record Separator	When emails handled by this email parser create multiple records, this field contains the separator between the information for those records. See Security Operations email parsing for more information.
Description	Description of this email parser, which tool it works with, the purpose, and so on.

4. When you have completed your entries, right-click in the form header and select **Save**.
   A **Field Transforms** tab appears. This tab shows how individual fields within the destination table are set based on the email contents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. To add **Field Transforms**, perform these steps.
   a. In the **Field Transforms** tab, click **New**.
   b. Fill in the fields on the form, as appropriate.

Option	Description
Field	**Description**
Store value in a field or a related list	Select where to find the value. Choices in clude: ○ Store the value into a field in the new record ○ Link to this value in a related list ○ Link to this value, creating a new record if a matching record does not exist **Note:** If the destination table does not have any related lists, this field is not displayed.
Field	Select the field to fill in with this value.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	Note: For choice fields, matches are made to existing choices using the underly ing choice label or value. If no match is found, the field is set, but no new entry is added to the choice list. For more in formation, see Choice lists. For reference fields, an entry is set on ly when a value matching the display name of the record or a valid `sys_id` is found. For more information, see Refer
Related list	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the related list to add information to.
Value field	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the field within the table displayed in the related list. It is used to look up and find an existing record. For example, if your relat ed list is **Affected CIs**, this field can contain **Name** or **Fully Qualified Domain Name**, or any other field in the CI record to be used to look up the CI added to the **Affected CIs** list.
Relationship data	When **Store value in a field or related list** is set to **Link to this value in a related list**, a record is created to link that record (such as a security incident) to the value (a CI, an Ob servable, and so on.). This field specifies any additional information (field and value pairs) that should be added to the linking record. For example, adding an Observable for a source IP, specify that this IP is the source, rather than destination IP. For multiple values, use a ^ separator, for example, type= Source IP^Active=true.
New record data	When **Store value in a field or related list** is set to **Link to this value, creating a new record if a matching record does not exist**, if no related record matching the parsed value is found, a record is created. This field speci

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	fies the static data to add to that record. For **Affected CI**s, if no matching CIs are found a CI record is created). When that happens, the value found in the email, is set to the **Value** field in the CI record. You can set additional data – a note indicating why the CI was cre ated, some information about what type of CIs you are working with and, so on. A sample would be: description=Created by Malware Scanner email parser^type=autodetect.
Search for value	Select the location in the email to search. Choices include: ○ **At the start of a line in the email body** ○ **Anywhere in the email body** ○ **In the email subject line** ○ **Always the static value** When you have defined a **Record Separator**, more options (**Anywhere within the record section** and **At the start of a line within the record section)** enable you to search only within the current section instead of in the entire email body (See Security Operations email parsing for more information. Information that is in a header or footer, ap plying to all records, is searched for in the en tire email body. The information that differs be tween records is searched for only within the section.
Value separator	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the separator to use for lists of items. for example a comma or semicolon when the data from the email is a list of IP ad dresses.
Value prefix	The text that always precedes the value placed within this field to extract.
End of value	Select what indicates the end of the value. Choices include: **End of line**, **End of email** (brings in all remaining text in the email), or **Until** (stops when it finds the specified text), or **Until** (stops when it finds the specified text).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Value suffix	When the **End of Value** is set to **Until**, this field specifies what text always follows the val ue placed within this field. For example, looking for a value that comes after “The affected computer is” and before “.” will parse out “AB123” from “The dement ed bunny virus has been found. The affected computer is AB123. Estimated time of infec tion was 3:45PM” in an email.
Value transform	Choose the field transformation entry to ap ply. Converts the value found in the email into a different value, used to fill in choice fields, occasionally reference, and other fields.
Order	The order in which the field transforms run, from lowest to highest. A field transform with an order entry of 100 is attempted first. Only if that field transform fails to find a value will a field transform with a higher order (200) on the same field run.
Email transform	The transform this field transform belongs to.
Destination table	Destination table of the email transform. It contains informational data from the email transform.
Active	The default is checked. When checked, the field transform is activated. Uncheck this box to deactivate the field transform.

a. Click **Submit**.
The new record is used to parse the information in the email into a new record.

Related topics

Create duplication rules in Security Operations

Create Security Operations field value transforms

Define Vulnerability Response email notifications

Edit email records in Security Operations

Add or create transforms in your existing email event records.

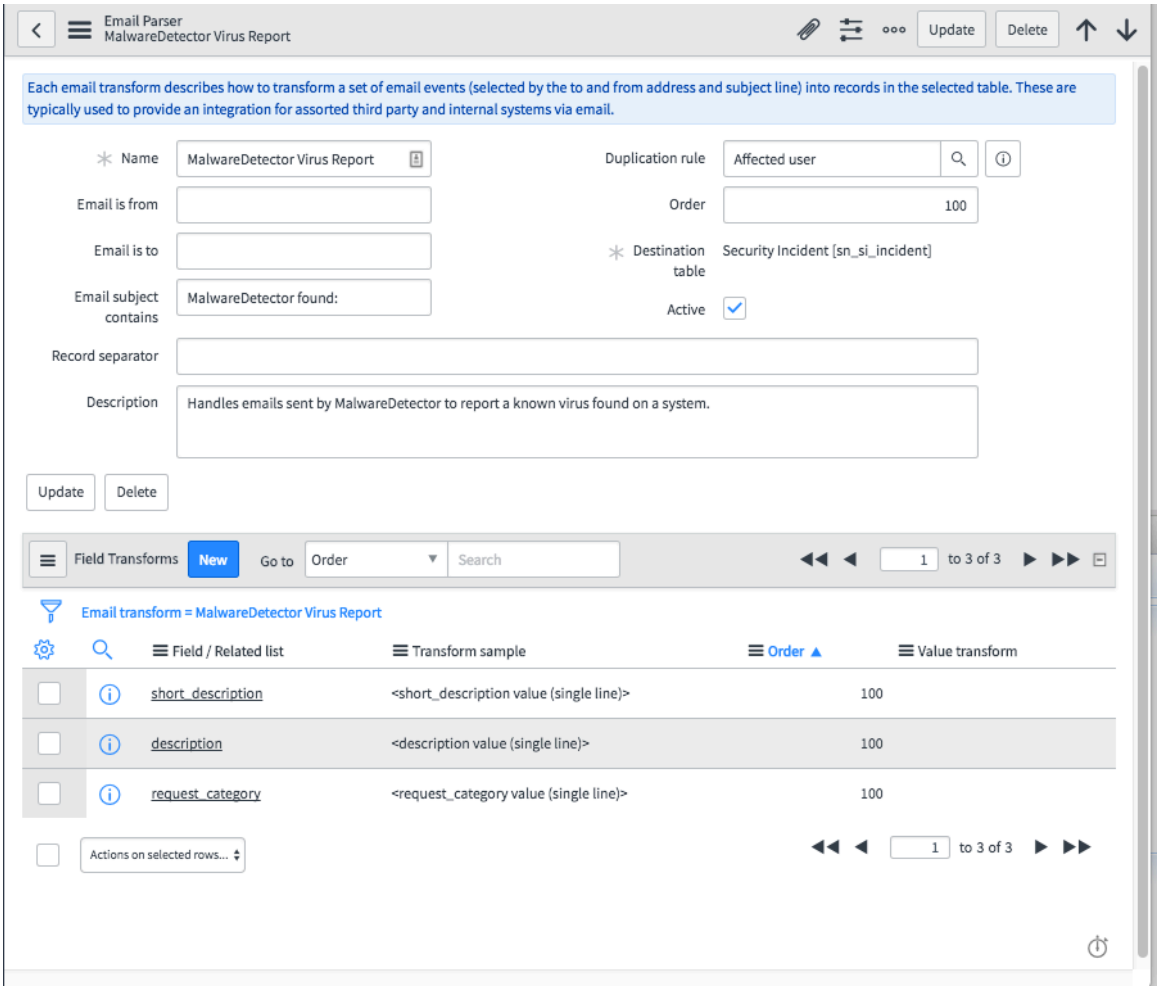
Before you begin

Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Email Parsing**.
2. Click the email parser to edit.
   If the record is read-only, click the here link in the header message.
   You are taken to the editable form of the transform.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Edit fields as appropriate.
4. To edit **Field Transforms**, click in the field and change as appropriate.
5. Click **Update.**

Unmatched Security Operations email events

Email events that do not match an email parser have their "matched" flag unset. You can view these email event records from the Unmatched Emails list, to reveal external detection systems whose emails are not yet parsed.

As you create email parsers, you can attempt to reprocess the email event (from the form or the list) to validate a new email parser.

View and reprocess unmatched Security Operations emails

You can review Unmatched Emails for discontinued filters or as candidates for a new filter to maintain or improve the rate at which you catch email threats.

Before you begin

Role required: sn_sec_cmn.read

Procedure

1. Navigate to **All** > **Security Operations** > **Unmatched Emails**.
   If any unmatched emails have been found, they are listed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. The fields on the form are as follows:

Security email events

Field	Description
From	Email address of the sender.
To	Email address of the recipients.
Subject	Subject line in the email.
Body	Contents of the body of the email.
Matched	Indicates if this email event was matched.

3. To reprocess this email, create an email record or edit an existing email record to match the information in this email.
   See Create email parsers in Security Operations.
4. Navigate back to **Security Operations** > **Unmatched Emails**.
5. Click **Reprocess Email Event** to attempt to process this email.
   It returns you to the Unmatched Emails main list. If the new email record matches, the email event is no longer in the list. A message indicates if it was matched or not.

Security Operations field mapping

Security Operations tables can be mapped to and from other tables, linking a security incident to a customer service case or a problem to other parts of the Security Operations system.

Field Mapping defines the mapping used when a record from the source table is used to create a new record in the destination table. Typically used to create a security incident from another record, these maps define which fields in a security incident are inserted into a new problem or which fields from an existing customer incident populate a new security incident.

Map tables to tables with Security Operations field mapping

Security Operations provides you with finer field-mapping granularity so you can map a Security Operations table to any other table.

Before you begin

Role required: sec_cmn.write

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Field Mapping**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

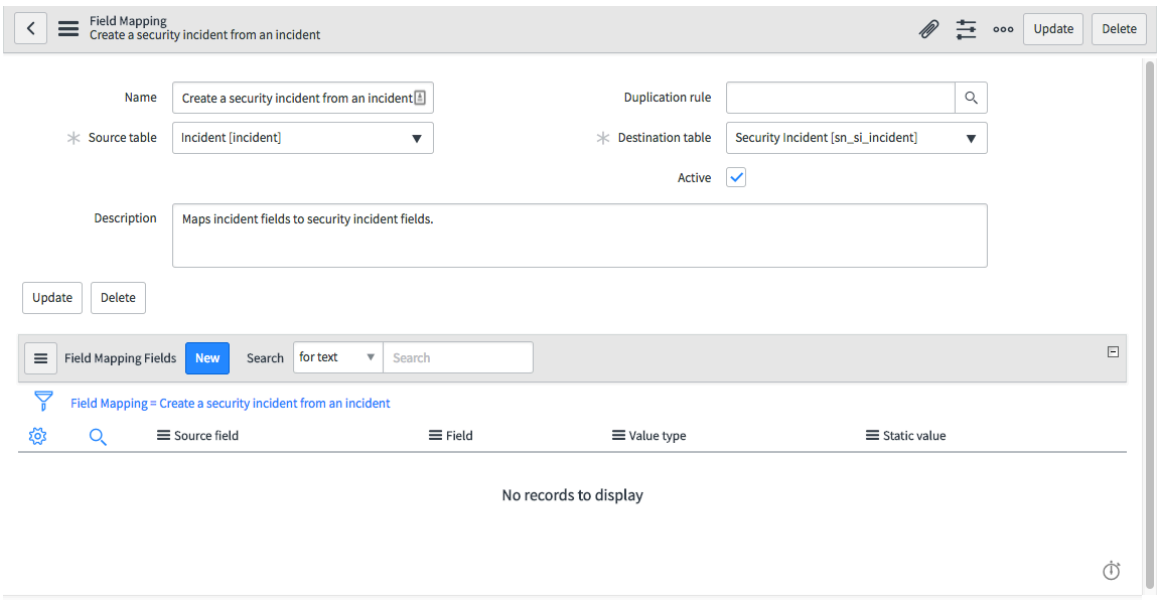
Field mapping

Field	Description
Name	The name of the field map.
Source table	The table that provides the data to use to create a record in the destination table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Duplication rule	Governs how to handle source records that would generate a duplicate record. For more information, see Shared data transformation.
Destination table	The table where new records are created.
Active	Select this check box to activate the mapping. **Note:** Only one mapping between tables can be active at a time. If two maps contain the same tables, then the older version is automatically deactivated.
Description	Description for the field map.

4. When you have completed your entries, right-click in the form header and select **Save**. **Field Mapping Fields** tab appears. This record defines what data is placed in the target field, in records created by this field transform.



5. Click **New**.
6. Fill in the fields on the form, as appropriate.

Option	Description
Field	**Description**
Store value in a field or a related list	Select where to find the value. Choices in clude: ○ Add new value into a field in the record ○ Link to this value in a related list

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	○ Link to this value, creating a record if a matching record does not exist **Note:** If the destination table does not have any related lists, this field is not displayed.
Field	When **Store value in a field or related list** is set to **Add new value into a field in the record** this field specifies the field to fill in. **Note:** For choice fields, matches are made to existing choices using the underly ing choice label or value. If no match is found, the field is set, but no new entry is added to the choice list. For more in formation, see Choice lists. For reference fields, an entry is set on ly when a value matching the display name of the record, or valid`sys_id` is found. For more information, see Refer
Related list	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the related list to add information to.
Value field	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the field within the table displayed in the related list, that is used to look up and find an existing record. For example, if your related list is **Affected CIs**, this field may con tain **Name** or **Fully Qualified Domain Name**, or any other field in the CI record that should be used to look up the CI is added to the **Af fected CIs** list.
Relationship data	When **Store value in a field or related list** is set to **Link to this value in a related list**, a new record is created to link that record (such as a security incident) to the value (a CI, an observable, and so on). This field specifies any additional information (field and value pairs) that should be added to that linking record. For example, adding an observable

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
	for a source IP, you can specify that this IP is the source, rather than destination IP. For mul tiple values, use a ^ separator, for example, type= Source IP^active=true.
New record data	**When Store value in a field or related list** is set to **Link to this value, creating a new record if a matching record does not exist**, if a related record matching the parsed val ue is not found, a new record is created. This field specifies the static data to add to that record. For example, for **Affected CIs**, if we cannot find the CI, this setting indicates that a new CI is created). The value found in the source record is set to the **Value** field in the CI record. You can set additional data – a note indicating why this CI was created, some information about what type of CIs you are working with. A sample would be: `descrip tion=Created by malware Inci dent report^type=autodetect`
Value separator	When **Store value in a field or related list** is set to **Link to this value in a related list** or **Link to this value, creating a new record if a matching record does not exist**, this field specifies the separator to use for lists of items, commonly a comma or semicolon.
Value type	When **Store value in a field or related list** is set to **Add new value into a field in the record** this field specifies the type of value. Choices include: ○ **Source field record** ○ **Append to the field as a new line** ○ **Static value** ○ **Static value plus source record field value**
Source field	Choose the source field that contains the val ue to be placed within the destination field or the selected related list.
Static field	Static value for the field.
Value transform	Choose the field value transformation entry to apply. It is used to map choice fields between records, for example, converting the set of **Category** choices for a security incident into the appropriate **Type** field for a Change Re quest.
Destination table	Auto-populated with the destination table.
Field Mapping	Auto-populated with the parent field map.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Description
Source table	Auto-populated with the source table.

7. Click **Submit.**

Security Operations field value transforms

Transforms unique customer field values into field values recognized by Security Operations email parsing, data enrichment or tables using field maps. Supports choice fields, references, and aligns external data into the standard terminology and format for your new record.

You can map data for fields such as Category, State, or Assignment Group into the values used within the Security Operations table. For example, map "In Analysis" to "Work in progress.

Create Security Operations field value transforms

Field Value Transforms defines one transformation between provided source data, and the replacement value to use.

Before you begin

Role required: sn_sec_cmn.basic or sn_si.basic

About this task

Define each transformation entry to apply either when there is a match to the search value, or when the search value is contained within the provided source data, or when no matches are found. Set a default value for when no match is found. If no default value is set, and no matches are found, the original source data is used.

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Field Value Transforms**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field value transforms

Field	Description
Name	The name of the field value transform.
Description	Description for the field map.
Field Value Transform Entries	The table list of entries. **a.** Under **Replace data**, double-click 'Insert a new row.' **b.** Choose one of the following: When the date for this field matches When the data for this field contains When no other transform entry matches the data (default) **c.** Click the green check mark. **d.** Double-click under **Search value**, add your search value. **e.** Click the green check mark.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	f. Double-click under **Replacement value** add the ServiceNow corresponding value. g. Repeat if necessary.
Active	Select this check box to activate the transform.
Application	Scope of the application.

4. Click **Submit.**

Security Operations enrichment data mapping

Enrichment Data Mapping transforms data from XML, JSON, or Properties files to ServiceNow records. Security Operations workflows use enrichment data maps and provide output data to security incidents.

Security Operations includes several enrichment data maps, triggered by various workflows, for example, Security Operations Integrations - Get Network Statistics workflow and Security Operations System Command Integration- Get Running Processes flow. Enrichment data map output from Security Operations workflows is displayed in the **Enrichment Data** tab on the security incident form.

Create a Security Operations enrichment data map

Transform data from JSON, XML, or Properties file format to ServiceNow records using enrichment data maps.

Before you begin

Role required: sn_sec_cmn.write

About this task

Existing enrichment data maps are used by workflows provided within Security Operations. You can view the list under **Enrichment Data Mapping**. To use a map, you need a trigger, either a business rule or workflow.

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Enrichment Data Mapping**.
2. Click **New**.
3. Fill in the fields, as appropriate.

Creating an enrichment data map

Field	Description
Name	Name of this enrichment data map.
Input format	Choose a format from the list: JSON (default) XML Properties File format
Prefix key	Use to limit the input data set to a specified key. The root of the input data set is set to this

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	key. In this example, if you entered file_info, then the input values would be limited to those values within file_info. <?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Application	Scope of the application.
Duplication rule	Rule defining when a record is considered a duplicate and what actions to take with duplicate records.
Destination table	Choose a table from the list.
Active	Select this check box to activate the map.
Description	Enter a description of the enrichment data map.

4. Click **Submit.**
   The Enrichment Data Mapping Fields tab appears.
5. Click **New**.
6. Fill in the fields on the form, as appropriate.

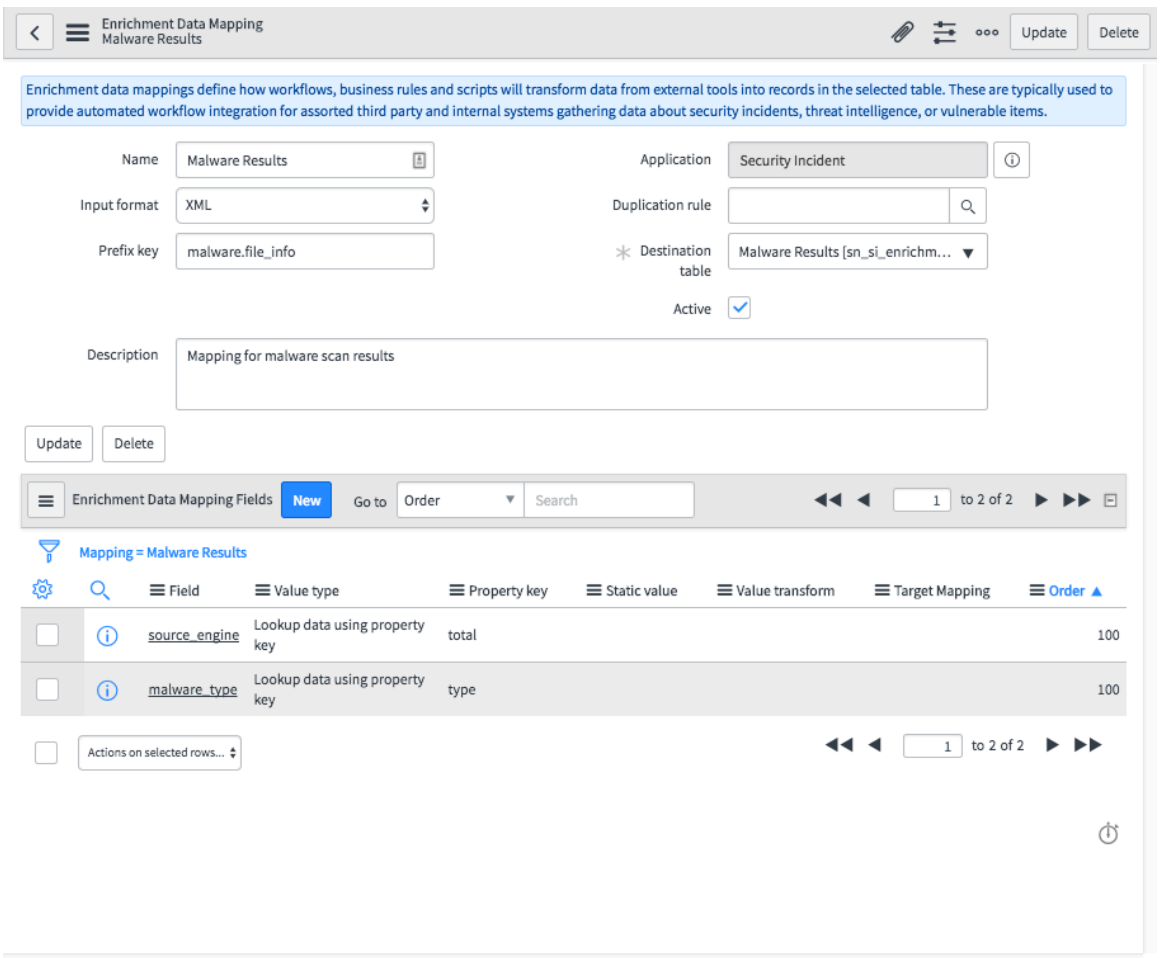
Enrichment data mapping fields

Field	Description
Field	Name of the enrichment data map.
Value type	Choose from the list: Lookup data using property key Static value

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Static value plus data from the property key Field is an array or object (raw data nesting) Each choice has different entries. Field values and arrays or objects require a Property key.
Property key	Determines the key for the input data search and the value written to the target field.
Value transform	The field value transform that maps one value to another.
Application	Scope of the application.
Order	In what order to consider the mapping. The first match is used. Default is 100.
Mapping	Name of the enrichment data map.
Destination table	The table to which the fields to map are going.

7. Click **Submit**.
The following is an example of an enrichment data map.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations user-defined escalation

You can create an escalation path for security incidents for issues requiring more attention or expertise. Once an escalation group exists, a button appears on any security incident in that group.

Create a Security Operations user-defined escalation group

Escalate a security incident to any group associated with the incident using Escalations.

Before you begin

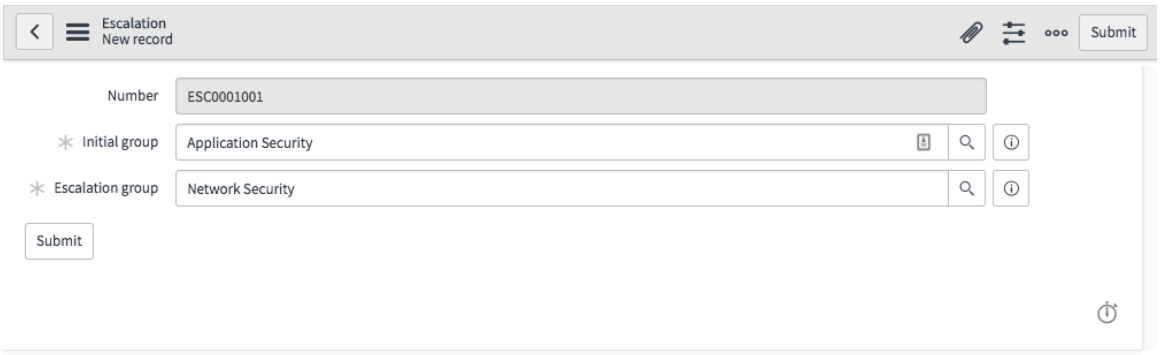
Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Groups** > **Escalations**.
2. Click**New**.
3. Fill in the fields on the form, as appropriate.

Escalations

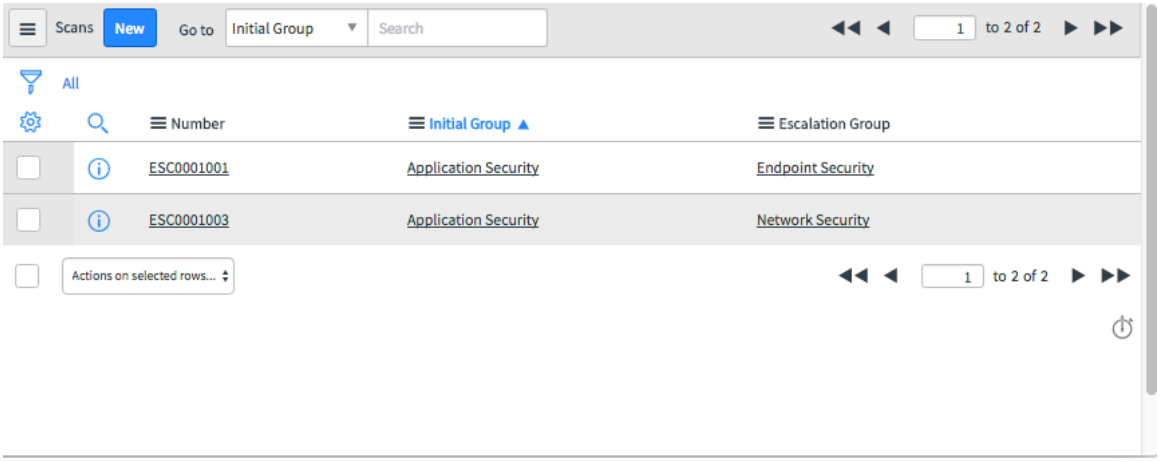
Field	Description
Number	Escalation incident number (field is auto-generated).
Initial group	Select group this security incident belongs to.
Escalation group	Select group to escalate the security incident to.



4. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

An escalation group is available for all security incidents in the initial group. You can create multiple groups.



Create domain-separated property overrides

When you use domain separation, you can create overrides to existing Security Operations properties that allow you to customize the functions of the applications in each of your domains.

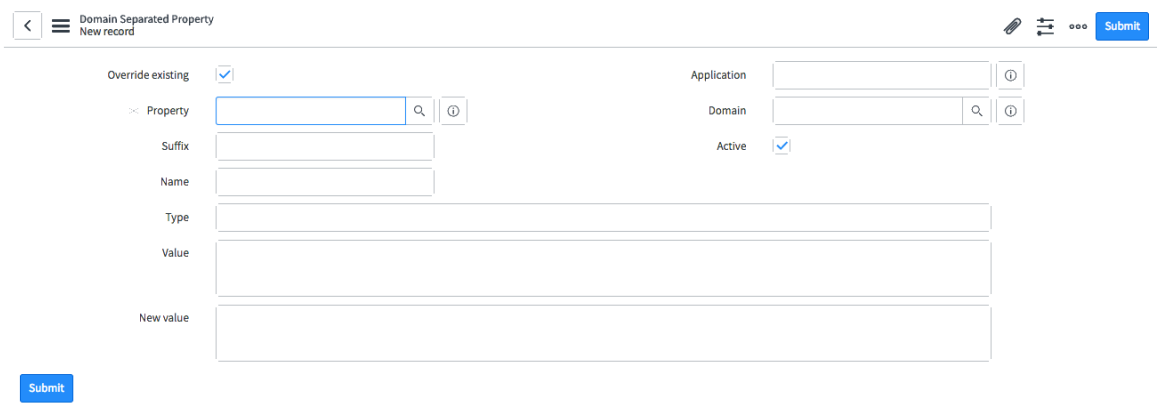
Before you begin

Requires that Domain Support - Domain Extensions be activated. You can also learn about the Domain Override Viewer.

Role required: admin

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Domain Separated Properties**.
2. Click **New**.



3. On the form, fill in the fields.

Domain Separation Property form

Field	Description
Override existing	Select this check box to create a domain-specific value for an existing property.
Application	Select the application that contains the property you want to override.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Property	Select the property for the selected application for which you want to create a domain-specific override.
Domain	Select the domain for which you are creating this property override.
Active	Turn the override on or off.
Suffix	Displays the property suffix.
Name	Displays the property name.
Type	Displays the property type.
Value	Displays the current value set for the property.
New value	Enter a new value for the property to be applied to this domain.

4. Click **Submit**.
   The property override is applied to the selected property in the specified domain. When the logic for this property is triggered, the system checks for domain-separated property overrides. If an override for the domain is found, the new value is used. Otherwise, the value for the default domain is used.

Related topics

Understanding domain separation

Create an operating system group

Operating system groups are used to map an operating system to specific process types and scripts in Security Incident Response workflows. The scripts define how running processes for the defined operating system groups are retrieved. New operating systems can be added as needed.

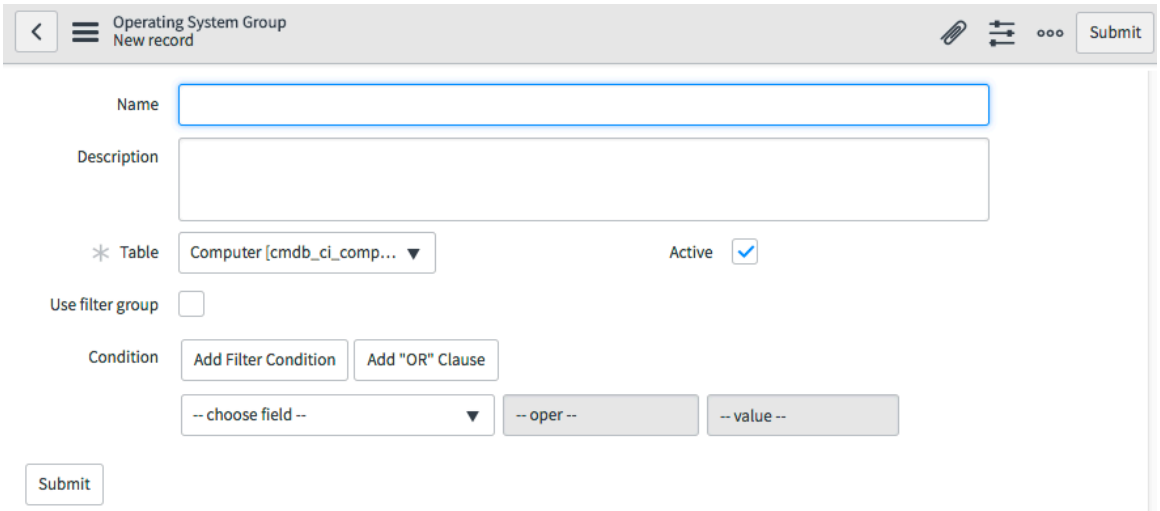
Before you begin

Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Utilities** > **Operating System Groups**.
   The base system includes scripts for three operating systems:
   - BSD-based OS
   - POSIX-based OS
   - Windows OS
2. Click **New**.

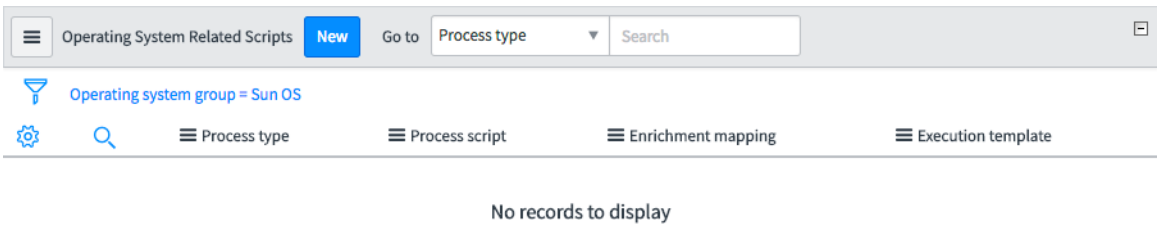
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Fill in the fields, as needed.

Field	Description
Name	The name of the operating system group.
Description	A description for the operating system group.
Table	The affected table.
Active	Select this check box to activate the operating system group.
Use filter group	Select this check box to use a filter group for locating matching records in the selected table.
Filter group	Select the filter group for locating matching records in the selected table. This field displays only if you selected the **Use filter group** check box.
Condition	The condition builder fields display only if you did not select the **Use filter group** check box.

4. Right-click in the form header and select **Save**.
The Operating System Related Scripts related list opens.



5. Click **New**.
6. Select scripts that correspond with the workflows you are using to get running processes, services, and/or network statistics.
7. Click **Submit**.

Related topics

Attach a script file to a file synchronized MID Server

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up security tag groups and tags

You can assign tags to security incidents, response tasks, vulnerable items, observables, IoCs, and security cases to create metadata on the responding record and define who should have access to specific types of security content. The tags can be added to security groups to organize them.

Before you begin

Role required: sn_si.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Security Tags** > **Groups**.
   Three default classification groups are included in the base system.
   - **Enrichment allow list/deny list**: This group defines whether a record is to be treated as a allow list or deny list record. Allow list records are generally of less significance, so they can be ignored. Deny list records are generally of higher interest.
   - **Metatag**: This group is provided as demo data. You can use it to create custom classification tags that are used by security operations applications.
   - **Traffic Light Protocol**: This group is used to ensure that sensitive information is shared with the correct audience. It employs four colors (White, Green, Amber, and Red) to indicate different degrees of sensitivity. For each color, you can assign the appropriate read/write access roles. When sharing observables to a trusted security circle, the tag assigned to the trusted security circle profile determines which TLP-tagged observables can be shared to the circle, as follows:
     - **TLP: WHITE:** Only observables with TLP: WHITE can be shared to a TLP: WHITE profile.
     - **TLP: GREEN:** Observables with TLP: GREEN and TLP: WHITE can be shared to a TLP: GREEN profile.
     - **TLP: AMBER:** Observables with TLP: AMBER, TLP: GREEN, and TLP: WHITE can be shared to a TLP: AMBER profile.
     - **TLP: RED:**All observables, regardless of their TLP tag, can be shared with a TLP: RED profile since TLP: RED is the highest ranked TLP tag.

   Note: You can add other TLP colors, but any in addition to the four colors included are considered not valid by the Forum for Incident Response and Security Teams (FIRST).

2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	Enter name of the security group.
Allow multi-selection	Check this box if you want to be able to assign multiple security tags to a record that shares a group.
Active	Turn the group on or off.
Description	Enter a description of this group.

4. Right-click the form header and select **Save**.
   The Security Tags related list appears.
5. In the Security Tags related list, click **New**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the classification tag.
Security Tag Group	If the tag was created using the **New** button in the group related list, this field defaults to the current group. If needed, you can add the tag to a different group, but this is optional.
Order	Specify the order the tag appears on forms or within a list.
Color	Select the color for this tag.
Enforce restricted access	Select this check box to assign read and/or write roles needed by users to read or write to records that have this security tag.
Active	Turn the tag on or off.
Description	A description of this tag.
Roles (read access)	To assign read access to a security tag, click the lock icon, select the appropriate access roles, and click the lock icon again. This field appears only if you selected the **Enforce restricted access** check box.
Roles (write access)	To assign write access to a security tag, click the lock icon, select the appropriate access roles, and click the lock icon again. This field appears only if you selected the **Enforce restricted access** check box.

7. Repeat as needed to create more security tags.
8. Click **Update**.

> **Note:** You can also create new tags by navigating to **Security Operations** > **Security Tags** > **Tags**. The procedure is the same.

Create security tag rules

Security tag rules provide filtering for security tag access.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Security Operations** > **Security Tags** > **Tags**.
2. Choose or create a security tag.
3. In the **Security Tag Rules** related tab, click **New**.
4. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the security tag rule.
Security Tag	The security tag to attach to the rule.
Active	Turn the security tag on or off.
Description	A description of this rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Determine **Record Filtering.**
6. Fill in the fields on the form, as appropriate.

Field	Description
Use filter group	Associates filter group to the rule.
Table	The table to contain the rule.
Condition	Add one or more filter conditions.

7. Click **Submit**

Import security tag rules

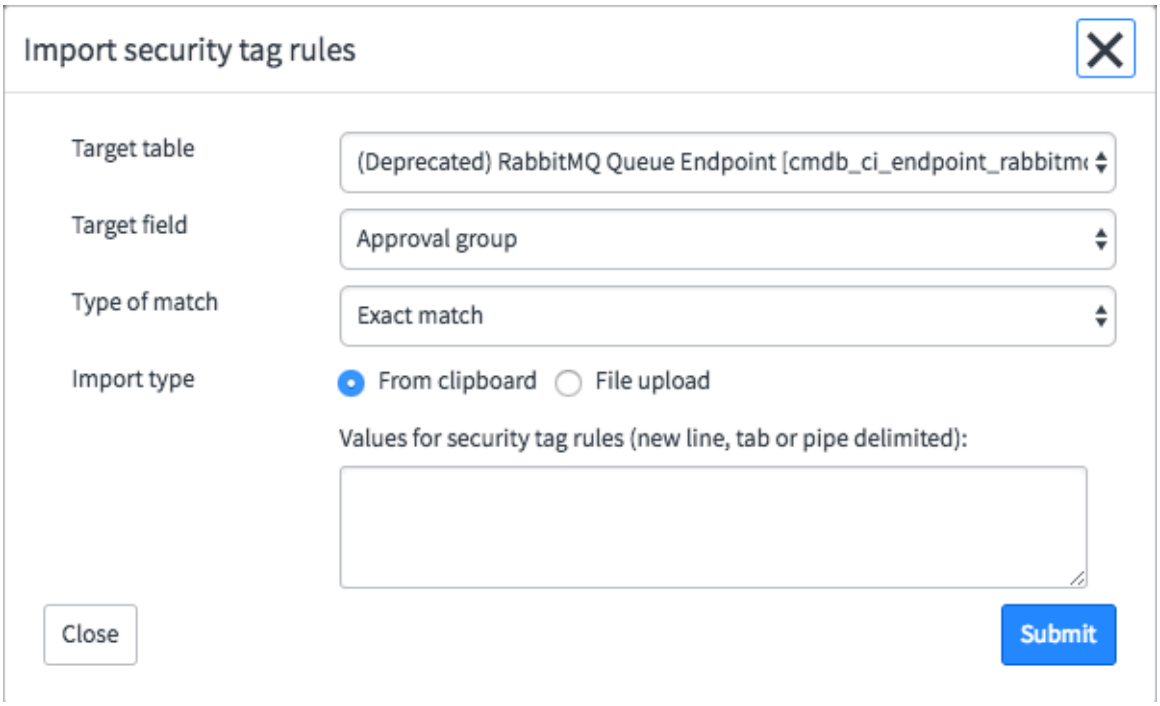
You can import security tag rules from other tables in your deployment.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Security Operations** > **Security Tags** > **Tags**.
2. Choose or create a security tag.
3. Click the **Import security tag rules** related link.



4. Fill in the fields on the form, as appropriate.

Field	Description
Target table	Choose the table to use to import rules.
Target field	Choose the field to use to import rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Type of Match	Choose how to match the imported rules to **Security Tags** from: Exact match (default) Contains Starts with Ends with Regular Expression
Import type	Choose: **From clipboard** Copy a list of delimited values into the text area. The values are parsed into security tags. **From file upload** Upload a file with delimited values. The values are parsed into security tags. Add values for the security tag rules using new line, or pipe delimiters.

5. Click **Submit**

Security annotations

A security annotation is a note of explanation or comments added to a configuration item, observable, or use on a security incident.

Multiple security annotations are available for users and observables (requires the Threat Intelligence plugin). Reports on security annotations are also available.

Create security annotations for CIs

Annotations on CIs allow you to track activity across incidents. You can add annotations to a single or multiple CIs.

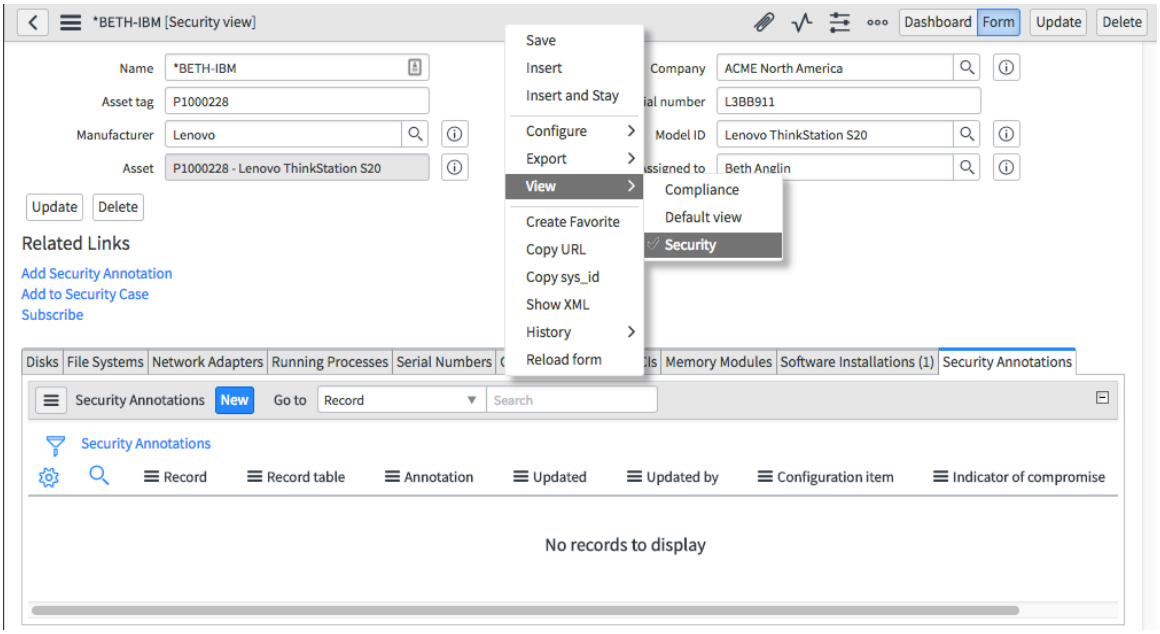
Before you begin

Role required: admin

Procedure

1. From a security incident or the Configuration Item table, open a CI.
2. Right click in the header and choose **View** > **Security**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. In the **Security Annotations** related list tab, click **New**.
4. Enter an annotation.
   Annotations can be in any text format.
5. Click **Submit.**

> **Note:** You can add the same annotation to multiple CIs by selecting CIs on the list, choose **Add security annotation**, enter an annotation in any text format, and click **Submit**.

Create security annotations for observables

You can select a single or multiple observables and apply security annotations to them using the **Actions on selected rows** choice menu.

Before you begin

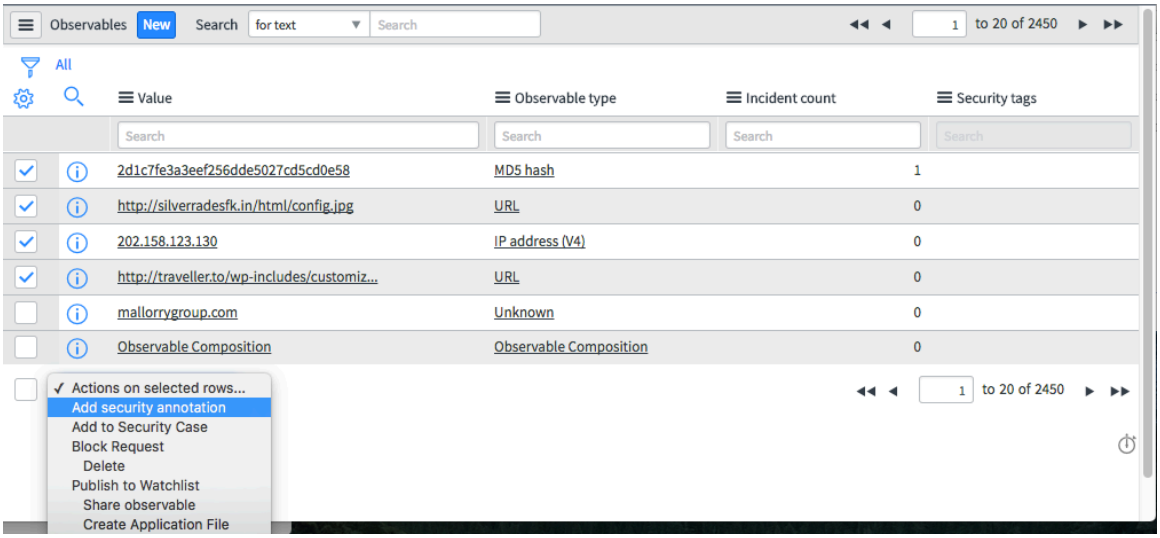
- Requires the Threat Intelligence plugin and activation. The Threat Intelligence plugin is available as a separate subscription.

Role required: admin

Procedure

1. Navigate to **All** > **Threat Intelligence** > **Observables**
2. Select one or more observables in the list.
3. From the **Actions on selected rows** drop-down menu, choose **Add security annotation**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Enter an annotation.
   Annotations can be in any text format.
5. Click **Submit**.

Create security annotations for users

You can select a single or multiple users and apply security annotations to them using the **Actions on selected rows** choice menu.

Before you begin

Requires the Threat Intelligence plugin and activation. The Threat Intelligence plugin is available as a separate subscription.

Role required: admin

Procedure

1. Navigate to **All** > **User Administration** > **Users**
2. Select one or more users in the list.
3. From the **Actions on selected rows** drop-down menu, choose **Add security annotation**.
4. Enter an annotation.
   Annotations can be in any text format.
5. Click **Submit**.

View security annotations reports

The Security Annotations report presents details stored in the Security Annotations [sn_sec_cmn_security_annotations] table. You can customize the columns in the report and group the data in any way that suits you.

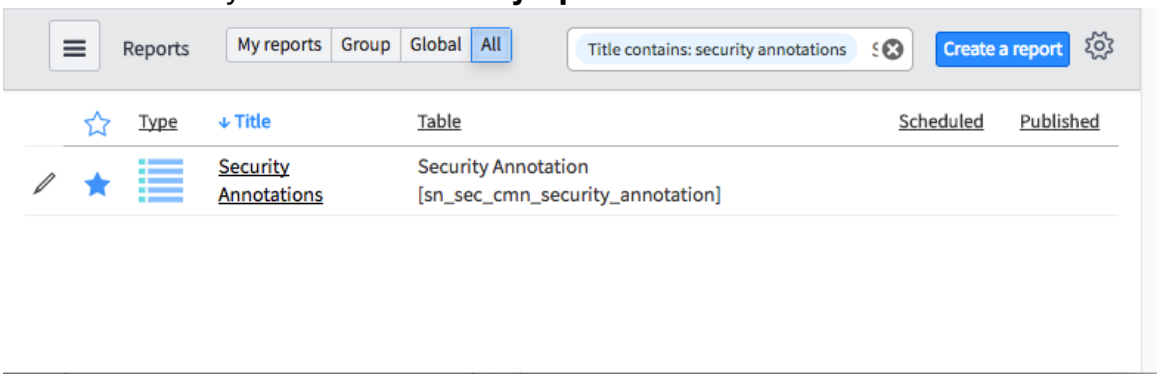
Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Reports** > **View/Run**.
2. Search for Security Annotations under **My reports** or **All.**



Related topics

View the Reports list

Components installed with Security Support Common

Several types of components are installed with Security Support Common. They provide common functionality for use across the various security applications, such as Security Incident Response.

Locating and viewing installed components

See View components installed with Security Support Common more information about locating and viewing installed components.

View components installed with Security Support Common

Several types of components are installed when you activate the Security Support Common plugin including but not limited to tables, user roles, and modules.

Locating components

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

If you want to limit the list of installed components to roles, scheduled jobs, and tables for the Security Support Common application, follow these steps:

View filtered lists for components installed with an application

Filter the Applications Files table so that only the roles, scheduled jobs, and tables that are installed with an application are displayed. The application you want to view these components for should be installed so that its files are loaded onto the instance and into the metadata table. Follow these steps to view filtered lists from the Applications Files table.

1. In the filter navigator, enter **sys_metadata.list** to navigate to the metadata table.
2. Select the condition builder (filter icon), and select, **Application** > **is** followed by the name of your application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In the condition builder, to add a second filter, click **AND**, then select, **Class** > **is a** and choose one of the following classes from the list: **Role**, **Scheduled job**, or **Table**.
4. Select **Run**.

The results for the class you selected are displayed in a filtered list.

Search Security Operations

You can find information quickly in any Security Operations application using the search icon in the screen header. Zing is the text indexing and search engine that performs all text searches in your instance.

Before you begin

Role required: sn_si.read or higher

Procedure

1. Click the search icon () in the upper right-hand corner of the screen.
2. Type in the criteria you want to search by, and press **Enter**.
   If you have the Security Incident Response plugin activated, the search criteria you entered present any matching short description text, CIs, IP addresses, or URLs in your security incidents, Security Incident Response tasks, or security requests. If you have the Vulnerability Response or Threat Intelligence plugins activated, the search results include vulnerabilities, vulnerable items, vulnerable entries, observables, IoCs, and attack mode/methods.

Related topics

Introduction to searching

Zing text search

Security Operations Integration Reference

Developers and ServiceNow partners can use the information in this section to gain understanding of the under-the-hood functionality of third-party integrations, including development guidelines, integration capabilities, and workflows.

ServiceNow Security Operations integration development guidelines

The ServiceNow platform provides several mechanisms for developing integrations with external systems. The ServiceNow Security Operations product suite adds integration capabilities intended to streamline the process of integrating with security-focused external systems.

Most of the concepts in this guide assume some familiarity with standard ServiceNow functionality. To integrate with the Security Operations suite, at a minimum, knowledge of the following ServiceNow concepts is required:

- Script includes
- Inbound/outbound web services
- Data sources
- Import sets
- Transform maps

Technology Partner Program

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Any requirements for application certification or guidelines given in the Technology Partner Program literature supersede any information in this guide. This guide is not a replacement for the Technology Partner Program literature and serves only as a supplement to existing documentation.

For more information, see Technology Partner Program training course blog post.

Types of ServiceNow integrations provided

The Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response) can be seamlessly integrated with other ServiceNow applications to enhance their functionality.

The following integrations are provided in the Security Operations base system.

Security Incident Response – Event Management integration

The capabilities of the Event Management application have been expanded to support Security Incident Response. The Security Incident Response Event Management support plugin automatically parses the contents of events in Event Management to populate fields in security incidents.

Use case covered:

Creation of security events in the Event Management system from Security Information and Event Management (SIEM) tools

Useful capabilities provided:

- Event management functionality – event correlation, event rules, and alert rules
- Automatic mapping of additional_information values to resulting security incident

Resources:

Security Incident event management support documentation

Event Management documentation

Security Incident Response - Import Set API integration

In addition to using Event Management to push security-related events, the Security Incident Response application provides an Import Set API that allows direct creation of security incidents. The REST endpoint for the Security Incident Import Set is http://localhost:8080/api/now/import/sn_si_incident_import.

This integration technique is useful when a) Event Management is not installed, or b) it is desired to simply create Security Incidents without going through the event > alert > Security Incident flow that is required when using Event Management.

Use case covered:

Creation of security incidents directly from SIEM tools.

Useful capabilities provided:

Automatic CI matching on Security Incident creation based on IP, NetBIOS, or fully qualified domain name.

Resources:

Platform Import Set API documentation

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Incident Web Service Import Set documentation

Threat Intelligence - lookup source integration

Lookup sources provide the ability to send data to external lookup sources to determine if that data is malicious. Generally, that data is an IP address, URL, file, or file hash.

Use case covered:

Lookup an IP address, URL, file, or hash with an external lookup service.

Useful capabilities provided:

- Consistent way to request lookups from catalog items and security incidents.
- Rate limiting and throttling capabilities provided with little/no coding.
- Automatic creation of Indicators of Compromise (IoC) observable entries for any issues found by lookup sources.

Threat Intelligence - threat source integration

Threat Sources provide the ability to pull in data from external threat intelligence repositories. This data is then imported into the various Indicators of Compromise tables that exist within the system. TAXII collections and simple blocklists are supported natively. To add new TAXII collections (or profiles based on a discovery or collection management service), it is as simple as adding an entry. Similarly, adding a new simple, single column blocklist is a matter of entering a new record and providing the URL of the blocklist. For more complicated sets of data, a custom integration can be provided to make a call to a URL and parse the response.

Use case covered:

Retrieve data from a threat intelligence source to load into IoC tables.

Useful capabilities provided:

- Support for simple blocklists and TAXII collections with no coding.
- Simple mechanism for executing REST messages for retrieving data.
- Decoupled data retrieval/processing for integration component reusability.
- Native support for processing passing data returned to data sources (and import sets/transform maps).
- Supports multiple data requests per integration (for paginated calls) with the ability to pass context to subsequent calls

Resources:

Define a threat source

Vulnerability Response - scanner invocation integration

Vulnerability Scanner Invocation is a lightweight integration entry point that supports invoking vulnerability scans from the instance. A third-party vulnerability scanner is called asynchronously to schedule a scan for configuration items or IP addresses.

Use case covered:

Make request to third-party scanner to scan a CI (using host information derived from CI) or IP address/IP addresses.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Useful capabilities provided:

- Simple framework for defining scanner implementations.
- Consistent way to request scans from catalog items, security incidents, and vulnerable items.
- Automatic updating of tasks with result of scan invocation.

Vulnerability Response - data integration

Vulnerability data integrations are intended to retrieve vulnerability data from third-party vulnerability systems. The expected outputs from these integrations are vulnerability entries and vulnerable items. This integration allows third-party vulnerability scanners to function independently, with the expectation that vulnerabilities can be worked and tracked within the instance.

Use cases covered:

- Retrieve vulnerability libraries
- Retrieve vulnerability/CI pairings
- Synchronize CIs with vulnerability management system

Useful capabilities provided:

- Decoupled data retrieval/processing for integration component reusability.
- Native support for processing passing data returned to data sources (and import sets/transform maps).
- Supports multiple data requests per integration (for paginated calls) with the ability to pass context to subsequent calls.

Resources:

Vulnerability data integration documentation

Security Operations Integration Configurations

Many of the integrations included in the base system require little or no setup, and operate in the same way. Certain integrations, such as the Qualys Cloud Platform, however, require separate steps for setting up the integration. Others support different sets of scan and lookup types and different rate limits.

This section describes the differences between the supported integrations and points you to more documentation, as needed.

- Carbon Black integration: allows you to investigate and respond to security incidents by using the Carbon Black APIs to query and interact with endpoints associated with security incidents.
- Check Point Anti-bot - Email Parser integration: uses an email parser that consumes email notifications from Check Point Anti-bot to create security incidents.
- Elasticsearch Incident Enrichment integration: searches your logs and adds relevant sighting information to your security incidents.
- Have I been pwned? integration: allows the list of breached accounts (email addresses and usernames) to be quickly searched via a RESTful service.
- HPE Security ArcSight ESM - Email Parser integration: uses an email parser that consumes email notifications from HPE ArcSight ESM to create security incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- HPE ArcSight Logger - Incident Enrichment integration: searches your logs and adds relevant sighting information to your security incidents.
- IBM QRadar - Incident Enrichment Integration: searches your logs and adds relevant sighting information to your security incidents.
- McAfee ESM - Email Parser integration: uses an email parser that consumes email notifications from McAfee ESM to create security incidents.
- McAfee ESM - Incident Enrichment Integration: searches your logs and adds relevant sighting information to your security incidents.
- OPSWAT Metadefender integration overview: allows threat data, detected by the third-party Metadefender scanner, to be downloaded to the Threat Intelligence application for tracking, prioritization, and resolution.
- Palo Alto Networks - AutoFocus integration: Palo Alto Networks AutoFocus, a threat intelligence cloud service, allows you to search for session information related to security incident observables.
- Palo Alto Networks - Firewall integration: Palo Alto Networks Firewall allows you to set up and maintain firewalls for preventing known and unknown threats across the network, cloud, and endpoints.
- Palo Alto Networks - WildFire integration: Wildfire integration allows you to programmatically query analysis jobs on Wildfire and retrieve historical results through a simple XML API interface.
- Understanding the Qualys Vulnerability Integration: Qualys Cloud Platform is used in Vulnerability Response.
- Splunk - Incident Enrichment integration: searches your logs and adds relevant sighting information to your security incidents.
- VirusTotal integration: used in Threat Intelligence. To use this lookup source, you must activate the VirusTotal Integration plugin.
- WhoisXML API integration setup: provides consistent, well-structured data from a Whois lookup. Keeps accurate Whois data accessible 24/7.

Activate and configure third-party integrations

You can activate the plugins for third-party integrations and configure them for use from the same screen.

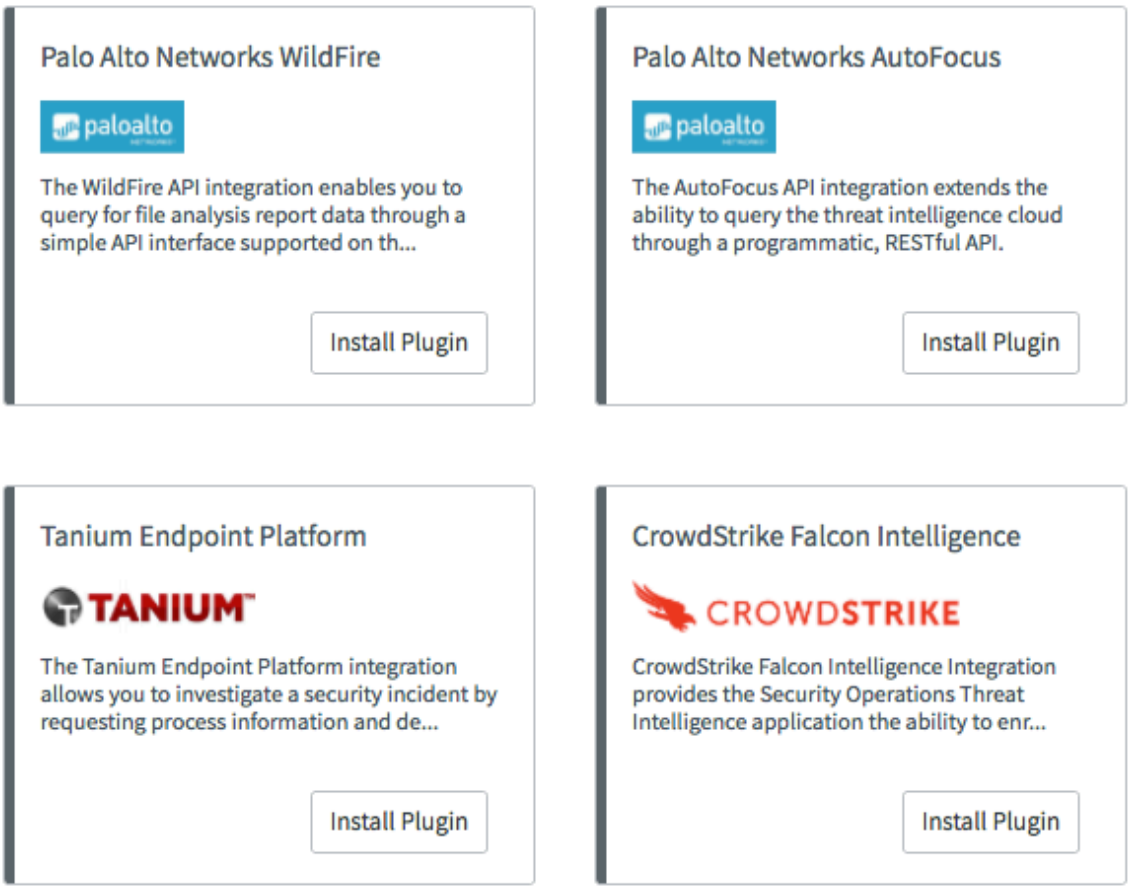
Before you begin

Role required: sn_sec_cmn.admin

Procedure

1. Navigate to **All** > **Security Operations** > **Integration Configuration**.
   The available security integrations appear as a series of cards, similar to the following group of cards. You can point to any card to get a description of the integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



2. To install the plugin for a given integration, click **Install Plugin**.

   a. On the System Plugin form, review the plugin details and click the **Activate/Upgrade** related link.

   b. Click **Activate**.
   When the activation is complete, the Security Integration screen reopens and the button for the integration you activated is labeled **Configure**.

3. Click **Configure**.

   Note: If you are configuring the Qualys Vulnerability Integration, see Installation of Vulnerability Response and supported applications.

4. Enter the **API Key**.
5. Click **Submit**.

Create an integration

You can create an integration and add the associated integration card to the Security Integrations screen. This procedure is intended for partners who create third-party integrations.

Before you begin

Role required: sn_sec_cmn.admin

Audience: Partners who create third-party integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the navigation filter, type sn_sec_core_integration_item.list and press the **Enter** key.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Field	Description
Name	The name of the integration.
Plugin ID	The plugin that must be activated to use the integration.
Order	Indicates the order that this integration card appears.
Banner Text	Click the link, select an image or logo to appear in the integration card, and click **OK**.
Installed	Read-only field that indicates whether the plugin has already been installed.
Configurable	Indicates whether you can configure the integration.
Categories	Used for filtering the integration cards.
Short description	A description of the integration that appears in the tooltip hint for the card.
Description	A longer description of the integration.

4. Right-click the form header and select **Save**.
   The **Integration and Configurations** related list appears. You can use this related list to define configuration options for the integration. These options appear when you click the **Configuration** button on the associated integration card.
5. Click **New**.
6. Fill in the fields on the form, as appropriate.

Field	Description
Label	The name of the integration item.
Name	The plugin that must be activated to use the integration.
Integration	Displays the integration for which you are defining integration items
Order	Indicates the order in which this integration item appears.
Type	From the list, select the type of field: ○ String ○ Integer ○ Decimal ○ Date ○ Boolean ○ Password ○ IPv4

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	○ IPv6 ○ URL
Value	Enter the value associated with the **Type** selected. If a value that is invalid for the selected **Type** is entered, no records are retrieved when the integration is run. For example, if you select the URL type and enter a value of 12.32.23.10, no records are retrieved.

7. Click **Submit**.

Tips for writing integrations

Avoid some of the pitfalls you can encounter when writing your own integrations by following these guidelines.

Use ServiceNow platform functionality whenever possible

Mostly, the integration capabilities built into Security Operations applications (Security Incident Response, Threat Intelligence, and Vulnerability Response) are intended to enhance or streamline existing ServiceNow platform integration functionality. When writing integrations, always make sure to use platform functionality when it exists. Here are some common ServiceNow functionalities that can be used rather than "rolling-your-own."

- Outbound web services – for most interactions with third-party systems, communication are through web services. In those cases, utilize platform outbound web services (REST and SOAP are supported).
- A data sources/import sets/transform map – for processing data and inserting into ServiceNow tables, the preferred mechanism is to use data sources and associated components.

Use Security Operations integration frameworks whenever possible

Because Security Operations integration mechanisms have solved many common problems, it is not necessary to reimplement basic functionalities for every integration. For example, the vulnerability data and threat source frameworks support handling multiple pages and passing that data to data sources/transforms/import sets. Similarly, the scan or lookup source framework provides configurable rate limiting functionality. As a rule, when implementing a feature or set of features, check to see if the existing Security Operations integration framework covers your use case. If so, use that framework.

Extend the existing Security Operations integration frameworks as needed

Most of the tables and scripts used by Security Operations integration frameworks were intended to be extended to suit future needs. If a use case is encountered while you are writing an integration, extend an integration table or script to better suit that use case.

Provide feedback to ServiceNow for issues encountered during integration

As an integration is being developed or tested, be sure to provide feedback when issues are encountered. Even if a workaround is required, Customer Service and Support personnel can provide an improvement in future releases that could alleviate the issue for future integrations.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Test under reasonable load

A common issue with integrations is that they are not equipped to handle realistic loads. Because each integration is a scoped application, there are more limitations imposed by the platform to ensure system stability. These limitations may result in long running jobs or API calls being terminated. You can ensure that long running processes or processes that process lots of data are handled gracefully by reducing the time each call or process takes (usually by providing a means of paginating API requests or chunking large sets of data).

Integration troubleshooting

These troubleshooting suggestions can help you resolve common issues you can encounter when setting up or running integrations.

Replace an untrusted or expired third-party SSL certificate

When an SSL connection is required in an integration, there are circumstances when the certificate provided by the third-party vendor is either not yet trusted in ServiceNow or has expired. You can replace it or add a new certificate.

Before you begin

Role required: sn_ti.write

Procedure

1. Acquire the SSL certificate from the third-party vendor.
   For example, you can import an X.509 Certificate (PEM) from an SSL endpoint in the Firefox browser, as follows.

   a. Enter the endpoint URL into the browser address bar.
      For example: `https://<3rdparty>/`.

   b. Click the lock icon in the address line.

   c. Click **More Information** and click the **Security** tab.

   d. Click **View Certificate** and click the **Detail** tab.

   e. Click **Export** to save the PEM into your local file system.

   f. Open the saved file in any text editor tool and copy the content into the clipboard.
      It must begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.

2. Navigate to **System Definition** > **Certificates**.
3. Click **New** and create a new record for the integration.
4. In **PEM Certificate**, paste in the certificate you downloaded and copied into the clipboard earlier.
5. Click **Save**.
   The other fields in the record are generated automatically.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrations Capabilities framework 2.0

The new Integration Capabilities Framework 2.0 has been redesigned to enable implementation of integrations in a simple and consistent manner. This ensures a consistent experience for similar types of integrations (for example: observable reputation lookup).

The new framework has capabilities implemented using Flows.

Benefits from the enhanced framework implementation include:

- The capability flows that include only business level components without any implementation specific logic.
- The capability flows now accept a broad array of inputs and formats for maximum flexibility (For example, observable references, CI references, tasks, any table or sys_id combinations).
- Rate limiting or throttling on integration executions are now easy to configure (removing the need to do this using custom code or changes to implementation workflows).
- Enhanced auditing and execution tracking capabilities now enable better reporting and easier troubleshooting.
- Robust error handling functions are built into the capability flows to avoid duplicating implementation routines.
- Ability to configure conditional triggering of the capabilities or the integrations. This provides flexibility to automatically launch automations based on incident category.
- A default filter condition has been introduced on all capabilities to filter allow listed observables before inputs are provided to the integrations.

Note: This new capability framework does not upgrade the current capability framework. Both frameworks can work in parallel. For instructions on how to leverage the new capability framework, see Using the new Capability Framework with an installed integration and Using the new Capability Framework with a Flow.

For more information on how to migrate from workflows to flows, using the Integration Capabilities Framework 2.0, see the KB1644337 article in the Now Support Knowledge Base.

Supported integrations and components

The Security Incident Response plugin includes all the capability flows listed in Integration Capabilities Framework 2.0, and standard high-level filters that you can enable or disable depending on your requirement.

Note: If you want to use the new Capability Integration Framework with the New York release, you must install the ServiceNow IntegrationHub Starter Pack Installer plugin. Contact Customer Support for assistance with the installation.

Supported application versions

Starting with Security Incident Response 10.0, the following integrations are supported:

Application	Minimum version required
Security Operations Hybrid Analysis Integration	10.0.0
Security Operations PhishTank Integration	10.0.0

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application	Minimum version required
Security Operations ThreatCrowd Integration	10.0.0
Security Operations CrowdStrike Intelligence Integration	10.0.0
Security Operations 'Have I been pwned?' Integration	10.0.0
Security Operations Metadefender Integration	10.0.0
Security Operations Recorded Future Integration	10.0.0
Security Operations VirusTotal Integration	10.0.0
Security Operations Reverse Whois Integration	10.0.0

Starting with Security Incident Response 10.4, the following integrations are supported:

Application	Minimum version required
Security Operations RiskIQ Integration	10.0.0
Security Operations Shodan Integration	10.0.0
Security Operations Whois Integration	10.0.0
Security Operations Carbon Black Integration	10.3.1
Security Operations Splunk Search Integration	10.3.0
Security Operations ArcSight Logger Integration	10.3.0
Security Operations McAfee ESM Integration	10.3.0
Security Operations Elasticsearch Integration	10.3.0
Security Operations IBM QRadar Integration	10.3.1
Security Operations CrowdStrike Falcon Host	10.3.0

Components included

The new Capability Integration Framework includes the following components:

- **Capabilities**: All of the following capabilities that exist in the product today as workflows have been redesigned using Flows:
  - **Block Request**: Provides a way to block observables associated with a security incident on a firewall, web proxy, or some other control point. This capability is used during incident response investigations to contain an identified threat.
  - **Email Search and Delete**: Provides a way to search an email server during a security investigation and if necessary, delete emails from the server.
  - **Enrich Configuration Item**: Provides a general way to enrich configuration items with additional information from a variety of sources. This capability is used during incident response investigations to enrich data associated with a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - **Enrich Observable**: Provides a general way to enrich observables with additional information from a variety of sources. This capability is used during incident response investigations to contain an identified threat.
  - **Event Ingestion**: Provides a general way to create a security incident by mapping events from an integration source to a security incident.
  - **Get Network Statistics**: Retrieves a list of active network connections from an endpoint or host. This capability is used for incident enrichment during investigations.
  - **Get Running Processes**: Retrieves a list of running processes from an endpoint or host. This capability is used for incident enrichment during investigations.
  - **Isolate Host**: Provides a way to isolate an endpoint or a host associated with a security incident. Isolate host is executed against a configuration item (CI).
  - **Publish to Watchlist**: Provides a way to add observables associated with a security incident to a watchlist that monitors for security events and generates alerts. This capability is used as part of incident response during investigations.
  - **Sightings Search**: Searches various SIEMs or other log stores for instances of observables. This capability is used to determine the presence of malicious IoCs in your environment.
  - **Threat Lookup**: Performs threat intelligence lookups to determine whether a certain observable is associated with a known security threat. This capability is used as part of incident response during investigations.
- **New tables**:
  - sn_sec_cmn_capability: Capability and flow that implements the capability.
  - sn_sec_cmn_capability_implementation: The actual implementation flow that provides the services of the capability.
  - sn_sec_cmn_capability_execution: The execution record for a capability at runtime.
  - sn_sec_cmn_capability_implementation_execution: The execution record for a capability implementation at runtime.
  - sn_sec_cmn_filter_condition: The filter conditions that can be applied at runtime to the capability or a capability implementation.
- **Include script**: CapabilityProcessor: Handles all the processing code for the framework.
- **Rate limit**: Capability Max Concurrent Req Per Period: Defines how many integrations can be executed in parallel.
- **Scheduled job process capability implementation**: Runs every 15 seconds and can be disabled in the Security Administration Properties page (**Security Incident** > **Administration** > **Properties**).
  - Enables or Disables the scheduled job, Process Capability Implementations: This job automatically schedules and manages capability implementation execution flows.
  - Enables or Disables Automated Lookups or Enrichments: Setting that activates or deactivates the scheduled job that performs automated threat lookup or enrichment of observables when observables are added to security incidents in the current capability framework.
  - Enables or Disables the scheduled job, Lookup Security Incident Observables: This job automatically schedules a Threat Lookup or Enrich Observables job when observables are added to a security incident.

Configurations in the new Capability Framework

This section describes the configurations available in the new framework.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

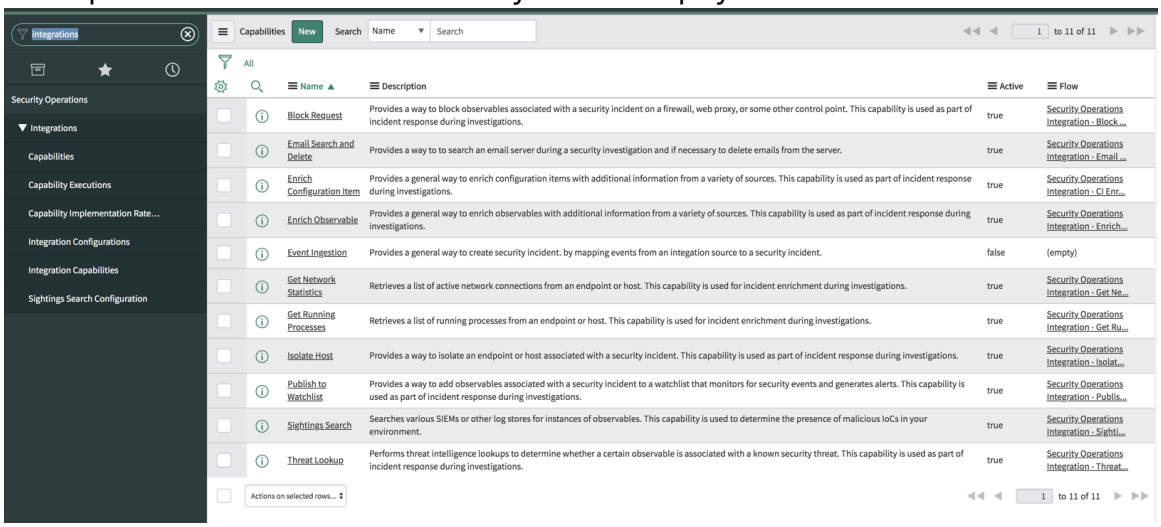
Role required: sn_si.admin, flow_designer, action_designer

Procedure

1. Navigate to **All** > **Security Operations** > **Integrations** > **Capabilities**.

   Note: Version 10.4: Starting with Security Incident Response 10.4, the menu name **Capabilities** has been changed to **Integration Capabilities (Flows)**.

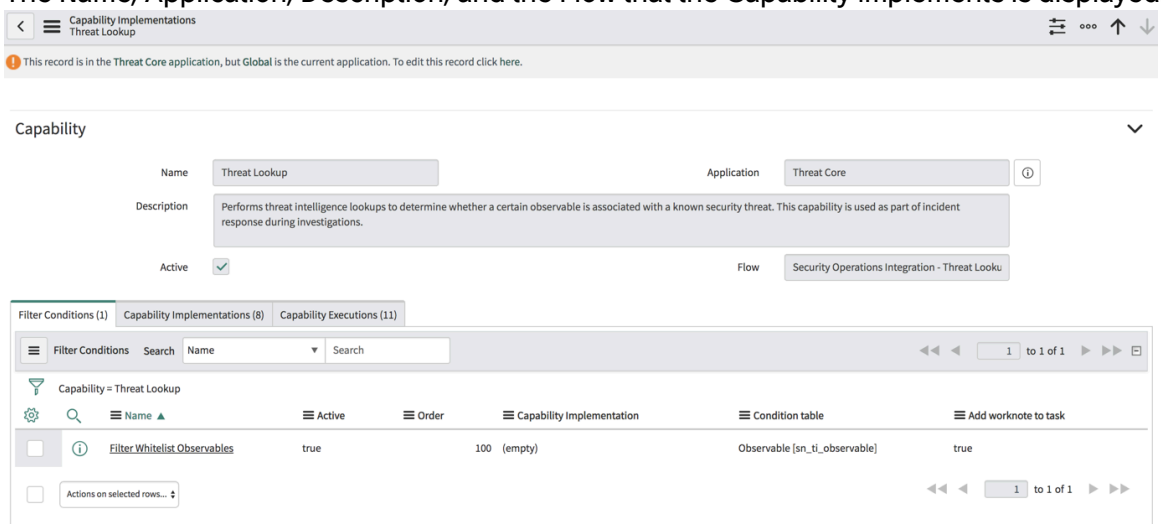
2. The capabilities available with the base system are displayed.



   Note:

   These are the capabilities provided with the base system. You can use the capabilities, or you can customize them as required. The following steps describe how to configure a capability and the integrations implemented for the capability.

3. Click the link in the Name column to configure a capability.
   The Name, Application, Description, and the Flow that the Capability implements is displayed.

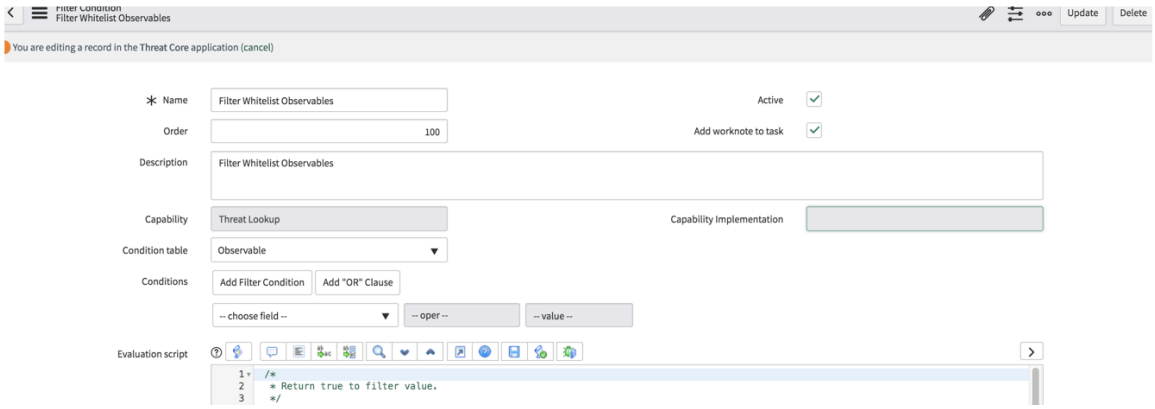


4. Select the **Active** check box to activate the capability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Filter conditions at the capability level**: When an integration capability implements a flow, the filter conditions associated with the flow will be executed before the capability flow is launched. For example, the Threat Lookup capability includes the Filter Allowlisted Observables condition as shown above. Click on the Name link to edit the filter condition.

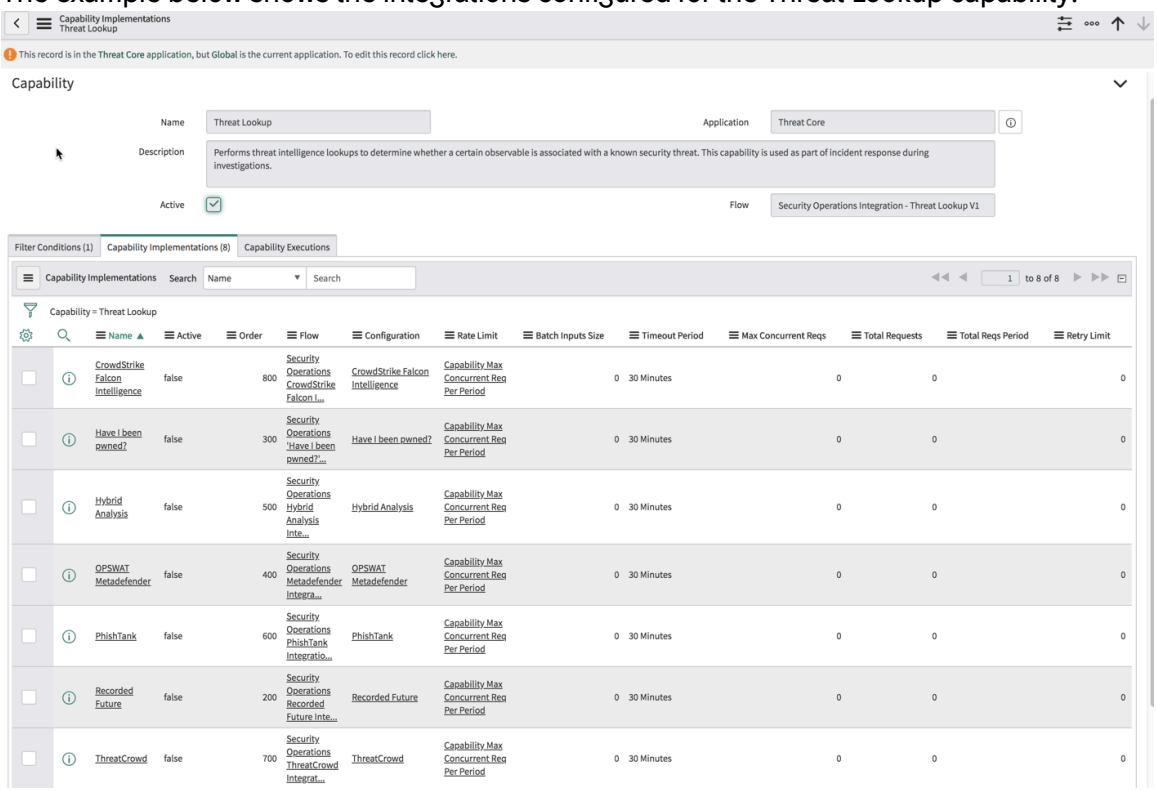
  Note: Select the **Add worknote to task** checkbox to add worknotes to include information on the filter conditions used.



You can either define filter conditions or a script, or a combination of both. In the above example, a script is used to define the filter conditions. When the capability flow is executed, the script searches for allowlisted observables and removes them from the table.

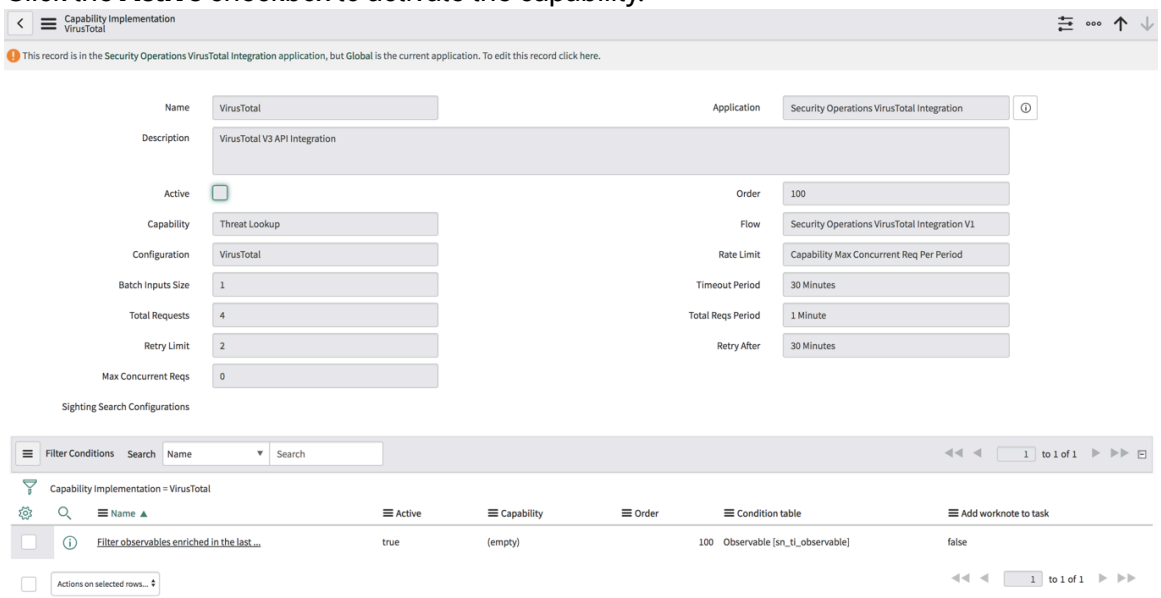
  Note: The filter conditions set here are applicable to all active integrations defined in the **Capability Implementations** tab.

- **Capability implementations**: Click the **Capability Implementations** tab. The implementations (integrations) that have been configured for the capability are displayed. The example below shows the integrations configured for the Threat Lookup capability:



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click the Name link to view the Capability Implementation.
   The Name, Application, Description, and the Flow that the capability implements is displayed.
6. Click the **Active** checkbox to activate the capability.



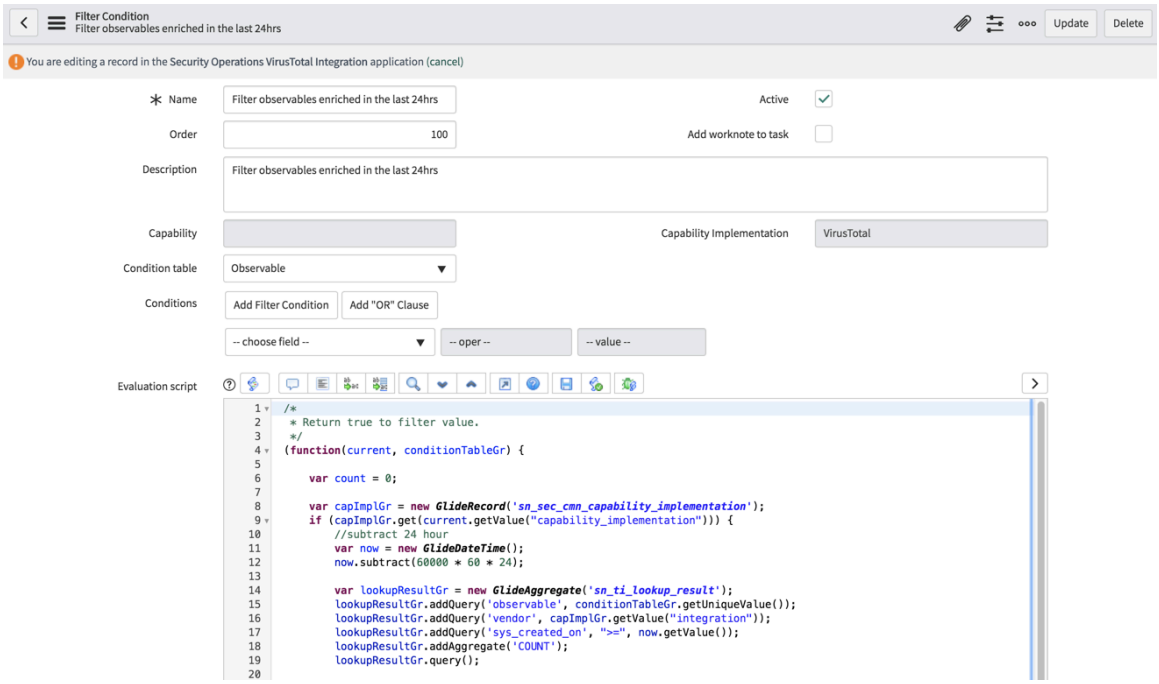
You can specify the following details:

Field Name	Description
Active	Select this check box to enable disable this integration. **Note:** If you configure this integration using the integration tile in the **Security Operations** > **Integrations** > **Integrations Configurations**page, this flag is automatically set to **Active**.
Order	Indicates the order in which the integrations are executed.
Capability	The capability implemented by this integration.
Flow	The subflow that implements the capability.
Configuration	The integration configuration for this capability. **Note:** This is initially set to the default configuration provided with the base system. When an integration is configuring using the integration tile in the **Integration Configurations** page, this value is automatically reset to the new configuration created.
Rate Limit	Indicates the number of integrations that can be executed at run-time (in parallel or per unit of time).
Batch Inputs Size	The batch input size for each execution. For example, for a Sighting Search integration you may want to group the observables into batches of 50 so that the queries generated do not become too large. 0 indicates that there is no limit.
Timeout Period	The maximum duration before the capability implementation flow is cancelled. 0 indicates that there is no timeout period.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field Name	Description
Total Requests	The total number of implementation execution requests. This field in conjunction with the Total Reqs Period field, can be used to limit the number of requests to the service. For example, you can limit the number to 4 requests per minute.
Total Reqs Period	The total number of execution requests allowed per period.
Retry Limit	The number of retries allowed for a failed execution request. This limit will be applicable if the **Retry** flag is set in your integration to retry an execution request when a condition is met. For example, a retry request is made when you have exceeded your license limit for that service for a time period or the service is down.
Retry After	The period after which an attempt is made to retry a failed execution request.
Max Concurrent Reqs	The maximum number of concurrent implementation execution requests. 0 indicates no limit.
Sighting Search Configurations	The default sighting search queries that can be executed.

Click the Name link in the Filter Conditions section to configure the conditions defined for the implementation. Add or delete filter conditions, modify the script if required and update the record.



Using the new Capability Framework with an installed integration

This section describes how to use the new framework for an existing integration.

Use the steps below to enable an already installed and configured integration (see supported list of Integrations in Supported integrations and components) to use the new capability framework.

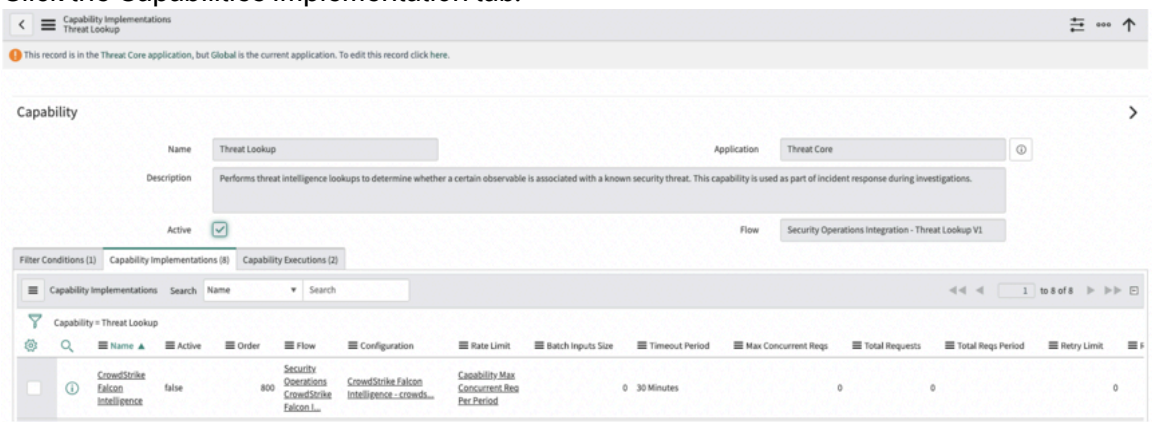
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Integration Capability Framework 2.0 available with Security Incident Response 10.0.2 supports implementations for the **Threat Lookup** and **Enrich Observable** capabilities. Implementations for other capabilities will be made available in a future release.

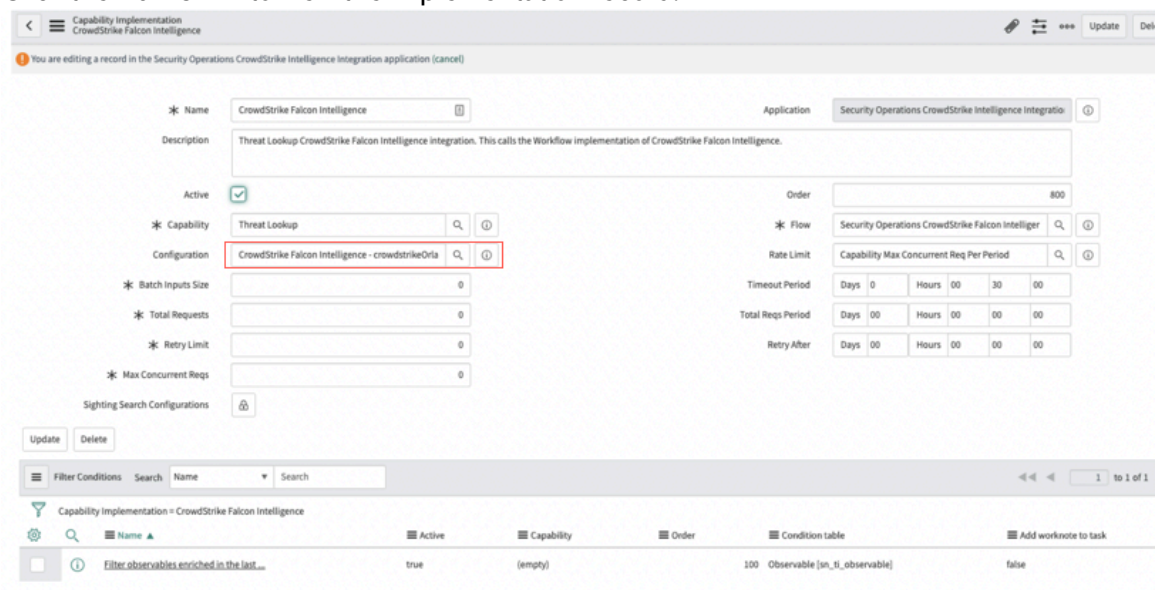
Before you begin

- Role required: sn_si.admin
- Security Incident Response 10.0.2

1. Navigate to **Security Operations** > **Integrations** > **Capabilities**.
2. Click on **Threat Lookup** capability.
3. Click the Capabilities Implementation tab.

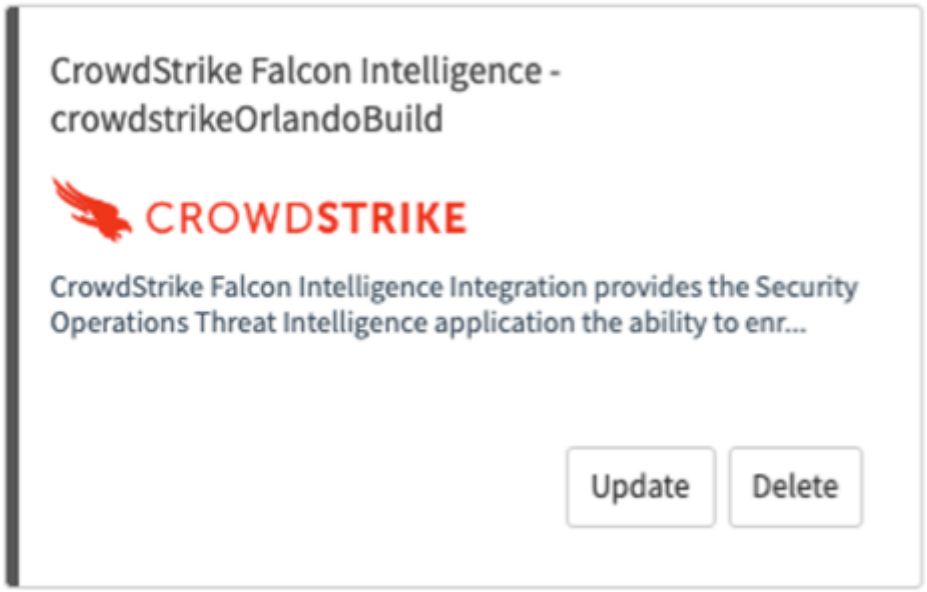


4. 4. View the Capability Implementation record for the integration of interest (example: Crowdstrike Falcon Intelligence). The **Active** column should have the value as **False**.
5. Click the **Name** link to view the implementation record.



6. Select the **Active** check box.
7. Ensure the implementation record is pointing to the right configuration record (the tile name for the integration in **Integration Configurations** > **Show Configurations (Yes)**).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



8. The implementation is enabled for use with the new framework.

Note: All supported Integrations when installed with Security Incident Response 10.0.2 will automatically be enabled under the new Integration Capability framework.

Using the new Capability Framework with a Flow

Use the steps below to create a flow and call the subflow provided by the new capability framework.

Before you begin

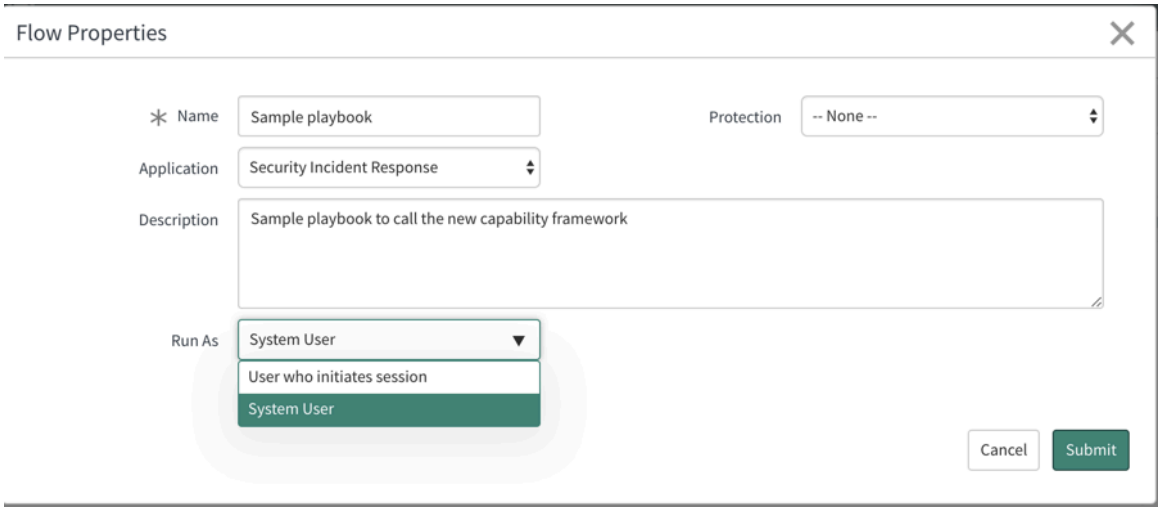
- Role required: sn_si.admin, flow_designer, action_designer
- Install one of the supported integrations (see Supported integrations and components)

The steps below describe how to create a sample flow and call one of the subflows provided with the new capability framework.

Procedure

1. Navigate to **All** > **Flow Designer** > **Designer**.
2. Click **New** to create a new flow and provide the necessary information for the properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

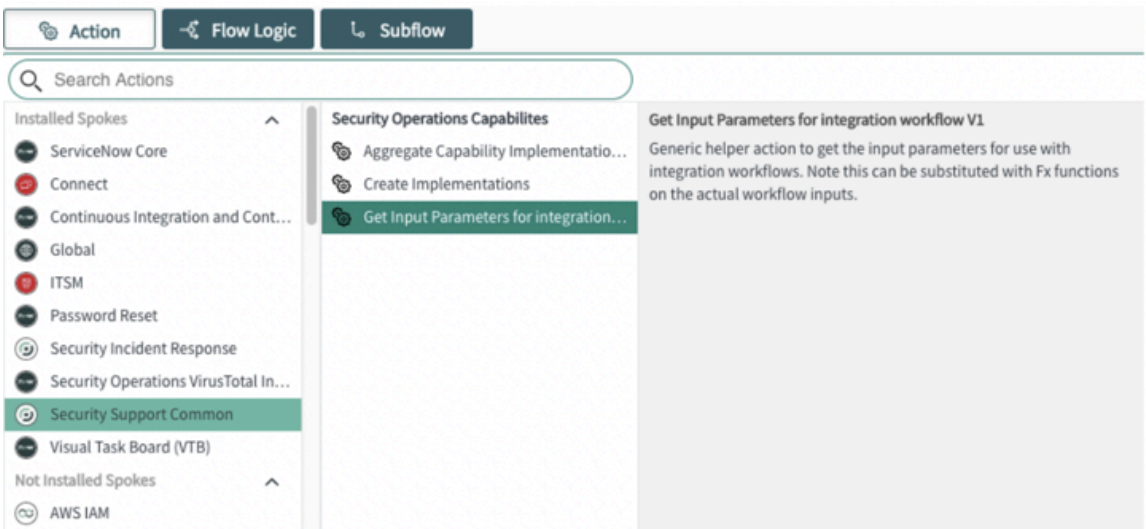


Note: Select **System User** in the Run As choice list as shown in the above image.

3. Select a Trigger condition for the flow (a common trigger is the creation of a security incident record for a certain incident category).



4. In step 1 of the flow, select an action to get inputs from the security incident (for example, observables).
   You can select an action from the actions provided with the base system with the Security Support Common Spoke.

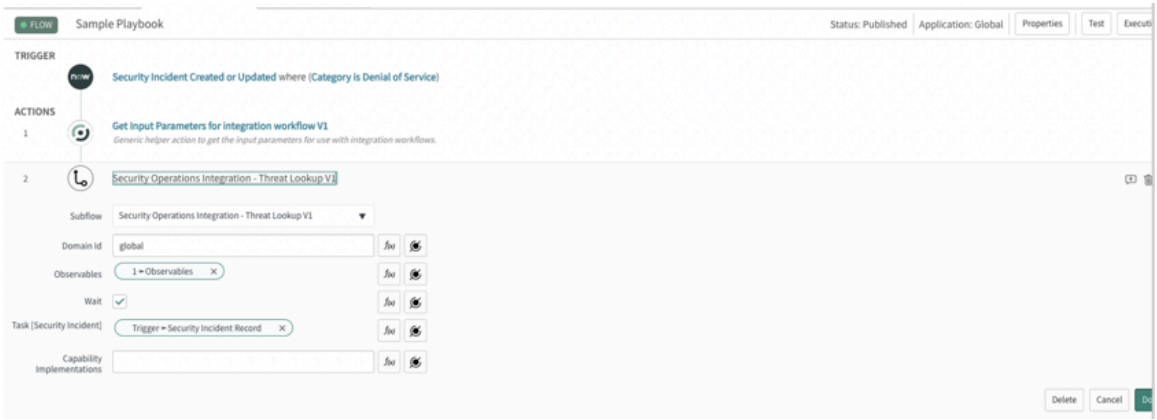


5. In step 2, select a subflow (for example, Threat Lookup).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Configure the subflow you have selected as shown below:



7. Save and publish the flow.

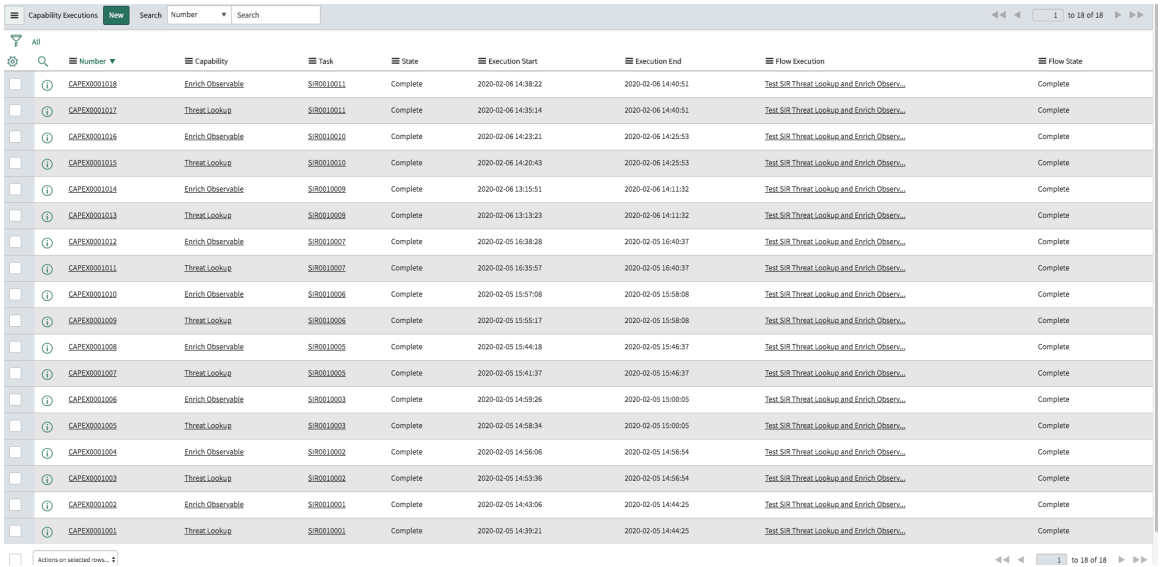
Troubleshooting Integration Capability flows

The Capability Executions option provides detailed information on each capability that has been executed.

Note: Completed executions are archived after 30 days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Navigate to **Security Operations** > **Integrations** > **Capability Executions.**.



2. Click on the Capability Executions link to view additional details.

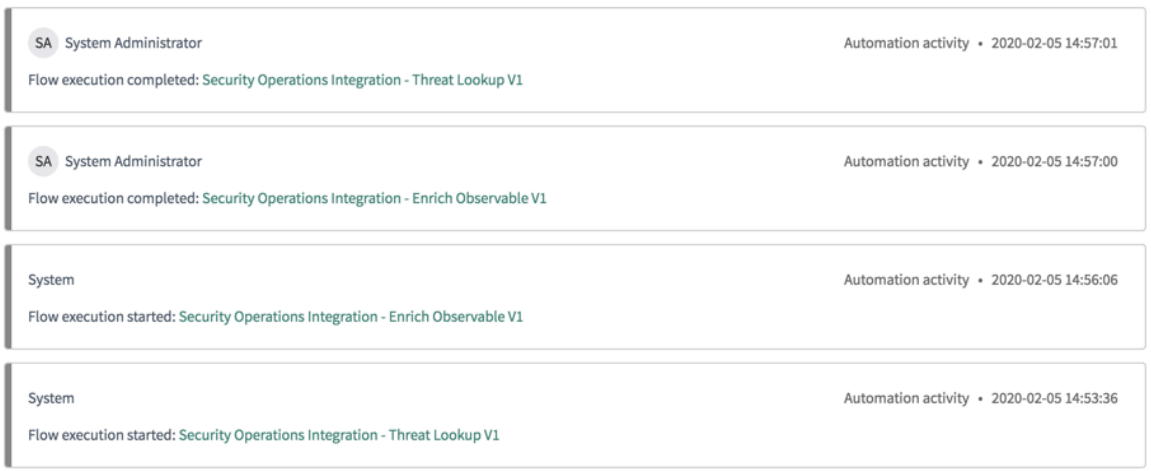
Security Incident Record Worknotes

When observables have been added to a security incident and the trigger condition for the flow is met, the Threat Lookup and Enrich Observable subflows are initiated and the following work notes are added to the security incident:

- Flow execution started: Security Operations Integration - Enrich Observable V1
- Flow execution completed: Security Operations Integration - Enrich Observable V1
- Flow execution started: Security Operations Integration – Threat Lookup V1
- Flow execution completed: Security Operations Integration – Threat Lookup V1

To view these worknotes, login as a user with the *sn_si.admin* or *sn_si.analyst*, and *flow_designer*, and *action_designer* roles.

Navigate to the security incident record page and click on these worknotes to view the flow execution details.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

REST APIs for third-party integration with Security Operations

The Security Operations base system includes a series of scripted REST APIs that allow customers and partners to easily integrate with an existing Security Operations deployment. The APIs allow you to gather data from outside of your system (for example, a Python script is used to receive data from VirusTotal) and send it back to your instance.

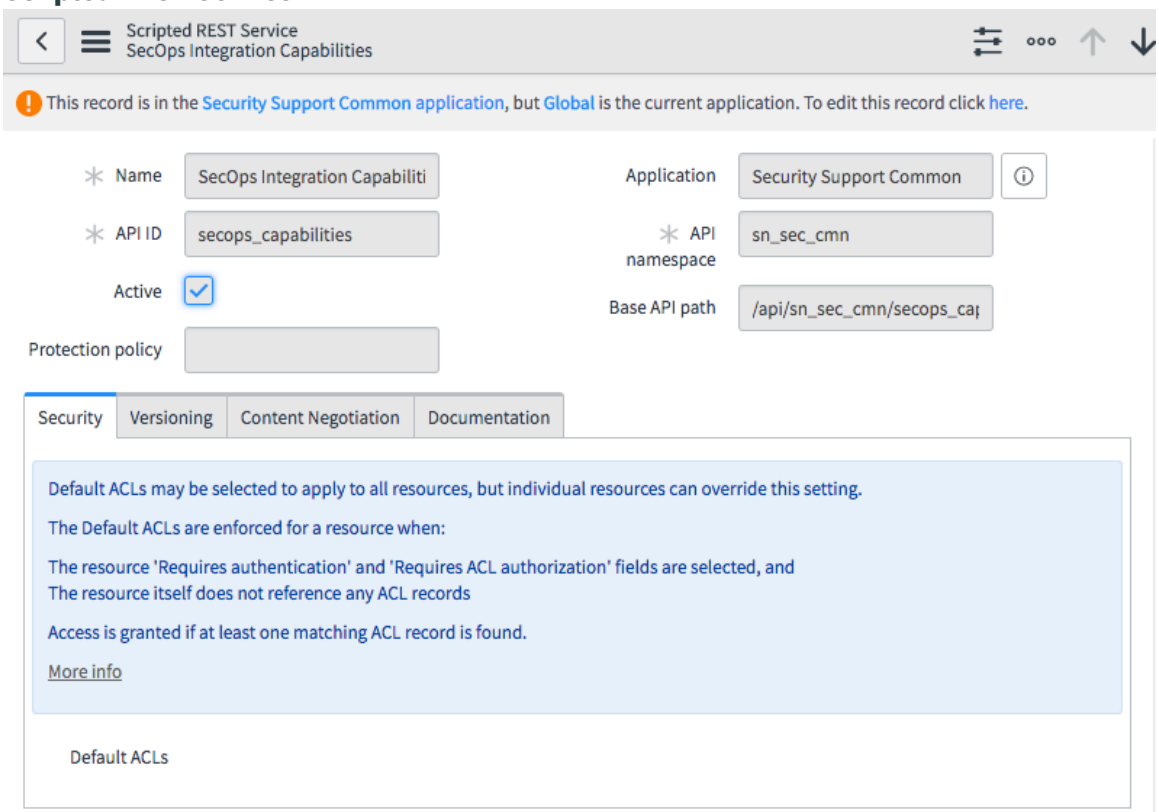
Scripts written in almost any language (Python, for example) can be used with the APIs to perform customer-specific processes. The scripts must be written in a language able to make an outside-facing HTTP Post call. For example, if you have a Java application, you must use a library, such as the `java.net.HttpUrlConnection` package, to construct an HTTP call and pass in a JSON string as Body for the message.

The API is solely used to add data that was gathered outside of our system. For example, if you entered VT python script and received data from VT, you could send that data back to the SN instance.

Authentication

All operations within the API definitions use platform authentication provided by the Scripted REST APIs operation feature. To access, navigate to **System Web Services** > **Scripted Web Services** > **Scripted REST APIs** and locate the **SecOps Integration Capabilities** API.

Scripted REST Service



The user and the user's domain are readily available within the context of the API. Records can be tied to a user, an audit path to be established, and domain separation accomplished. Also, since you are authenticated as a specific user, you can use Using GlideRecordSecure to prevent any unauthorized access to data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Authorization

To protect the record creation process from users outside of the Security Operations application, you must have the sn_sec_cmn.api_write role. Only users with this role can access the APIs.

Configuration request parameters

The following request parameters are available.

Name	Default	Description
ignore_mandatory_fields	false	If set to true, the record persists even if mandatory fields are not filled in.
include_wrap	false	If set to true, the response includes the instance-provided standard wrapper for Scripted REST APIs.
simple_response	false	If set to true, the response includes only whether the operation was successful.

Error responses

The following error responses may occur.

Error message	When does it occur?	Solution
Insufficient access	User does not have the sn_sec_cmn.api_write role.	Add the role to the user.
Invalid post body	Request body is empty or an empty object.	Conform to the API definition.
No fields supplied	Data fields provided to persist are empty.	Conform to the API definition.
Mandatory fields missing: x,y,z	Mandatory fields are missing.	Conform to the table definition of the target table or set **ignore_mandatory_fields** to true.
Unable to persist record	Unable to persist parsed record.	GlideRecord insert() failed, further analysis is required.
Unknown error	Occurs if no known error path has been followed.	Further analysis is required.

CI enrichment use case

Using your third-party scripts, you can write to the Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result] table for CI enrichment. The enrichment records are based on existing capabilities that provide detailed information about a record from a third-party source.

Sample request and responses for the CI enrichment use case are shown here.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create-Request for CI enrichment

```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```

Create-Response for CI enrichment

```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```

Observable enrichment use case

Using your third-party scripts, you can write to the Observable Enrichment Result `[sn_ti_observable_enrichment_result]` table for observable enrichment. The enrichment records are based on existing capabilities that provide detailed information about a record from a third-party source.

Sample request and responses for the observable enrichment use case are shown here.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create-Request for observable enrichment

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

Create-Response for observable enrichment

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

Note: In addition to enriching existing records, you can also use Security Operations enrichment data mapping to add new records to tables by passing in an **enrichment_mapping_id** for an existing enrichment mapping and a corresponding **raw_data** string that can be parsed by the mapping process.

Threat lookup use case

Using your third-party scripts, you can write to the Threat Lookup Result [sn_ti_lookup_result] table for threat lookup results. The lookup records are based on existing capabilities that provide detailed information about a record from a third-party source.

Sample request and responses for the threat lookup use case are shown here.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create-Request for threat lookups


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create-Response for threat lookups


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Integration capabilities

The Integration Capabilities framework provides a consistent architecture to support interoperability with third-party integrations. This abstracted interface and data model insulates integrations from changes to the core application and ensures a consistent experience for similar types of integrations.

Each integration capability persists in the Integration Capability `[sn_sec_cmn_integration_capability]` table. Integration capability workflows cannot be executed alone, and require the launch of an implementation workflow. Any plugin that provides an implementation of the capability adds their implementation to the child table: Integration Capability Implementation `[sn_sec_cmn_integration_capability_implementation]`.

The implementation specifies the workflow to be executed, the related integration (plugin id), and the capability it implements. These workflows can be executed in parallel using the parallel workflow launcher; however, sequential execution is the default in the base system. If needed, you can change the order of execution.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration- Block Request capability

The Block Action capability blocks observables associated with a security incident on a firewall, web proxy, or other control point using implementation flows. This capability is used during incident response investigations to contain an identified threat.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Block Request capability has a flow, Security Operations Integration - Block Request Flow, that executes the request to block. This flow accepts a list of observables, finds any implementing capabilities, and executes the request based on the configured flow.

Note: If no implementations are available, capability actions are not displayed in product menus.

Run Block Request

Blocks communication with observables associated with a security incident.

Before you begin

Role required: sn_si.analyst

About this task

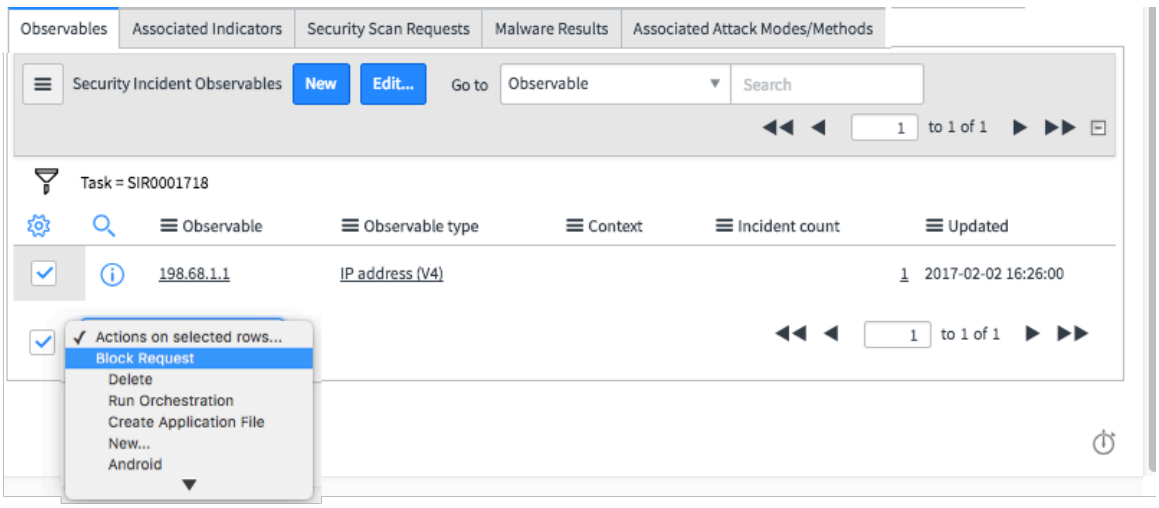
Note: If no implementations are available, capability actions are not displayed in product menus.

The **Security Operations Integration - Block Request** flow can be triggered from an observable form, or from the **Security Incident Observables** related list on a security incident.

This example shows a Block Request from a security incident.

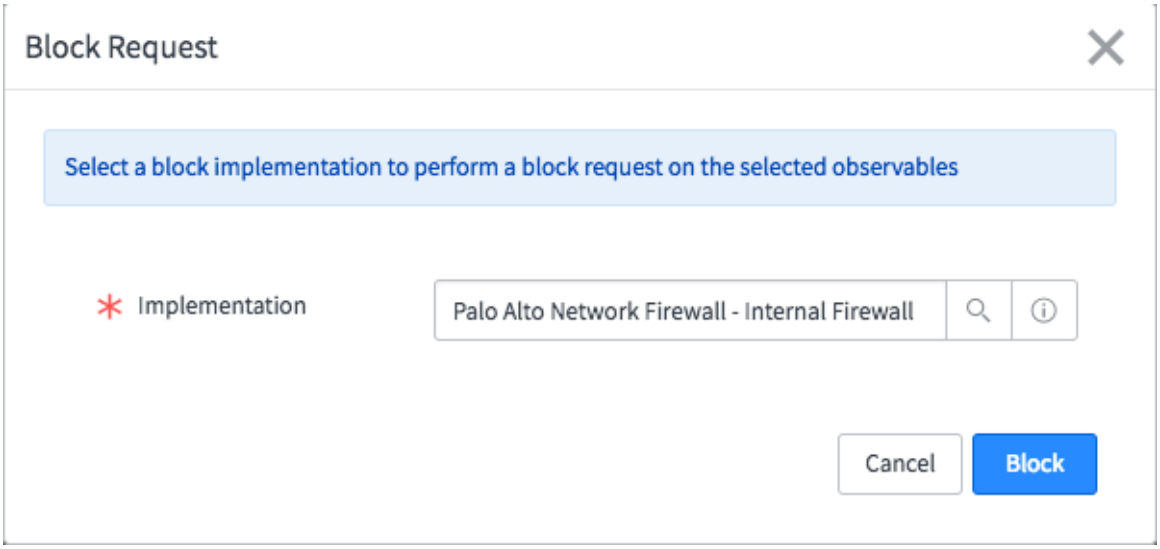
Procedure

1. Navigate to a security incident.
2. Select observables from the **Related List** tab.
3. Click **Block Request** in the **Actions on selected rows...** drop-down menu.

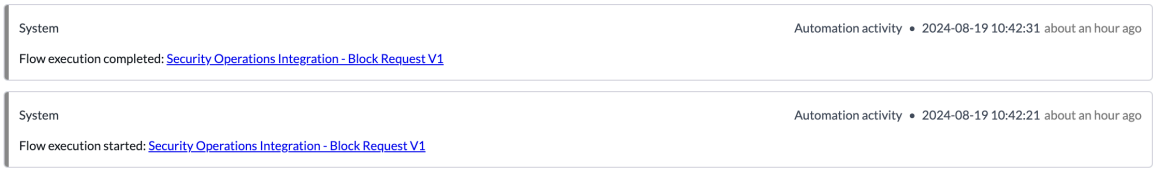


The dialog box appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Choose the implementation.
5. Click **Block**.
   The flow execution audit is displayed in the work notes section.



Security Operations Integration - Block Request Flow

The Security Operations Integration - Block Request flow is a high-level flow independent of integrations. It blocks observables associated with a security incident. Use it to fulfill an integration such as Palo Alto Networks - Firewall.

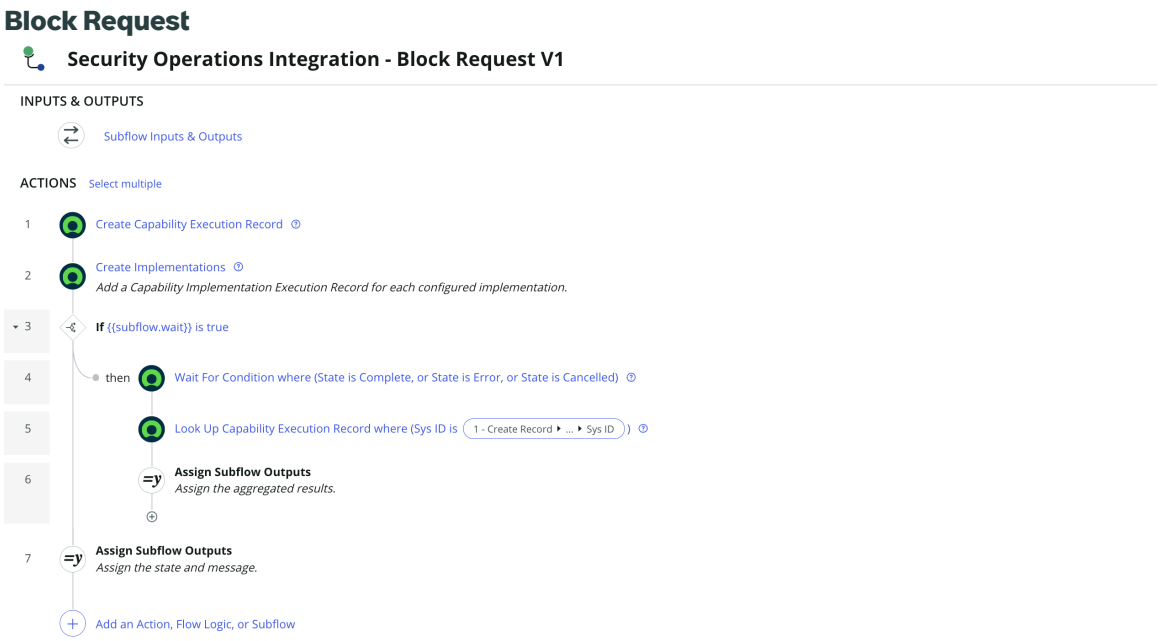
Before you begin

Role required: sn_si.analyst

About this task

The **Security Operations Integration - Block Request** flow can be triggered on an observable form, or from the **Security Incident Observables** related list on a security incident. On a list, it is in the drop-down action menu. On a form, it is a related link. Blocking a request is available only when you have an implementation installed for the block request capability.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Security Operations Integration- Email Search and Delete capability

The Email Search and Delete capability returns the number of threat emails from an email server search and, optionally, returns details for each email found. After the email search is completed, you can delete the emails.

The Email Search and Delete capability has one flow that executes the email search and delete processes.

Note: If no implementations are available, capability actions are not displayed in product menus. Additionally, if none of the **Email Search and Delete** capability implementations are active, the **Email Search** related link on a security incident is not displayed.

Security Operations Integration - Email Search and Delete flow

The Security Operations Integration - Email Search and Delete flow returns the number of threat emails from an email server search and, optionally, return details for each email found. After the email search is completed, you can delete the emails.

Before you begin

Role required: sn_si.analyst

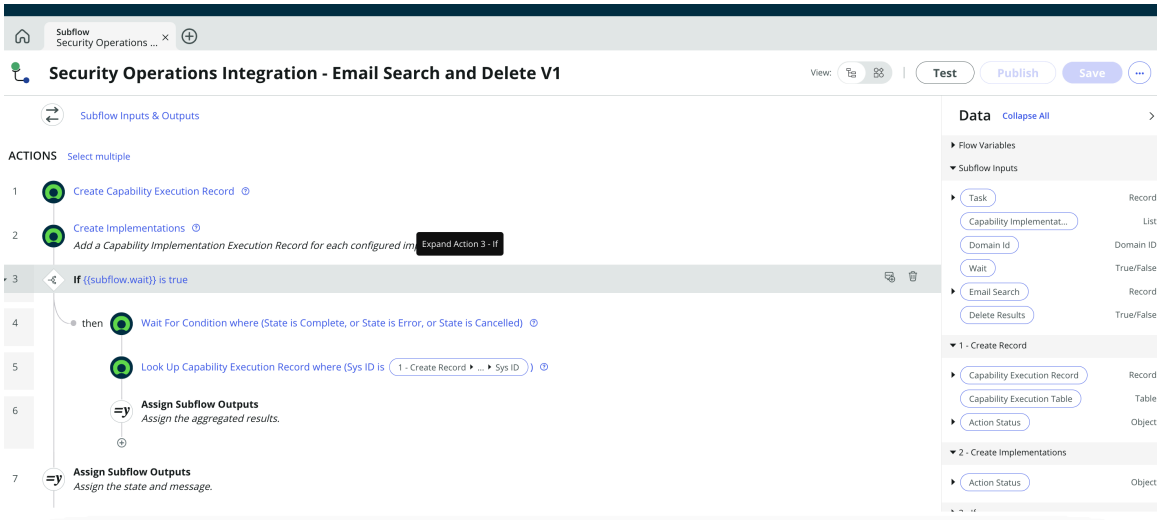
About this task

The search query can take some time to complete. After the count is received, approval is required to delete emails from an email server.

This flow is triggered by the **Delete from Email Server(s)** and **Search on Email Server(s)** buttons on the **Email Search** form in a security incident. For more information, see Search for and delete phishing emails.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Email Search and Delete



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

The flow process activities include:

Execution Tracking Begin (Mail Search) activity

The Execution Tracking - Begin (Mail Search) capability execution activity creates an execution tracking record and marks the record state as Started. This activity is used by all capability and implementation workflows to keep track of their state.

Results

Possible results for this activity are:

Results

Result	Description
Success	Execution tracking record has been created.
Failure	Could not create execution tracking record.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
capabilityId	System identifier of the Integration Capability being executed.
implementationId	System identifier of the integration capability implementation being executed.
taskId	System identifier for any task associated with the workflow.
workflowContextId	System identifier of the associated workflow context record. Supplied by the system.
workflowName	Name of the workflow. Supplied by the system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
parentCapabilityExcutionId	System identifier of the audit record that launched the implementation workflow. Only required for Integration Capability implementation workflows, such as Splunk, Elasticsearch.
emailsearchId	The sysid of the email search record in the Email Search [sn_sec_cmn_email_search] table.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
capabilityExecutionId	System identifier of the execution tracking record.

- Get Supported Security Capabilities activity
- Capability Execution Tracking- No Impls activity

Security Operations Integration- Enrich CI capability

The Enrich CI capability allows you to enrich data for configuration items associated with a security incident.

The **Enrich CI** capability has a workflow, Security Operations Integration - CI Enrichment flow. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform enrichment on the selected CIs, or you can perform the enrichment using all implementations.

Note: This enriched data is not the type of data you would want to store in your CMDB as it is forensic data that is specific to a given investigation--for example, performing a memdump from a CI. Instead, the data is stored in the Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result] table.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - CI Enrichment flow

The Security Operations Integration - CI Enrichment flow allows you to enrich data in configuration items (CI) associated with a security incident.

Before you begin

Role required: sn_si.analyst

About this task

This flow is triggered from Security Incident Response in two ways.

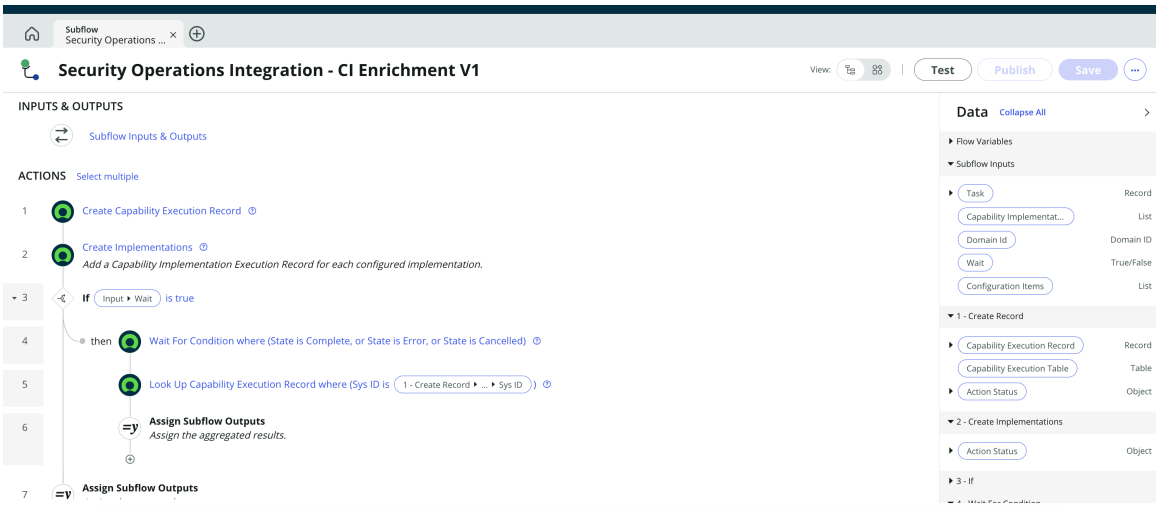
- by selecting one or more CIs from the **Configuration Items** tab (under the **Affected Items** related link) and selecting **Run CI enrichment** from the **Actions on selected rows** choice list.
- by opening a CI record and clicking the **Run CI enrichment** related link.

Either method then allows you to specify which implementations to be used to enrich the selected CIs. The associated implementation flows are executed to perform the enrichment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The base system does not include an implementation flow for this capability. To enrich CIs, you must create your own implementation flow.

CI Enrichment



Actions specific to this flow are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

The flow process actions include:

- Execution Tracking - Begin Flow Action
- Security Operations Integration - CI Enrichment flow
- Capability Execution Tracking- No Impls activity
- Get Supported Security Capabilities activity

Security Operations Integration- Enrich Observable capability

The Enrich Observable capability allows you to enrich observables with additional information from a variety of sources using implementation workflows. This capability is used during incident response investigations to contain an identified threat.

The Enrich Observable capability has a workflow, Security Operations Integration - Enrich Observable workflow. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform enrichment on the selected observables, or you can perform the enrichment using all implementations that match the supported observable types.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - Enrich Observable workflow

The Security Operations Integration - Enrich Observable sub flow allows you to enrich observables with additional information from a variety of sources using implementation flow designer.

Before you begin

Role required: sn_si.analyst

About this task

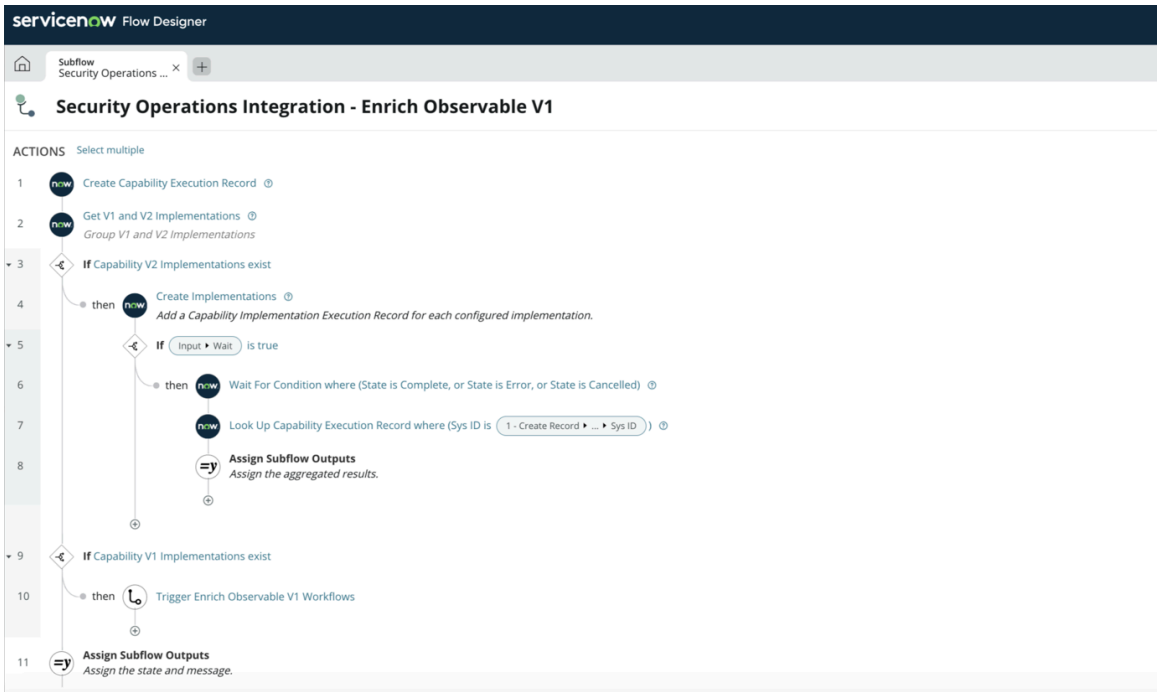
This workflow can be triggered from either Security Incident Response or Threat Intelligence in two ways.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- by selecting one or more observables from the Observables list and selecting **Run observable enrichment** from the **Actions on selected rows** choice list.
- by opening an observable record and clicking the **Run observable enrichment** related link.

Either method then allows you to specify which implementations to be used to enrich the selected observables. The associated implementation workflows are executed to perform the enrichment.

Enrich Observable



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Workflow process activities include:

- Capability Execution Tracking- No Impls activity
- Get Supported Security Capabilities activityCapability Execution Tracking- No Impls activity

Security Operations Integration- Get Network Statistics capability

The Get Network Statistics capability retrieves a list of active network connections from a host or endpoint. It can be used for incident enrichment during investigations. This capability is triggered automatically when a configuration item is added to a security incident.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integrations - Get Network Statistics workflow

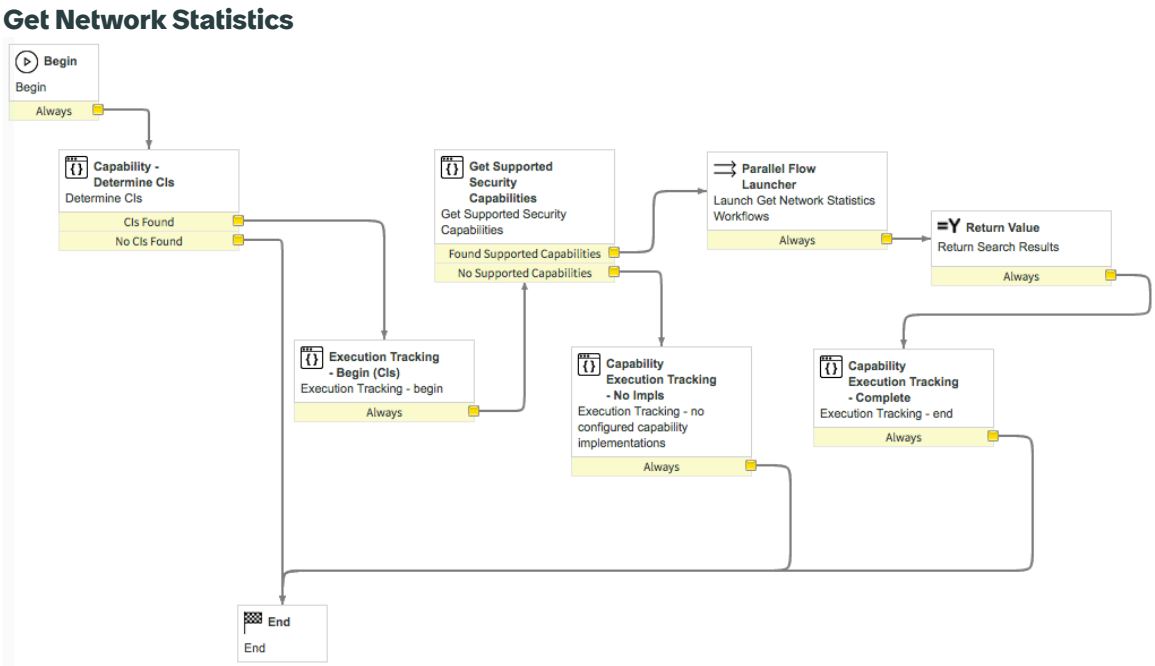
The Security Operations Integrations - Get Network Statistics workflow retrieves a list of active network connections from a host or endpoint.

Before you begin
Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

This workflow runs automatically when a configuration item is added to a security incident.



Activities specific to this workflow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Workflow activities include:

- Capability - Determine CIs activity
- .

Execution Tracking - Begin (CIs) Flow Action

The **Execution Tracking - Begin (CIs)** flow action starts the auditing process for a Security Operations Integration flow that operates on configuration items (CIs).

The **Execution Tracking - Begin (CIs)** flow action can be used with any CI flow to begin recording the progress of the flow in an audit.

Results

Possible results for this flow action are:

Results

Result	Description
Success	An audit record is created.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
capabilityId	System identifier of the Integration Capability being executed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
isImpl	Flag that specifies whether auditing is done for an Integration Capability flow or an Integration Capability implementation flow. Possible values are: • false - denotes auditing on an abstract Integration Capability flow such as Sightings Search. (default.) • true - denotes auditing on an Integration Capability implementation flow. For example, Splunk or Elasticsearch.
taskId	System identifier for any task associated with the flow.

ciList	One or more Configuration Items (CI)s to perform the desired action against in the following format:
	`["sysId", "sysId"]`
	or
	`"sysId"`
	Used as a flow input.

flowContextId	System identifier of the associated flow context record. Supplied by the system.
flowName	Name of the flow. Supplied by the system.
parentCapabilityExcutionId	System identifier of the audit record that launched the implementation flow. Only required for Integration Capability implementation flows such as Splunk, Elasticsearch.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
capabilityExecutionId	System identifier of the audit record.

Security Incident Response- Get Network Statistics Flow

The **Security Incident Response** > **Get Network Statistics** flow retrieves the network statistics for an affected Windows-based resource when added to a security incident in the **Analysis** state.

Before you begin

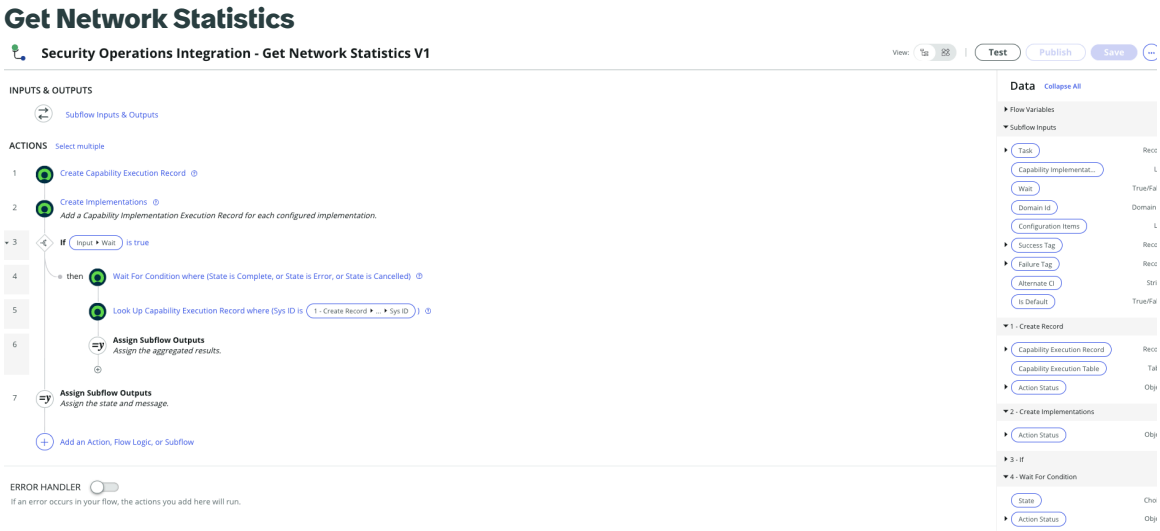
Role required: sn_si.analyst

About this task

For new security incidents that contain configuration items, the flow runs automatically when the state changes to **Analysis**.

Existing security incidents are automatically updated when you are in the **Analysis** state and you add a new configuration item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The flow process actions include:

Get Configuration Item FQDN Flow Action

Determine Shell Script by OS

If statement is executed by Powershell

Execution Tracking - Begin Flow Action

Get Network Statistics via netstat Flow Action

Capability Execution Tracking- Failure Flow Action

Create Enrichment Data records Flow Action

Capability Execution Tracking- Failure Flow Action - Returns enrichment ID.

Procedure

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click **Update**.
   Security Incident Response Orchestration provides network statistics information in the **Related Links** > **Security Incident Enrichments** tab. For more information see, Security Operations enrichment data mapping.

   Actions specific to this flow are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

Security Operations Integration- Get Running Processes capability

The Get Running Processes capability retrieves a list of running processes on a configuration item (CI) from a host or endpoint. This capability is used for incident enrichment during investigations.

The Get Running Processes capability has two implementation workflows:

- Security Operations Carbon Black Integration - Get Running Processes Flow
- Security Operations System Command Integration- Get Running Processes flow

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If no implementations are available, capability actions are not displayed in product menus.

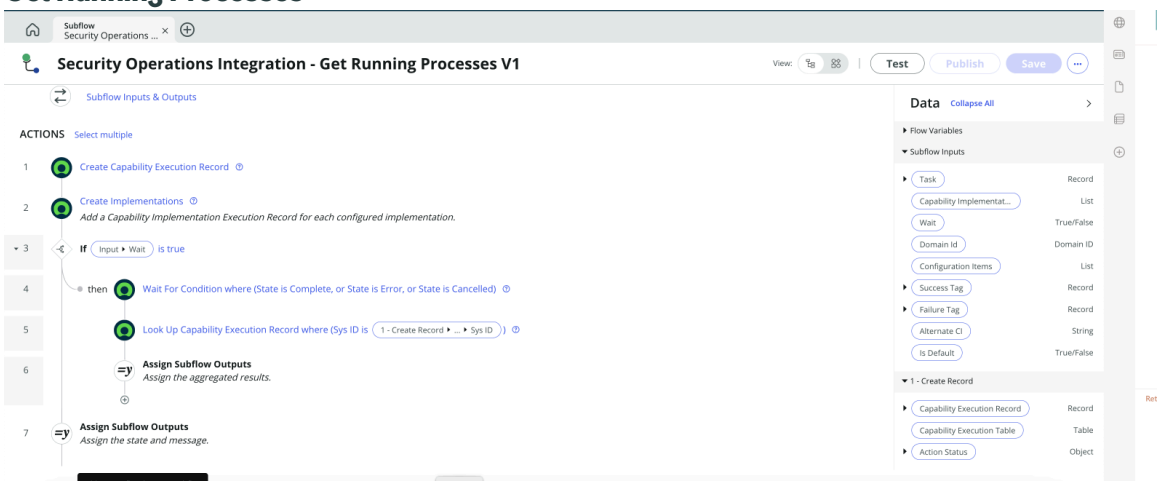
Activities specific to this workflow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Security Operations - Get Running Processes Flow

The Security Operations - Get Running Processes flow is a high-level flow independent of integrations. It retrieves a list of running processes on a configuration item (CI) from a host. Use it to fulfill an integration, such as Carbon Black, or for a Windows-based security incident.

Role required: sn_si.analyst

Get Running Processes



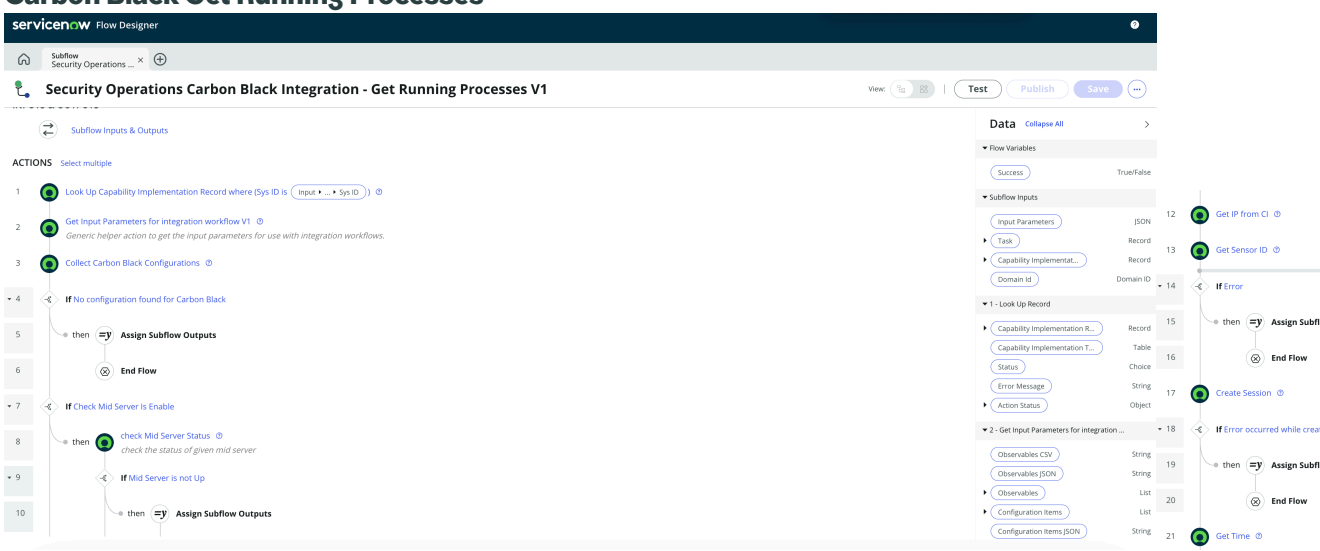
Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Security Operations Carbon Black Integration - Get Running Processes Flow

The Security Operations Carbon Black Integration - Get Running Processes is the implementation for the Carbon Black integration launched by the Security Operations Integration - Get Running Process flow.

Role required: sn_si.analyst

Carbon Black Get Running Processes



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Collect Carbon Black Configurations Flow Action

The Collect Carbon Black Configurations flow action gathers configuration information to use in the flow.

The Collect Carbon Black Configurations flow action gathers Carbon Black configuration information to use in the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Configuration succeeded.
Failure	An error occurred while attempting to verify the configuration. More error information is available in the flow action output error.

Input variables

There are no input variables for this flow action.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
endpoint_base	Base URL of the third-party integration API.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.
api_token	Third-party integration API key.

Check MID Server Status

Determines whether the MID Server identified in the **MID Server Host** field of the integration's configuration is up and running. If the field is set to **Any**, the flow action verifies that any MID Server is up and running.

The Check MID Server Status flow action can be used with any flow to check for the presence of a running MID Server within the flow.

Results

Possible results for this flow action are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Results

Result	Description
Success	Session status returned.
Failure	Session status error. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
capabilityExecutionId	The ID of the capability being executed.
flowName	The name of the flow being executed.
mid_server_host	The MID Server identified in the integration's configuration i

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
mid_server_live	Identifies whether the MID Server identified in the **MID Server Host** field of the integration's configuration is up and running. If the field is set to **Any**, the flow action verifies that any MID Server is up and running.

Get Sensor ID Flow Action

The Get Sensor ID flow action gathers sensor identifiers to use in the flow.

The Get Sensor ID flow action can be used with any flow to gather sensor information to use in the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Found sensor identifiers.
Failure	No sensors found. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
api_token	Carbon Black API key.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.
endpoint_base	Base URL of the Carbon Black API.
ci_ip_address	Configuration item IP address.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
Array Element type	API variables.
sensor_detail	Description of the Carbon Black sensor in JSON format.

Create Session Flow Action

The Create Session flow action establishes a Carbon Black session to use in the flow.

The Create Session flow action can be used with any flow to create a Carbon Black session within the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Session created.
Failure	Session not created. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
endpoint_base	Base URL of the Carbon Black API.
sensor_id	Sensor identifier.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
output	API variables

Check Session Status Flow Action

Determines the status of a Carbon Black session within the flow.

The Check Session Status flow action can be used with any flow to check Carbon Black session status within the flow .

Results

Possible results for this flow action are:

Results

Result	Description
Success	Session status returned.
Failure	Session status error. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
endpoint_base	Base URL of the Carbon Black API.
session_id	Session identifier.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
output	Information on Carbon Black running processes.

Create Command Process Flow Action

The Create Command Process flow action create a Carbon Black command process to use in the flow .

The Create Command Process flow action can be used with any flow to create a Carbon Black command process within the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Command process created.
Failure	Command process not created. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
endpoint_base	Base URL of the Carbon Black API.
session_id	Session identifier.
command_id	Command identifier.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
output	API variables

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Check Command Status and Get Process Flow Action

Checks the Carbon Black command status and retrieves processes to use in the flow.

The Check Command Status and Get Process Flow Action can be used with any flow to check a Carbon Black command status and get processes within the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Command status returned and processes created.
Failure	Command status or process error. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
endpoint_base	Base URL of the Carbon Black API.
session_id	Session identifier.
command_id	Command identifier.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
output	API variables

Map Processes Data Flow Action

The Map Processes Data flow action maps Carbon Black process data within the flow.

The Map Processes Data flow action can be used with any flow to map Carbon Black processes.

Results

Possible results for this flow action are:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Results

Result	Description
Success	Processes mapped
Failure	Processes not mapped. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
affected_ci	Configuration item affected.
implementation_id	Implementation identifier.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
output	Formatted return data on running processes used by the abstract workflow.
processes	List of processes in an array.

Close Session Flow Action

Closes a Carbon Black session within the flow.

The Close Session activity can be used with any flow to close a Carbon Black session.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Session closed.
Failure	Session not closed. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
endpoint_base	Base URL of the Carbon Black API.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
session_id	Session identifier.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
output	API variables

Security Operations System Command Integration- Get Running Processes flow

The Security Operations System Command Integration - Get Running Processes flow retrieves the running processes of a configuration item when added or updated to a Windows or Unix-based security incident in the **Analysis**state.

Before you begin

Role required: sn_si.analyst

About this task

For new security incidents, the flow runs automatically when you submit the incident with a selected configuration item, when the state automatically changes to **Analysis**. If it remains in the **Draft** state, then it does not run.

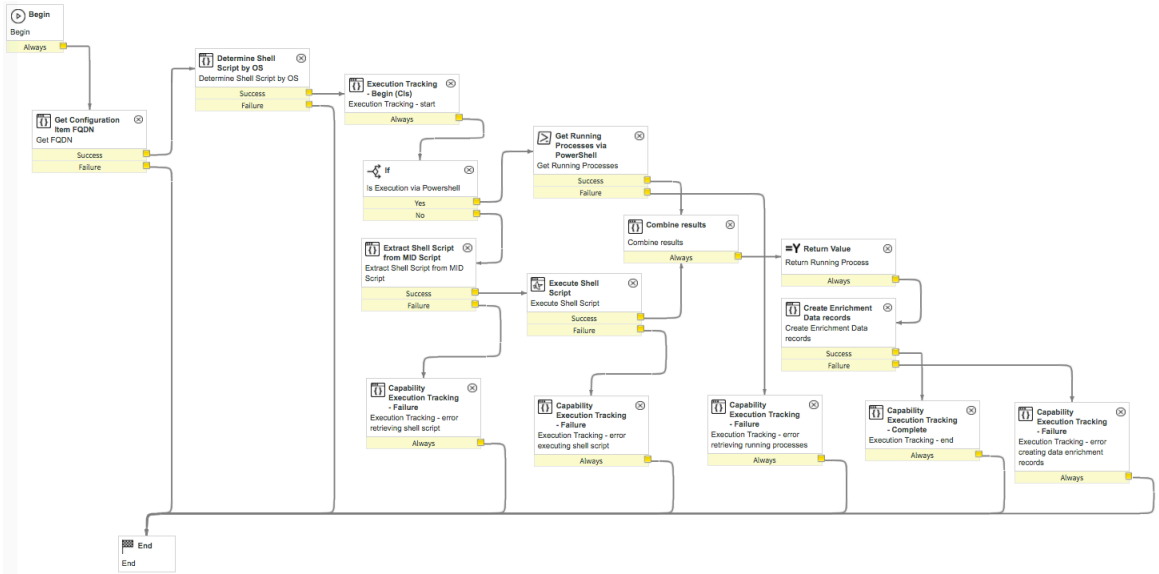
Existing security incidents are automatically updated when you are in the **Analysis** state and you add a new configuration item.

The flow process actions include:

- Get Configuration Item FQDN Flow Action
- Determine Shell Script by OS Flow Action
- Execution Tracking - Begin Flow Action
- Get Running Processes via PowerShell
- Execute Shell Script activity
- Capability Execution Tracking- Failure Flow Action
- Extract Shell Script from MID Script activity
- Combine Results and return values in an array
- Create Enrichment Data records Flow Action

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get Running Processes



Procedure

1. Open a security incident.
2. Update the **State** to **Analysis**, if necessary.
3. Add a configuration item (computer, server, or similar).
4. Click **Update**.
   Security Incident Response Orchestration provides running process information in the **Related Link** > **Security Incident Enrichments**tab. For more information, see Security Operations enrichment data mapping.

   Actions specific to this flow are described here. For more information on other actions, see Common Security Operations integration flows and orchestration Flow Actions.

Combine results activity

The Combine results workflow activity merges the results from third-party integrations to use in the workflow.

The Combine results activity can be used with any workflow to execute a MID server shell script in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Results combined.
Failure	Combination failed. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
inputA	Result set A
inputB	Result set B
implementation_id	Implementation identifier.
affected_ci	Configuration item

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
result	Result set A or Result set B based on which one is filled.

Execute Shell Script activity

The Execute Shell Script workflow activity runs a MID server shell script within the workflow.

The Execute Shell Script activity can be used with any workflow to execute a MID server shell script in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Found shell script
Failure	No shell script found. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
target	IP or fully-qualified domain name (FQDN) of the target CI.
scriptValue	Script, as a string value, executed on a Unix system.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response	Raw output. Running processes data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Extract Shell Script from MID Script activity

The Extract Shell Script from MID script workflow activity pulls a MID server shell script to use with in the workflow.

The Extract Shell Script from MID Script activity can be used with any workflow to extract a MID server shell script to include in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Found shell script
Failure	No shell script found. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
sysId	System identifier

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
scriptValue	Script, as a string value, executed on a Unix system.

Get Running Processes via PowerShell activity

The Get Sensor ID workflow activity gathers running processes using PowerShell to use in the workflow.

The Get Running Processes via PowerShell workflow activity can be used with any workflow to retrieve processes to include in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Found processes
Failure	No processes found. More error information is available in the activity output error.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
target	IP or fully-qualified domain name (FQDN) of the target CI.
processingScript	ECC script run on a Windows-based system.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response	Raw output. Running processes data.

Security Operations Integration- Isolate Host capability

The **Isolate Host** capability restricts system connections to other devices. Isolate host is executed against a configuration item (CI).

The **Isolate Host** capability has a flow, Security Operations - Isolate Host Flow that accepts one or more CIs and optionally an implementation. You can specify an implementation to use to isolate the host or for the flow to attempt to isolate the host using all implementations.

Note: While not integrated with a capability, a flow, Security Operations Carbon Black Integration- Remove Host Isolation Flow is available for orchestration to restore communication with an isolated host.

Note: If no implementations are available, capability actions are not displayed in product menus.

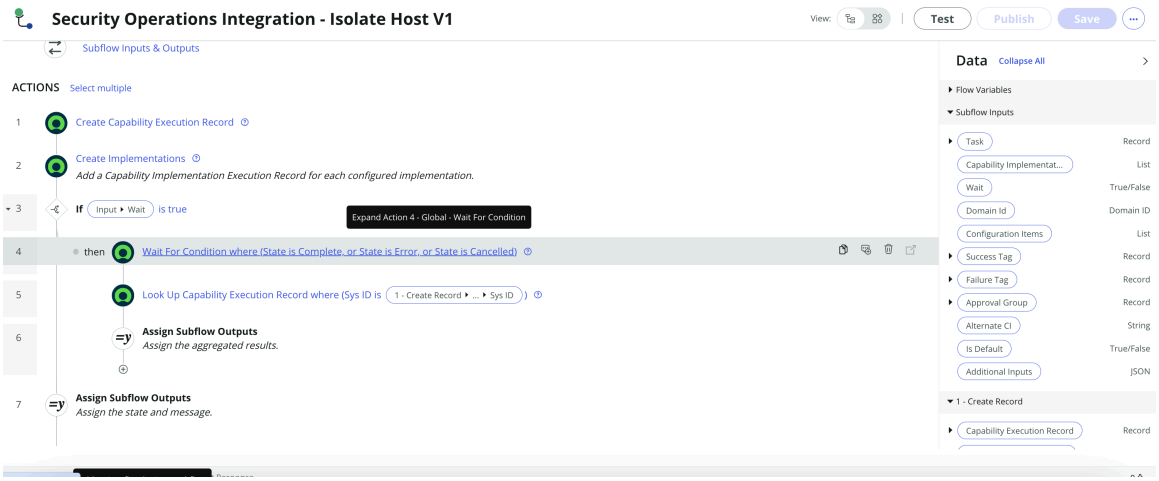
Security Operations - Isolate Host Flow

The **Security Operations - Isolate Host** flow is a high-level flow independent of integrations. It uses the configured queries to search for a set of configuration items. Use it to fulfill an integration, such as Carbon Black.

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Isolate Host



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Run Isolate Host

Isolate Host restricts system connections to other devices.

Before you begin

Role required: sn_si.analyst

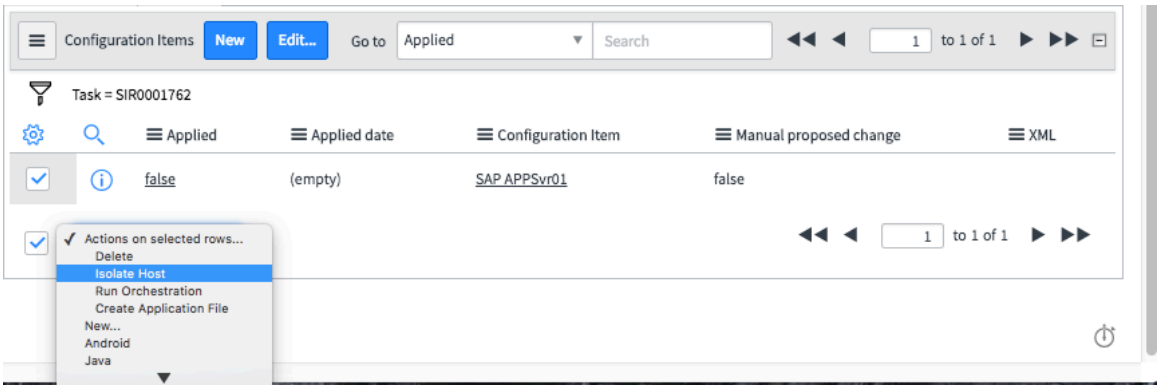
About this task

Note: If no implementations are available, capability actions are not displayed in product menus.

The **Security Operations Integration - Isolate Host or Endpoint** flow can be triggered from the related list on a security incident.

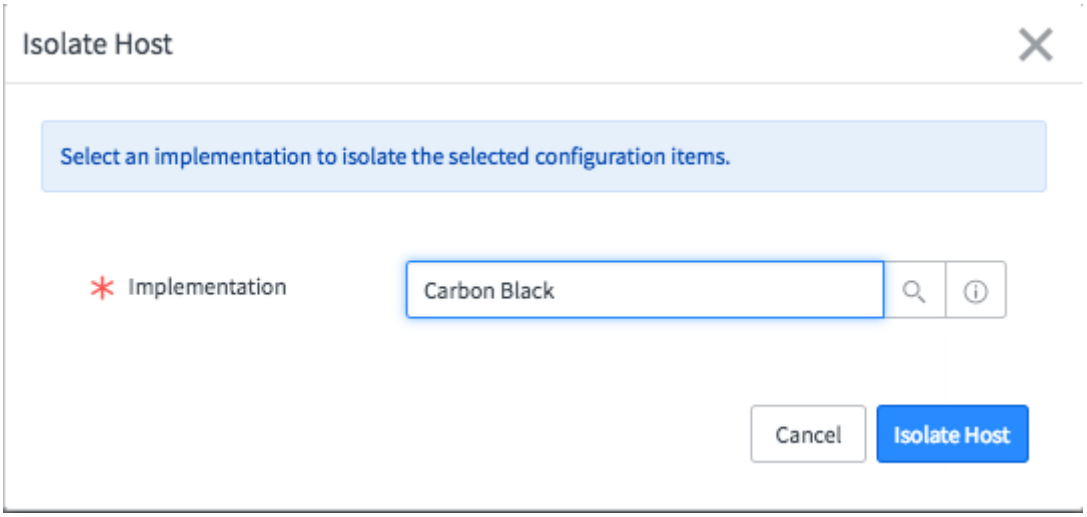
Procedure

1. Navigate to a security incident.
2. Select **Configuration Items** from the **Related List** tab.
3. Click **Isolate Host** in the **Actions on selected rows...** drop-down menu.

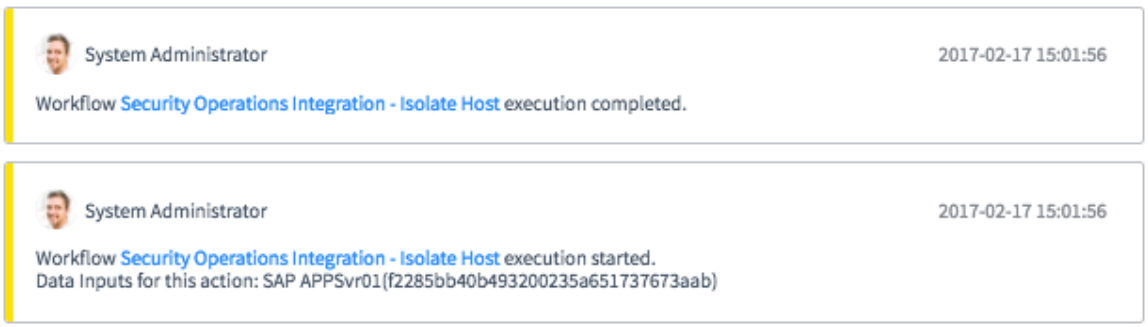


The dialog box appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. Choose the implementation.
5. Click **Isolate Host**.
   The flow execution audit is displayed in the work notes section.



Security Operations Carbon Black Integration - Isolate Host Flow

The Security Operations Carbon Black Integration - Isolate Host is the implementation for the Carbon Black integration launched by the Security Operations Integration - Isolate Host flow.

Before you begin

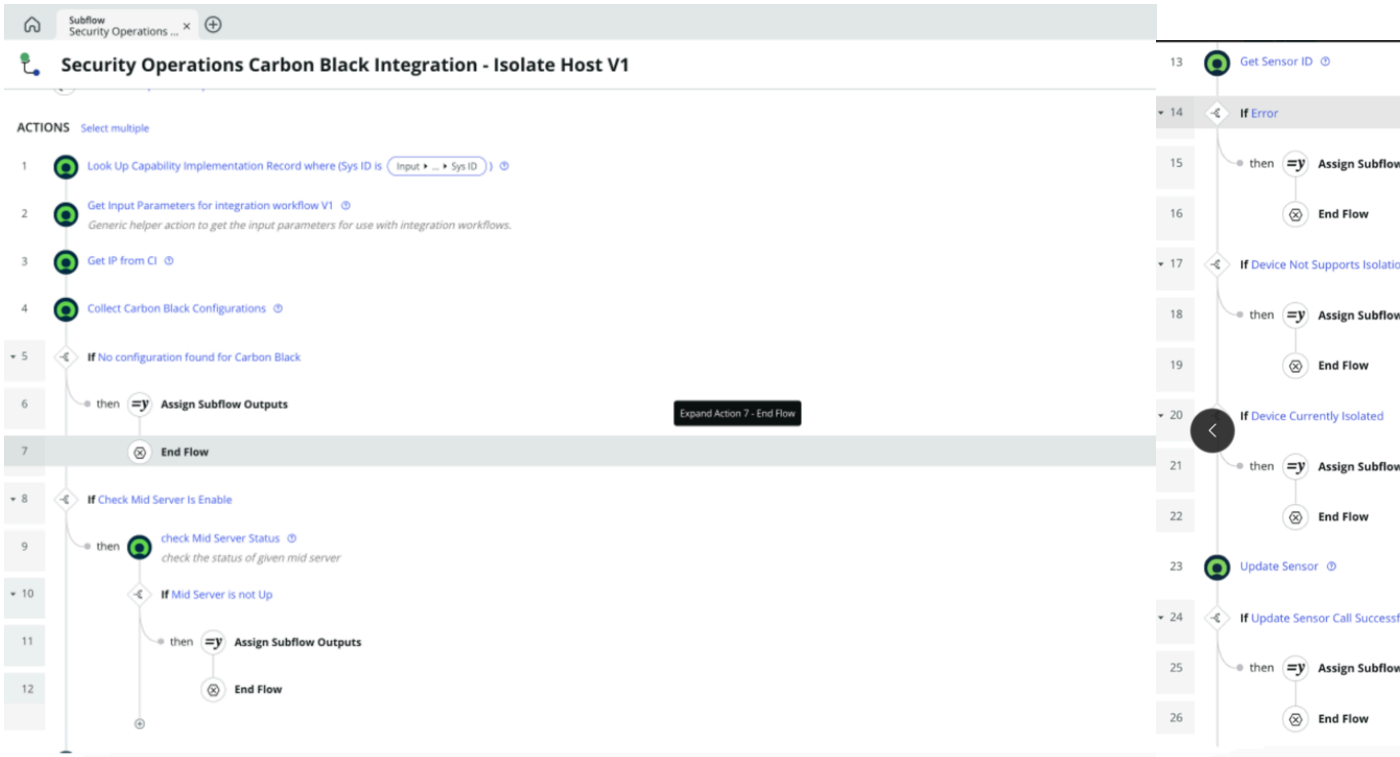
Role required: sn_si.analyst

About this task

The flow process flow action include:

- Execution Tracking - Begin (CIs) Flow Action
- Get IP from CI
- Collect Carbon Black configurations
- Capability Execution Tracking- Failure Flow Action
- Get Sensor ID
- Set Network Isolation Enabled Flow Action
- Update Sensor - returns Isolate Host result.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Get Sensor ID Flow Action

The Get Sensor ID flow action gathers sensor identifiers to use in the flow.

The Get Sensor ID flow action can be used with any flow to gather sensor information to use in the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Found sensor identifiers.
Failure	No sensors found. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.
endpoint_base	Base URL of the Carbon Black API.
ci_ip_address	Configuration item IP address.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.
Array Element type	API variables.
sensor_detail	Description of the Carbon Black sensor in JSON format.

Set Network Isolation Enabled Flow Action

The Set Network Isolation Enabled flow action enables network isolation.

The Set Network Isolation Enabled flow action can be used with any flow to enable network isolation.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Network isolation enabled.
Failure	Network isolation cannot be enabled. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
sensor_detail	Description of the Carbon Black sensor in JSON format.
disable	Determines whether the host is isolated or removes host isolation. True = disable isolation False = isolation remains enabled

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
sensor_detail	Description of the Carbon Black sensor in JSON format.

Update Sensor Flow Action

The Update Sensor flow action updates the sensor to isolate hosts or endpoints.

The Update Sensor flow action can be used with any flow to isolate hosts or endpoints.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Updated sensor.
Failure	Unable to update sensor. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
api_token	Carbon Black API key.
use_mid_server	Determines whether the REST flow action uses the MID server to interact with Carbon Black or not.
endpoint_base	Base URL of the Carbon Black API.
sensor_id	Sensor identifier.
sensor_detail	Description of the Carbon Black sensor in JSON format.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
status_code	Determines if the request was successful. If not, displays an HTTP error code and message.

Security Operations Carbon Black Integration- Remove Host Isolation Flow

The **Security Operations Carbon Black Integration - Remove Host Isolation** flow unblocks communication with a specified host or endpoint in a Carbon Black system.

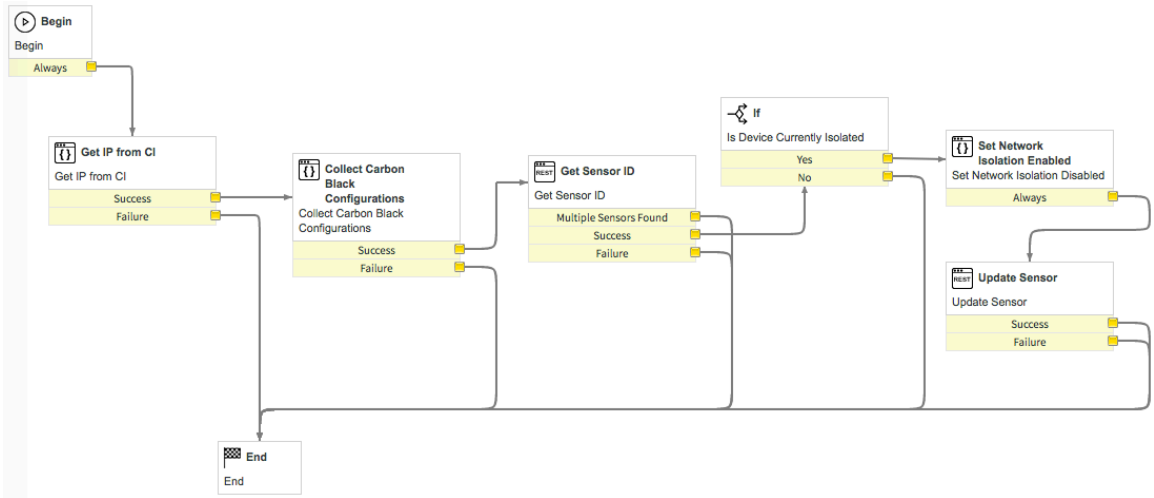
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_si.analyst

About this task
This flow is not part of a capability and needs a custom orchestration in order to run.
The flow process activities include:

- Get IP from CI Flow Action
- If successful- Collect Carbon Black Configurations Flow Action
- Get Sensor ID Flow ActionGet Sensor ID
- If- Device supports isolation- and device is not isolated-Set Network Isolation Enabled Flow Action to disabled.
- Update Sensor Flow Action- returns Isolate Host result.

Carbon Black Integration- Remove Host Isolation



Security Operations Integration- Publish to Watchlist capability

The Publish to Watchlist capability adds observables and indicators associated with a security incident to a third-party watchlist that monitors for security events and generates alerts. This capability is used as part of incident response during investigations.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - Publish to Watchlist Flow

The **Security Operations Integrations - Publish to Watchlist** flow is a high-level flow independent of integrations. It adds observables to third-party watchlist that support the capability. Use it to fulfill an integration.

Before you begin
Role required: sn_si.analyst

About this task
This flow is visible and runs only when an integration is available. It is triggered from the **Observables** or **Associated Indicators** tab on a security incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Security Operations Integration- Sightings Search capability

The **Sightings Search** capability accepts a set of observables, finds any integrations that support a Sightings Search, then executes these searches.

The Sightings Search capability has a workflow, Security Operations Integration - Sightings Search Flow, that executes the sightings search. This workflow accepts a list of observables, finds any implementing capabilities, creates the queries based on Sightings Search Configurations, and executes the searches based on the configured workflow. Once the search is complete, a note is added to the incident Work notes including whether any sightings were found and if so, how many.

To view Sightings Search Configurations, navigate to **Security Operations** > **Integrations** > **Sightings Search Configurations**.

Note: If no implementations are available, capability actions are not displayed in product menus.

Create sightings search configuration records

Create multiple sightings search configuration records and use them while querying multiple log stores or varying the search parameters.

Before you begin

Role required: sn_si.admin

- The CIM add-on must be installed on the Splunk instance.
- Saved Searches and Inplace queries are supported for Splunk Integration only.

About this task

You can also create sightings search configuration records to invoke saved searches on the Splunk enterprise log store.

Note: The search configuration queries rely on Splunk log data to be Splunk Common Information Model (CIM) compliant.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With saved search configurations, you can:

- Create custom searches that combine multiple event records.
- Design-efficient and effective searches.
- Use parametrized inputs in the Splunk saved search.

The base system includes the sample configurations as shown in this image:

Saved search configurations

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

The saved search and Inplace configuration queries are example queries and can be substituted with appropriate parameters for your environment. Create additional saved search configurations as required. When you define a saved search configuration, the name and the parameters in the search query must match the saved configuration defined on your Splunk instance. If the name and parameters are not the same, you may not see accurate results when you perform a sightings search.

Note: On your Splunk instance, navigate to the Searches, Reports, and Alerts page and locate your saved search query. Click the **Permissions** link to navigate to the Permissions page. Select the **All Apps** radio button and enable the **Read Permission** option for **Everyone**. This will change the Sharing column value from Private to App for your saved search query. If this is not set, saved search query may not return any results.

To verify if the saved search configuration matches the configuration defined on your Splunk instance:

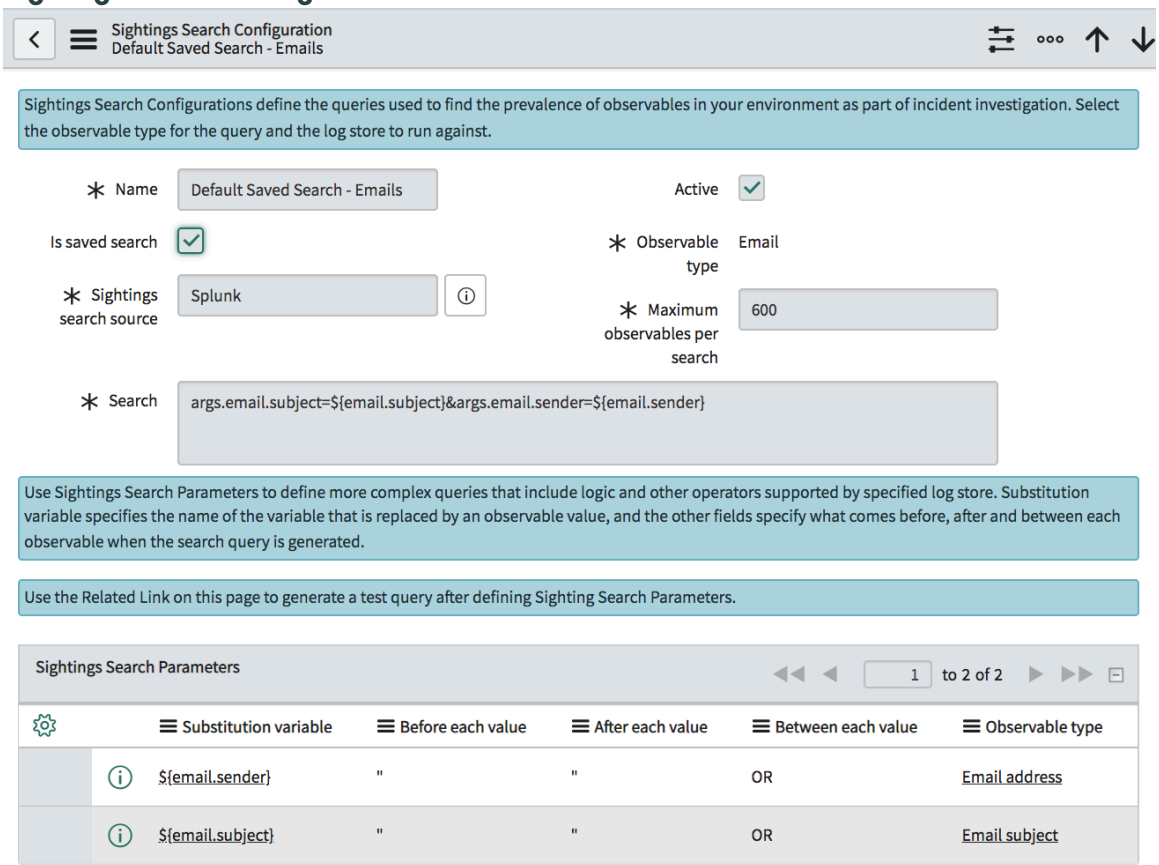
1. Navigate to **Settings** > **Searches, Reports, and Alerts**.
2. Change **App Context** to **All**.

   A list of search reports is displayed.
3. Confirm that the saved search query is present in the list.

For example, the Sightings Search Configuration form contains the email address and email sender as search parameters:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sightings Search Configuration form



In your Splunk instance, define the saved search with the same name, Default Saved Search - Emails, and the same search parameters for the email address and email subject. If the name and search parameters are not the same, sightings search does not generate accurate result.

Procedure

1. Navigate to **Security Operations** > **Integrations** > **Sightings Search Configuration** and create a new record (see table for field descriptions).

Sightings Search Configuration form

Field	Description
Name	Name of the configuration.
Is saved search	Saved search configuration is created if you select this option.
Sightings search source	The source for the sightings search. Select the Splunk log store as the source.
Active	Option for the saved search status. Only active search configurations can be used to perform a sightings search.
Observable type	Observable type can be any observable type such as IP, hash value, URL, domain name, and so on.
Maximum observables per search	Maximum number of observables to be returned from the search.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Search	The default search string is `$(observable)`, but you can define your own search query by specifying parameters that are supported by the Splunk log store.

2. Click **Submit**.

Result
You have created a sightings search configuration record.

What to do next
After defining the search query, click **Generate Sightings Search Test Query**, and specify a list of observable values to generate a test query based on this saved search configuration.

Run a Sightings Search

Determine the prevalence of a threat over time or test remediation or eradication efforts. You can select individual or multiple observables and the date range for your search from a security incident. Results are included in the **Security Incident Observables** related list.

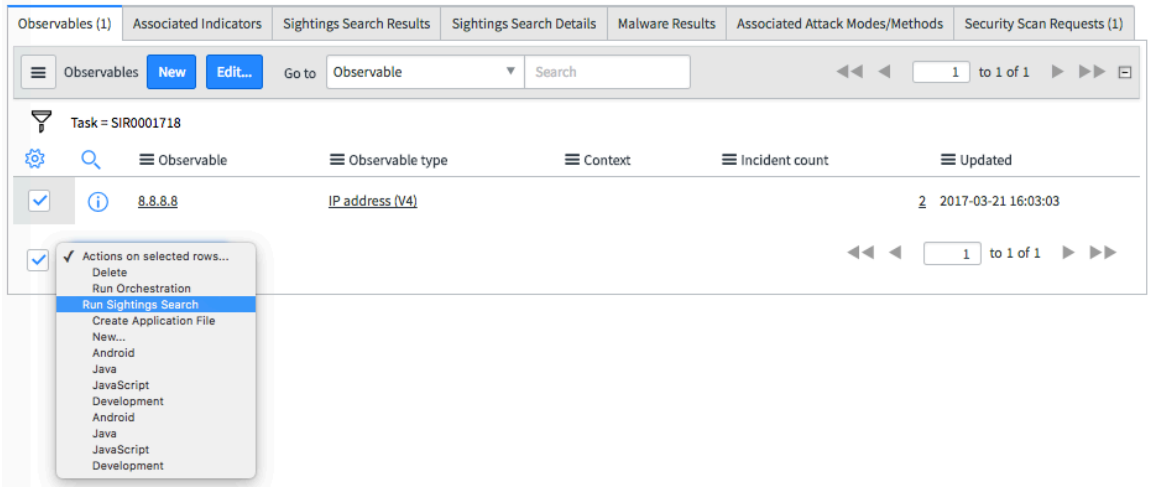
Before you begin
Role required: sn_si.analyst

About this task
The Sightings Search capability has a flow, Security Operations Integration - Sightings Search Flow, that executes the sightings search. This flow accepts a list of observables, finds any implementing capabilities, creates the queries based on Sightings Search Configurations, and executes the searches based on the configured flow.

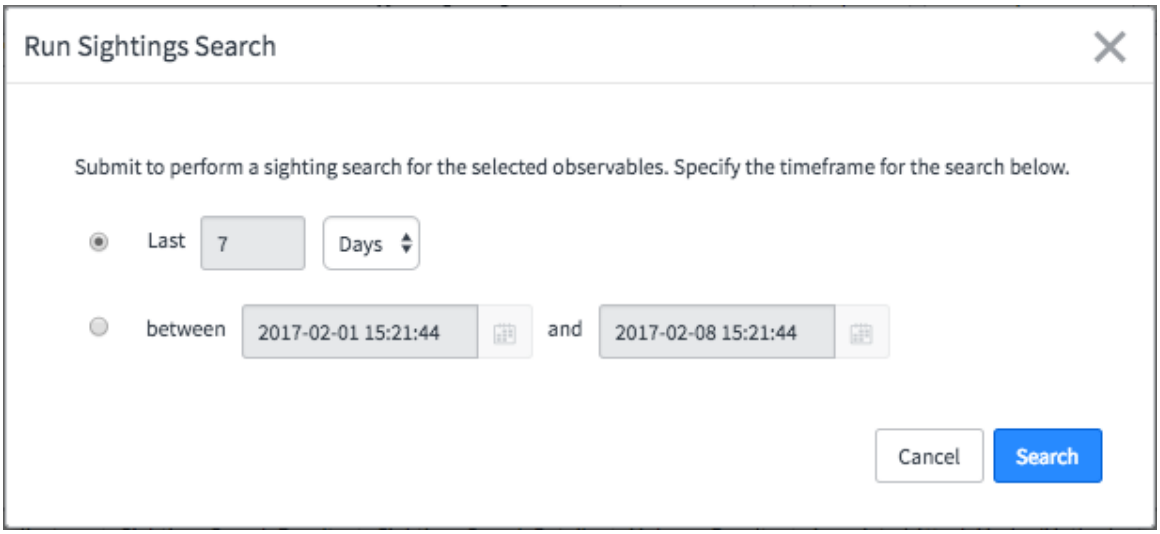
> **Note:** An active implementation must be configured. Sightings Search supports Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger, and QRadar incident enrichment. If no implementations are available, capability actions, such as **Run Sightings Search**, are not displayed in product menus.

Procedure
1. Navigate to a security incident.
2. Click the **Show IoC** related link.
3. Select **Observables** from the Related List tab.
4. Select the observables you want to perform a sightings search on.
5. Click **Run Sightings Search** in the **Actions on selected rows...** drop-down menu.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The Run Sightings Search dialog box opens.



Note: Values entered in the dialog box overwrite capability configuration values for this run.

6. Choose the number of days or a date range to search for data.

Option	Description
Last	The number of hours or days prior to the cre ation of the incident to search. The default is 7 days. The limit is 99 hours or days.
between	Range of dates to search. Default dates are: The date and time the incident was opened. The date and time seven days prior to the opening of the incident.

Note: **Last** is the number of hours or days prior to the creation of the incident to search. The default is 7 days. The limit is 99 hours or days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Click **Search**.
   A Sightings Search record is created. Aggregate and associated sightings data are displayed in the security incident under the **Sightings Search Results** and **Sightings Search Details** tabs.

   Note: Sightings search results data can be shared with Trusted Security Circle, with the exception of raw data in the case of implementations configured to include raw data.

Sightings Search Results

Result	Description
Number	The identifier for the sightings search.
Observable count	Number of observables searched for by query.
Internal sightings	Count of internal sightings.
External sightings	Count of external sightings. (Received from threat sharing.)
Matched configuration items	Count of configuration items that matched an existing record in your cmdb for each observable found in your environment.
Start date range	Time to start looking for sightings.
End date range	Time to stop looking for sightings.
Updated	Date and time of the last modification.

Note: If the implementation used for the sightings search is configured to include raw data, and at least one sighting is found, an attachment containing raw data samples appears at the top of the security incident.

Sighting Search Details

Detail	Description
Sighting search	The identifier for the sightings search.
Observable	Observable searched for by query.
Observable type	Type of observable searched for by query.
Internal sightings	Aggregated count of internal sightings.
External sightings	Aggregated count of external sightings. (Received from threat sharing.)
Updated	Date and time of the last modification.

Security Operations Integration - Sightings Search Flow

Security Operations Integration - Sightings Search flow is a high-level flow independent of integrations. It uses the configured queries to search for a set of observables based on the configured integrations which support the capability. Use it to fulfill an integration such as Splunk or Elasticsearch.

Before you begin

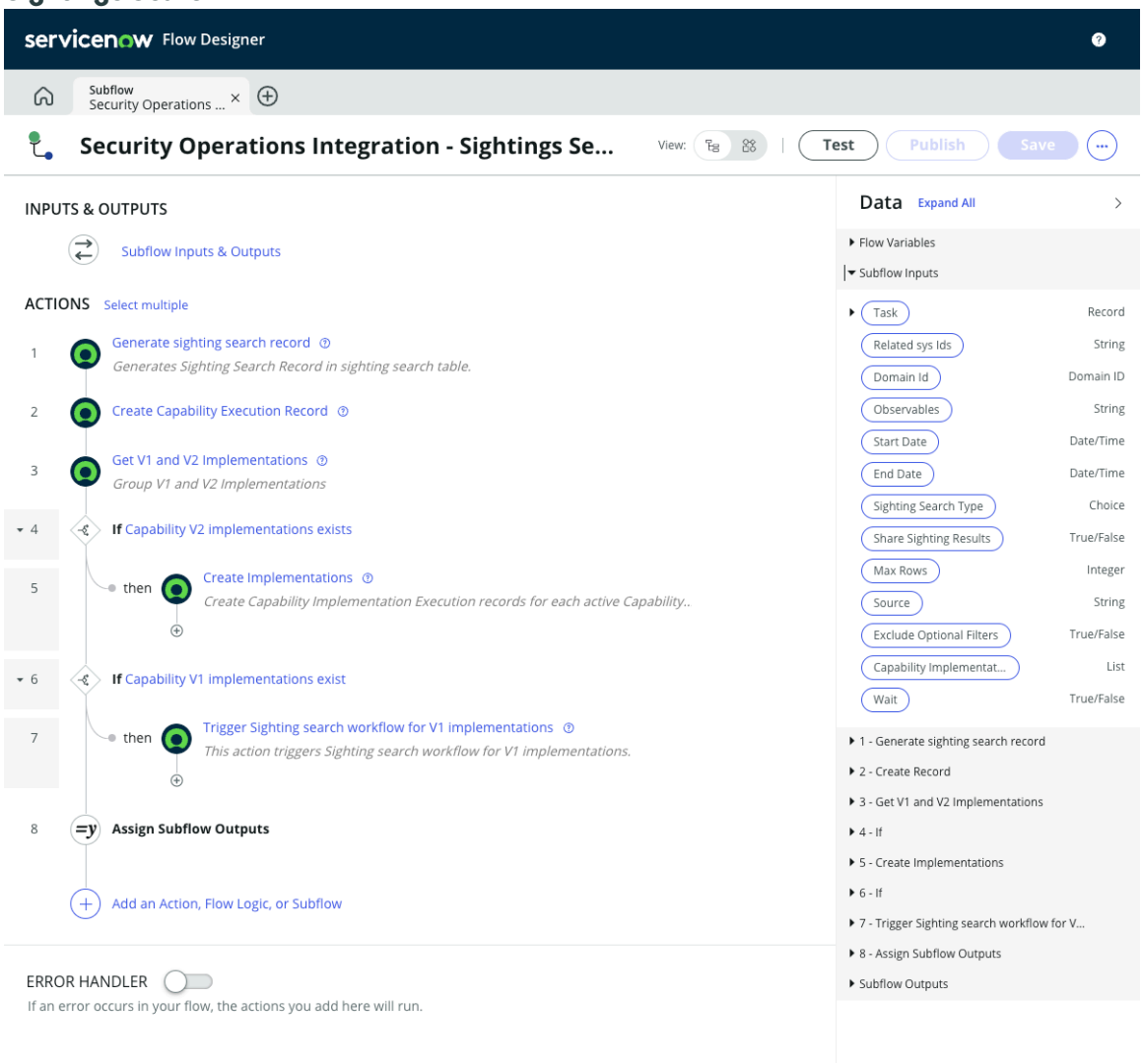
Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

If a security incident has an observable attached to it, this flow is triggered when you click on **Run Sighting Search** in the **Actions on selected rows...** drop-down menu in the **Security Incident Observables** tab.

Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

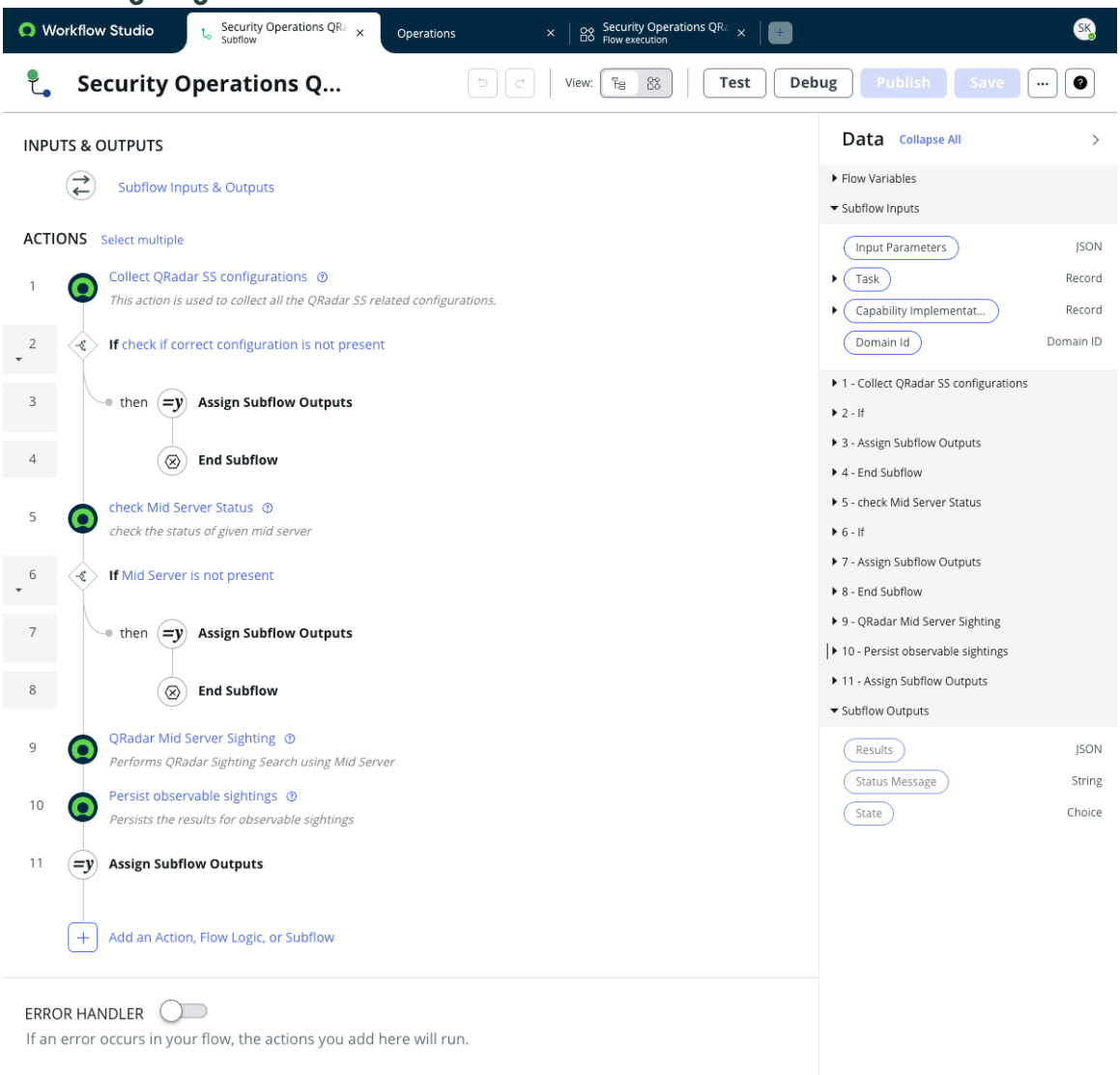
Security Operations - QRadar Sightings Search Flow

Security Operations - QRadar Sightings Search flow is the implementation for the IBM QRadar integration launched by the **Security Operations Integration - Sightings Search flow**.

Role required: sn_si_analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

QRadar Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

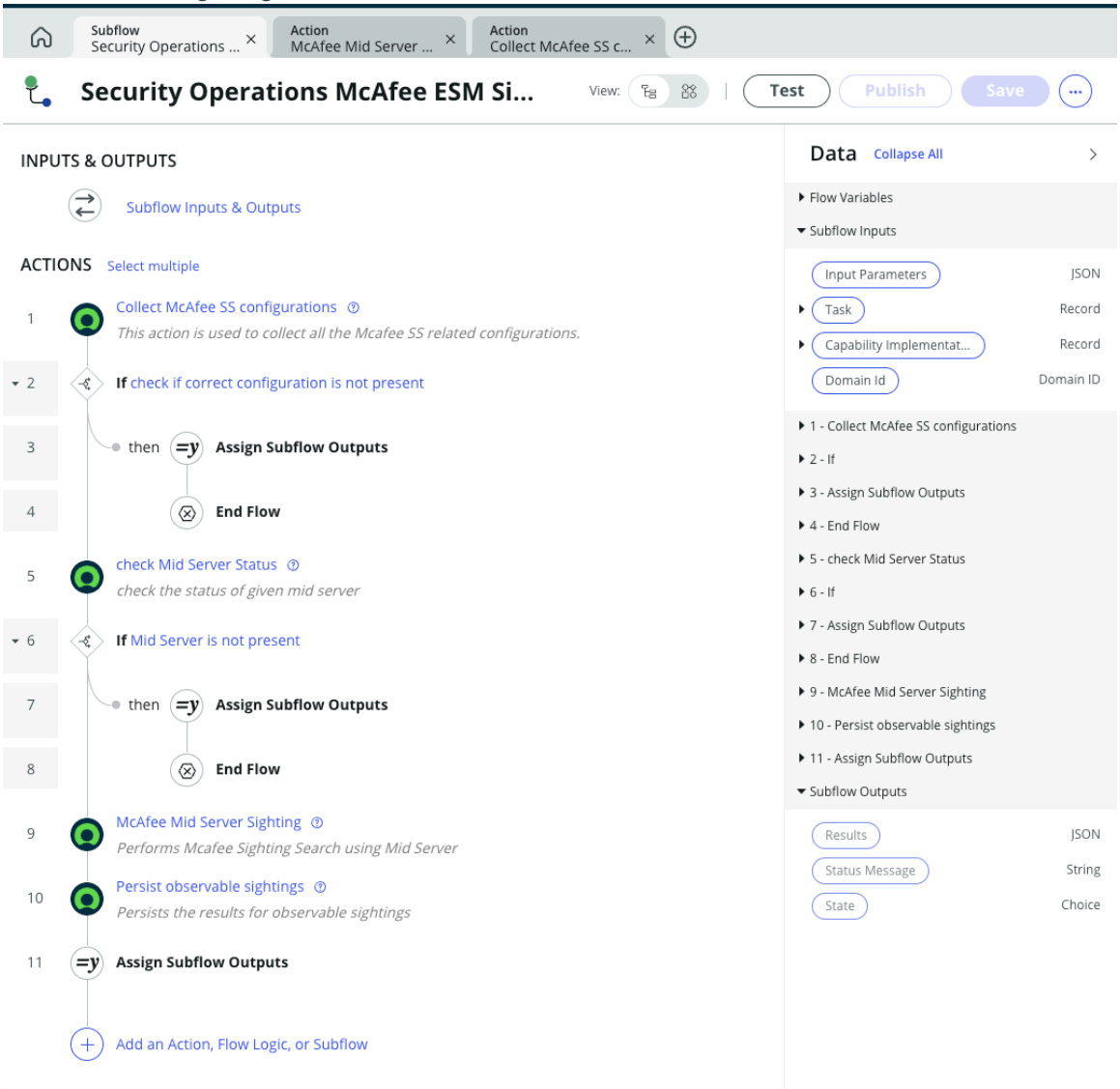
Security Operations - McAfee ESM Sightings Search Flow

Security Operations - McAfee ESM Sightings Search flow is the implementation for the McAfee Sighting Search implementation launched by the **Security Operations Integration - Sightings Search Flow**.

Role required: sn_si_analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

McAfee ESM Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

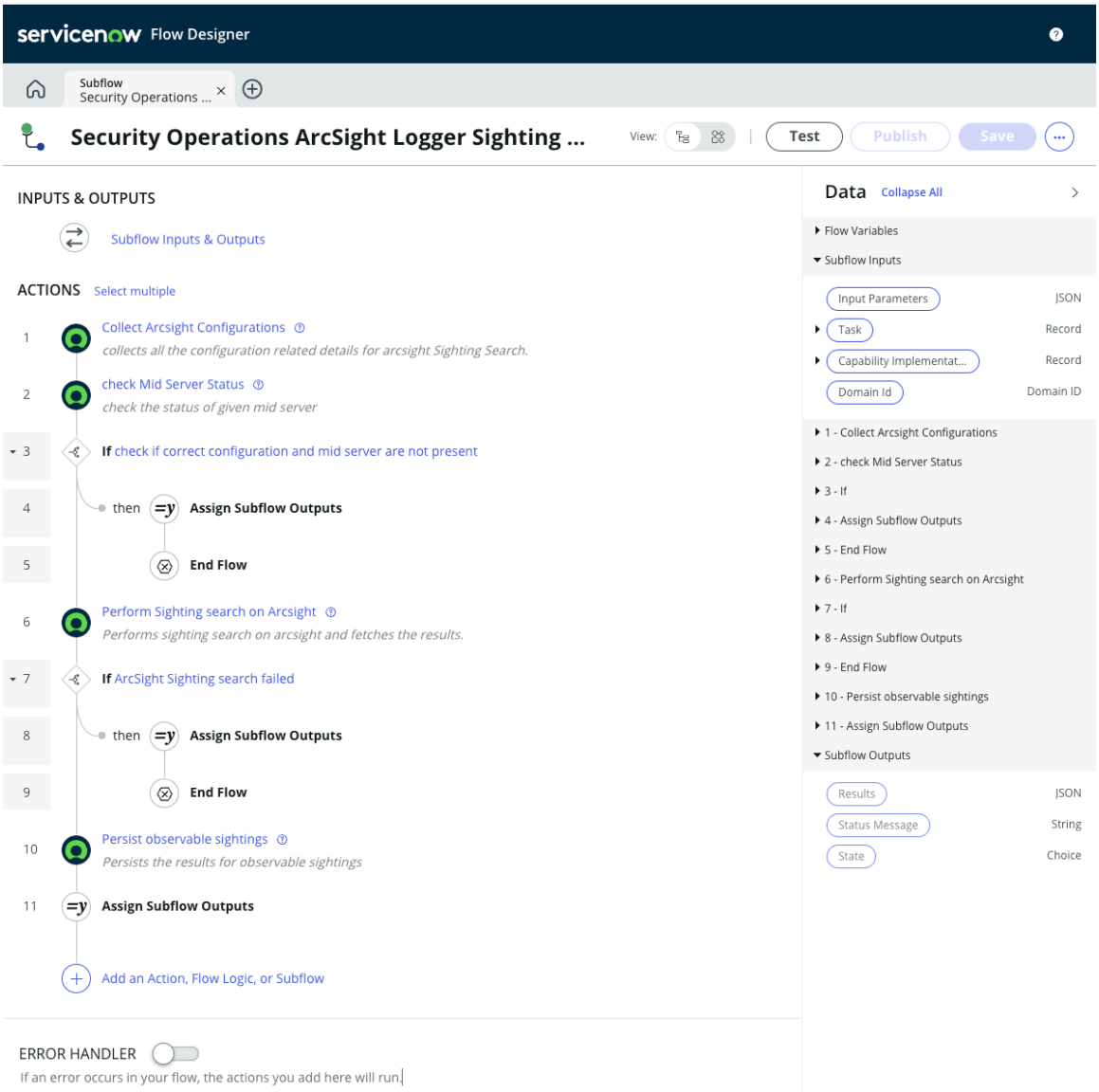
Security Operations - Arcsight Logger Sightings Search Flow

Security Operations - ArcSight Logger Sightings Search flow is the implementation for the Splunk integration launched by the **Security Operations Integration - Sightings Search Flow**.

Role required: sn_si_analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Arcsight Logger Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

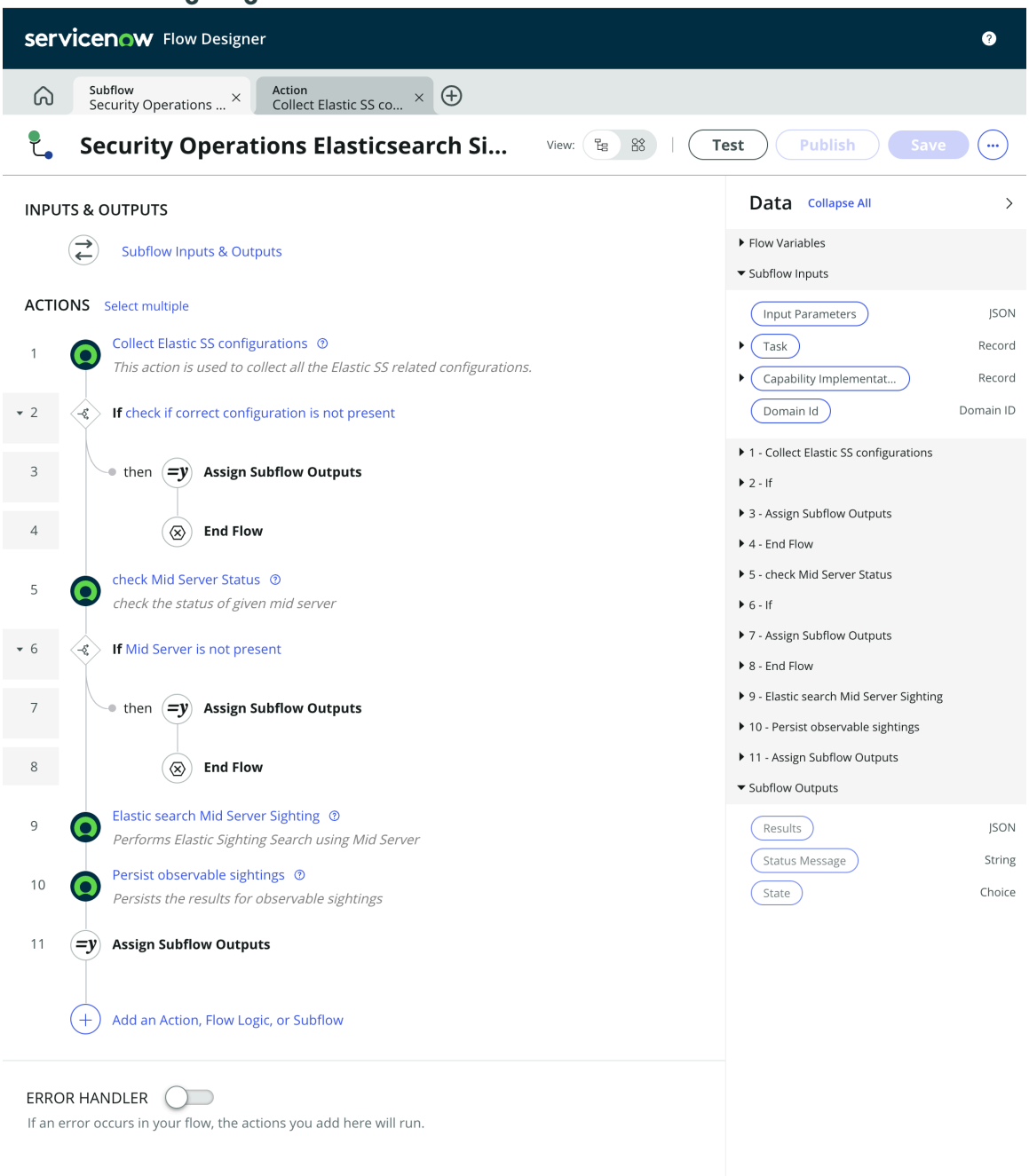
Security Operations - Elasticsearch Sightings Search Flow

Security Operations - Elasticsearch Sightings Search flow is the Elasticsearch implementation launched by the **Security Operations Integration - Sightings Search** flow.

Role required: sn_si.analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Elasticsearch Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

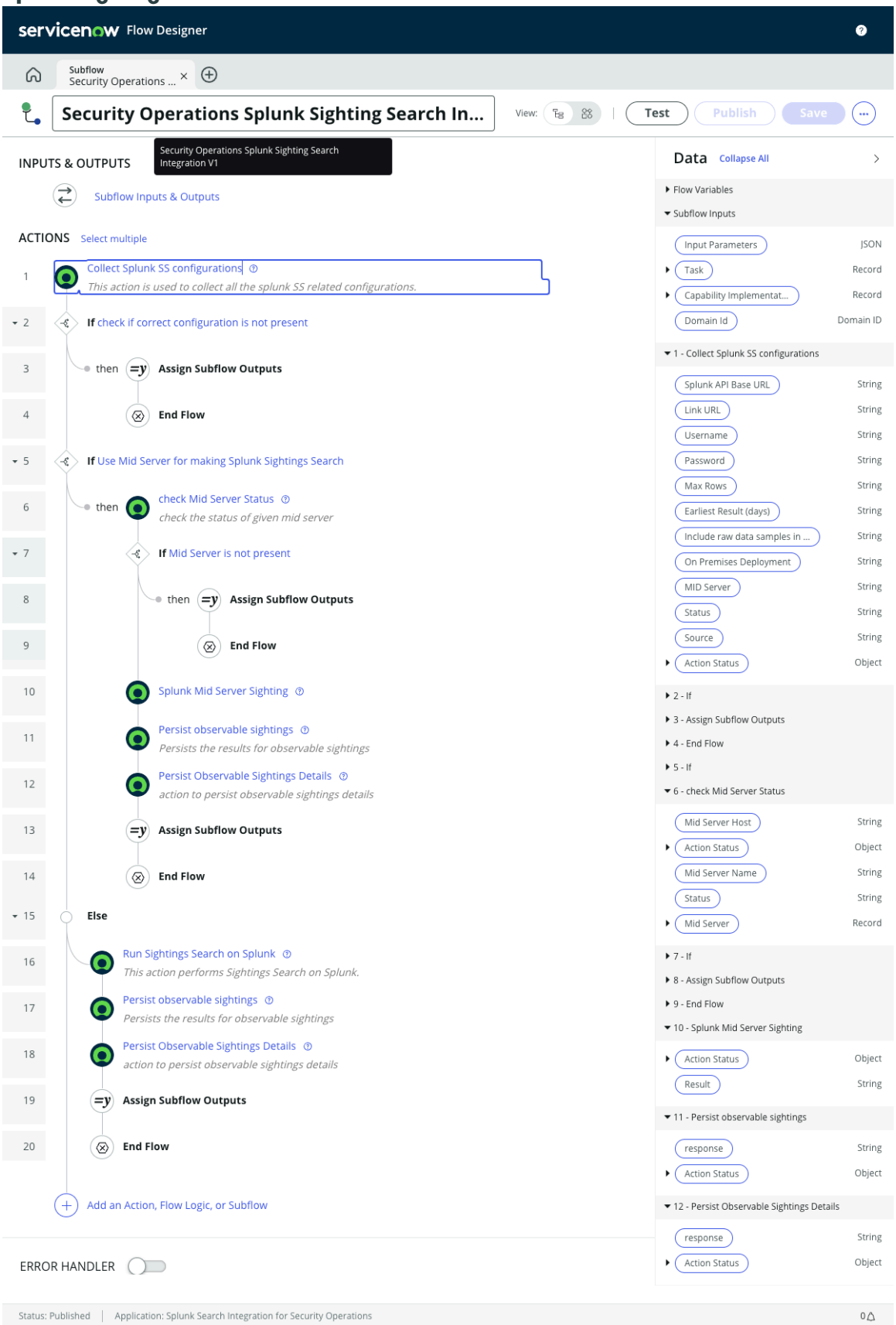
Security Operations Integration - Splunk Sightings Search Flow

Security Operations - Splunk Sightings Search flow is the implementation for the Splunk integration launched by the **Security Operations Integration - Sightings Search flow**.

Role required: sn_si_analyst

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Splunk Sightings Search



Activities specific to this flow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

View Sightings Search Results

You can review Sightings Search Results for internal and external malicious indicators.

Before you begin

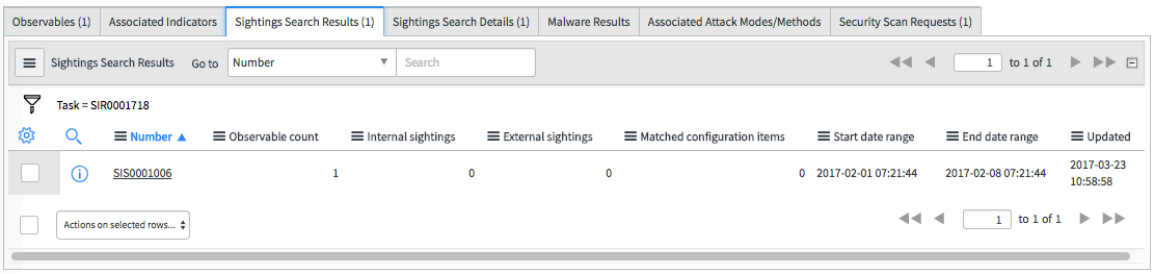
Role required: sn_si.analyst

About this task

.

Procedure

1. Navigate to a security incident.
2. Select the **Sightings Search Results** tab from **Show IoC** Related List group to view the list of sightings searches.



Note: This data can be shared with Trusted Security Circle.

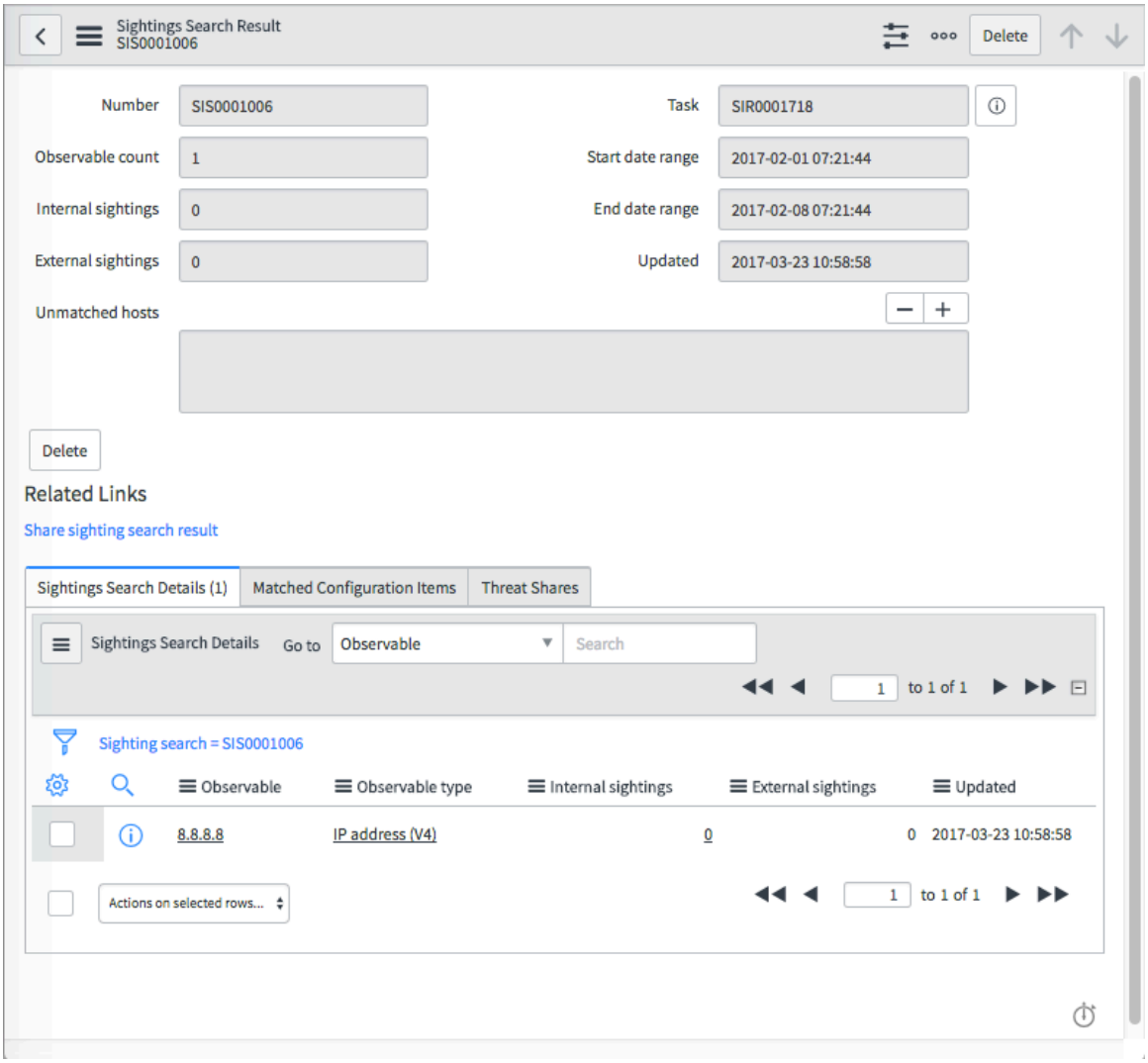
Sightings Search Results

Result	Description
Number	Sightings Search identifier.
Observable count	Number of observables searched for.
Internal Sightings	Aggregated count of internal sightings.
External Sightings	Aggregated count of external sightings. (Received from threat sharing.)
Matched configuration items	Aggregated count of configuration items that matched an existing record in your cmdb.
Start date range	Time to start looking for sightings.
End date range	Time to stop looking for sightings.
Updated	Date and time of last modification.

To view the details of a single search:

3. Click on a Sightings Search in the **Sightings Search Results** list.
The Sightings Search Result form displays.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Sightings Search Results form

Detail	Description
Number	Internal Sightings Search identifier.
Observable count	Count of observables searched for by this query.
Internal sightings	Count of internal sightings for this search.
External sightings	Count of external sightings for this search. (Received from Trusted Security Circle.)
Unmatched hosts	List of potential configuration items for this search that were not matched with any records in your `cmdb`.
Task	Security incident task identifier.
Start date range	Time the sightings search started.
End date range	Time the sightings search stopped.
Updated	Date and time of last modification.
Sightings Search Details	Type, number of sightings and modification date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Detail	Description
Matched Configuration Items	Count of configuration items that matched an existing record in your `cmdb`. Lists the CI and the Sighting.
Threat Shares	List of the threats shared with Trusted Security Circle.

Share Sightings Search results

You can share local sightings details or results that are associated with a particular search with your Trusted Security Circle.

Before you begin

Role required: sn_si.analyst

About this task

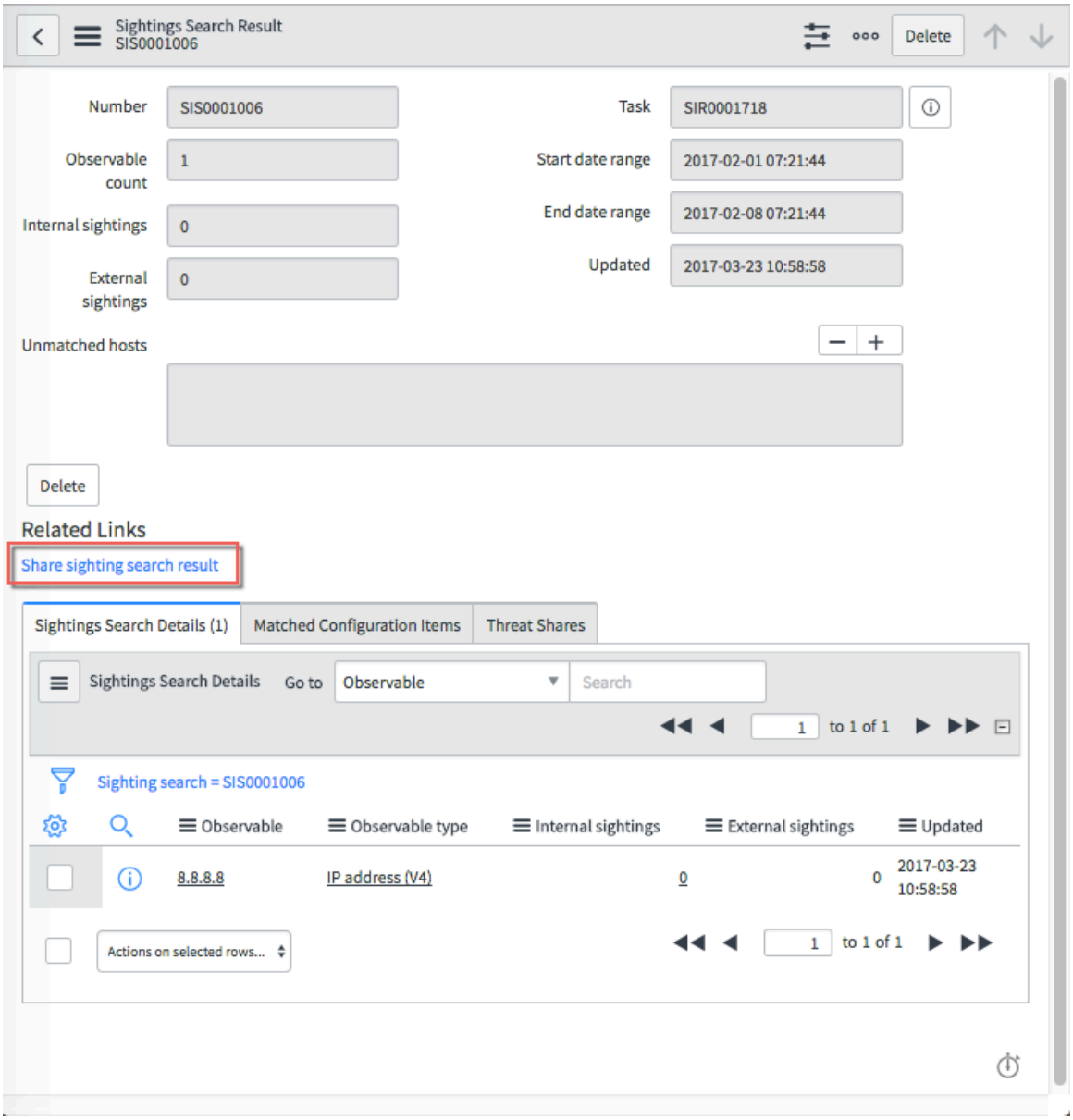
Sharing can be automated using the following Security Incident Response **Properties**.

- Automatically share the results of a sightings search to the default ServiceNow trusted circle
- Include observables with no local sightings when automatically sharing sightings search results
- Respond with local sightings whenever a threat share is received from a trusted circle

Procedure

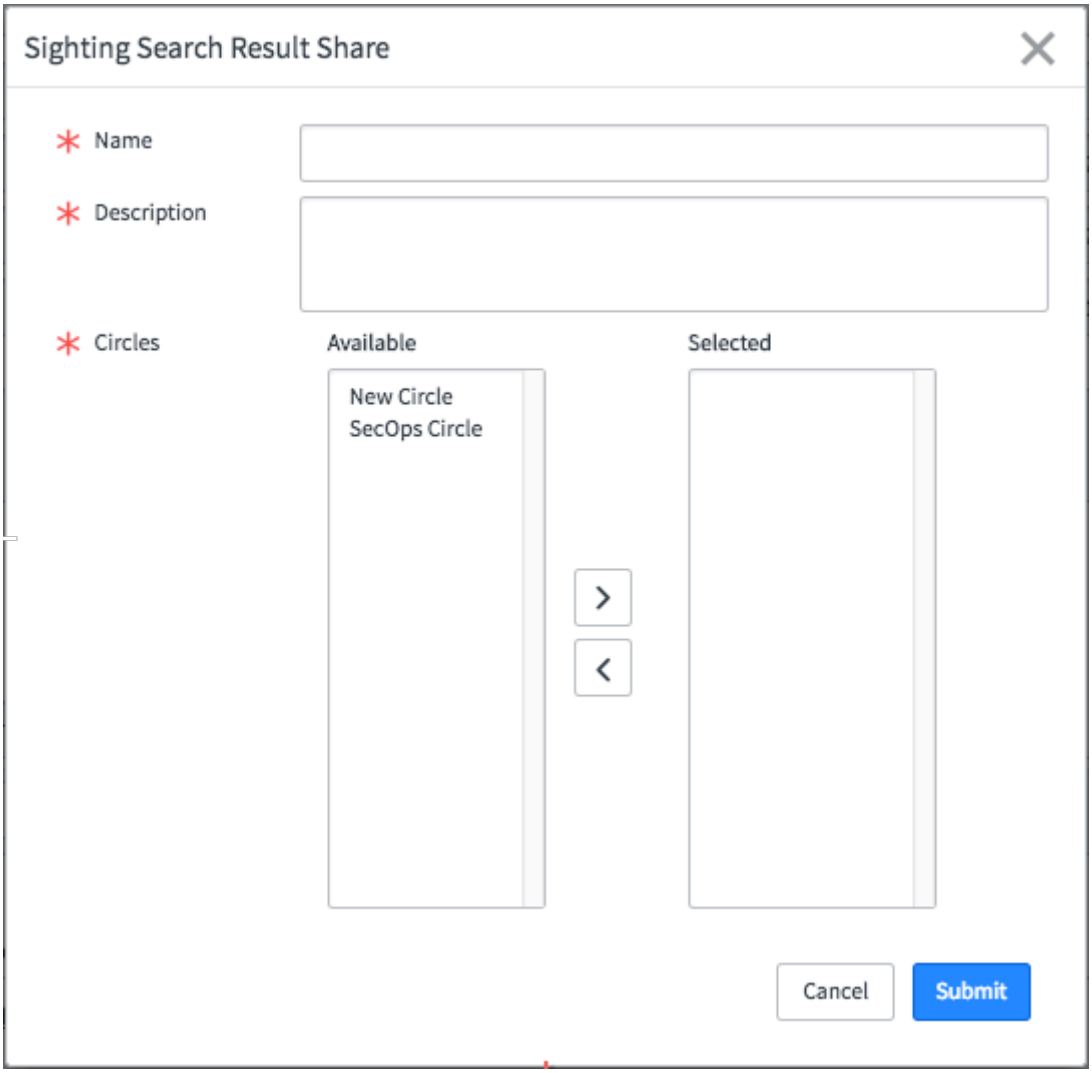
1. Navigate to a security incident.
2. Click the **Show IoC** related list and select the **Sightings Search Results** tab to view the list of sightings searches.
3. Click on a sightings search result.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. On the **Sightings Search Result**form, click the **Share sighting search result** related link.
   The Sighting Search Result Share dialog box appears.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. Enter a **Name** for this observable share record.
6. Enter a **Description**of the observables to share.
7. Choose **Circles** to share the observables with.
8. Click **Submit**.
   The observable(s) are shared with the specified Trusted Circle.

Share observables from a security incident

Observables can be shared from a security incident in Security Incident Response to members in your trusted circle.

Before you begin

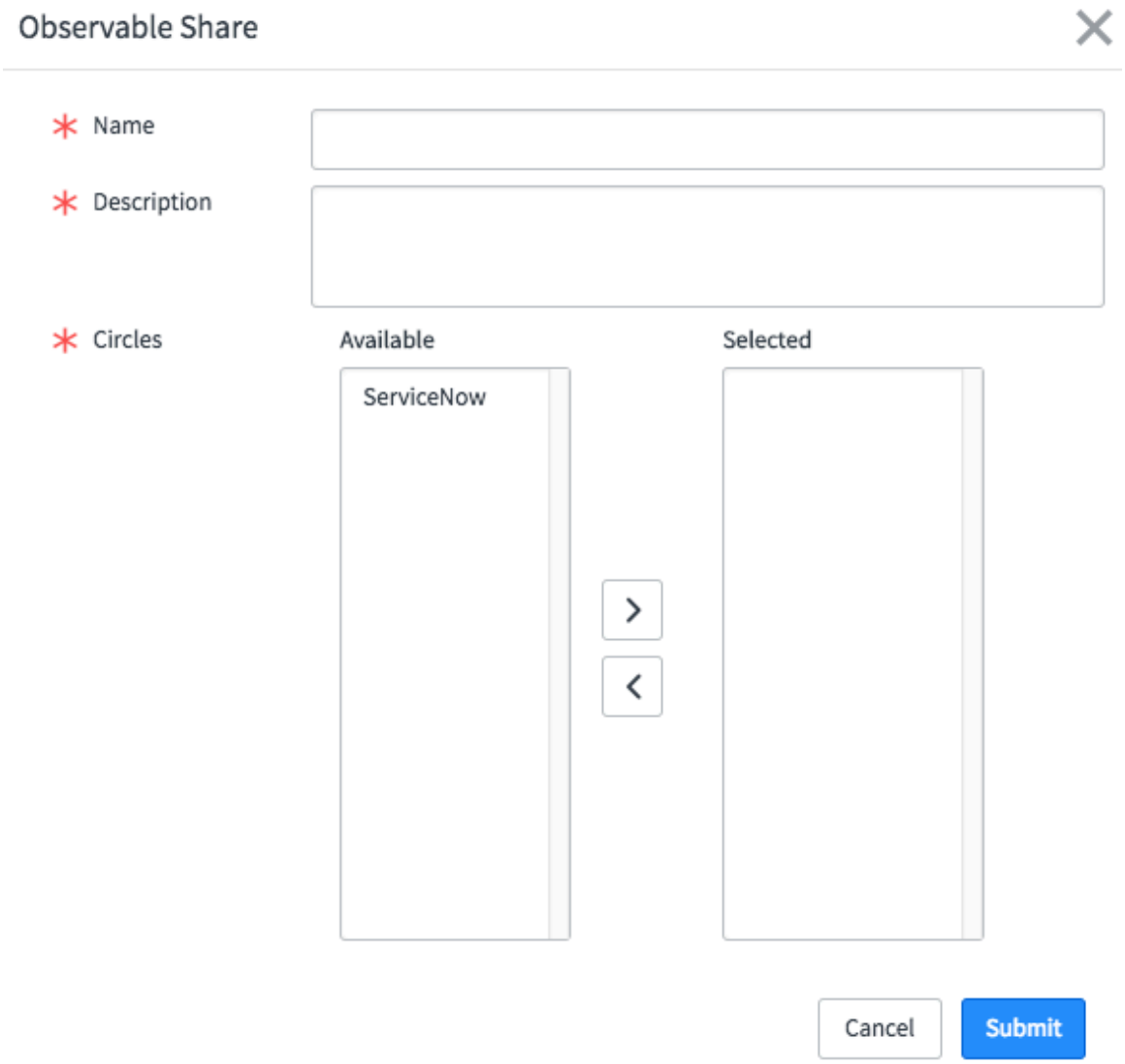
Role required: sn_si.analyst

Procedure

1. Navigate to a security incident.
2. Select the **Observables** tab from **Show IoC** Related List group.
3. Click on an observable.
4. On the **Observable** form click the **Share observable** related link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Observable Share dialog box appears.



5. Enter a **Name** for this threat share record.
6. Enter a **Description**of the selected observables.
7. Choose **Circles** to share the observables with.
8. Click **Submit**.
   The observable(s) are shared with the specified Trusted Circle.
9. You can view the threat share records by clicking the **Threat shares** tab.
10. If any of the shared observables contain sightings, the sightings are also shared and can be viewed by clicking the **Sightings** tab.

View Sightings Search Details

Review the aggregate details of all sighting searches.

Before you begin

Role required: sn_si.analyst

About this task

.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to a security incident.
2. Select the **Sightings Search Details** tab from **Show IoC** Related List group to view the list of sightings searches.

Note: This data can be shared with Trusted Security Circle.

Sightings Search Details

Detail	Description
Observable	List of all observables searched for by query.
Observable type	
Internal sightings	Count of internal sightings for all searches.
External sightings	Count of external sightings for all searches. (Received from threat sharing.)
Sighting search	Sightings Search identifier.
Updated	Date and time of last modification.

View Sightings Search Data

Review the aggregate data of all sighting searches.

Before you begin

Role required: sn_si.analyst

Procedure

1. Navigate to a security incident.
2. Select the **Sightings Search Data** tab from **Show All Related Lists** Related List group to view the list of sightings searches.

Note: This data can be shared with Trusted Security Circle.

Sightings Search Data

Result	Description
End date range	Time to stop looking for sightings.
External Sightings	Aggregated count of external sightings. (Received from threat sharing.)
Internal Sightings	Aggregated count of internal sightings.
Is Local	Indicates whether the sightings came from the current or a shared environment.
Observable	List of all observables searched for by query.
Sighting count	Number of sightings searched for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result	Description
Sighting search	Sightings Search identifier.
Sighting search detail	Aggregate detail of the sighting search.
Sighting search link	Link pointing to the Sighting search portal. The search query is automatically applied upon clicking the Sighting search link.
Sighting search query	Query to identify the instance. 172.10.0.171 is substitutable and gets substituted in the observable selected. (search 172.10.0.171 | head 10) **Note:** Selection of days will not be applicable to Saved search.

Security Operations Integration - Threat Lookup capability

The **Threat Lookups** capability performs threat intelligence lookups to determine whether one or more observables are associated with known security threats.

The **Threat Lookups** capability has a workflow, Security Operations Integration - Threat Lookup workflow. When the capability workflow runs, it executes additional workflows for the activated implementations. You can specify an implementation to use to perform a lookup on the selected observables, or you can perform the lookup using all implementations.

Note: If no implementations are available, capability actions are not displayed in product menus.

Security Operations Integration - Threat Lookup workflow

The **Security Operations Integration - Threat Lookup** capability workflow accesses available threat lookup implementations and executes the implementation workflows associated with each to perform threat lookups of selected observables.

Before you begin

Role required: sn_ti.write

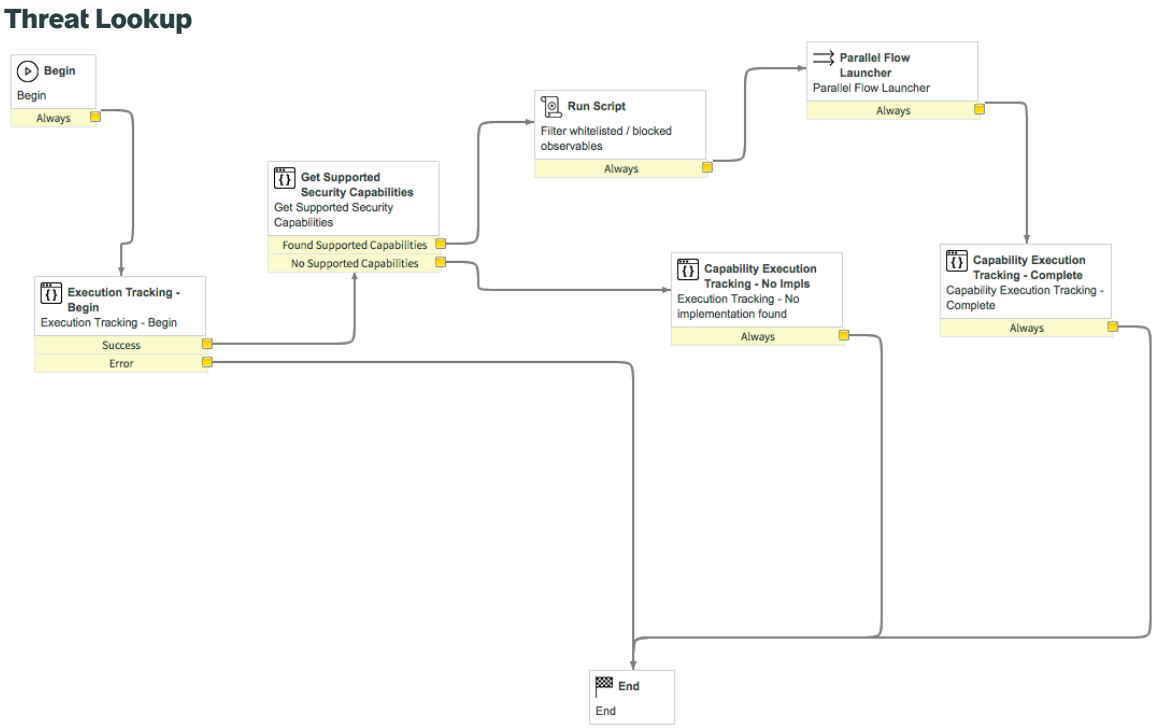
About this task

This workflow can be triggered in these ways.

- by selecting one or more observables from the Observables list and selecting **Run threat lookup** from the **Actions on selected rows** choice list.
- by opening an observable record and clicking the **Run threat lookup** related link.
- From the Observables related list in a security incident.

Each method then allows you to specify which lookup implementations to be used to scan the selected observables. The associated implementation workflows are executed to perform the lookups.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Activities specific to this workflow are described here. For more information on other activities, see Common Security Operations integration flows and orchestration Flow Actions.

Workflow process activities include:

- Get Supported Security Capabilities activity
- Capability Execution Tracking- No Impls activity

Change the order of workflow execution

Integration capability implementations specify the workflow to be executed. In the base system, workflows are executed sequentially, in the order specified in the implementation. You can change the order as needed.

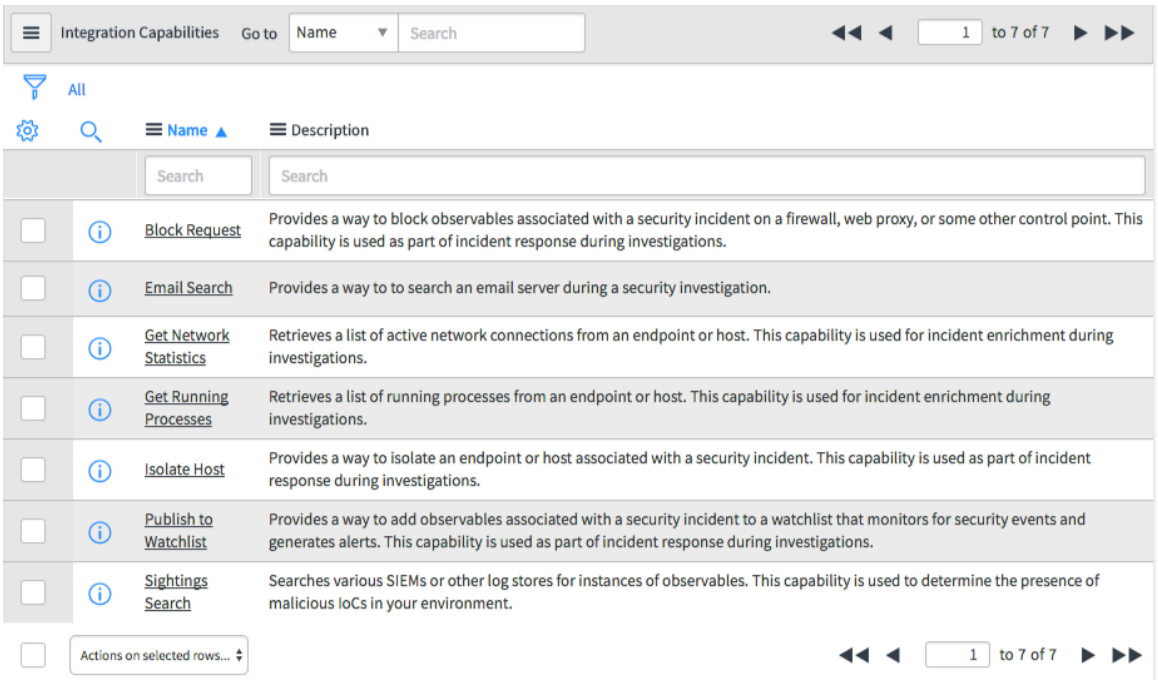
Before you begin

Role required: sn_sec_cmn.write

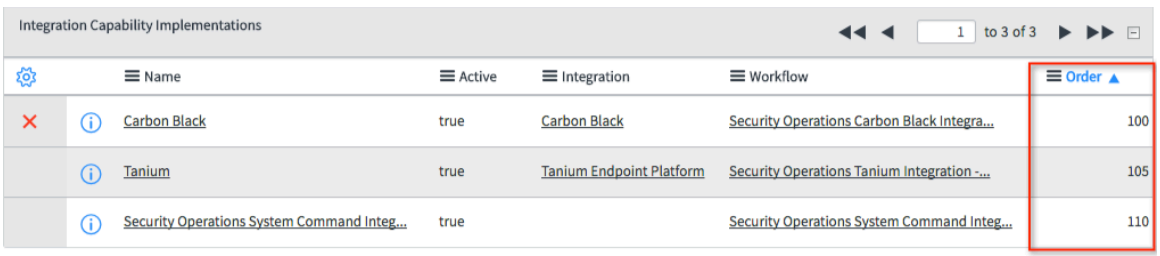
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

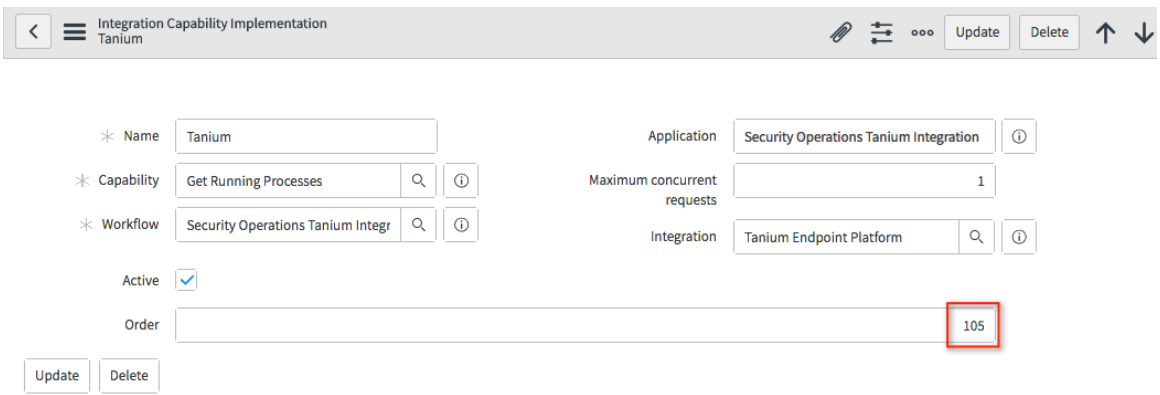
1. Navigate to **All** > **Security Operations** > **Integrations** > **Integration Capabilities**.



2. Select the integration capability for which you want to change the execution order.



3. Select the implementation you want to modify.



4. Change the **Order** to a higher or lower number.
   Lower numbers have a higher execution priority.
5. Click **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Common Security Operations integration flows and orchestration Flow Actions

Many of the flows associated with third-party integrations include the same flow actions. For example, flow actions for beginning and completing processing.

Execution Tracking - Begin Flow Action

The Execution Tracking - Begin flow action starts the auditing process for a Security Operations Integration flow that operates on observables.

The Execution Tracking - Begin flow action can be used with any flow to begin recording the progress of the flow in an audit.

Results

Possible results for this flow action are:

Results

Result	Description
Success	An audit record is created.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
capabilityId	System identifier of the Integration Capability being executed.
isImpl	Flag that specifies whether auditing is done for an Integration Capability flow or an Integration Capability implementation flow. Possible values are: • false - denotes auditing on an abstract Integration Capability flow such as Sightings Search. (default.) • true - denotes auditing on an Integration Capability implementation flow. For example, Splunk or Elasticsearch.
taskId	System identifier for any task associated with the flow.
observableList	One or more observable SysIDs to perform the desired action. Used as a flow input.
flowContextId	System identifier of the associated flow context record. Supplied by the system.
flowName	Name of the flow. Supplied by the system.
parentCapabilityExcutionId	System identifier of the audit record that launched the implementation flow. Only required for Integration Capability implementation flows such as Splunk, Elasticsearch, and VirusTotal.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
capabilityExecutionId	System identifier of the audit record.

- Get Supported Security Capabilities activity
- Capability Execution Tracking- No Impls activity

Capability Execution Tracking - Complete Flow Action

The Capability Execution Tracking - Complete flow action updates the audit record when the flow is complete.

The Capability Execution Tracking - Complete flow action can be used with any flow to record the completion of the flow.

Note: The **Return Value** array from the **Parallel Launcher** core flow action contains an array of results from all integration flows run and prompts the successful completion of execution tracking.

Results

Possible results for this flow action are:

Results

Result	Description
Success	The audit record state is updated to **Complete**.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
capabilityExecutionId	System identifier for the audit record. This field was the output from any of the Begin auditing activities.
flowName	Name of the flow. Supplied by the system.
message	Completion message.

Output variables

There are no output variables.

Capability Execution Tracking- Failure Flow Action

The Capability Execution Tracking - Failure flow action records a failure to the audit record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Capability Execution Tracking - Failure flow action can be used with any flow to record a failure condition.

Results

Possible results for this flow action are:

Results

Result	Description
Success	The audit record state is set to **Error** and a message indicating the error is recorded.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
capabilityExecutionId	System identifier for the audit record. This is the output from any of the Begin auditing activities.
errorMessage	Message indicating the reason for the failure.
flowName	Name of the flow. Supplied by the system.

Output variables

There are no output variables.

Capability - Determine CIs activity

The Capability - Determine CIs workflow activity determines which configuration items (CIs) to include in the workflow.

The Capability - Determine CIs activity can be used with any workflow to determine which CIs to include in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Found configuration items.
Failure	No CIs found. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
task_sys_id	Task identifier (maps security incident to CIs).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
cis_affected	Configuration items.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
cis_affected	Filtered CIs
task_sys_id	Task identifier (maps security incident to CIs).

Create Enrichment Data records Flow Action

The **Create enrichment data records** flow action creates or updates enrichment records to use in the flow.

The **Create Enrichment Data records** flow action can be used with any flow to update enrichment records in the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Enrichment record updated.
Failure	Enrichment record not updated. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
task_id	Task identifier.
content	Raw content (running processes data).
enrichment_mapping_id	Enrichment mapping identifier.
ci_id	Configuration item identifier.
reference_value	Unused.

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
result	GlideRecords created using the enrichmentUtils script.

Get Configuration Item FQDN Flow Action

The **Security Common Orchestration** > **Get Configuration Item FQDN** flow action retrieves the fully qualified domain name (FQDN) of a configuration item. This flow action can accelerate the investigation and remediation process.

The Get Configuration Item FQDN flow action can be used with any flow to retrieve the fully qualified domain name (FQDN) of a configuration item.

Input variables

Input variables determine the initial behavior of the flow action.

Input variables

Variable	Description
cmdb_ci.id [string]	The system identifier (sys_id) of a configuration item record.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
fqdn [string]	The fully qualified domain name (FQDN) of the configuration item.

Additional Notes

The fqdn field on the configuration item must be populated.

Determine Observables activity

The **Determine Observables** workflow activity determines which observable to include in the workflow

The **Determine Observables** activity can be used with any workflow to determine which observables to include in the workflow.

Results

Possible results for this activity are:

Results

Result	Description
Success	Found observables
Failure	No observables found. More error information is available in the activity output error.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
task_sys_id	Task identifier (maps security incident to observables).
observables	IP addresses, hash, URLs, domain names.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
observables	Filtered observables

Get Supported Security Capabilities activity

The Get Supported Capabilities workflow activity retrieves the name and number of integrations that are active and support the requested capability.

The Get Supported Capabilities activity can be used with any workflow to determine which capabilities are supported.

Results

Possible results for this activity are:

Results

Result	Description
Success	Integration that supports the capability found.
Failure	An error occurred while attempting to find an active integration that supports the capability. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
capabilityName	Name of the capability.
taskId	System identifier for any task associated with the workflow.
domainId	System identifier for any domain associated with the workflow.

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
supportedCapabilities	List of integrations that support the capability.
capabilityCount	Number of integrations that support the capability.

Capability Execution Tracking- No Impls activity

The Capability Execution Tracking - No Impls workflow activity creates an error record when no integration capability implementation is found.

The Capability Execution Tracking- No Impls activity can be used with any abstract integration capability workflow to handle the error condition when no configured capability implementation is available.

Results

Possible results for this activity are:

Results

Result	Description
Success	The execution tracking record state is set to **Error** and a message indicating the error is recorded.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
capabilityExecutionId	System identifier for the audit record. Output from the activity used to begin execution tracking.
workflowName	Name of the workflow. Supplied by the system.

Output variables

There are no output variables.

Create Compliance Search Action

The Create Compliance Search action creates a compliance search for emails in the designated Exchange server(s) using the search queries defined and returns the name of compliance search created.

Input variables

Input variables determine the initial behavior of the action.

Variable	Description
search_query	Mandatory search query used to find emails in the Exchange Server across all mailboxes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
exchange Location	Mandatory location field used to search across location defined. Values are: • All • Name of specific mailbox
targetId	Mandatory target host identifier field where the Exchange Server is located.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
response	Name of the compliance search created.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Search Creation Failed	When search creation fails due to exception in exchange server.
Search Created Successfully	When search creation is successful.
Search Creation Failed due to a Parsing Error	When search creation fails due to parsing issue.
Error	When exception occurs in flow action.

Get IP from CI activity

This workflow activity determines the IPV4 address associated with a configuration item (CI).

The **Get IP from CI** activity can be used with any workflow to retrieve the IPv4 address of a CI.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
ci_sys_id [string]	Configuration item system identifier

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
ip_addr [string]	IPv4 address. If the IP address cannot be determined, this value is empty.

Exit Conditions

Possible results for this activity are:

Conditions

Condition	Description
Success	An IPv4 address was returned.
Failure	An IPv4 address could not be determined.

Get Network Statistics via netstat Flow Action

The Security Common Orchestration - Get Network Statistics via netstat flow action retrieves the network statistics for an affected resource on a Windows-based system. This flow action can accelerate the investigation and remediation process.

The Get Network Statistics via netstat flow action can be used with any flow to retrieve network statistics from a Windows-based system. The machine is queried with the **netstat** command including the **-a** and **-o** parameters. To enhance the output data, **get-process** command is also invoked.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Network statistics were retrieved in JSON format.
Failure	An error occurred while attempting to retrieve network statistics. More error information is available in the flow action output error.

Input variables

Variable	Description
target [string]	The fully qualified domain name (FQDN) or IP address of the target system.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response [string]	A JSON string representing the current running processes on the target machine.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables (continued)

Variable	Description
	JSON data includes: **pid** Process identifier **local _port** Local port for the network transaction **state** Status of the TCP connection. **Note:** This field is null for UDP connections. **local_address** Local fully qualified domain name (FQDN) or IP address **remote_address** Remote fully qualified domain name (FQDN) or IP address **protocol** TCP or UDP **remote_port** Remote port of the network transaction **path** The file path of the process executable **hash** The hash value of the process executable. The hash is in SHA-256 for PowerShell V4 or higher. Otherwise, the hash is in MD5.

Restrictions

The MID Server must support PowerShell.

SHA-256 hash requires PowerShell V4.

Get running processes via WMI activity

The**Get Running Processes** workflow activity retrieves the running processes of a configuration item on a Windows-based system. This activity can accelerate the investigation and remediation process.

The **Get Running Processes via WMI** activity can be used with any workflow to retrieve running processes on a Windows-based system.

Input variables

Input variables determine the initial behavior of the activity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Input variables

Variable	Description
target [string]	The fully qualified domain name (FQDN) or IP address of the target system.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
response [string]	A JSON string representing the current running processes on the target system. JSON data includes: **pid** The process identifier **name** The name of the process Also, if available: **Owner** The name of the process owner **owner_sid** The system identifier of the process owner **owner_domain** The domain of the process owner **path** The file path of the process executable **hash** The hash value of the process executable. The hash is in SHA-256 for PowerShell V4 or higher. Otherwise, the hash is in MD5.

Restrictions

The MID Server must support **PowerShell**.

SHA-256 hash requires PowerShell V4.

Check Compliance Search Status Action

The Check Compliance Search Status action check the status of created compliance search on exchange server and if the status is completed return the information regarding email search found for the compliance search.

Input variables

Input variables determine the initial behavior of the action.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable	Description
targetId	Mandatory target host identifier field where the Exchange Server is located.
searchName	Mandatory name of compliance search created on exchange server.

Output variables

The output variables contain data that can be used in subsequent actions.

Output variables

Variable	Description
response	Contains status of the compliance search and number of emails found on the exchange server for the compliance search.

Exit Conditions

Possible exit conditions for this action are:

Exit Conditions

Variable	Description
Search In Progress	When status of compliance search is in progress.
Search Complete - No Threat Emails Found	When status of compliance search is completed, and no emails are found as a part of compliance search.
Search Complete - Threat Emails Found	When status of compliance search is completed, and emails are found as a part of compliance search.
Error Checking Status	When status checking fails due to exception in exchange server.
Error	When exception occurs in flow action.

Update Task Worknotes activity

The **Security Common Orchestration - Update Task Worknotes** workflow activity updates the **Activity** section (work notes) of a task record. This is useful for logging information.

The **Update Task Worknotes** activity can be used with any workflow to update the work notes of any task record.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
task_id [string]	The system identifier (sys_id) of a task record.
content [string]	The data written into the work notes of a task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
result [string]	Indicates whether the update was successful.

Roll up lookup info to security incident activity

The **Roll up lookup info to security incident** activity can be used with any workflow to gather information from a threat lookup and output a summary of the contents as well as the ID of the originating security incident in task work notes.

Results

Possible results for this activity are:

Results

Result	Description
Success	Lookup report summary rolled up to security incident.
Failure	Originating task and lookup summary report are empty.

Input variables

Variable	Description
scanID[string]	Lookup identifier.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
sild[string]	Security incident identifier.
response [string]	Summary of lookup results including: IoC value, Result, Failure reason, lookup reference, and so on.

Update security incident with lookup results workflow

The **Update security incident with lookup results** workflow updates existing security incidents with lookup results.

Before you begin

Role required: sn_si.basic

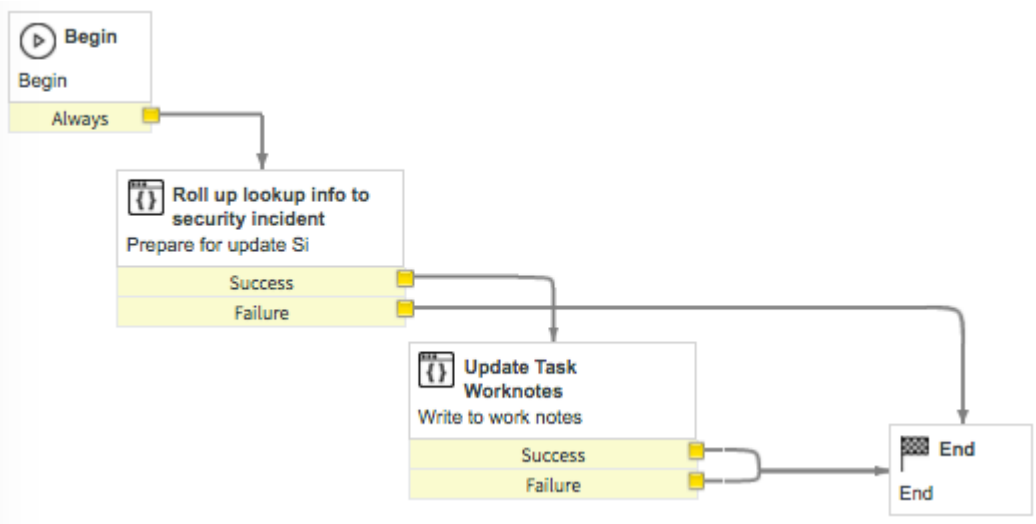
About this task

This workflow is triggered by a business rule on the lookup table which monitors when the **Result** field changes to Failed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Workflow process activities include:

- Roll up lookup info to security incident activity
- Update Task Worknotes activity



Filter Allowlisted Observables activity

The Filtered Allowlisted Observables workflow activity removes observables that can be ignored from the list of observables. This activity can accelerate the investigation and remediation process.

The Filter Allowlisted Observables activity can be used with any workflow to filter observables prior to taking any action.

Results

Possible results for this activity are:

Results

Result	Description
Success	Filter list created.
Failure	An error occurred while attempting to filter the observables. More error information is available in the activity output error.

Input variables

Input variables determine the initial behavior of the activity.

Variable	Description
observables	List of available observables.

Output variables

The output variables contain data that can be used in subsequent activities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Output variables

Variable	Description
filteredObservables	Filtered observables.

Write content to record as attachment activity

This activity writes the content passed in from an input and creates a designated attachment to a given record.

The **Write content to record as attachment** activity can be used with any workflow to write content and attach it to a record.

Input variables

Input variables determine the initial behavior of the activity.

Input variables

Variable	Description
tablename [string]	The table name for the record. This input field is mandatory.
sysid [string]	The system identifier (sys_id) of a task record. This input field is mandatory.
payload	The plain text content to be written as an attachment. This input field is mandatory.
filename	The attachment file name.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
result [string]	Indicates whether the update was successful.

Get IP from CI Flow Action

The Get IP from CI flow action gathers the IP address from configuration items (CIs) to use in the flow.

The Get IP from CI flow action can be used with any flow to gather configuration item (CI) IP addresses to use in the flow.

Results

Possible results for this flow action are:

Results

Result	Description
Success	Found IP addresses.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Results (continued)

Result	Description
Failure	No IP addresses found. More error information is available in the flow action output error.

Input variables

Input variables determine the initial behavior of the flow action.

Variable	Description
ci_sys_id	Configuration item identifier.

Output variables

The output variables contain data that can be used in subsequent activities.

Output variables

Variable	Description
ip_addr	IP addresses.

Security Operations workflow triggers

Security Operations workflow triggers contain a condition on a table. All workflows attached to the workflow trigger record run when the condition is met.

Create Security Operations workflow triggers

Create a workflow trigger that contains a condition on a table.

Before you begin

Security Operations contains several workflow triggers in the base system:

Configuration item changes on an active Security Incident

Uses integration to enrich CI-related data as configuration items change.

Rescan vulnerable group

Rescans a vulnerable group, using the Scan vulnerability workflow, when you **Close/Ignore** the group.

Rescan vulnerable item

Rescans a vulnerable item, using the Scan vulnerability item workflow when you **Close/Ignore** the item.

Roles required:

- To read: sn_sec_cmn.read
- To create or update: sn_sec_cmn.write
- To delete: sn_sec_cmn.admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

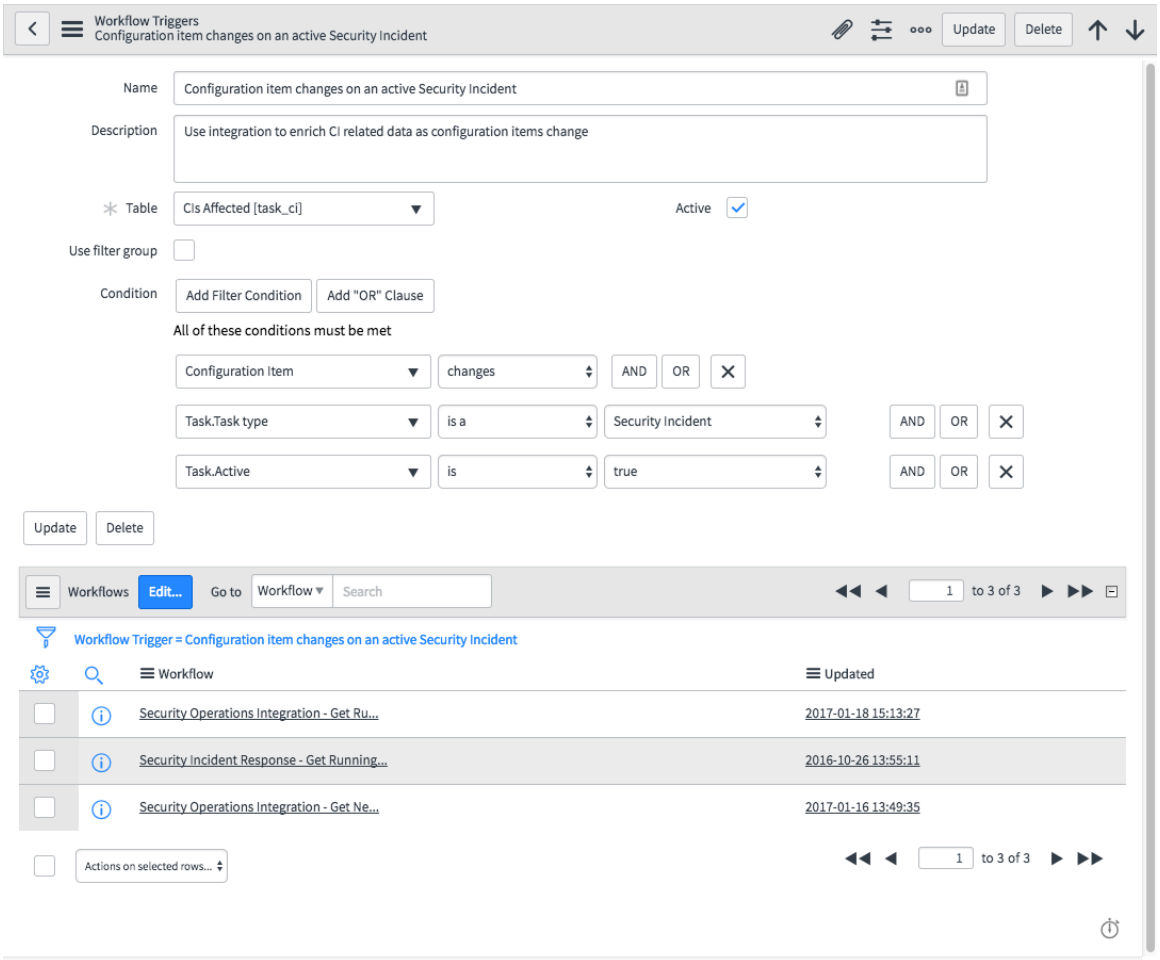
1. Navigate to **All** > **Security Operations** > **Utilities** > **Workflow Triggers**.
2. Click **New**.
3. Fill in the fields on the form, as appropriate.

Workflow Triggers

Field	Description
Name	The name of the workflow trigger.
Description	Enter a description for the workflow trigger.
Table	The table containing the workflow trigger. If you selected the **Use filter group** check box and selected a filter group, this field defaults to the table associated with the selected filter group.
Condition	Use the condition builder to define the criteria for the workflow trigger. If you selected the **Use filter group** check box and selected a filter group, the **Condtion** fields are not displayed.
Active	Select this check box to activate the workflow trigger.
Use filter group	Select this check box to use a predefined filter group or create a new filter group to define the workflow trigger criteria.
Filter group	Select the filter group to use for defining workflow triggers. This field appears only if the **Use filter groups** check box is selected.

4. When you have completed your entries, right-click in the form header and select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Workflows** tab appears. It contains workflows that are run when all filter conditions or filter group conditions are met.

5. To add workflows, perform these steps.
   a. In the **Workflows** tab, click **Edit**.
   b. Use the condition builder, if needed, to locate the workflows you want to select, or use the slushbucket to select workflows and move them to the Workflows List.
   c. Click **Save**.
   The selected workflows are added.
6. Click **Update**.

Security Operations Orchestration

Users can interact with and retrieve data from Windows or UNIX-based systems and environments using activity packs and workflows in Security Operations Orchestration.

Security Operations Orchestration saves time by eliminating manual processes and obtaining contextual information to remediate incidents. The Security Operations products have standard activity packs and workflows that are included and activated in each of the plugins.

To create and access additional orchestration activities that are not available with the standard offering Security Operations products, purchase a full orchestration license.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Incident Response Orchestration workflows:
  - Security Incident Response- Get Network Statistics Flow
  - Security Operations System Command Integration- Get Running Processes flow
  - Create Lookup Request for IoC Changes Flow
  - Security Operations Integration - Email Search and Delete flow
- Threat Intelligence Orchestration workflows:
  - Threat Intelligence - Run IoC Lookup workflow
  - Update security incident with lookup results workflow
- Vulnerability Response Orchestration workflows:
  - Scan vulnerability workflow
  - Scan vulnerability item workflow

Security Operations and the ServiceNow Store

Starting with Madrid, all Security Operations applications and supported integrations are available for download from the ServiceNow Store. This allows you to obtain new and updated features more rapidly. Before you can use any Security Operations applications, you must verify that you have entitlement to them (that is, you have valid licenses to use them), download them from the ServiceNow Store, and activate them.

The ever-growing list of Security Operations applications available for download includes:

- Security Incident Response (and supported integrations)
- Vulnerability Response (and supported integrations)
- Threat Intelligence (and supported integrations)
- Configuration Compliance
- Trusted Security Circle
- Data Loss Prevention Incident Response

Watch this five-minute video to learn about downloading Security Operations and GRC applications from the ServiceNow Store.

The process you use to obtain Security Operations applications and integrations depends on whether you are downloading an application for the first time, updating an application that you previously downloaded from the ServiceNow Store, or upgrading from one family release to the next one.

Download an application from the ServiceNow Store for the first time

Downloading an application from the ServiceNow Store for the first time involves a number of easy steps. Some of the steps are performed on the ServiceNow Store and some in your instance.

The ServiceNow Store allows you to download core products and applications. A product contains one or more applications that are licensed as a group. For example, Security Incident Response is a product. The process involves these steps:

Role required: admin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- In the ServiceNow Store, you must ensure that you have entitlements (or licenses) to the application and its dependent applications.

  Note: This process applies only to applications that are downloaded to production instances. If you're downloading applications to non-production or development instances, it's not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

- Finally, you can activate the application and run it on your instance.

Note: Starting with previous versions of Rome and later releases, dependency plugins are automatically activated when you activate a core application. For example, when you activate the Vulnerability Response application, the Vulnerability Response Dependencies plugin is also activated. For more information, see Activate a ServiceNow Store application.

Get entitlement for a Security Operations product or application

The first step in installing a Security Operations application is to verify that the application or the product and its associated applications have valid ServiceNow entitlements.

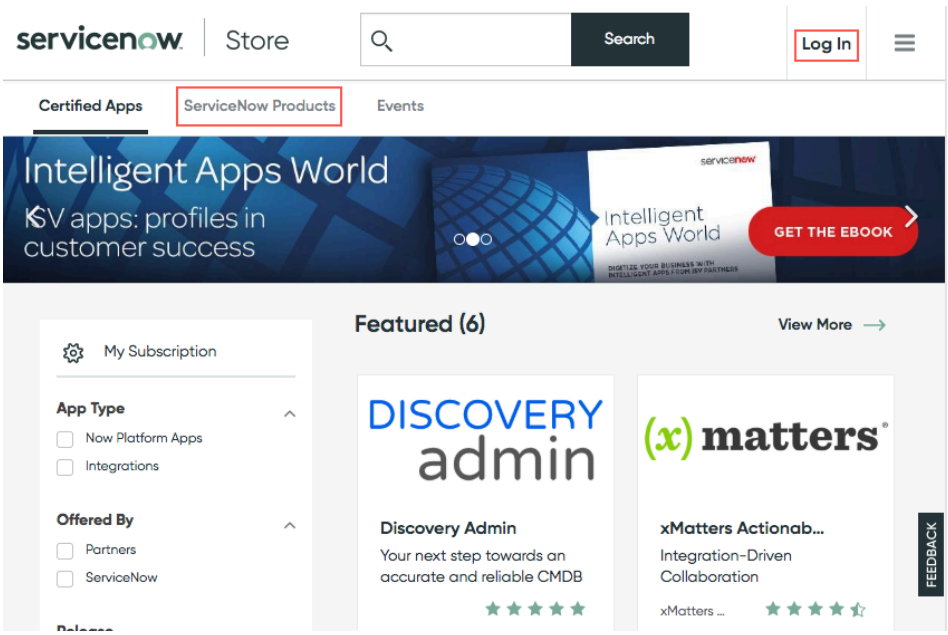
Before you begin

Role required: admin
Individuals performing entitlement must have a Now Support account and have permission to request applications for the instances under consideration.

Note: This process applies only to applications downloaded to production instances. If you are downloading applications to sub-production or development instances, it is not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

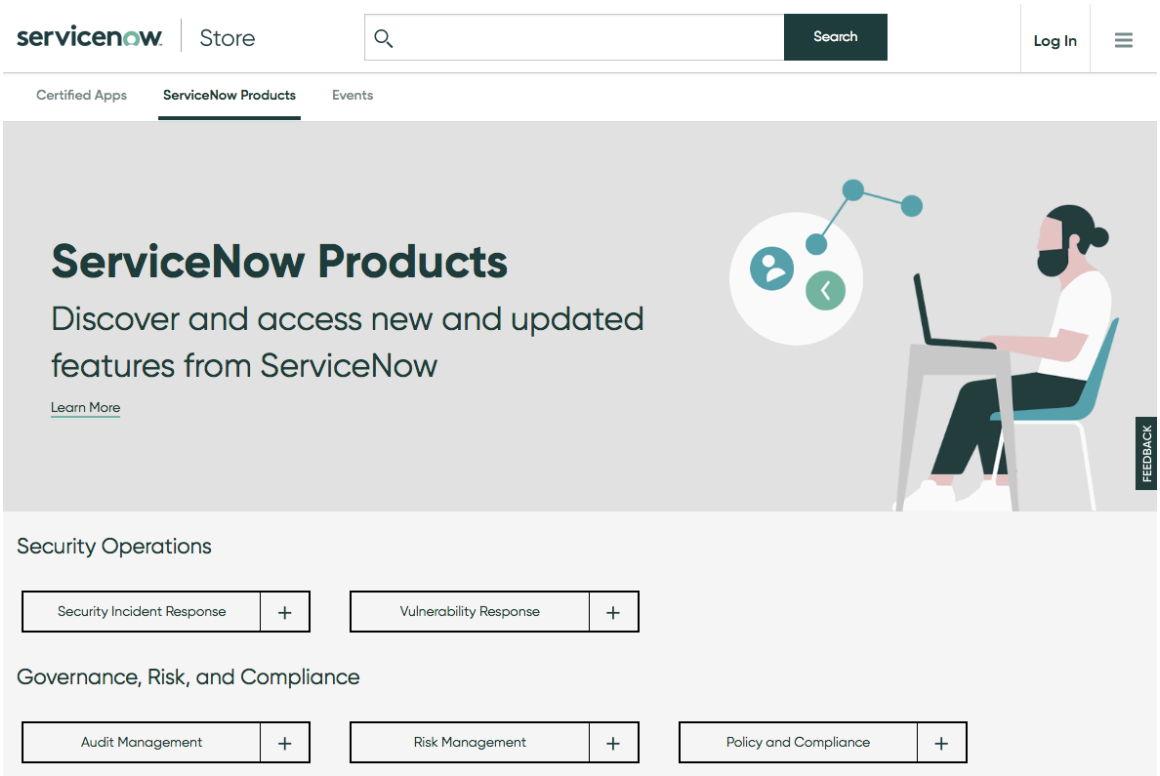
Procedure

1. Navigate to the ServiceNow Store.



2. Click **Login** and log in using your HI credentials.
3. Click the **ServiceNow Products** tab to view all available ServiceNow products. Integrations and other types of content are shown on the **Certified Apps** tab.

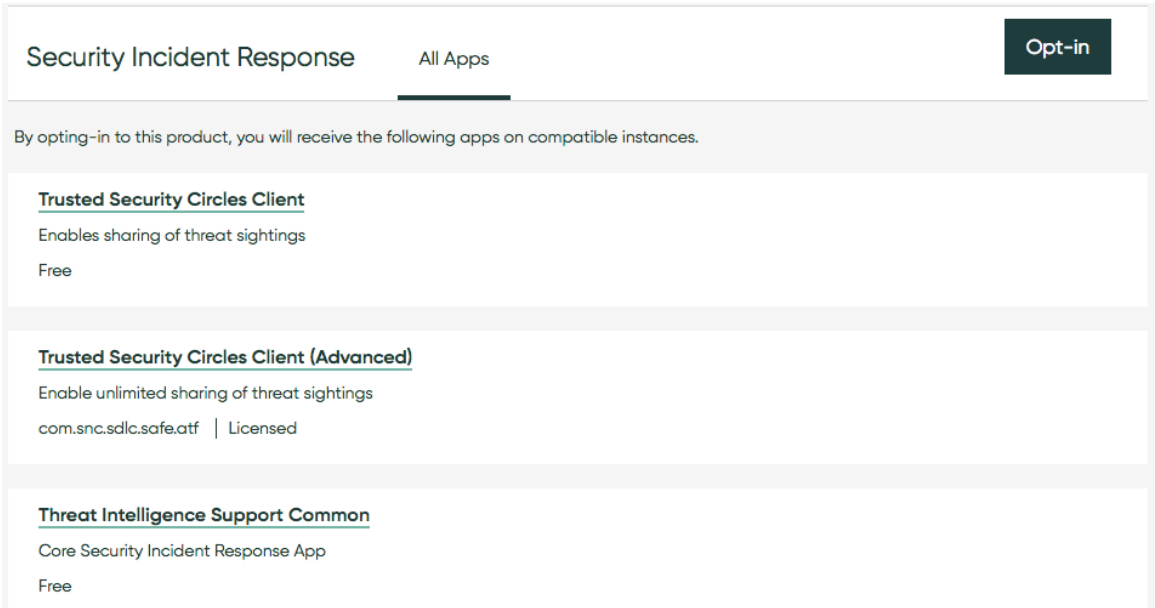
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: For the sake of this example, assume you're acquiring entitlement for the Security Incident Response product.

4. Click the plus (+) sign next to the product name that you are getting entitlement to.
   All applications associated with the product you're entitling are listed. When you have obtained entitlement to the core product, the applications listed under it are also entitled.

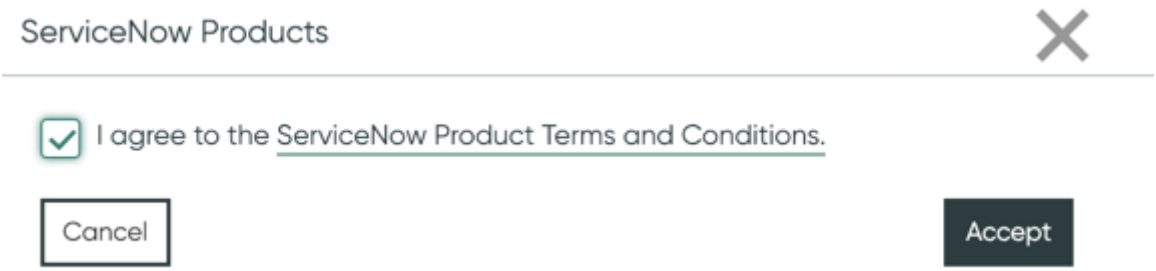
Note: You can also click the product name to view more information about the product and its associated applications.



5. Click **Opt-in** to verify that you have entitlement to the product and the applications listed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You are prompted to read and accept the ServiceNow terms and



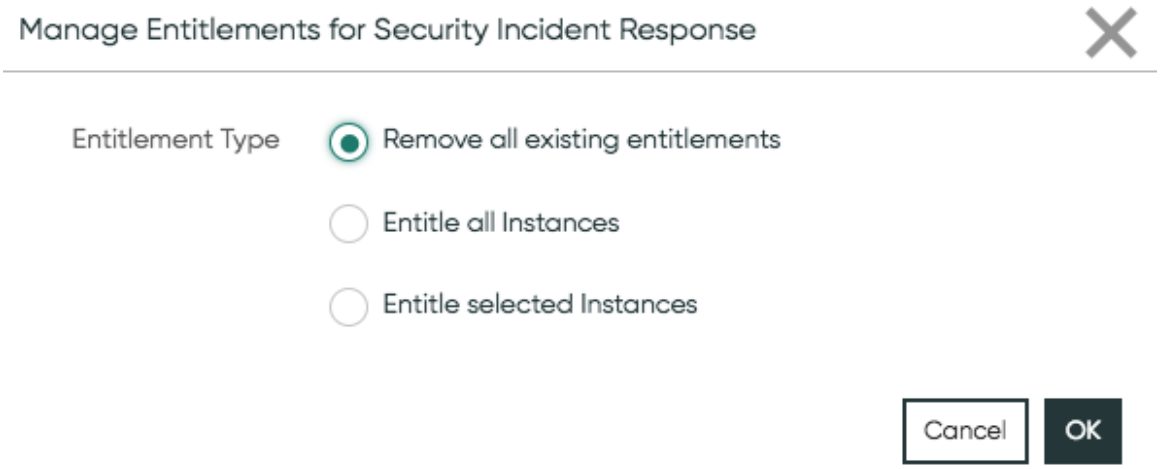
conditions.

6. Select the check box and click **Accept**.
7. Notice that a check mark appears next to the product name and the Manage Entitlements button appears.

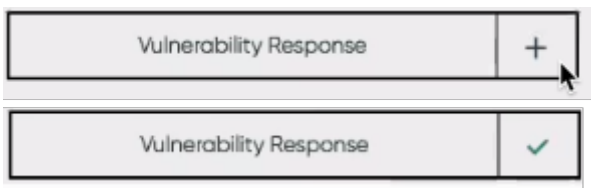


The check mark indicates that you have subscribed to the product and its associated applications. It is time to manage your entitlements. This is a one-time process for this product and any other products you want to install in the future.

8. **Optional:** You can click **Manage Entitlements** to change the instances affected by the applications to which you are entitled.



9. After you have agreed to the ServiceNow Terms and Conditions and managed entitlements, you can entitle other products with a single click.



Note: You are ready to activate the product.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activate a ServiceNow Store application

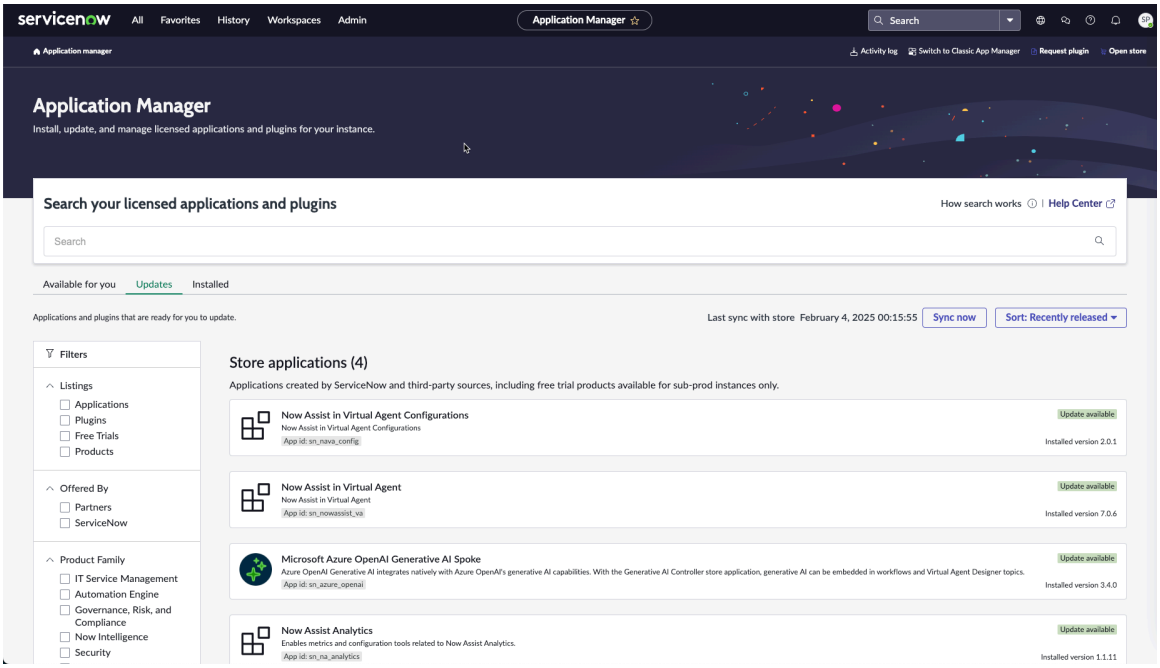
After an application has been given entitlement, you must activate its dependencies plugin and activate the application. This process also applies to applications downloaded to sub-production instances.

Before you begin

Role required: admin

Procedure

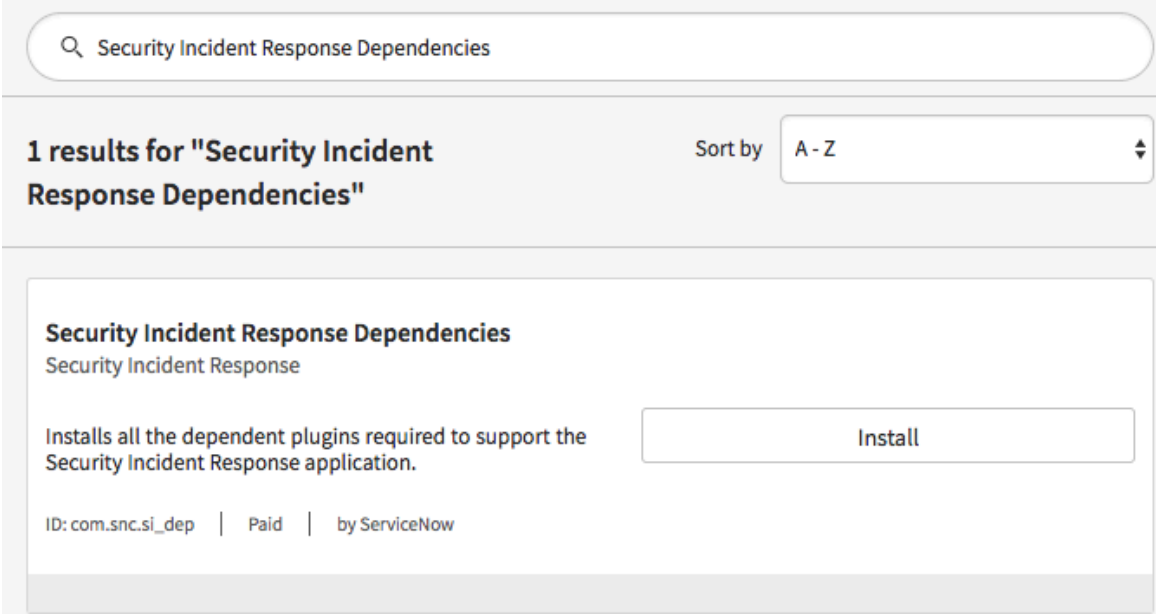
1. Navigate to **System Applications** > **All Available Applications** > **All**.



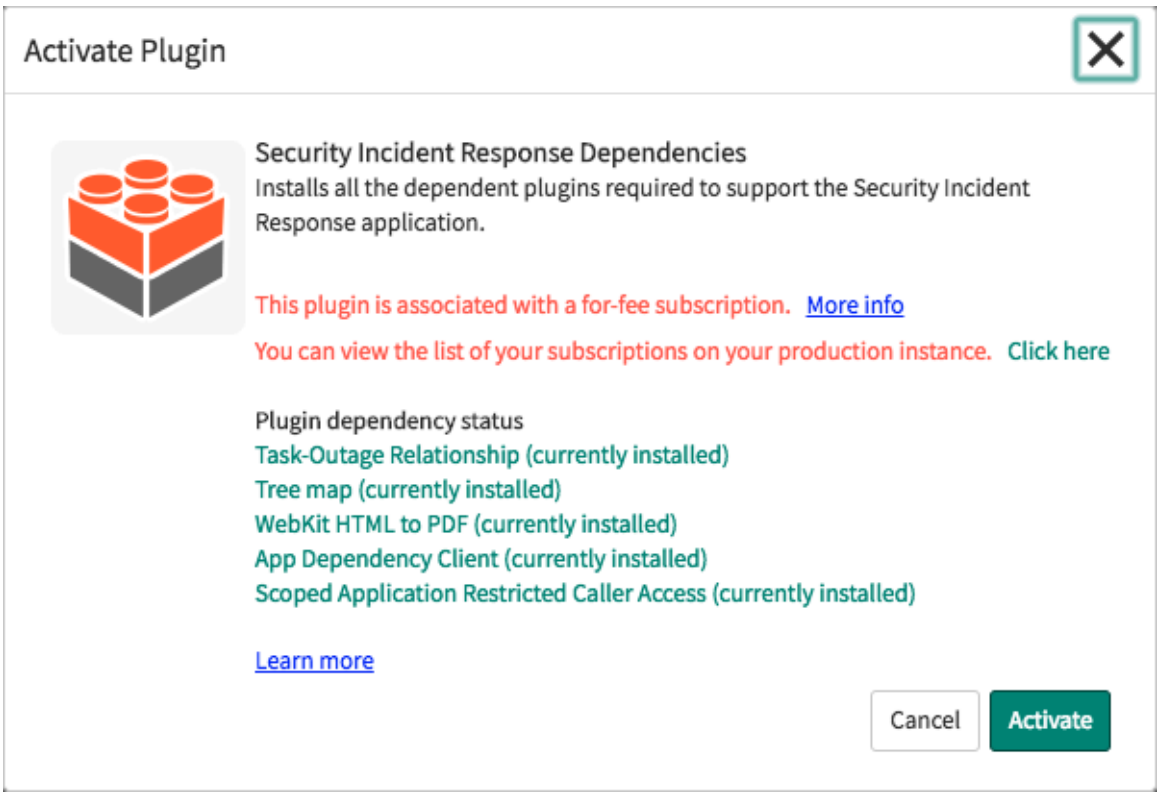
> **Note:** Starting with Orlando, dependency plugins are automatically activated when you activate a core application. For example, when you activate the Vulnerability Response application, the Vulnerability Response Dependencies plugin is also activated. Hence, steps 2 through 5 are optional.

2. Search for the dependencies plugin for the application you want to activate.
   For example, if you are activating Security Incident Response, locate the Security Incident Response Dependencies plugin.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. Click **Install**.
   The Activate Plugin dialog box appears.



4. In the **Activate Plugin** dialog box, click **Activate**.
5. When the activation is complete, click **Close & Reload Form**.
6. Now locate the core product you are activating, click the **Install with demo data** check box if you want to load demo data, and click **Install**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your application is automatically installed on your instance.

Note: If you do not select the **Install with demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Work around to install demo data if application is already installed [KB0722909] article in the HI Knowledge Base.

Install a Security Operations integration

All ServiceNow integrations are available on the ServiceNow Store. Core applications, such as Security Incident Response, are visible in the **ServiceNow Products** tab on the store. Integration add-ons are visible in the **Certified Apps** tab.

Before you begin

Role required: admin

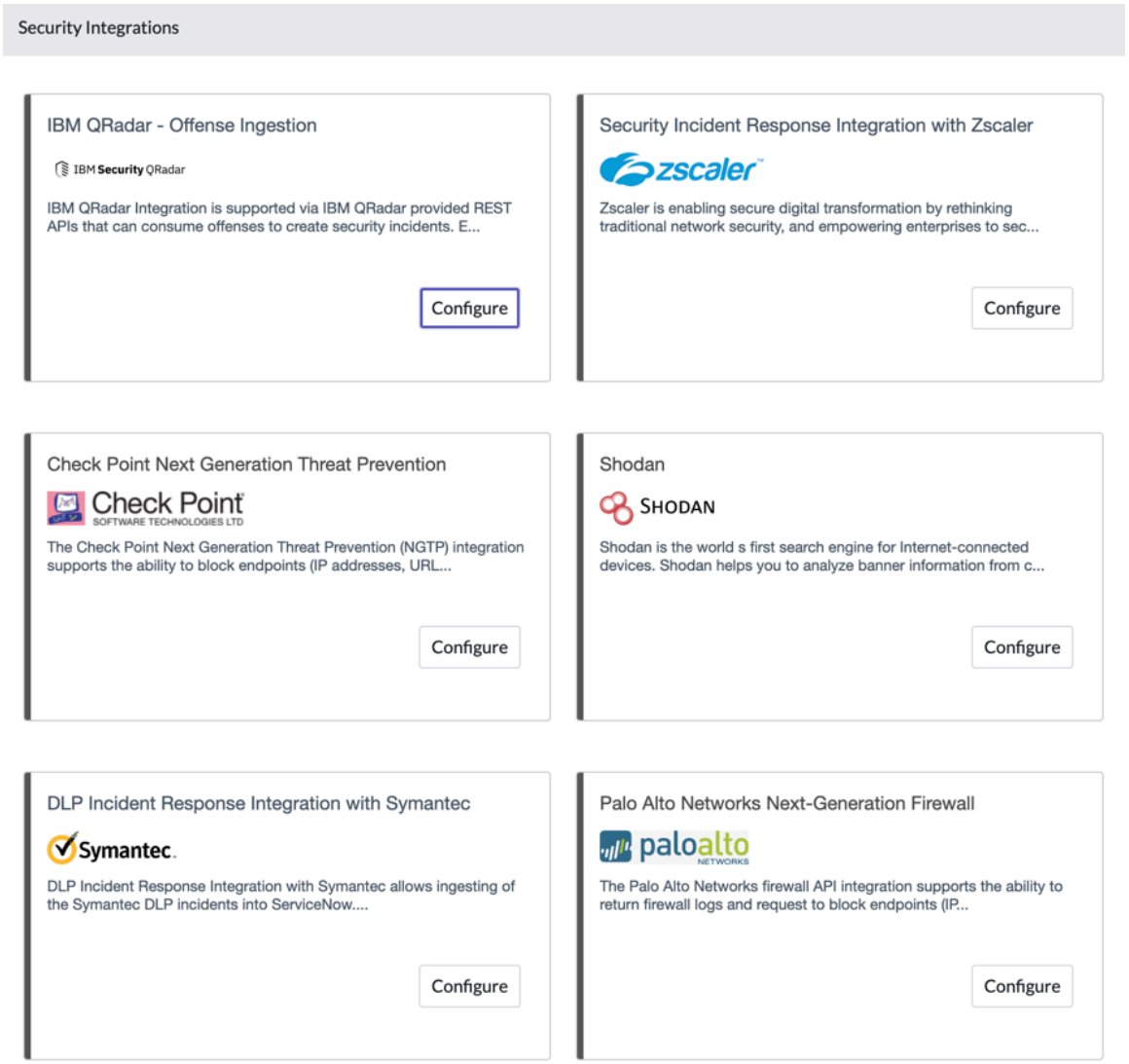
Store installations require a Now Support account and permission to request applications for the instances under consideration.

Procedure

1. Navigate to **Security Operations** > **Integrations** > **Integration Configurations** after you install the application from ServiceNow store.
   Configuration tiles for the integrations appears

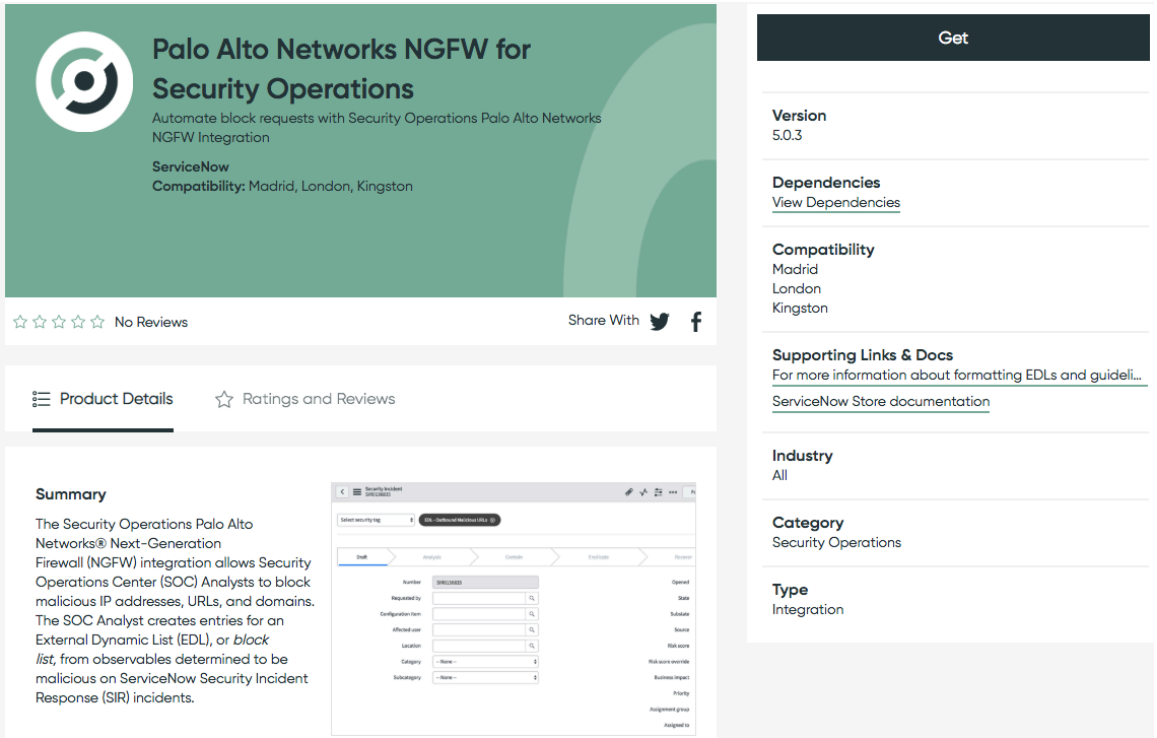
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:



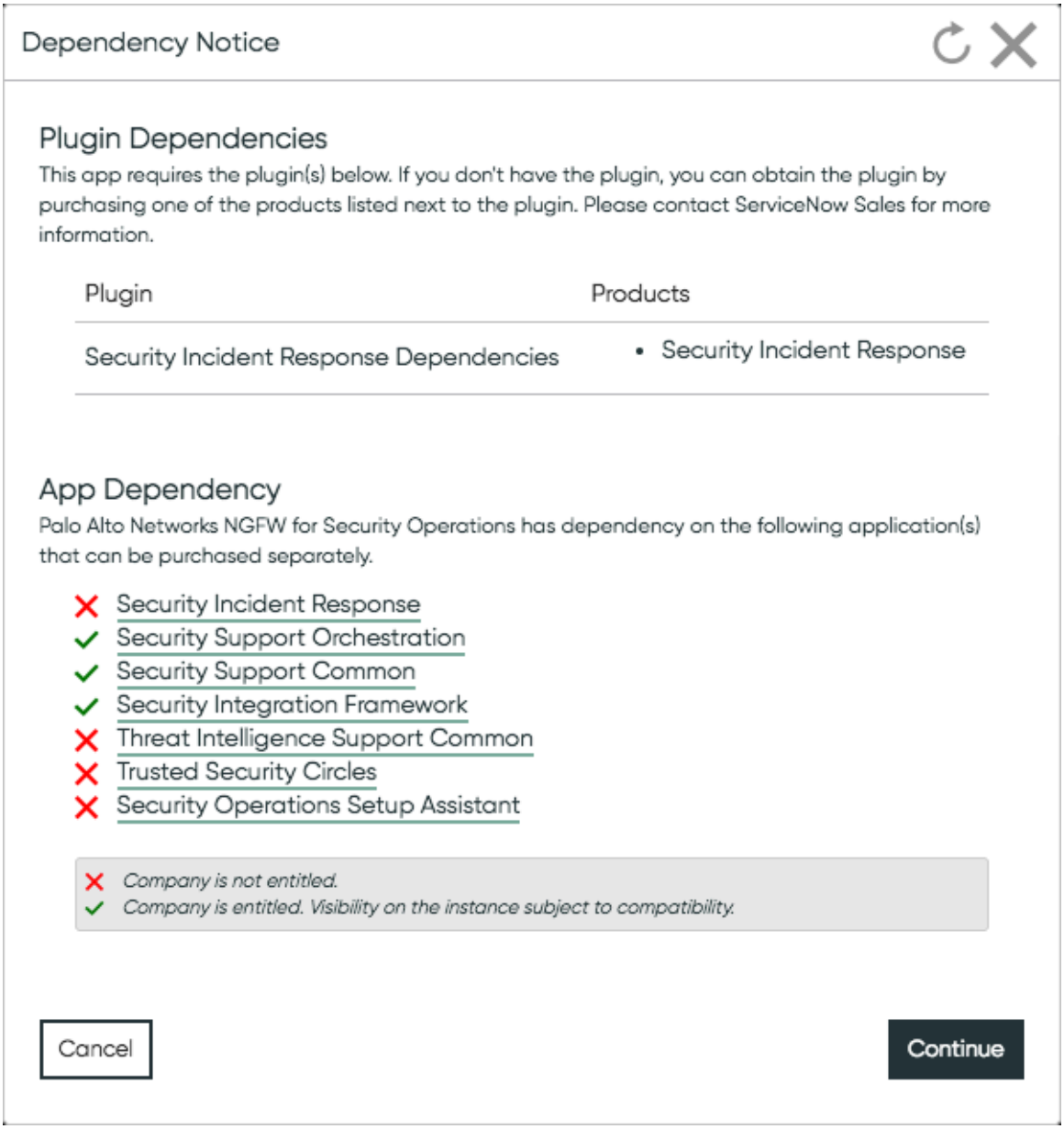
2. Locate the integration you want to install and click **Configure**.
   The selected integration is shown in the ServiceNow Store

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



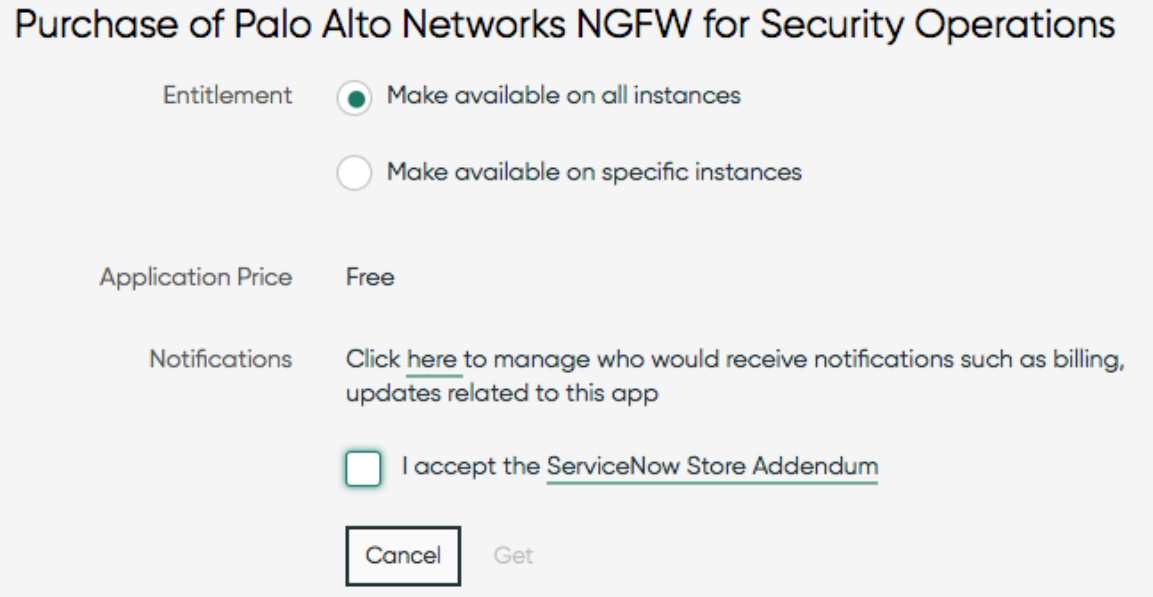
3. Click **View Dependencies** and review the app dependencies listed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



4. If the integration has any core application dependencies, such as Security Incident Response, to which your company is not yet entitled:
   a. Follow these instructions to obtain entitlements, download dependency plugins, and activate the applications.
   b. Return to this procedure.
   c. Click **Continue**.
5. Click **Get**.
   The ServiceNow Terms and Conditions appear.
6. Click **Continue**.
   A Purchase screen similar to the following opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Identify which instances you want the integration to be available on, manage your notifications, and select the **ServiceNow Store Addendum** check box.
8. Click **Get**.

   Note: If you are downloading an application for purchase, click **Buy**. If you are downloading an application that requires you to get prior approval from the vendor, click **Request App**.

9. Enter the instance name and a reason for the request, then click **Request**.
   You are sent an email with detailed installation instructions.
10. Navigate to **System Applications** > **All Available Applications** > **All**.
    A list of applications available for installation is displayed.
11. Locate the application, select it, and click **Install**.
    Your integration is automatically installed on your instance.

Update an application previously downloaded from the ServiceNow Store

If you have previously downloaded an application from the ServiceNow Store and a new version is available, you can update it in your instance.

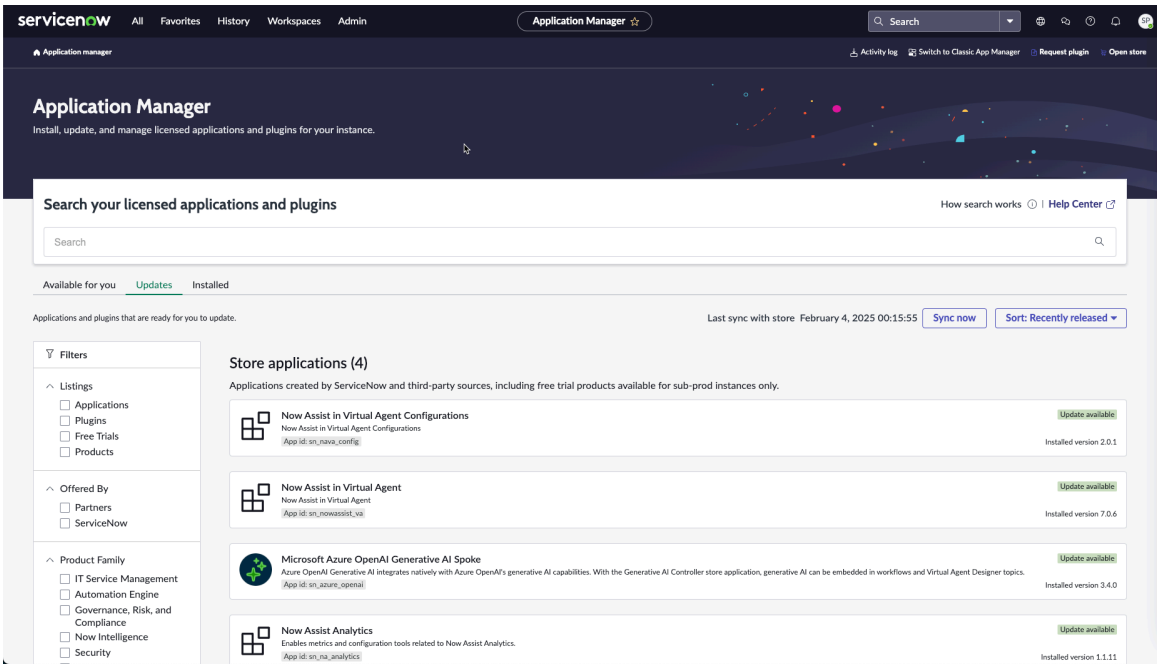
Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **System Applications** > **All Available Applications** > **All**.



2. Search for the application you want to update.
3. Select the version you want to upgrade to and click **Update**.
   Your application is automatically installed on your instance.

Upgrade your instance to the next family release

If you are currently running a family release (Washington for example) and want to upgrade to the next release, it is not necessary to acquire the applications from the ServiceNow Store. The application is automatically updated when the platform is updated to the minimum required version.

Role required: admin

For more information, see the family release notes to learn how to navigate the redesigned release notes and find the information you're looking for and steps for upgrading and Xanadu General Availability release highlights for new features.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.